Семинар 1. Квадратичные вычеты и суммы квадратов

Введение в теорию чисел, весенний семестр 2024 г.

ФАКУЛЬТЕТ МАТЕМАТИКИ, НИУ ВШЭ

Через p в этом листке обозначается нечётное простое число.

Задача 1. (а) Покажите, что количество квадратичных вычетов по модулю p равно количеству невычетов.

(б) Выпишем все ненулевые вычеты по модулю p подряд таким образом: $[1]_p$, $[2]_p$, $\ldots$, $[p-1]_p$. Заменим каждый квадратичный вычет на букву R, а невычет — на букву N. Полученное слово обозначим через W_p. Выпишете W_p для $p = 17$.

Задача 2. Найдите количество подслов вида RR, RN, NR и NN в слове W_p

(а) для $p = 17$; (б) для произвольного p.

Рассматриваются только подслова, состоящие из подряд идущих букв.

Задача 3. При каких условиях на p вычет $[-1]_p$ будет квадратичным?

Задача 4. Разложите 30 на простые множители над целыми гауссовыми числами.

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

(б) Докажите, что если простое число p представляется в виде суммы двух квадратов, то такое представление единственно. *Подсказка: используйте единственность разложения на простые в кольце целых гауссовых чисел* $\mathbb{Z}[i]$.

Задача 6. Докажите, что p представляется в виде суммы двух квадратов тогда и только тогда, когда -1 является квадратичным вычетом по модулю p. *Подсказка: воспользуйтсь следующим изомофизмом факторколец*

$$\mathbb{Z}[i]/(p) \simeq (\mathbb{Z}/p\mathbb{Z})[x]/(x^2+1).$$