Алгебра и геометрия, осенний семестр 2019 г.

Семинар 10. Арифметика

факультет математики, НИУ ВШЭ

Задача 1. (а) Нарисуйте все гауссовы целые числа, которые делятся на $1+i$ и не превосходят по модулю 5.

(б) Найдите все обратимые гауссовы целые числа.

(в) Предложите алгоритм деления с остатком в $\mathbb{Z}[i]$.

(г) Найдите наибольший общий делитель гауссовых целых чисел $11+7i$ и $18-i$ в кольце $\mathbb{Z}[i]$.

Определение 1. *Ненулевой и необратимый элемент $x \in R$ в коммутативном кольце R называется простым, если из $x|ab$ всегда следует, что либо $x|a$, либо $x|b$.*

Ненулевой элемент $x \in R$ в области целостности R (=коммутативном кольце без делителей нуля) называется неприводимым, если его нельзя представить в виде произведения двух необратимых элементов.

Задача 2. (а) Покажите, что в области целостности все простые элементы неприводимы.

(б) Покажите, что элемент $2 \in \mathbb{Z}[\sqrt{5}]$ неприводим, но не прост.

Задача 3. Какие из простых чисел 2, 3, 5, 7, 11, 13, 17, 19, 23, 29 останутся простыми в кольце $\mathbb{Z}[i]$?

Задача 4. (а) Вычислите $(1+x+x^2+x^3+\ldots)^2$ в кольце формальных степенных рядов $\mathbb{F}[[x]]$ (через $\mathbb{F}$ обозначается произвольное поле).

(б) Найдите элемент обратный по умножению для $(1+2x+3x^2+4x^3+\ldots)$ в кольце $\mathbb{F}[[x]]$.

(в) Найдите все обратимые элементы в кольце $\mathbb{F}[[x]]$.

Задача 5. (а) Докажите, что кольцо вычетов $\mathbb{F}_2[x]/(x^2+x+1)$ по модулю многочлена x^2+x+1 является полем. Сколько в нём элементов?

(б) Постройте поле из девяти элементов.

Задача 6. Назовём два простых элемента кольца *существенно различными*, если один не получается из другого умножением на обратимый элемент кольца. Докажите или опровергните: `В кольце` $\mathbb{F}[[x]]$ `бесконечно много существенно различных простых элементов.` Почему доказательство Евклида бесконечности множества существенно различных простых чисел в $\mathbb{Z}$ не применимо в этом случае?

Определение 2. *Кольцо $\mathbb{Z}[i]/p\mathbb{Z}[i]$ гауссовых вычетов по модулю p — это множество классов эквивалентности гауссовых целых чисел относительно следующего отношения эквивалентности: $z \sim w$, если $z-w$ делится на p. Сложение и умножение в этом кольце определяются через сложение и умножение в кольце $\mathbb{Z}[i]$.*

Задача 7. (а) Нарисуйте по одному представителю для каждого класса эквивалентности из $\mathbb{Z}[i]/p\mathbb{Z}[i]$ при $p = 2, 3$ и 5.

(б) Сколько элементов в $\mathbb{Z}[i]/p\mathbb{Z}[i]$?

Задача 8. Докажите эквивалентность следующих трёх утверждений:

(1) Кольцо $\mathbb{Z}[i]/p\mathbb{Z}[i]$ является полем.

(2) Уравнение $x^2+y^2=p$ не имеет решений в $\mathbb{Z}$.

(3) Сравнение $x^2 \equiv -1 \mod p$ не имеет решений в $\mathbb{Z}$.

Задача 9. Какие натуральные числа представимы в виде суммы двух полных квадратов?