Упражнения

28. Для комплексного числа $z = 2 + i$ отметьте на комплексной плоскости числа iz, $-z$, $-iz$.

29. Ассоциированные с числом z числа – это в точности числа вида εz, где ε – делитель единицы. Докажите это.

30. Докажите, что а) числа $1 + i$ и $1 - i$ ассоциированы; б) числа $a + bi$ и $a - bi$ ассоциированы в том и только том случае, когда выполнено хотя бы одно из условий: $a = 0$, $b = 0$, $a = b$, $a = -b$.

Доказательство теоремы Ферма–Эйлера

Доказательство леммы 2

Вернемся к лемме 2, от которой мы надолго отвлеклись, чтобы придать смысл разложению $m^2 + 1 = (m + i)(m - i)$. Числу p не кратен ни один из множителей $m + i$ и $m - i$, но кратно произведение $m^2 + 1$. Что это значит? Как может произведение быть кратно p, если ни один из множителей не кратен p? Неужели арифметика гауссовых чисел настолько своеобычна, что в ней нет никаких привычных нам законов? Например, мы привыкли к тому, что разложение натурального числа на простые множители единственно с точностью до порядка множителей. Вдруг основная теорема арифметики неверна для $\boldsymbol{Z}[i]$?

Оказывается, все не так плохо. Разложение на простые множители в $\boldsymbol{Z}[i]$ единственно в том же смысле, в каком оно единственно для обычных целых чисел (мы докажем это в разделе «Основная теорема арифметики»). А кажущееся противоречие устраняется тем, что простое число p может перестать быть простым при расширении $\boldsymbol{Z}$ до $\boldsymbol{Z}[i]$. Например, $2 = (1 + i)(1 - i)$ и $5 = (1 + 2i)(1 - 2i)$. Вообще, $p = (a + bi)(a - bi)$ для всякого числа $p = a^2 + b^2$.

Итак, разрешим себе пофантазировать: вообразим, что мы уже доказали теорему о единственности разложения целых гауссовых чисел на простые множители, и докажем лемму 2. Делитель p числа $(m + i)(m - i)$ не может быть простым гауссовым числом. Значит,

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

где целые гауссовы числа $(a + bi)$ и $(c + di)$ – не делители единицы. Поскольку модуль произведения равен произведению модулей, имеем

$$p = \sqrt{a^2 + b^2}\,\sqrt{c^2 + d^2},$$

т. е. $p^2 = \left(a^2 + b^2\right)\left(c^2 + d^2\right)$, откуда $p = a^2 + b^2 = c^2 + d^2$. Лемма 2, а заодно и теорема 4 доказаны.

Разложение простого числа на простые множители

Заголовок этого подраздела мог бы удивить, если бы выше мы не разлагали уже простые натуральные числа на простые гауссовы множители. Какие же простые натуральные числа останутся простыми во множестве целых гауссовых чисел, а какие станут составными? И как устроены разложения «новых составных» чисел?

Теорема 8. *Всякое простое натуральное число вида $p = 4n + 3$ является простым в $\boldsymbol{Z}[i]$; число 2 ассоциировано с квадратом простого гауссова числа $1+ i$; всякое простое натуральное число вида $p = 4n + 1$ разлагается на два сопряженных множителя: $p = (a + bi)(a - bi)$, причем множители $a + bi$ и $a - bi$ – простые гауссовы числа.*

Доказательство. Если число $p = 4n + 3$ представлено в виде произведения двух целых гауссовых чисел $p = (a + bi)(c + di)$, то

$$|p| = |a + bi| \cdot |c + di|,$$

откуда $p^2 = \left(a^2 + b^2\right)\left(c^2 + d^2\right)$. Значит, либо один из множителей $\left(a^2 + b^2\right)$ и $\left(c^2 + d^2\right)$ равен 1, а другой равен p^2, либо $p = a^2 + b^2 = c^2 + d^2$. В первом случае ясно, что число p было представлено в виде произведения делителя единицы и ассоциированного с p числа. Второй случай невозможен в силу теоремы 3.

С числом 2 дело обстоит еще проще: $2 = -i(1 + i)^2$. Впрочем, мы должны объяснить, почему число $1 + i$ простое.

Лемма 3. *Простое натуральное число p нельзя представить в виде произведения более чем двух целых гауссовых чисел, не являющихся делителями единицы. (Другими словами, если p ассоциировано с произведением двух не являющихся делителями единицы целых гауссовых чисел, то эти числа – простые.)*

Доказательство леммы 3. Если $p = (a + bi)(c + di)(e + fi)$, то

$$|p| = |a + bi| \cdot |c + di| \cdot |e + fi|,$$

откуда $p^2 = \left(a^2 + b^2\right)\left(c^2 + d^2\right)\left(e^2 + f^2\right)$. Квадрат простого числа никак не может быть произведением трех отличных от 1 натуральных чисел. Лемма 3 и теорема 8 доказаны.

Упражнения

31. Изобразите на комплексной плоскости все числа, на которые нацело делится число $5 - i$.

32. Сколько среди делителей числа а) $3 - 11i$; б) $6 + 12i$ таких, у которых и вещественная, и мнимая части положительны?

33. Разложите на простые гауссовы множители числа а) 16; б) 1001; в) $47 + i$.

Доказательство теоремы 2

Помните, мы обещали получить теорему 2 как одно из следствий теории целых гауссовых чисел? Настало время это сделать. Пусть простое число p не представимо в виде суммы двух квадратов и сумма квадратов $x^2 + y^2$ кратна p. Из теоремы 8 следует, что всякое простое натуральное число p либо является простым гауссовым числом, либо представимо в виде суммы квадратов двух целых чисел. Значит, в рассматриваемой ситуации p – простое гауссово число. Поскольку произведение $(x + iy)(x - iy) = x^2 + y^2$ кратно p, хотя бы один из сомножителей кратен p. Это в точности означает, что x и y кратны p. Теорема 2 доказана.

Количество представлений

Единственность представления простого числа в виде суммы двух квадратов

По теореме Ферма–Эйлера любое простое число p, которое при делении на 4 дает остаток 1, представимо в виде суммы двух квадратов. Давайте докажем, что такое представление единственно с точностью до порядка слагаемых.