

Liczby całkowite Gaussa

Prezentacja

Kacper Paluch, Wiktor Witkowski, Szymon Włoczewski

Politechnika Warszawska

29 stycznia 2021

Zadanie 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 resztą).

Zadanie 1

Niech

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

Istnieją takie liczby całkowite m, n że:

$$|x - m| < 1$$

$$|y - n| < 1$$

Stąd

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

Zadanie 1

Weźmy $t = m + ni$

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

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 $r = 0$.

Zadanie 2

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

Zadanie 2

Element odwracalny (jedność)

Element, dla którego istnieje element do niego odwrotny względem tego działania.

Mnożenie przez element odwracalny nie zmienia modułu liczby całkowitej Gaussa.

Zadanie 2

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

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

Zadanie 2

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:

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

Zadanie 3

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.

Podstawowe twierdzenie arytmetyki

Twierdzenie (Euclid's lemma)

If two numbers by multiplying one another make some number, and any prime number measure the product, it will also measure one of the original numbers.

Twierdzenie (Euclid, Elements Book VII, Proposition 32)

Any number either is prime or is measured by some prime number.

Twierdzenie (Euclid, Elements Book IX, Proposition 14)

If a number be the least that is measured by prime numbers, it will not be measured by any other prime number except those originally measuring it.

Zadanie 3

Przez u oznaczamy pewną jedność.

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

Wyberzmy 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.

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

$$u = u$$

Liczba $1+i$ oraz liczby stowarzyszone

Twierdzenie (o Gaussowskich liczbach pierwszych)

Gaussowską liczbą pierwszą nazywamy różną od zera liczbę ze zbioru $\mathbb{Z}[i]$, która nie jest ani jednością ani nie jest rozkładalna.

Liczba $1+i$ oraz liczby stowarzyszone

Twierdzenie (o Gaussowskich liczbach pierwszych)

Gaussowską liczbą pierwszą nazywamy różną od zera liczbę ze zbioru $Z[i]$, która nie jest ani jednością ani nie jest rozkładalna.

Liczbę $z \in Z[i]$ nazywamy jednością (lub elementem odwracalnym) w $Z[i]$, jeżeli istnieje $w \in Z[i]$ takie, że $zw = 1 + 0i$.

Liczba $1+i$ oraz liczby stowarzyszone

Twierdzenie (o Gaussowskich liczbach pierwszych)

Gaussowską liczbą pierwszą nazywamy różną od zera liczbę ze zbioru $\mathbb{Z}[i]$, która nie jest ani jednością ani nie jest rozkładalna.

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

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

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

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

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

Liczba $1 + i$ nie jest jednością

Liczba $1+i$ oraz liczby stowarzyszone

Twierdzenie (o Gaussowskich liczbach pierwszych)

Gaussowską liczbą pierwszą nazywamy różną od zera liczbę ze zbioru $\mathbb{Z}[i]$, która nie jest ani jednością ani nie jest rozkładalna.

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

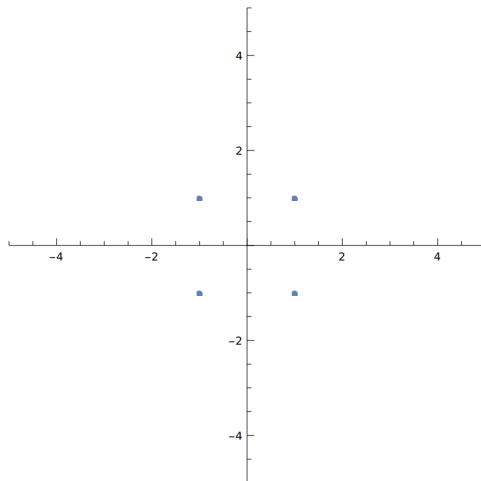
Liczba $1 + i$ nie jest rozkładalna

Liczba $1+i$ oraz liczby stowarzyszone

Twierdzenie (o liczbach stowarzyszonych)

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

Liczba $1+i$ oraz liczby stowarzyszone



Dzielniki rzeczywistych liczb pierwszych p , w postaci $4k+1$

Twierdzenie (Fermata)

Każda liczba formy $4k+1$ rozkłada się i to w jeden tylko sposób na sumę dwóch kwadratów.

Dzielniki rzeczywistych liczb pierwszych p , w postaci $4k+1$

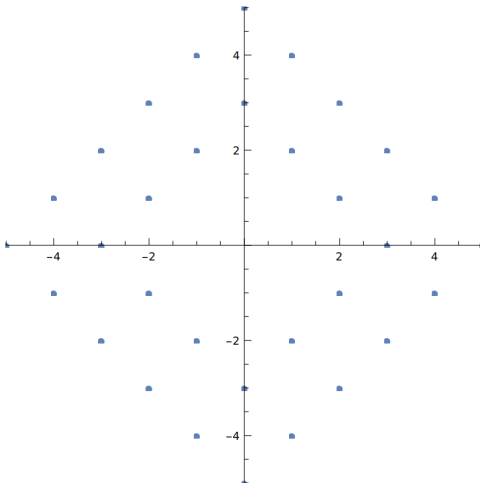
Twierdzenie (Fermata)

Każda liczba formy $4k+1$ rozkłada się i to w jeden tylko sposób na sumę dwóch kwadratów.

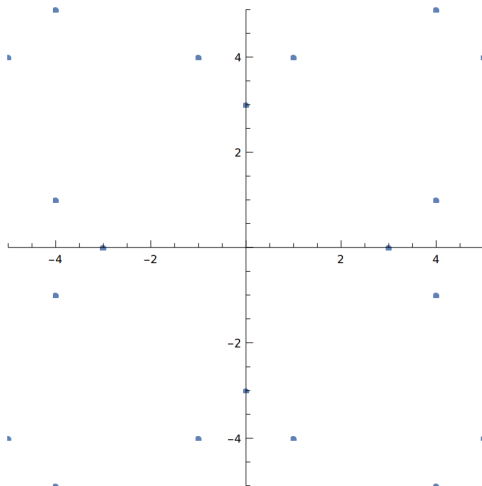
$$p = a^2 + b^2$$

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

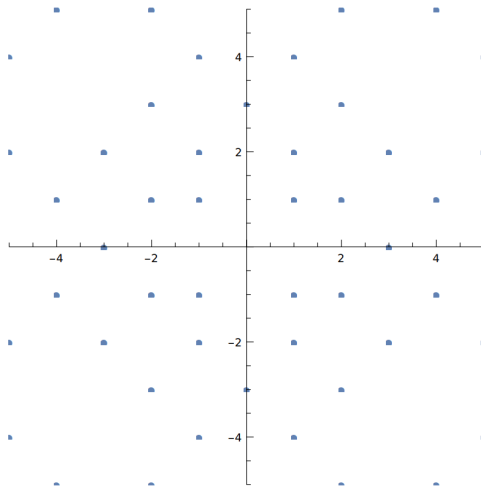
Dzielniki rzeczywistych liczb pierwszych p , w postaci $4k+1$



Rzeczywiste liczby pierwsze p , w postaci $4k+3$ oraz liczby z nimi stowarzyszone



Wszystkie liczby pierwsze



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.

Twierdzenie (Fermata o sumie dwóch kwadratów)

Każda liczba formy $4k+1$ rozkłada się i to w jeden tylko sposób na sumę dwóch kwadratów.

Dowód twierdzenia fermata o sumie dwóch kwadratów

$$p = 1 + 4k$$

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

Ponieważ p jest liczbą nieparzystą - a jest nieparzyste, a b jest parzyste

$$p = x^2 + (2y)^2$$

$$p = x^2 + 4y^2$$

Dowód twierdzenia fermata o sumie dwóch kwadratów

$$p = 1 + 4k$$

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

Ponieważ p jest liczbą nieparzystą - a jest nieparzyste, a b jest parzyste

$$p = x^2 + (2y)^2$$

$$p = x^2 + 4y^2$$

$$p = x^2 + 4zy$$

Dowód twierdzenia fermata o sumie dwóch kwadratów

$$p = 1 + 4k$$

$$41 = x^2 + 4zy$$

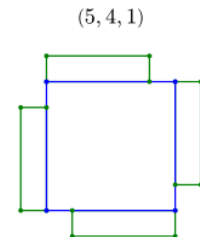
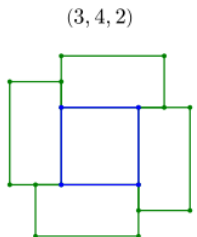
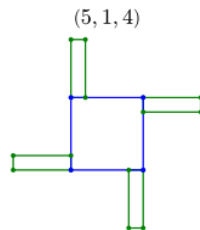
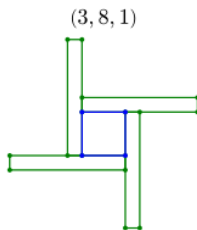
x	z	y
1	10	1
1	1	10
1	5	2
1	2	5
3	8	1
3	1	8
3	4	2
3	2	4
5	2	2
5	1	4
5	4	1

Dowód twierdzenia fermata o sumie dwóch kwadratów

$$p = 1 + 4k$$

$$41 = x^2 + 4zy$$

x	z	y
1	10	1
1	1	10
1	5	2
1	2	5
3	8	1
3	1	8
3	4	2
3	2	4
5	2	2
5	1	4
5	4	1

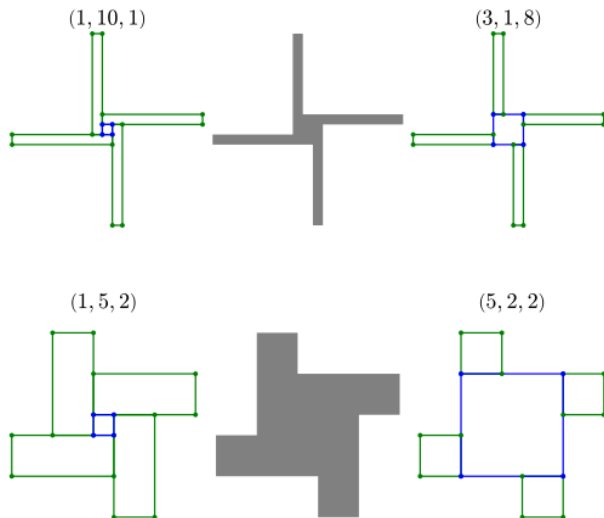


Dowód twierdzenia fermata o sumie dwóch kwadratów

$$p = 1 + 4k$$

$$41 = x^2 + 4zy$$

x	z	y
1	10	1
1	1	10
1	5	2
1	2	5
3	8	1
3	1	8
3	4	2
3	2	4
5	2	2
5	1	4
5	4	1

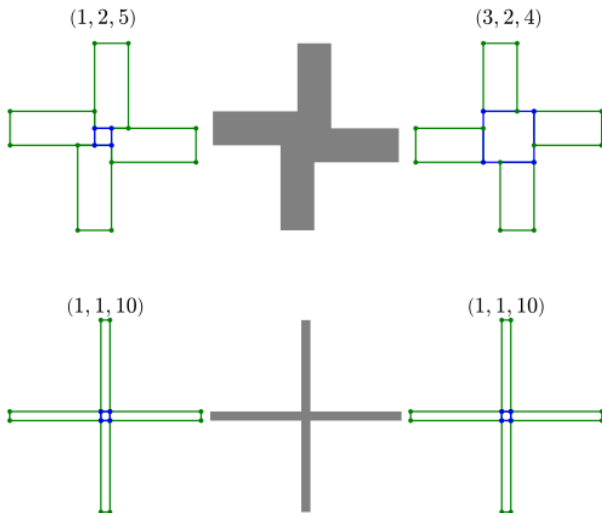


Dowód twierdzenia fermata o sumie dwóch kwadratów

$$p = 1 + 4k$$

$$41 = x^2 + 4zy$$

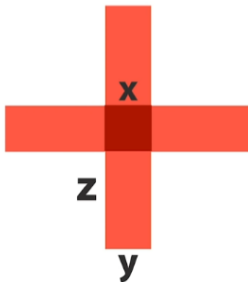
x	z	y
1	10	1
1	1	10
1	5	2
1	2	5
3	8	1
3	1	8
3	4	2
3	2	4
5	2	2
5	1	4
5	4	1



Dowód twierdzenia fermata o sumie dwóch kwadratów

$$p = x^2 + 4yz$$

$$p = x^2 + 4xz$$



Dowód twierdzenia fermata o sumie dwóch kwadratów

$$p = x^2 + 4xz$$

$$p = x(x + 4z)$$

Liczba p jest pierwsza, zatem dzieli się jedynie przez 1 i samą siebie.

$$p = 1(1 + 4z)$$

$$p = 1 + 4z$$

$$z = k$$

$$p = 1 + 4k$$

Dowód twierdzenia fermata o sumie dwóch kwadratów

Dowód Zagier'a

$$(x, y, z) \mapsto \begin{cases} (x + 2z, z, y - x - z) & \text{if } x < y - z \\ (2y - x, y, x - y + z) & \text{if } y - z < x < 2y \\ (x - 2y, x - y + z, y) & \text{if } 2y < x \end{cases}$$

Twierdzenie (Fermata)

Każda liczba formy $4k+1$ rozkłada się i to w jeden tylko sposób na sumę dwóch kwadratów.

Twierdzenie (Fermata)

Każda liczba formy $4k+1$ rozkłada się i to w jeden tylko sposób na sumę dwóch kwadratów.

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

Twierdzenie (Fermata)

Każda liczba formy $4k+1$ rozkłada się i to w jeden tylko sposób na sumę dwóch kwadratów.

$$a^2 + b^2$$

$$(-a)^2 + b^2$$

$$a^2 + (-b)^2$$

$$(-a)^2 + (-b)^2$$

$$b^2 + a^2$$

$$(-b)^2 + a^2$$

$$b^2 + (-a)^2$$

$$(-b)^2 + (-a)^2$$