Разложение на множители

Общая теория

Понятия. Кольцо, кольцо без делителей нуля, делитель.

Упражнение 1. В кольце без делителей нуля можно сокращать на общий множитель.

Понятия. Деление с остатком, норма, алгоритм Евклида, НОД. Обратимый элемент.

Упражнение 2. Однозначно ли восстанавливаются частное и остаток для многочленов? А для целых чисел?

Упражнение 3. Каким свойством должна обладать норма, чтобы алгоритм Евклида проходил?

Упражнение 4. Линейное представление НОД. $(a, b) = sa + tb$ для некоторых элементов s, t.

Упражнение 5. Единствен ли НОД? Как связаны два различных НОД?

Понятия. Мультипликативная норма (с натуральными значениями). Простой элемент. Ассоциированные простые.

Упражнение 6. Элемент нормы 1 обратим.

Лемма. Если ab делится на простое p, то либо a делится на p, либо b делится на p.

Указание. Воспользоваться линейным представлением НОД.

Теорема. Представление в виде произведения простых существует и единственно (с точностью до чего?).

Целые гауссовы числа

Это числа вида $a + bi$, где a и b целые. Здесь норма — просто квадрат модуля.

Упражнение 7. Докажите, что $1 + 6i$ — простое гауссово.

Упражнение 8. Разложить на множители $18 + 41i$.

Упражнение 9. Как выглядит в решетке целых гауссовых множество всех чисел, кратных $a + bi$?

Задача 1. Докажите, что в целых гауссовых числах есть деление с остатком.

Упражнение 10. Докажите, что простое целое число раскладывается не более чем на два простых гауссовых.

Упражнение 11. Пусть целое число N делится на простое гауссово (нецелое!) p. Верно ли, что N делится на $p\overline{p}$?

Задача 2. Найдите все такие α, что α/π и $\operatorname{tg}\alpha$ рациональны.

Задача 3. Пусть $n \geq 2$. Докажите, что существует бесконечно пар взаимно простых целых чисел (x, y) таких, что $x^2 + y^2$ является n-й степенью целого числа.

Задача 4. Докажите, что существует число, представимое в виде суммы двух квадратов более, чем миллиоом способов.

Задача 5 (в сторону). а) Пусть $p = 4n + 3$ — простое число. Докажите, что, если $a^2 + b^2$ делится на p, то и a делится на p.

б) Пусть $p = 4n + 1$ — простое. Тогда существуют такие a, b, что $a^2 + b^2 = pm$, $m \leq p/2$.

Задача 6. Докажите, что $p = 4n + 1$ не может быть простым гауссовым.

Задача 7 (письменная). Решите в натуральных числах уравнение $x^2 + 4 = y^3$.

Задача 8. Докажите, что для любого n можно провести окружность, проходящую ровно через n узлов сетки.

Задача 9. а) Пусть $p = 4n + 1 = q\overline{q}$, целое гауссово z не делится на q. Докажите, что $z^{p-1} - 1$ делится на q.

б) Как выглядит аналог этого утверждения для $p = 4n + 3$?

Задача 10. Докажите, что остатки по модулю q (или $p = 4n + 3$) из предыдущей задачи образуют поле.

Задача 11. Натуральные x, y, z попарно взаимно просты, причем $x^2 + y^2 = z^{2n}$, причем число $p = 4n - 1$ простое. Докажите, что xy делится на p.