Zespo w tlce

Andrzej Pręgowski
andpreg@boss.staszic.waw.pl

July 7, 2023

Po co to komu? Liczby zespolone dostarczają wiele pięknych narzędzi do badania liczb całkowitych, zobacz [5]. Są też bardzo użyteczne w rozwiązywaniu równań diofantycznych i, czasami, wkurzaniu znajomych.

Definicje:
0°) Niech $a = x + y\sqrt{D}$.Przez $\bar{a}$ oznaczmy $x - y\sqrt{D}$
1°) $\mathbb{Z}[i] = \{a + b \cdot i | a, b \in \mathbb{Z}\}$ (Są to liczby całkowite Gaussa)
2°) Niech $\alpha = a + b \cdot i$, gdzie $a, b \in \mathbb{Z}$. Wtedy $\bar{\alpha} = a - b \cdot i$
3°) Niech α jak powyżej. Zdefiniujmy funkcję $N : \mathbb{Z}[i] \to \mathbb{Z}^{\geqslant 0}$, $N(\alpha) = \alpha\bar{\alpha} = a^2 + b^2$
4°) Niech $\alpha, \beta \in \mathbb{Z}[i]$. Mówimy że $\beta|\alpha \iff \exists_{\gamma \in \mathbb{Z}[i]} \alpha = \beta \cdot \gamma$

Ćwiczenie 0: Kiedy $c + di | a + bi$, gdy $a, b, c, d \in \mathbb{Z}$?
Ćwiczenie 1: Udowodnij że dla $\alpha, \beta \in \mathbb{Z}[i]$ mamy $N(\alpha\beta) = N(\alpha)N(\beta)$
Ćwiczenie 2: Udowodnij że jeśli dla $\alpha, \beta \in \mathbb{Z}[i]$ $\beta|\alpha$, to $N(\beta)|N(\alpha)$

Twierdzenie o dzieleniu z resztą w $\mathbb{Z}[i]$:
Niech $\alpha, \beta \in \mathbb{Z}[i]$. Istnieją wtedy $\psi, \phi \in \mathbb{Z}[i]$, takie że $\alpha = \beta\psi + \phi$ i $N(\phi) < N(\beta)$.Nie są zdefiniowane jednoznacznie!.
Dowód:
Niech $\frac{\alpha}{\beta} = x + yi$. Zdefiniujmy $c, d \in \mathbb{Z}$ tak, by $|x - c| \leqslant \frac{1}{2}$ i $|y - d| \leqslant \frac{1}{2}$. Wtedy $x = c + e$,$y = d + f$ dla pewnych $0 \leqslant |e|, |f| \leqslant \frac{1}{2}$. Czyli $\alpha = (c + di) \cdot \beta + \beta \cdot (e + fi)$. Oczywistym jest, że $\beta(e + fi) \in \mathbb{Z}[i]$. Policzmy teraz $N(\beta(e + fi)) = N(\beta)N(e + fi) \leqslant N(\beta)((\frac{1}{2})^2 + (\frac{1}{2})^2) = \frac{1}{2} \cdot N(\beta) < N(\beta)$. Czyli biorąc $\psi = c + di, \phi = \beta \cdot (e + fi)$ widzimy że spełniają one warunki twierdzenia. ■

Kolejne definicje:
5a°) Niech $\alpha, \beta \in \mathbb{Z}[i]$ i niech $\alpha|\beta$ i $\beta|\alpha$. Mówimy wtedy że $\alpha \sim \beta$ (czyt. alfa stowarzyszone z beta)
5b°)Elementem odwracalnym należącymn do $\mathbb{Z}[i]$ nazwiemy taki element α dla którego $\exists_{\beta \in \mathbb{Z}[i]} \alpha\beta = 1$. Nazywane są one również jednościami w $\mathbb{Z}[i]$.
6°) Niech dane będą $\alpha, \beta \in \mathbb{Z}[i]$. Przez $NWD(\alpha, \beta)$ rozumiemy taką liczbę $\delta \in \mathbb{Z}[i]$,że $\delta|\alpha, \beta$ i że jeżeli $\epsilon \in \mathbb{Z}[i]$ i $\epsilon|\alpha, \beta$, to $\epsilon|\delta$ (wybieramy dowolną liczbę z taką własnością, bo reszta jest z nią stowarzyszona).
7°) Liczbę $\pi \in \mathbb{Z}[i]$ nazywamy liczbą pierwszą gdy spełniony jest warunek:
dla dowolnych $\alpha, \beta \in \mathbb{Z}[i]$ $\pi|\alpha\beta \implies \pi|\alpha \vee \pi|\beta$

Ćwiczenie 3a: Dla danej $\alpha \in \mathbb{Z}[i]$ znaleźć liczby stowarzyszone z α.

Ćwiczenie 3b: Wyznacz elementy odwracalne w $\mathbb{Z}[i]$
Ćwiczenie 4: Wykaż że dla $\alpha, \beta \in \mathbb{Z}[i]$ $\exists_{\gamma,\delta\in\mathbb{Z}[i]}\alpha\gamma + \beta\delta \sim NWD(\alpha, \beta)$
Ćwiczenie 5: Wykaż że 2 i 5 nie są liczbami pierwszymi w $\mathbb{Z}[i]$, ale 3 i 7 są (Wskazówka:normy!)
Ćwiczenie 6: Udowodnij iż jeśli $\pi \in \mathbb{Z}[i]$,π jest liczbą pierwszą w $\mathbb{Z}[i]$ i $\pi = \alpha\beta$, to $\alpha \sim 1 \vee \beta \sim 1$. Udowodnij również zależność odwrotną

Twierdzenie Fermata o sumie dwóch kwadratów:
Liczba pierwsza jest sumą dwóch kwadratów wtedy i tylko wtedy gdy przystaje do 1 mod 4 lub jest równa 2.
Dowód trywialny. ■

Ćwiczenie 7: Udowodnij, że jeśli $p \in \mathbb{P}$ i $p \equiv 3 \mod 4$, to p jest liczbą pierwszą w $\mathbb{Z}[i]$
Ćwiczenie 8: Udowodnij, że jeśli $\alpha \in \mathbb{Z}[i]$ i $N(\alpha) \in \mathbb{P}$,to α jest liczbą pierwszą w $\mathbb{Z}[i]$
Ćwiczenie 9: Dana jest nierzeczywista liczba pierwsza Gaussa π. Wykaż że $\forall_{z\in\mathbb{Z}[i]}\exists_{n\in\{0,1,..,N(\pi)-1\}} z \equiv_\pi n$. Czy π może być rzeczywista?

Twierdzenie: Charakteryzacja liczb pierwszych w $\mathbb{Z}[i]$:
Niech $p \in \mathbb{P}$. Mamy wtedy następujące rozkłady
(1) $2 = -i(1+i)^2$
(2) $p = p$, gdy $p \equiv 3 \mod 4$
(3) $p = (a+bi)(a-bi)$, gdy $p \equiv 1 \mod 4$
Dowód: Triv. ■

Twierdzenie: Rozkład liczb na czynniki pierwsze w $\mathbb{Z}[i]$:
Każda niezerowa, niestowarzyszona z 1 liczba w $\mathbb{Z}[i]$ może zostać zapisana jako iloczyn liczb pierwszych w $\mathbb{Z}[i]$, przy czym występuje forma jednoznaczności: jeśli mamy dwa takie rozkłady, to różnią się one co najwyżej tylko przemnożeniem odpowiednich liczb występujących w rozkładzie przez jedności
Dowód: Triv ■
Ćwiczenie 10: Udowodnić, iż jeśli $\alpha, \beta, \gamma \in \mathbb{Z}[i]$ i $\alpha\beta = \gamma^k$,$k \in \mathbb{Z}$,$NWD(\alpha, \beta) \sim 1$, to α, β są stowarzyszone z k-tymi potęgami
Ćwiczenie 11: Wyznacz $NWD(a+bi, a-bi)$
Ćwiczenie 12: Rozwiązać w $\mathbb{Z}$ równanie: $z^2 = y^2 + x^2$
Ćwiczenie 13: Przedstawić $(a^2+b^2)(c^2+d^2)$ jako sumę kwadratów
Ćwiczenie 13b: Przedstawić $(a^2+eb^2)(c^2+ed^2)$ jako x^2+ey^2
Ćwiczenie 14: Wykazać iż równanie $x^2+y^2 = z^3$ ma nieskończenie wiele rozwiązań w $\mathbb{Z}$ takich, że $x \perp y$
Ćwiczenie 15: Rozwiązać w $\mathbb{Z}$ równanie: $x^3 = y^2 + 1$

Dalsze jeszcze definicje:
8°) Niech dana będzie liczba całkowita bezkwadratowa D. Przez τ_D oznaczmy:
$\sqrt{D}$, gdy $D \equiv 2, 3 \mod 4$
$\frac{1+\sqrt{D}}{2}$, gdy $D \equiv 1 \mod 4$
9°) Niech $\mathbb{Z}[\tau_D] = \{a + b \cdot \tau_D | a, b \in \mathbb{Z}\}$
10°) Niech $\alpha \in \mathbb{Z}[\tau_D]$ i $\alpha = a + b \cdot \tau_D$. Zdefiniujmy znowu $N_D : \mathbb{Z}[\tau_D] \to \mathbb{Z}$ jako $\alpha\bar{\alpha}$
11°) Elementem odwracalnym (jednością) nazwiemy element $\alpha \in \mathbb{Z}[\tau_D]$ taki że $\exists_{\beta\in\mathbb{Z}[\tau_D]}\alpha\beta = 1$.

Normowo Euklidesowe pierścienie kwadratowe:

W zbiorach $\mathbb{Z}[\tau_D]$, zachodzi twierdzenie o dzieleniu z resztą wtedy i tylko wtedy
gdy D=-2,-3,-7,-11,2,3,5,6,7,11,13,17,19,21,29,33,37,41,57,73. W tych zbiorach da się również wyznaczać NWD i jest jednoznaczność rozkładu na czynniki pierwsze. Dowód tego jest nietrywialny i trudny
Twierdzenie: Jedności w $\mathbb{Z}[\tau_D]$, gdzie $D > 0$:
W takich zbiorach istnieje nieskończenie wiele jedności i istnieją dwie wyróżnione jedności które generują wszystkie inne
Dowód: Równania Pella (mniej więcej, jeśli $D \equiv 1 \mod 4$ to jest trochę trudniej) ■
Przykład:
(1) $D = 2$. Jedności fundamentalne to $(1 \pm \sqrt{2})$. Wszystkie inne jedności to są ich potęgi.
(2) $D = 5$. Jedności fundamentalne : $\frac{1\pm\sqrt{5}}{2}$
Ćwiczenie 16: Sfromułować i udowodnić analogiczne tezy do ćwiczeń (0),(1),(2),(3),(4),(8),(10) dla wartości D wymienionych w powyższym twierdzeniu ((3) tylko dla $D < 0$, bo dla innych jest nieskończenie wiele, np dla D=2 są to liczby postaci $(1 + \sqrt{2})^n \cdot \alpha$)
Ćwiczenie 16.2: Wykazać iż jeśli $a_n + b_n\sqrt{2} = (1 + \sqrt{2})^n$, to $a_n^2 - 2b_n^2 = \pm 1$.
Ćwiczenie 17: Przedstawić $(a^2 + ab + b^2)(c^2 + cd + d^2)$ w postaci $(x^2 + xy + y^2)$
Ćwiczenie 18: Rozwiązać równanie $x^3 = y^2 + 2$ w $\mathbb{Z}$
Ćwiczenie 19: Rozwiązać równianie $x^3 = y^2 + 11$ w $\mathbb{Z}$
Ćwiczenie 20: Rozwiązać równanie $y^5 = 2y^2 + 1$ w $\mathbb{Z}$
Ćwiczenie 21 [OM73 2 etap]: Dodatnie liczby całkowite spełniają równość

$$a^3 + 4b + c = abc$$

przy czym $a \geqslant c$ oraz liczba $p = a^2 + 2a + 2$ jest pierwsza. Wykazać, że p jest dzielnikiem liczby $a + 2b + 2$
Ćwiczenie 22: Rozwiązać równanie $x^p = y^2 + 1$ w $\mathbb{Z}$ dla $p = 2, 5, 7$
Ćwiczenie 23: Rozwiązać równanie $x^{2137} = 2y^2 + 1$ w $\mathbb{Z}$
Ćwiczenie 24: Rozwiązać równanie $x^3 = y^2 + 9$ w $\mathbb{Z}$
Ćwiczenie 25: Dane są liczby $a, b, c, d \in \mathbb{Z}$ spełniające układ równań:
$ac + 3bd = 1$
$ad + cb = 1$
Wykazać iż albo $a^2 - 3b^2 = 1$, albo $c^2 - 3d^2 = 1$ i że jest nieskończenie wiele takich liczb a, b, c, d
Ćwiczenie 26: Udowodnić WTF dla $n = 3$
Ćwiczenie 27: Istnieje nieskończenie wiele $x, y, z \in \mathbb{Z}$ takich że $x^3 + 1 = y^3 + z^3$
Ćwiczenie 28: Znaleźć przykłady podobne do zadania 25
Ćwiczenie 29 (nagroda: czekolada dla pierwszej osoby z dowodem niekorzystającym z WTF,powodzenia; update: czekolada zjedzona,już nieważne):
Wykaż, że dla dodatniej liczby całkowitej $m > 2$ podzielnej przez 2 równanie $z^3 - y^2 = 3^3 \cdot 2^m \cdot x^{m+2}$ nie ma rozwiązań w liczbach całkowitych x, y, z takich, że są one parami względnie pierwsze
Ćwiczenie 30: Rozwiązać w $\mathbb{N}$ równanie $y^2 + 1 = 5^n$
Ćwiczenie 31: $x^p = 2y^2 + 1$, gdzie $p \in \mathbb{P}$ i $p \equiv 3 \mod 4$ nie ma rozwiązań w $\mathbb{Z}$ innych niż (1,0)
Ćwiczenie 32: Wykaż iż jeśli wierzchołki wielokąta foremnego są punktami kratowymi, to jest on kwadratem
Ćwiczenie 33: Rozwiązać równanie $2^n = y^2 + 7$ w $\mathbb{Z}$. Znaleźć związek z liczbami trójkątnymi i liczbami Mersenna (Więcej info w [6])

Inne pierścienie kwadratowe z jednoznacznością rozkładu
Może się zdarzyć iż w zbiorze $\mathbb{Z}[\tau_D]$ nie ma dzielenia z resztą, ale wszystkie ideały są główne (nie chce mi się pisać co to znaczy,jest w [3]). Dla pierścieni urojonych zdarza się to tylko gdy $D = -19, -43, -67, -163$. Dla pierścienie rzeczywistych zdarza się to na przykład gdy $D = 14, 22, 31, 38, 46, \ldots$ .Nie wiadomo czy jest ich nieskończenie wiele. Daje nam to istnienie NWD jako linowej kombinacji dwóch liczb, elementów pierwszych i jednoznaczności rozkładu.
Rozwiązania niektórych ćwiczeń:

Ćwiczenie 0:
Mamy $\frac{a+bi}{c+di} = \frac{(a+bi)(c-di)}{c^2+d^2} = \frac{ac+bd}{c^2+d^2} + i \cdot \frac{bc-ad}{c^2+d^2}$. Jeśli należy to do $\mathbb{Z}[i]$ to $\frac{ac+bd}{c^2+d^2}, \frac{bc-ad}{c^2+d^2} \in \mathbb{Z}$. Jest to warunek wystarczający i konieczny
Ćwiczenie 3a:
Niech $\beta \in \mathbb{Z}[i]$ będzie takie że $\alpha \sim \beta$.Wtedy $\alpha|\beta \iff \alpha = u \cdot \beta$, co dzięki C3 daje nam $N(\alpha)|N(\beta)$. Mamy też $N(\beta)|N(\alpha)$, co razem z tym iż $N(x) \geqslant 0$ daje $N(\alpha) = N(\beta)$. Jednocześnie $N(\alpha) = N(u \cdot \beta) = N(u)N(\beta) \implies N(u) = 1$, co, zapisując $u = a + bi$ daje równanie $a^2 + b^2 = 1$, którego rozwiązaniami są pary $(1,0), (-1,0), (0,1), (0,-1)$, co odpowiada liczbom $1, -1, i, -i$.Czyli liczby stowarzyszone do $\alpha \in \mathbb{Z}[i]$ to liczby $-\alpha, -i\alpha, i\alpha$.
Ćwiczenie 3b:
Niech ψ będzie elementem odwracalnym w $\mathbb{Z}[i]$. Czyli $\exists_{\phi \in \mathbb{Z}[i]} \phi \cdot \psi = 1$, czyli $1 = N(\psi\phi)$, co daje nam $N(\psi) = 1$,co daje $\psi = 1, -1, i, -i$(patrz rozw.4a). Czyli jedyne elementy odwracalne to $1, -1, i, -i$
Ćwiczenie 7:
Wystarczy skorzystać z lematu:
Jeśli $p \in \mathbb{P}$ i $p|a^2 + 1$, to $p \equiv 1 \mod 4$
Ćwiczenie 8:
Niech dana będzie liczba $\alpha \in \mathbb{Z}[i]$ taka że $N(\alpha) \in \mathbb{P}$. Załóżmy iż $\alpha = \beta\gamma$ i że β, γ nie są stowarzyszone z 1. Wtedy $N(\alpha) = N(\beta\gamma) = N(\beta)N(\gamma) \in \mathbb{P}$. Oczywista sprzeczność.
Ćwiczenie 11:
Przepisane z [1]
Niech $d = NWD(a,b)$. Wtedy $NWD(a+bi, a-bi) = d \cdot NWD(\frac{a+bi}{d}, \frac{a-bi}{d})$. Niech $e = a/d, f = b/d$. Niech $\delta \sim NWD(e+fi, e-fi)$. Wtedy $\delta|2e, 2fi$. Ale $\exists_{x,y \in \mathbb{Z}} ex + fy = 1$, czyli $\delta|2ex + 2fyi = 2$. Czyli $\delta \sim 1$ lub $\delta \sim 1+i$ lub $\delta \sim 2$. Ostatni przypadek zachodzić nie może. Łatwo też sprawdzić iż $(1+i)|(x+yi)$ iff $x \equiv y \mod 2$, gdyż $x \equiv y \mod 2$ iff układ równań $u - w = x, u + w = y$ ma rozwiązanie, czyli też wtedy gdy $(1+i)(u+wi) = (x+yi)$.
Ćwiczenie 12:
Możemy założyć $x \perp y$. Wtedy $(x+yi)(x-yi) = z^2$. Chcemy sprawdzić czy $x+yi \perp x-yi$, co z C15 jest równoważne temu że $x \not\equiv y \mod 2$, co jest oczywiste. Czyli zgodnie z C10 mamy $x + yi = \epsilon(a+bi)^2$, co daje $x = \pm(a^2 - b^2), y = \pm 2ab$ lub $x = \pm 2ab, y = \pm(a^2 - b^2)$. Oczywiście $z = \pm(a^2 + b^2)$
Ćwiczenie 16(4):
Dla $D = -3$ to pierwiastki 6-tego stopnia z 1, dla reszty(oprócz -1) to ± 1
Ćwiczenie 17:
Skorzystać z N_{-3}. $x = (ac - bd), y = (cb + ad + bd)$
Ćwiczenie 20
Oczywiste jest to że $2 \not| x$. Wykorzystajmy jednoznaczność rozkładu w $Z[\tau_{-2}]$.
Mamy $x^5 = (1+y\sqrt{-2})(1-\sqrt{-2}y)$. Niech $\delta \sim NWD(1+y\sqrt{-2}, 1-y\sqrt{-2})$. Wtedy $\delta|1+\sqrt{-2}y+1-\sqrt{-2}y = 2$. Czyli $\delta \sim 1$ lub $\delta \sim \sqrt{-2}$ lub $\delta \sim 2$. Jeśli $\sqrt{-2}|\delta$, to $2 = N_{-2}(\sqrt{-2})|N_{-2}(\delta)|N_{-2}(1+y\sqrt{-2}) = x^5$, czyli $\delta \sim 1$. Czyli $1 + y\sqrt{-2} = (\pm 1)^5(a + b\sqrt{-2})^5$, gdzie $a, b \in \mathbb{Z}$. Rozwiązanie tego jest trywialne i daje rozwiązania $(x,y) = (1,0), (3, \pm 11)$.
Literatura:
Zadania o numerach $10, 11, 17, 30, 22, 18, 19, 32$ są z [1]
Warto poczytać o równaniu Pella (np. na stronce Imomath)
[1]: Adam Neugebauer, Algebra i Teoria Liczb, Wydawnictwo Szkolne Omega, Wydanie 2 poprawione
[2]: Wacław Sierpiński, Elementary theory of numbers,PAN, Warszawa 1964
[3]: Wacław Sierpiński, Teoria liczb, ,Warszawa - Wrocław 1950
[4]: https://youtube.com/playlist?list=PLSibAQEfLnTwq2-zCB-t9v2WvnnVKd0wn
[5]: Michał Krych, Szereg Leibniza i punkty kratowe, magazyn Delta, Styczeń 2019
[6]: Wacław Sierpiński, Liczby trójkątne, Państwowe Zakłady Wydawnictw Szkolnych,Warszawa Grudzień 1962
Link do [2]: http://matwbn-old.icm.edu.pl/kstresc.php?wyd=10&tom=42&jez=en

Link do [3]: http://matwbn-old.icm.edu.pl/kstresc.php?tom=19&wyd=10&jez=pl