Гауссовы целые числа

04.12.2019
25/20/15 з. на 5/4/3

Определение 1. Числа вида $a + bi$, где $a, b \in \mathbb{Z}$, называются *гауссовыми целыми числами* или просто *гауссовыми числами*. Множество всех гауссовых чисел обозначается $\mathbb{Z}[\sqrt{-1}]$. Легко видеть, что сумма и произведение гауссовых чисел – снова гауссовы. Как обычно, скажем, что гауссово число x *делит* гауссово число y, если существует такое гауссово z, что $y = xz$. Гауссово число x называется *обратимым*, если оно делит 1. Гауссово необратимое число $x \neq 0$ называется *простым*, если для любого разложения $x = yz$ какое-то из чисел y, z обратимо.

Задача 1. Найдите все обратимые гауссовы числа.

Задача 2. **а)** Верно ли, что натуральное простое число всегда будет гауссовым простым?
б) Верно ли, что квадрат модуля гауссова простого числа всегда будет натуральным простым?
в) Пусть для гауссова числа z квадрат модуля $|z|^2$ — простое целое число. Верно ли, что z — простое гауссово число?

Задача 3. **а)** Нарисуйте на плоскости все гауссовы числа, кратные $2 + 3i$.
б) Докажите, что для любых гауссовых чисел x, y, $y \neq 0$ найдутся такие гауссовы q, r, что $x = qy + r$ и $|r| < |y|$. Единственны ли такие q, r? Если нет, то сколько их может быть?

Задача 4. Определите наибольший общий делитель двух гауссовых чисел, докажите, что он существует и представляется в виде их линейной комбинации (коэффициенты — гауссовы).

Задача 5. **а)** Верно ли, что если натуральные числа взаимно просты, то у них нет общих гауссовых необратимых делителей?
б) Верно ли, что если гауссовы числа не имеют общих необратимых делителей, то их квадраты модулей взаимно просты?

Задача 6. Докажите, что если гауссово простое p делит произведение xy, то оно делит либо x, либо y.

Задача 7. Сформулируйте и докажите основную теорему арифметики для гауссовых чисел.

Задача 8. Решите в целых числах уравнение $y^3 = x^2 + 1$.

Задача 9. **а)** Докажите, что ни при каком n число $(3 + 4i)^n$ не является вещественным.
б) Докажите, что угол $\operatorname{arctg} 3/4$ не выражается рациональным числом градусов.
в)* Найдите все такие натуральные k, что $\cos \pi/k$ и $\sin \pi/k$ рациональны.

Задача 10. Докажите, что если два числа представимы в виде $a^2 + db^2$ (где d — фиксированное натуральное число), то и их произведение представимо в таком виде.

Задача 11. **а)** Дайте определение $\mathbb{Z}[\sqrt{-n}]$. **б)** Найдите все обратимые числа в $\mathbb{Z}[\sqrt{-n}]$. **в)** Верно ли утверждение задачи 3б) для $\mathbb{Z}[\sqrt{-n}]$? **г)** Однозначно ли разложение на множители в $\mathbb{Z}[\sqrt{-n}]$?

Задача 12. **а)** Обозначим через $r(n)$ количество решений уравнения $a^2 + b^2 = n$ в натуральных числах. Докажите, что если m, n взаимно просты, то $r(mn) = r(m)r(n)$. **б)*** Обозначим через $r_d(n)$ количество решений уравнения $a^2 + db^2 = n$ в целых числах. Верно ли предыдущее утверждение при $d > 1$?

Задача 13. Докажите, что число $1000009 = 235^2 + 972^2$ составное.

Задача 14. Найдите все гауссовы простые числа, квадрат модуля которых не превосходит 100.

Задача 15. Докажите, что если простое число p имеет вид $4k + 3$, то оно остаётся простым в области гауссовых чисел.

Определение 2. Пусть p — натуральное простое. Назовём *мнимой единицей по модулю* p такое целое число m, что $m^2 \equiv 1 \pmod p$, но $m \not\equiv \pm 1 \pmod p$. Назовём целое число a *квадратичным вычетом по модулю* p, если оно не делится на p и существует такое целое число b, что $b^2 \equiv a \pmod p$.

Задача 16. Пусть $p \in \mathbb{N}$ — простое. **а)** Докажите, что если $a^2 \equiv b^2 \pmod p$, то $a \equiv \pm b \pmod p$. **б)** Докажите, что для любого нечётного p имеется ровно $\frac{p-1}{2}$ квадратичных вычетов по модулю p (числа, сравнимые по модулю p, считаются задающими один и тот же квадратичный вычет). **в)** Докажите, что если $p = 4k + 3$, то мнимой единицы по модулю p нет, а если $p = 4k + 1$, то их ровно две. (*Указание:* разбейте $2k$ квадратичных вычетов на пары взаимно обратных.) **г)** (Рождественская теорема Ферма) Докажите, что простое число вида $4k + 1$ раскладывается в произведение двух гауссовых простых.

Задача 17*. **а)** Как посчитать $r(n)$ из задачи 12? **б)** Для каких натуральных k существует окружность, на которой лежит ровно k точек с целыми координатами?

1	2 а	2 б	2 в	3 а	3 б	4	5 а	5 б	6	7	8	9 а	9 б	9 в	10	11 а	11 б	11 в	11 г	12 а	12 б	13	14	15	16 а	16 б	16 в	16 г	17 а	17 б