

Целые гауссовы числа

Определение 1. Комплексное число $a + bi$ называется *целым гауссовым*, если a и b — целые числа. Множество целых гауссовых чисел обозначается $\mathbb{Z}[i]$. Нормой $\|a + bi\|$ такого числа называется квадрат его модуля, то есть $a^2 + b^2$.

Определение 2. Целое гауссово число u кратно целому гауссовому числу v , если существует целое гауссово число w такое, что $u = vw$.

Определение 3. Целое гауссово число u называется обратимым, если 1 кратно u , то есть существует целое гауссово v такое, что $uv = 1$.

Определение 4. Ненулевое целое гауссово число u называется *простым*, если оно необратимо и имеет только тривиальные делители, то есть обратимые числа, а также произведения обратимых чисел на u . Необратимые числа, не являющиеся простыми, называются *составными*.

1. Найдите все обратимые целые гауссовы числа.
2. (а) Докажите, что для целых гауссовых чисел возможно деление с остатком: для любых $a, b \in \mathbb{Z}[i]$, $b \neq 0$, существуют $q, r \in \mathbb{Z}[i]$ такие, что $a = bq + r$ и $\|r\| < \|b\|$.

Замечание: такие q и r определены, вообще говоря, неоднозначно.

(б) Осознайте, что для нахождения НОД двух гауссовых чисел можно применять алгоритм Евклида, как и для обычных целых. Докажите, что если a, b — два гауссовых целых числа и $d = (a, b)$ — их НОД, то существуют целые гауссовы x, y такие, что $d = ax + by$.

(в) **Лемма Евклида.** Докажите, что если p — простое гауссово и ab делится на p , то a или b делится на p .

(г) **Основная теорема арифметики.** Докажите, что любое целое гауссово число, отличное от обратимых, единственным образом (с точностью до порядка множителей и умножения на обратимые) представляется в виде произведения простых гауссовых.

3. (а) Докажите, что простое число p либо является простым гауссовым числом, либо представляется в виде $z\bar{z}$, где $z = a + bi$, $\bar{z}$ — простые гауссовы числа.
(б) Докажите, что простое число вида $4k + 3$ является простым гауссовым.
(в) Докажите (или вспомните, как доказывается), что для простого $p = 4k + 1$ существует m такое, что $m^2 + 1$ делится на p .
(г) Докажите, что простое $p = 4k + 1$ представляется в виде произведения сопряжённых простых гауссовых чисел.
(д) Используя предыдущий пункт, докажите, что простое число вида p представляется в виде суммы квадратов, если и только если $p = 2$ или $p = 4k + 1$, причём в этом случае такое представление единственно.

4. (а) **Рождественская теорема Ферма.** Какие натуральные числа представляются в виде суммы двух квадратов?

- (б) Пусть $m = 2^\alpha p_1^{\alpha_1} \dots p_r^{\alpha_r}$, где все простые числа p_i различны и имеют вид $4k + 1$, а все числа α_i нечётны. Докажите, что количество представлений числа m в виде $a + b$, где a и b — точные квадраты, равно $(\alpha_1 + 1)(\alpha_2 + 1) \cdot \dots \cdot (\alpha_r + 1)$.
5. Дано простое целое гауссово число p . Какое наибольшее количество целых гауссовых чисел можно выбрать так, чтобы разность никаких двух из них не делилась на p ?
6. Решите в целых числах уравнение (а) $x^2 + 1 = y^3$; (б) $x^2 + 4 = y^3$.
7. Даны натуральные числа x, y, z , удовлетворяющие уравнению $xy = z^2 + 1$. Докажите, что существуют целые a, b, c, d такие, что $x = z^2 + b^2$, $y = c^2 + d^2$ и $z = ac + bd$.