

Liczby całkowite Gaussa

Kacper Paluch, Szymon Włoczewski, Wiktor Witkowski

29 stycznia 2021

Część teoretyczna 1

Pokazać, że dla dowolnych $z, w \neq 0+0i \in \mathbb{Z}[i]$ istnieją $t, r \in \mathbb{Z}[i]$ takie, że $z = t \cdot w + r$ oraz $r = 0$ lub $N(r) < N(w)$ (tzw. dzielenie z reszt).

Niech

$$x + yi = \frac{z}{w}$$

Istnieją takie liczby całkowite m, n że:

$$\begin{aligned} |x - m| &< 1 \\ |y - n| &< 1 \end{aligned}$$

Stąd

$$N(x - m + (y - n)i) < 1$$

Weźmy $t = m + ni$

$$\begin{aligned} z &= t \cdot w + r, \text{ gdzie} \\ r &= w(x - m + (y - n)i) \end{aligned}$$

Wiedząc, że $N(x - m + (y - n)i) < 1$, otrzymujemy nierówność $N(r) < N(w)$, a w szczególnym przypadku $x = m$ i $y = n$ otrzymujemy $r = 0$.

Część teoretyczna 2

Pokazać, że liczby: 1, -1, i, -i są jedynymi jednościami w zbiorze $\mathbb{Z}[i]$.

Jeśli $a+bi$ jest elementem odwracalnym to istnieje $c+di \in \mathbb{Z}$, takie że

$$(a + bi)(c + di) = 1 + 0i$$

Stąd

$$|(a + bi)(c + di)| = |1 + 0i|$$

Więc

$$(a^2 + b^2)(c^2 + d^2) = 1$$

Wiemy, że $a, b, c, d \in \mathbb{Z}$, więc ostatnia równość jest możliwa jedynie w przypadku, gdy

$$a^2 + b^2 = c^2 + d^2 = 1$$

To jest możliwe tylko gdy

$$(a^2 = 1 \wedge b^2 = 0) \vee (a^2 = 0 \wedge b^2 = 1)$$

Oznacza to, że $a + bi = 1$ lub $a + bi = -1$ lub $a + bi = i$ lub $a + bi = -i$. Elementami odwracalnymi mogą być tylko liczby:

$$1, -1, i, -i.$$

Część teoretyczna 3

Pokazać, że każda liczba całkowita Gaussa różna od jedności i Gaussowskiej liczby pierwszej, daje się przedstawić w postaci iloczynu Gaussowskich liczb pierwszych. Rozkład ten jest jednoznaczny z dokładnością do kolejności czynników i elementów stowarzyszonych.

Każda liczba pierwsza z definicji dzieli się tylko przez jedność i przez samą siebie. Dla dowolnych liczb zespolonych a i b zachodzi

$$N(ab) = N(a) * N(b)$$

Zbiorem wartości normy N są tylko takie liczby naturalne, które da się rozłożyć na sumę dwóch kwadratów.

Dla każdej liczby całkowitej Gaussa z możemy rozważyć podział liczby $N(z)$ na dzielniki pierwsze w zbiorze liczb naturalnych, a dzielniki te przedstawić jako liczby postaci $4k + 1$ lub $4k + 3$. Naturalne liczby pierwsze postaci $4k + 1$ można rozłożyć na dzielniki pierwsze w zbiorze liczb całkowitych Gaussa, co pokażemy w dalszej części pracy. Jeśli $N(p)$ jest podzielnikiem liczby $N(z)$ i $N(p)$ jest naturalną liczbą pierwszą postaci $4k + 1$ to p i liczby z nią stowarzyszone są dzielnikami pierwszymi liczby z w zbiorze liczb całkowitych Gaussa. Liczb pierwszych postaci $4k + 3$ nie da się rozbić na sumę kwadratów, więc jeśli liczba p tej postaci jest podzielnikiem liczby $N(z)$ to $N(p) = p^2$ również będzie jej podzielnikiem (w innym wypadku liczby $N(z)$ nie dałoby się przedstawić w postaci sumy kwadratów dwóch liczb całkowitych, co jest sprzeczne z definicją),

a także p i liczby z nią stowarzyszone są dzielnikami pierwszymi liczby z w zbiorze liczb całkowitych Gaussa.

W taki sposób uzyskujemy jednoznaczny rozkład liczby z na iloczyn Gaussowskich liczb pierwszych.

Spróbujmy przedstawić pewną liczbę z w postaci iloczynu liczb pierwszych Gaussa na różne sposoby. Przez u oznaczamy pewną jedność.

$$z = u_0 * p_1 * p_2 * \dots * p_n = u'_0 * q_1 * q_2 * \dots * q_n$$

Wybermy pewien czynnik z powyższego iloczynu, na przykład p_1 .

$$p_1 | z \Rightarrow p_1 | q_i \Rightarrow q_i = p_1 * u_1$$

Wnioskujemy, że q_i jest elementem stowarzyszonym z p_1 . Obie strony równości skracamy przez p_1 i analogicznie postępujemy wobec pozostałych czynników.

$$u_0 = u'_0 * u_1 * u_2 * \dots * u_n$$

$$u = u$$

Wobec tego jedyne różnice pomiędzy takimi rozkładami to: kolejność czynników i elementy stowarzyszone. Rozkład jest jednoznaczny zgodnie z założeniem.

Część teoretyczna 4

Pokazać, że są, trzy klasy Gaussowskich liczb pierwszych:

1. liczba $1 + i$ oraz liczby z nią stowarzyszone;
2. rzeczywiste liczby pierwsze p , dla których $p \equiv_4 3$ oraz liczby z nimi stowarzyszone;
3. dzielniki rzeczywistych liczb pierwszych p , takich że $p \equiv_4 1$.

Liczba $1 + i$ oraz liczby z nią stowarzyszone

Najpierw udowodnijmy, że liczba $z = 1 + i$ jest liczbą pierwszą.

1. Aby liczba ta była jednością, musi istnieć takie $w \in \mathbb{Z}[i]$, że $z \cdot w = 1 + 0i$:

$$z \cdot w = 1 + 0i$$

$$(1 + i)(a + bi) = 1 + 0i$$

$$a - b + i(a + b) = 1 + 0i$$

$$\begin{cases} a - b = 1 \\ a + b = 0 \end{cases}$$

$$\begin{cases} a = \frac{1}{2} \\ b = -\frac{1}{2} \end{cases}$$

Jak widać, $a, b \notin \mathbb{Z}$, zatem z nie jest jednością.

2.

$$z = 1 + i = (a + bi)(c + di)$$

Nie istnieją takie liczby $a, b, c, d \in \mathbb{Z}$ które spełniają powyższe równanie, zatem z jest nierozkładalne.

Udowodniliśmy tym samym, że $z = 1 + i$ jest liczbą pierwszą. Co do liczb z nią stowarzyszonych, skorzystamy z twierdzenia:

Twierdzenie. *Każda liczba zespolona całkowita, która jest stowarzyszona lub sprzężona z liczbą zespoloną pierwszą, jest również liczbą zespoloną pierwszą.*

Dowód. Skorzystamy z definicji liczby zespolonej pierwszej, która brzmi następująco:

Liczba zespolona pierwsza z to taka liczba, która nie jest stowarzyszona z liczbą 1 i nie ma żadnego dzielnika nie stowarzyszonego ani z liczbą 1, ani z liczbą z .

Jeśli α jest liczbą zespoloną i $N(\alpha) > 1$ oraz jeśli $\alpha = uv$ dla $N(u) > 1$ i $N(v) > 1$, to u nie może być stowarzyszona ani z 1 (bo wtedy $N(u) = 1$), ani z α (bo wtedy $N(u) = N(\alpha)$, zatem $N(\alpha) = N(u)N(v)$ co daje $N(v) = 1$). Wynika zatem, że α nie jest liczbą pierwszą.

Na odwrót, jeśli α jest liczbą zespoloną o normie $N(\alpha) > 1$, która nie jest pierwsza, wówczas dzielnik u nie jest stowarzyszony ani z 1, ani z α . Zatem dla $\alpha = uv$ v jest liczbą całkowitą zespoloną.

Gdyby $N(u) = 1$, to u byłaby stowarzyszona z 1 wbrew założeniu.

Gdyby $N(v) = 1$, to v byłaby stowarzyszona z 1, a wtedy dla $\alpha = uv$ liczba u byłaby stowarzyszona z α wbrew założeniu.

Zatem zawsze jest spełnione $N(u) > 1$ i $N(v) > 1$, a zatem liczba α jest iloczynem dwóch liczb całkowitych o normach większych od 1, co należało dowieść. $\square$

Liczba naturalna która, jest pierwsza w dziedzinie liczb naturalnych jest również pierwsza w dziedzinie liczb zespolonych. Nie zawsze tak jest jednak w odwrotnym przypadku. Przykładem może być liczba 2:

$$\begin{aligned} 2 &= (1 + i)(1 - i) \\ N(1 + i) &= N(1 - i) = 2 > 1 \end{aligned}$$

Liczyby $u = 1 + i$ i $v = 1 - i$ są pierwsze w dziedzinie liczb zespolonych. Otrzymujemy zatem

$$N(u)N(v) = N(uv) = 2$$

a więc $N(u) = 1$ lub $N(v) = 1$, co pokazuje, że u lub v jest liczbą stowarzyszona z 1.

Liczyby u i v są ze sobą stowarzyszone (ponieważ $1 - i = -(1 + i)$), zatem liczba 2 jest stowarzyszona z kwadratem liczby pierwszej zespolonej.

Opierając się na twierdzeniu, które brzmi

Dla wszelkich liczb całkowitych zespolonych a, b, c z $(a, b) = 1$ i $b|ac$ wynika $b|c$.

możemy wywnioskować, że każda liczba całkowita zespolona (o normie większej od 1) ma dokładnie jeden rozkład na czynniki zespolone pierwsze.

Aby sklasyfikować pozostałe liczby zespolone pierwsze, wykorzystamy powyższą własność ale tylko w obrębie liczb zespolonych pierwszych. Muszą być to liczby pierwsze naturalne nieparzyste (wykazaliśmy powyżej, że liczba 2 nie jest pierwsza w dziedzinie liczb zespolonych). Pozostały zatem liczby pierwsze w formie $4k + 1$ i $4k + 3$.

Rzeczywiste liczby pierwsze p , dla których $p \equiv_4 3$ oraz liczby z nimi stowarzyszone

Żałujemy, że dla $p = 4k + 3$ istnieje rozkład na czynniki zespolone całkowite o normach większych od 1.

$$p = (a + bi)(c + di)$$

$$p^2 = (a^2 + b^2)(c^2 + d^2)$$

Otrzymujemy zatem, że $a^2 + b^2 > 1$ i $c^2 + d^2 > 1$, a ponieważ p jest liczbą pierwszą w dziedzinie liczb naturalnych, musiałyby być spełnione $p = a^2 + b^2$ co dla $p = 4k + 3$ jest niemożliwe - na mocy poniższego lematu

Lemat 1. *Żadna liczba formy $4k + 3$ (pierwsza lub złożona) nie rozkłada się na sumę dwóch kwadratów*

Dowód. Jeśli obie liczby a i b są parzyste lub nieparzyste, to suma ich kwadratów będzie również parzysta i nigdy nie da reszty 3 z dzielenia przez 4.

Zaś jeśli jedna z liczb będzie parzysta a druga nieparzysta, to

$$a^2 + b^2 = (2x)^2 + (2y + 1)^2 = 4x^2 + 4y^2 + 4y + 1$$

$a^2 + b^2$ daje resztę 1.

Wynika zatem, że dla żadnej sumy obu kwadratów nie otrzymamy reszty 3. $\square$

Dzielniki rzeczywistych liczb pierwszych p , takich że $p \equiv_4 1$.

W myśl twierdzenia Fermata

Twierdzenie. *Każda liczba pierwsza w postaci $4k + 1$ rozkłada się tylko na jeden sposób na sumę dwóch kwadratów*

istnieją takie liczby a i b , że

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

$$p = (a + bi)(a - bi)$$

$$N(a \pm bi) = a^2 + b^2 = p > 1$$

Liczba p zatem, nie jest pierwsza w dziedzinie liczb zespolonych. Czynniki $(a+bi)$ i $(a-bi)$ natomiast już są, ponieważ dla $a+bi = uv$, gdzie

$$N(u) > 1, N(v) > 1$$

otrzymujemy $a-bi = u'v'$, zatem

$$p = (a+bi)(a-bi) = uu'vv' = N(u)N(v)$$

co wobec powyższego założenia dotyczącego norm, jest niemożliwe, ponieważ liczba p jest pierwsza w dziedzinie liczb naturalnych.

Pozostałe liczby

Należy jeszcze pokazać, że w dziedzinie liczb zespolonych nie ma żadnych innych liczb pierwszych.

Niech p będzie liczbą pierwszą zespoloną. Jeśli jest stowarzyszona z liczbą naturalną n , to musi być ona zarówno pierwsza, jak i naturalna - czyli w postaci $4k+3$.

Niech natomiast p nie będzie stowarzyszona z żadną liczbą naturalną. Wówczas $p = a+bi$, gdzie $a+b$ są liczbami całkowitymi i $b \neq 0$. Skoro p jest liczbą zespoloną, to jest nią również liczba sprzężona $p' = a-bi$, czyli $pp' = a^2 + b^2$. Żeby liczba $N(p) = a^2 + b^2$ nie była pierwsza w dziedzinie liczb naturalnych, to $pp' = a^2 + b^2 = xy$ gdzie x, y są liczbami naturalnymi większymi od 1. Dla iloczynu xy przynajmniej jeden czynnik musiałby być podzielny przez p , np. $x = pn$. Liczba n nie byłaby stowarzyszona z 1 (ponieważ p nie jest stowarzyszona z żadną liczbą naturalną). W takim razie z równości $pp' = xy$ wynika, że $p' = yn$, gdzie zarówno y jak i n nie są stowarzyszone z liczbą 1, co jest niemożliwe, gdyż p' jest liczbą pierwszą.

Zatem liczba $a^2 + b^2 = pp'$ jest pierwsza w dziedzinie liczb naturalnych i jako suma dwóch kwadratów jest ona albo 2, albo liczbą pierwszą w postaci $4k+1$.

Część teoretyczna 5

Pokazać, że każda liczba pierwsza postaci $4k+1$ da się, przedstawić w postaci sumy dwu kwadratów liczb całkowitych na 8 sposobów. Rozkłady różniące się, kolejnością, lub znakiem traktujemy jako różne.

Binarną formą kwadratową, nazywamy wyrażenie

$$Q(x, y) = ax^2 + bxy + cy^2$$

ze zmiennymi a, b, c .

Teoria Fermata o sumie kwadratów jest równoważne stwierdzeniu, że liczba pierwsza p , jest zapisana w formie $x^2 + y^2$ (gdzie $a = c = 1, b = 0$) wtedy i tylko wtedy, gdy p jest przystające do 1 (mod 4).

Wyróżnikiem formy kwadratowej nazywamy wyrażenie $b^2 - 4ac$. Zgodnie z powyższym, wyróżnikiem $x^2 + y^2$ jest -4 .

Dwie formy $ax^2 + bxy + cy^2$ i $a'x'^2 + b'x'y' + c'y'^2$ są sobie równe, gdy istnieją podstawienia na współczynniki całkowite:

$$\begin{aligned}x &= \alpha x' + \beta y' \\ y &= \gamma x' + \delta y'\end{aligned}$$

oraz $\alpha\delta - \beta\gamma = \pm 1$. Formy równoważne posiadają taki sam wyróżnik, a zatem tą samą parzystość współczynnika b . Ponadto, równoważne formy będą reprezentować te same liczby całkowite, ponieważ tego rodzaju podstawienia są odwracalne.

Aby udowodnić twierdzenie Fermata, należy znaleźć dowolną dodatnio określoną formę wyróżnika -4 , który reprezentuje p . Dla naszego przykładu, skorzystajmy z wyrażenia:

$$px^2 + 2mxy + cy^2$$

gdzie $a = p$, a $b = 2m$ (ponieważ - co wykazaliśmy wcześniej - b musi być parzyste). Jak widać, po podstawieniu $x = 1$ i $y = 0$, wyrażenie jest równe p :

$$p * 1^2 + 2m * 1 * 0 + c * 0^2 = p$$

Aby wyróżnik był równy -4 , musimy wyznaczyć odpowiednią wartość współczynnika c . Wyznaczamy wzór:

$$\begin{aligned}b^2 - 4ac &= 4m^2 - 4pc \\ 4m^2 - 4pc &= -4 \\ c &= \frac{m^2 + 1}{p}\end{aligned}$$

Aby postacie kwadratowe były sobie równe, c musi być liczbą całkowitą. Zatem twierdzenie będzie prawdziwe, jeśli znajdziemy takie m , dla którego wyrażenie $m^2 + 1$ jest podzielne przez p .

Ponieważ p należy do liczb rzeczywistych, nie dzieli żadnej z liczb Gaussa $m + i$ i $m - i$ (ponieważ nie dzieli ich urojonych części), aczkolwiek dzieli ich iloczyn $m^2 + 1$, to wynika z tego, że p nie może być elementem pierwszym liczb Gaussa. Musi zatem istnieć inny rozkład p na czynniki.

Ponieważ norma jest multiplikatywna ($N(ab) = N(a) * N(b)$) oraz $N(p) = p^2$ wiemy, że rozkład p musi dawać dwa czynniki, czyli być w postaci

$$p = (a + bi)(a - bi)$$

co daje inną możliwą postać:

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

co należało wykazać.

Powyższa forma zapisu liczby $p = 4k + 1$, pozwala zapisać ją na 8 różnych sposobów:

$$\begin{aligned}
 &a^2 + b^2 \\
 &(-a)^2 + b^2 \\
 &a^2 + (-b)^2 \\
 &(-a)^2 + (-b)^2 \\
 &b^2 + a^2 \\
 &(-b)^2 + a^2 \\
 &b^2 + (-a)^2 \\
 &(-b)^2 + (-a)^2
 \end{aligned}$$

Część praktyczna 1

Przedstawić graficznie podzielniki Gaussowskie liczb całkowitych.

Realizacja zadania metodą brutalną jest w języku Python dość prosta. Potrzebne będą jedności i norma.

```
units = [1, -1, 1j, -1j]
```

```
def norm(x):
    return x.real*x.real + x.imag*x.imag
```

Za sprawdzenie podzielności odpowiedzialna jest funkcja gidivisible.

```
def gidivisible(a, b):
    x = a*b.conjugate()
    nb = norm(b)
    return (x.real % nb == 0) and (x.imag % nb == 0)
```

Wyznaczenie podzielników Gaussowskich danej liczby całkowitej realizuje funkcja gidivisors.

```
def gidivisors(n):
    r = set()
    nn = norm(n)
    for x in range(0, n+1):
        for y in range(0, n+1):
            g = complex(x, y)
            if g != 0 and gidivisible(n, g):
                r.update([g*u for u in units])
    return r
```

Dane uzyskane dzięki tej realizacji można przedstawić na różne sposoby, na przykład wykorzystując bibliotekę pyplot. Inna reprezentacja danych dostępna jest pod adresem: <https://mion.elka.pw.edu.pl/~wwitkows/mat1-gi/>.

```
import matplotlib.pyplot as plt

def points_from_divisors(d):
    return [(x.real, x.imag) for x in d]

def plot(x):
    data = points_from_divisors(gdivisors(x))
    plt.scatter([d[0] for d in data], [d[1] for d in data])
    plt.show()
```

Dostępna jest również realizacja w programie mathematica.

```
a = 15;
Dzielniki = Divisors[a,GaussianIntegers->True]
Gauss = {};
Gauss = Flatten[Append[Gauss,Dzielniki]];
Gauss = Flatten[Append[Gauss,Dzielniki(-1)]];
Gauss = Flatten[Append[Gauss,Dzielniki(I)]];
Gauss = Flatten[Append[Gauss,Dzielniki(-I)]];
ComplexListPlot[Flatten[Gauss], PlotRange -> {{-a,a},{-a,a}}]
```

Część praktyczna 2

Przedstawić na płaszczyźnie zespolonej wizualizację rozmieszczenia liczb pierwszych Gaussa.

Zadanie zrealizować można w Wolfram Mathematica z wykorzystaniem poniższej formuły:

```
f[x_]:=ArrayPlot[Boole[Table[PrimeQ[a+b*I,GaussianIntegers->True],
                             {a,-x,x}, {b,-x,x}]]]
```

lub w języku Python z wykorzystaniem zamieszczonego niżej programu:

```
#!/bin/env python3

import argparse
import matplotlib.pyplot as plt

def is_prime(x):
    if x <= 1: return False
    i = 2
    while i*i <= x:
        if x % i == 0:
```

```

        return False
    i += 1
    return True

def norm(x):
    return x.real**2 + x.imag**2

def is_gaussian_prime(x):
    if x.real != 0 and x.imag != 0:
        return is_prime(norm(x))
    elif x.real != 0:
        return is_prime(abs(x.real)) and (abs(x.real)-3) % 4 == 0
    elif x.imag != 0:
        return is_prime(abs(x.imag)) and (abs(x.imag)-3) % 4 == 0
    else:
        return False

def plot(centerx=0, centery=0, delta=100, deltax=None, deltay=None):
    if deltax is None:
        deltax = delta
    if deltay is None:
        deltay = delta
    data = []
    for xi in range(centerx-deltax, centerx+deltax+1):
        for yi in range(centery-deltay, centery+deltay+1):
            if is_gaussian_prime(xi+yi*1j):
                data.append([xi, yi])

    plt.scatter([d[0] for d in data], [d[1] for d in data])
    plt.show()

if __name__ == "__main__":
    parser = argparse.ArgumentParser()
    parser.add_argument("--centerx", type=int, default=0)
    parser.add_argument("--centery", type=int, default=0)
    parser.add_argument("--delta", type=int, default=50)
    parser.add_argument("--deltax", type=int, default=None)
    parser.add_argument("--deltay", type=int, default=None)
    args = parser.parse_args()
    plot(args.centerx, args.centery, args.delta, args.deltax, args.deltay)

```

Część praktyczna 3

Zobrazować graficznie liczbę rozkładów dowolnej liczby naturalnej na sumę dwu kwadratów liczb całkowitych. Sprawdzić, czy uzyskane

przedstawienie jest zgodne z twierdzeniem Jacobiego.

W ramach zadania opracowany został zamieszczony poniżej program.

```
#!/bin/env python3

import argparse
import matplotlib.pyplot as plt
import math

def squaresR2(x):
    count = 0;
    i = math.ceil(math.sqrt(x))
    while i > 0:
        # rozkłady z zerem zostaną policzone tylko raz
        # dzięki temu po przemnożeniu uzyskamy dobry wynik
        j = 0
        while j*j <= x:
            if j*j + i*i == x:
                count += 1
            j += 1
        i -= 1
    # każda z liczb może być ujemna
    # więc każda kombinacja ma 4 różne warianty
    return count*4

def jacobiR2(x):
    count = 0;
    for i in range(1, x+1, 2):
        if x%i != 0:
            continue
        elif (i-1) % 4 == 0:
            count += 1
        elif (i-3) % 4 == 0:
            count -= 1
    return count*4;

def plot(start=0, end=None, mid=None, delta=50, strategy="both"):
    if mid is not None:
        start = mid - delta
        end = mid + delta + 1
    if end is None or end < start:
        end = start + delta
    if strategy == "jacobi":
        R = [jacobiR2(i) for i in range(start, end)]
    else:
        R = [squaresR2(i) for i in range(start, end)]
```

```

if strategy == "both":
    # check whether our results match up with Jacobi's Theorem
    R2 = [jacobiR2(i) for i in range(start, end)]
    confirmed = True
    for i in range(end-start):
        if R[i] != R2[i]:
            print("Our result for {} doesn't match Jacobi's Theorem"\
                  .format(i))
            confirmed = False
    if confirmed:
        print("both strategies gave the same result")
# make a plot
plt.scatter(range(start, end), R, marker=".")
plt.ylim(min(R)-1, max(R)+1)
plt.show()

if __name__ == "__main__":
    parser = argparse.ArgumentParser()
    parser.add_argument("--start", type=int, default=0)
    parser.add_argument("--end", type=int, default=None)
    parser.add_argument("--mid", type=int, default=None)
    parser.add_argument("--delta", type=int, default=100)
    parser.add_argument("--strategy", \
                        choices=["brutal", "jacobi", "both"], \
                        default="jacobi")
    args = parser.parse_args()
    plot(args.start, args.end, args.mid, args.delta, args.strategy)

```

Ponadto ilość rozkładów danej liczby na sumę kwadratów można również użyć w Wolfram Mathematica dzięki funkcji SquaresR: <https://reference.wolfram.com/language/ref/SquaresR.html>