

33. Гауссовы числа и другие расширения

20 июля

Сегодня мы изучим некоторые полезные теоретико-числовые свойства колец $\mathbb{Z}[i]$ (кольцо гауссовых чисел), $\mathbb{Z}[\sqrt{-2}]$ и $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$.

Мы можем воспринимать данные кольца как «расширения» кольца \mathbb{Z} целых чисел.

Естественный вопрос. Какие свойства, аналогичные кольцу \mathbb{Z} есть у данных колец?

Для начала хочется научиться сравнивать числа в этих кольцах между собой. Для этого полезно вспомнить понятие нормы.

Определение. Нормой гауссова числа $z = a + bi$ называется

$$N(z) = z\bar{z} = (a + bi)(a - bi) = a^2 + b^2.$$

Определение. Нормой числа $z = a + b\sqrt{-2}$ называется $N(z) = a^2 + 2b^2$.

Определение. Нормой числа $z = a + b\omega$, где $\omega = \frac{1+\sqrt{-3}}{2}$ называется $N(z) = a^2 + ab + b^2$. Если переписать элемент кольца в виде $a_1 + b_1\sqrt{-3}$ для рациональных a_1 и b_1 , то $N(z) = a_1^2 + 3b_1^2$.

Замечание. Норма является мультипликативной функцией, то есть для любых z_1, z_2 выполнено $N(z_1 \cdot z_2) = N(z_1) \cdot N(z_2)$.

Норма нужна нам для того, чтобы научиться «сравнивать» между собой гауссовы числа. Из этого естественным образом возникает следующее свойство.

Деление с остатком. В следующих кольцах возможно деление с остатком, то есть любых чисел z_1 и z_2 , где $z_2 \neq 0$, существуют числа u и r из того же кольца такие, что $z_1 = z_2u + r$ и $N(r) < N(z_2)$.

- Кольцо гауссовых чисел $\mathbb{Z}[i]$ с нормой $N(a + bi) = a^2 + b^2$.
- Кольцо $\mathbb{Z}[\sqrt{-2}]$ с нормой $N(a + b\sqrt{-2}) = a^2 + 2b^2$.
- Кольцо $\mathbb{Z}[\omega]$, где $\omega = \frac{1+\sqrt{-3}}{2}$, с нормой $N(a + b\omega) = a^2 + ab + b^2$.

Замечание. Мы взяли кольцо $\mathbb{Z}[\omega]$, а не $\mathbb{Z}[\sqrt{-3}]$ для того, чтобы существовало деление с остатком.

Упражнение для желающих. Покажите, что кольца $\mathbb{Z}[\omega]$, где $\omega = \frac{1+\sqrt{-7}}{2}$ или $\frac{1+\sqrt{-11}}{2}$ также допускают деление с остатком относительно стандартной нормы.

Соглашение. В дальнейшем всегда $\omega = \frac{1+\sqrt{-3}}{2}$.

Определение. Наибольшим общим делителем двух чисел z_1, z_2 из кольца $\mathbb{Z}[i]$ ($\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\omega]$) называется их общий делитель, имеющий наибольшую норму.

Замечание. Наибольший общий делитель определен с точностью до домножения на обратимый элемент.

Теорема о линейном представлении НОД. Для любых двух чисел $z_1, z_2 \in \mathbb{Z}[i]$ ($\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\omega]$) существуют числа $u, v \in \mathbb{Z}[i]$ ($\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\omega]$) такие, что $(z_1, z_2) = uz_1 + vz_2$.

Определение. Число z в кольце $\mathbb{Z}[i]$ ($\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\omega]$) называется простым, если оно не раскладывается в произведение двух чисел из кольца с меньшей нормой.

Основная теорема арифметики. Любое ненулевое число из кольца $\mathbb{Z}[i]$ ($\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\omega]$) можно разложить в произведение простых чисел из данного кольца, причем это разложение единственно с точностью до порядка сомножителей и домножения на обратимые элементы кольца.

Полезный контрпример. Кольцо $\mathbb{Z}[\sqrt{-5}]$ не удовлетворяет основной теореме арифметики, поскольку $21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$.

Теперь немного поговорим про простые элементы в наших кольцах. Заметим, что не все простые числа \mathbb{Z} являются простыми числами в наших кольцах.

Теорема. (а) Целое число $z > 0$ является простым в кольце $\mathbb{Z}[i]$ тогда и только тогда, когда оно простое в \mathbb{Z} и $z \equiv 3 \pmod{4}$.

(b) Целое число $z > 0$ является простым в кольце $\mathbb{Z}[\sqrt{-2}]$ тогда и только тогда, когда оно простое в \mathbb{Z} и $z \equiv 5 \pmod{8}$ или $z \equiv 7 \pmod{8}$.

(c) Целое число $z > 0$ является простым в кольце $\mathbb{Z}[\omega]$ тогда и только тогда, когда оно простое в \mathbb{Z} и $z = 2$ или $z \equiv 1 \pmod{3}$.

Теорема. Если $N(z)$ является простым числом в \mathbb{Z} , то z является простым числом в $\mathbb{Z}[i]$ ($\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\omega]$).

Замечание. Как мы понимаем, обратное утверждение неверно.

Упражнение. Взаимно простые в совокупности целые числа a , b и c таковы, что $a^2 + b^2 = c^2$. Докажите, что существуют такие целые числа u и v , что $a = u^2 - v^2$, $b = 2uv$ или наоборот.

Для самостоятельного решения

1. Рассмотрим число $4 = 2 \cdot 2 = (1 - \sqrt{-3}) \cdot (1 + \sqrt{-3})$. То есть мы получили противоречие с основной теоремой арифметики для $\mathbb{Z}[\omega]$? Где мы вас обманываем?

2. **(а)** Докажите, что каждое простое число представляется в виде $x^2 + y^2$ для целых x и y не более чем одним способом с точностью до знаков x и y .

(b) Верно ли, что каждое простое число представляется в виде $x^2 + 2y^2$ для целых x и y не более чем одним способом с точностью до знаков x и y ?

(c) Верно ли, что каждое простое число представляется в виде $x^2 + 3y^2$ для целых x и y не более чем одним способом с точностью до знаков x и y ?

3. Опишите все решения уравнения $a^2 + b^2 = c^3$ в натуральных числах.

4. **(а)** Решите в целых числах уравнение $x^2 + 4 = y^3$.

(b) Решите в целых числах уравнение $y^2 + 2 = x^3$.

Указание. Это уравнение нужно решать уже в $\mathbb{Z}[\sqrt{-2}]$.

5. Докажите, что уравнение $x^n = y^2 + 1$ не имеет решений в натуральных числах при натуральном $n > 1$.

6. Решите в целых числах уравнение $x^2 + 2 = y^n$.

7. Натуральные числа x , y , z таковы, что $xy = z^2 + 1$. Докажите, что найдутся такие целые a , b , c , d , что $x = a^2 + b^2$, $y = c^2 + d^2$, $z = ac + bd$.

8. Даны взаимно простые целые a и b разной четности. Известно, что $a^2 + 3b^2$ является кубом целого числа. Докажите, что существуют целые s и t такие, что $a = s^3 - 9st^2$, $3t(s^2 - t^2)$.