# Algebraiczna teoria liczb

Karol Janowicz

February 2020

## 1 Wprowadzenie

Rozważmy następujący problem. Niech $x \in \mathbb{Z}$ będzie dowolną liczbą całkowitą dodatnią. Pytamy, czy istnieją liczby całkowite $a, b \in \mathbb{Z}$ takie, że $x = a^2 + b^2$. Innymi słowy, szukamy wszystkich liczb naturalnych dających zapisać się jako suma kwadratów dwu liczb całkowitych.

Chwila zastanowienia wystarczy, by stwierdzić, że jeśli dwie liczby dodatnie $x, y \in \mathbb{Z}$ można przedstawić w ten sposób, to ich iloczyn $xy$ – także. Istotnie, jeśli $x = a^2 + b^2$ i $y = c^2 + d^2$, to rozważmy liczby zespolone $z = a + bi \in \mathbb{C}$ oraz $w = c + di \in \mathbb{C}$. Oczywiście wtedy $x = |z|^2$ i $y = |w|^2$, zatem $xy = |z|^2 \cdot |w|^2 = |zw|^2$ z multiplikatywności normy. A zatem pisząc $zw = p + qi$ dla $p, q \in \mathbb{Z}$ dostajemy, że $xy = p^2 + q^2$ (oczywiście $p, q$ można podać bezpośrednio: $p = ac - bd$ i $q = ad + bc$).

Ta obserwacja motywuje do szukania wszystkich liczb pierwszych $p$, które dają się przedstawić w postaci sumy kwadratów. Co więcej, powyższa sztuczka konstruowania pewnych liczb zespolonych motywuje także do rozważania pierścienia $\mathbb{Z}[i]$, tj. pierścienia $\mathbb{Z}[X]/(X^2+1)$. Grupa addytywna tego pierścienia jest izomorficzna z $\mathbb{Z}^2$, a więc możemy o niej myśleć jak o kracie całkowitoliczbowej w $\mathbb{R}^2$.

Oczywiście liczba pierwsza 2 jest sumą kwadratów: $2 = 1^2 + 1^2$. Udowodnimy

**Twierdzenie 1.1.** *Liczba pierwsza $p > 2$ jest sumą kwadratów dwu liczb całkowitych wtedy i tylko wtedy, gdy $p \equiv 1 \mod 4$.*

*Dowód.* Dla dowodu przypuśćmy, że liczba pierwsza $p > 2$ jest sumą kwadratów. Ponieważ kwadraty przystają do 0 lub 1 mod 4, musi być $p \equiv 1 \mod 4$ ze względu na nieparzystość $p$.

Na odwrót, niech $p = 4k+1$ dla pewnego $k \in \mathbb{Z}$. Z twierdzenia Wilsona wynika, że $(4k)! \equiv -1 \mod p$. Ponadto, dla $i = 1, \ldots, 2k$ mamy $2k+i \equiv -(2k+1-i) \mod p$, skąd wniosek, że $(-1)^{2k}(2k)!^2 \equiv -1 \mod p$, czyli $-1$ jest resztą kwadratową mod $p$. Niech $x \in \mathbb{Z}$ będzie takie, że $x^2 \equiv -1 \mod p$. Wtedy w pierścieniu $\mathbb{Z}[i]$ zachodzi podzielność $p|(x+i)(x-i)$. Gdyby więc $p \in \mathbb{Z}[i]$ był elementem nierozkładalnym, to mielibyśmy $p|x+i$ lub $p|x-i$, co jest niemożliwe. Zatem $p$ jest elementem rozkładalnym w $\mathbb{Z}[i]$. Ponieważ norma elementu $p$ jest równa $p^2$, toteż norma nietrywialnego dzielnika $p$ w $\mathbb{Z}[i]$ jest równa $p$, co dokładnie oznacza, że $p = a^2 + b^2$ dla pewnych $a, b \in \mathbb{Z}$. ■

Z twierdzenia 1.1 i obserwacji poczynionej na początku wynika

**Twierdzenie 1.2.** *Niech $a \in \mathbb{Z}$ będzie liczbą całkowitą dodatnią. Wówczas $a$ jest sumą kwadratów dwu liczb całkowitych wtedy i tylko wtedy, gdy każdy czynnik pierwszy $p$ przystający do $3 \mod 4$, znajdujący się w rozkładzie $a$, występuje w potędze parzystej.*

*Dowód.* Wiemy z wcześniej udowodnionych obserwacji, że jeśli liczba całkowita dodatnia $a$ ma rozkład opisany jak powyżej, to $a$ jest sumą. Na odwrót, jeśli $a$ jest sumą kwadratów i $p \equiv 3 \mod 4$ jest liczbą pierwszą dzielącą $a$ z wykładnikiem nieparzystym $m$. to pisząc $a = x^2 + y^2$ i biorąc $d := NWD(x, y)$ mamy

$$a' = (x')^2 + (y')^2$$

gdzie $a = d^2a'$, $x = dx'$, $y = dy'$. Wtedy $NWD(x', y') = 1$ oraz $p|a'$ z naszego założenia. Zatem $-1$ jest resztą kwadratową modulo $p$, co jest niemożliwe, bo $p \equiv 3 \mod 4$. Ta sprzeczność kończy dowód twierdzenia. ■

Zauważmy, że kluczową rolę w powyższym dowodzie odgrywa pierścień liczb Gaussa $\mathbb{Z}[i]$ wraz z normą nań określoną: $|\ | : \mathbb{Z}[i] \to \mathbb{Z}_{\geqslant 0}$ dziedziczoną z $\mathbb{C}$. Ta norma jest euklidesowa, toteż $\mathbb{Z}[i]$ jest dziedziną z jednoznacznym rozkładem, co jest fundamentalną własnością tego pierścienia. Fakt ten jest zupełnie jasny geometrycznie; dla dowolnych elementów $\alpha, \beta \in \mathbb{Z}[i]$, gdzie $\beta \neq 0$, badamy element $\frac{\alpha}{\beta} \in \mathbb{C}$. Ten leży w pewnym kwadracie wyznaczonym przez punkty $(a, b), (a + 1, b), (a, b + 1), (a + 1, b + 1) \in \mathbb{Z}^2$; wybieramy element $\gamma \in \mathbb{Z}[i]$ odpowiadający jednemu z tych punktów w ten sposób, by odległość $|\frac{\alpha}{\beta} - \gamma|$ była jak najmniejsza; jest jasne, że

$$|\frac{\alpha}{\beta} - \gamma| \leqslant \frac{\sqrt{2}}{2} < 1$$

wobec czego $|\alpha - \beta\gamma| < |\beta|$.

Dokonamy klasyfikacji elementów pierwszych w dziedzinie $\mathbb{Z}[i]$.

**Twierdzenie 1.3.** *Niech $\pi \in \mathbb{Z}[i]$ będzie elementem nierozkładalnym. Wówczas*

1. *$\pi = 1 + i$,*
2. *$\pi = a + bi$, gdzie $a^2 + b^2 = p$ i $p$ jest liczbą pierwszą przystającą do $1 \mod 4$ lub*
3. *$\pi = p$, gdzie $p$ jest liczbą pierwszą przystającą do $3 \mod 4$*

*z dokładnością do stowarzyszenia w pierścieniu $\mathbb{Z}[i]$.*

*Dowód.* Jest jasne, że wyżej wymienione elementy są rzeczywiście pierwsze w $\mathbb{Z}[i]$. Niech więc $\pi \in \mathbb{Z}[i]$ będzie nierozkładalny. Przypuśćmy, że norma $N(\pi)$ **nie jest liczbą pierwszą**. Napiszmy $N(\pi) = p_1 \cdot \ldots p_n$, gdzie $p_i$ są niekoniecznie różnymi liczbami pierwszymi. Skoro $\pi$ jest pierwszy, to bez straty ogólności $\pi|p_1 =: p$ w $\mathbb{Z}[i]$. Stąd zaś $N(\pi)|N(p) = p^2$, czyli $N(\pi) = p^2$. Wykażemy, że $\pi$ jest elementem stowarzyszonym z $p$. Istotnie, element $\frac{p}{\pi} \in \mathbb{Z}[i]$ ma normę 1, toteż jest elementem odwracalnym w $\mathbb{Z}[i]$. Pozostaje zauważyć, że musi być $p \equiv 3 \mod 4$. (bo $\pi = p$ jest nierozkładalny w $\mathbb{Z}[i]$, więc z twierdzenia 1.1 $p$ nie może przystawać do $1 \mod 4$). ■

Intuicyjnie, liczby Gaussa powinny grać podobną rolę w ciele $\mathbb{Q}(i)$, co liczby całkowite w ciele liczb wymiernych $\mathbb{Q}$. Okazuje się, że zachodzi

**Twierdzenie 1.4.** *Pierścień $\mathbb{Z}[i]$ jest zbiorem dokładnie tych elementów $x \in \mathbb{Q}(i)$, że $x$ jest pierwiastkiem wielomianu unormowanego*

$$F(x) = x^2 + ax + b$$

*dla pewnych $a, b \in \mathbb{Z}$.*

*Dowód.* Element $a+bi \in \mathbb{Z}[i]$ jest pierwiastkiem wielomianu $x^2 - 2ax + a^2 + b^2 \in \mathbb{Z}[X]$. Na odwrót, niech $a+bi \in \mathbb{Q}(i)$ będzie pierwiastkiem unormowanego wielomianu stopnia 2 nad $\mathbb{Z}$. Wtedy $2a \in \mathbb{Z}$ i $2b \in \mathbb{Z}$. Ponieważ liczba całkowita $(2a)^2 + (2b)^2$ jest podzielna przez 4, to musi być $2a \equiv 0 \mod 2$ i $2b \equiv 0 \mod 2$, czyli $a, b \in \mathbb{Z}$. ■

Powyższa charakteryzacja pierścienia liczb Gaussa $\mathbb{Z}[i]$ jest o tyle wygodna (i naturalna), że nie odwołuje się do bazy ciała $\mathbb{Q}(i)$ nad $\mathbb{Q}$ (niezmienniczość ze względu na współrzędne). Co więcej okazuje się, że dla dowolnego skończonego rozszerzenia $\mathbb{Q} \subset K$ zbiór tych elementów ciała $K$, które są pierwiastkami wielomianu unormowanego nad $\mathbb{Z}$ **jest pierścieniem** (zawierającym $\mathbb{Z}$, zawartym w ciele $K$).

Zobaczmy inne teorioliczbowe zastosowanie pierścienia $\mathbb{Z}[i]$. **Trójką pitagorejską** nazywamy trójkę liczb całkowitych dodatnich $(a, b, c)$ czyniącą zadość równości: $c^2 = a^2 + b^2$. Trójkę taką nazywamy **pierwotną** wtedy i tylko wtedy, gdy $NWD(a, b, c) = 1$. Naszym celem jest znalezienie wszystkich pierwotnych trójek pitagorejskich.

**Twierdzenie 1.5.** *Niech $(a, b, c) \in \mathbb{Z}^3$ będzie dowolną, pierwotną trójką pitagorejską, taką, że $2|b$. Wówczas istnieją liczby całkowite $x, y > 0$ takie, że*

$$a = x^2 - y^2$$

$$b = 2xy$$

$$c = x^2 + y^2$$

*Dowód.* Dowód powyższego twierdzenia opiera się na spostrzeżeniu, które zdążyliśmy już poczynić, to znaczy iż pierścień liczb Gaussa $\mathbb{Z}[i]$ jest dziedziną z jednoznacznym rozkładem. Wszystkie trzy liczby całkowite $a, b, c$ nie mogą rzecz jasna być nieparzyste. Mamy

$$a^2 + b^2 = c^2 \iff (a + bi)(a - bi) = c^2$$

Oczywiście $NWD(a+bi, a-bi) = 1$ w pierścieniu $\mathbb{Z}[i]$, toteż z powyższej równości wynika, że $a+bi$ jest kwadratem: $a + bi = (x + iy)^2 = x^2 - y^2 + 2xyi$, skąd natychmiast, że $a = x^2 - y^2$ i $b = 2xy$. W konsekwencji $c = \sqrt{a^2 + b^2} = \sqrt{x^4 + y^4 + 2x^2y^2} = x^2 + y^2$. ■

Widać (mam nadzieję) z powyższych twierdzeń jaka moc drzemie w twierdzeniu o jednoznacznym rozkładzie w pierścieniu liczb Gaussa. Nasz dalszy plan postępowania jest następujący: uogólnimy pojęcie pierścienia $\mathbb{Z}[i]$ jako pierścienia o własności podanej w twierdzeniu 1.2 i zbadamy jego ogólne własności. Sprawdzimy też, że nie zawsze jest tak dobrze, jakby się chciało, to znaczy nie każdy pierścień całkowity ma jednoznaczny rozkład. Okaże się jednak, że ideały w takich pierścieniach rozkładają się jednoznacznie na ideały pierwsze.