Семинар 2. Евклидовы кольца

Алгебра в криптографии, осенний семестр 2021 г.

ФАКУЛЬТЕТ МАТЕМАТИКИ, НИУ ВШЭ

Задача 1. Найдите формальный степенной ряд, обратный относительно умножения к многочлену $1 - x - x^2$.

Задача 2. Разложите 30 на простые множители над целыми гауссовыми числами.

Задача 3. (а) Сколько всего попарно неассоциированных простых формальных степенных рядов?

(б) Почему рассуждение Евклида[1] не работает для формальных степенных рядов?

Задача 4. Сколькими способами можно поделить с остатком одно целое гауссово число на другое? Перечислите все возможные варианты.

Задача 5. (а) Докажите, что если два целых числа представляются в виде суммы двух полных квадратов, то их произведение тоже так представляется.

(б) Докажите, что простое натуральное число p представляется в виде суммы двух квадратов тогда и только тогда, когда -1 является квадратичным вычетом по модулю p.

Задача 6. Какие из колец евклидовы?

(а) $\mathbb{Q}[x]$; (б) $\mathbb{Z}[x]$; (в) $\mathbb{Q}[[x]]$; (г) $\mathbb{Z}[i]$; (д) $\mathbb{Z}[\sqrt{-2}]$; (е) $\mathbb{Z}[\sqrt{-3}]$; (ё) $\mathbb{Z}[e^{\frac{2\pi i}{3}}]$.

[1] Какое бы конечное множество простых чисел мы не взяли, всегда найдётся большее множество простых чисел. Пусть A, B, C — данные простые числа. Я покажу, что есть и другие простые числа, кроме A, B, C. Возьмём $D = ABC + 1$. Тогда D либо простое, либо нет. Если D — простое, то мы нашли простое число, которое превосходит A, B, C. Если D — не простое, то оно делится на простое число E. Я покажу, что E не совпадает ни с одним из чисел A, B, C. Потому что если совпадает, то E делит ABC. Но E делит и D. Тогда E делит и 1, что абсурдно. Поэтому E не совпадает ни с одним из чисел A, B, C, и по предположению является простым. (Евклид, "Начала", книга IX, Предложение 20)