Листок 13

Кольца и поля вычетов. Линейная алгебра над конечным полем.

В этом листке кольцо вычетов по модулю n обозначается $\mathbb{Z}_n$, p всегда обозначает простое число, а $\mathbb{F}_p = \mathbb{Z}_p$ — поле из p элементов.

1. Диофантовы уравнения.

Задача 1. Докажите, что следующие уравнения не имеют решений в целых числах:
(а) $x^2 - 3y^2 = 17$;
(б) $x^3 + 14y^3 = 12$;
(в) $x^5y + 5x^3 - xy^5 = 1$ (здесь может пригодиться малая теорема Ферма).

2. Группа корней из единицы, первообразные корни. Как обсуждалось на семинаре, все корни степени n из 1 образуют группу по умножению, которая обозначается $\mathbf{U_n}$. Это циклическая группа (то есть все её элементы являются степенями некотрого элемента a).

Задача 2. Докажите, что всякая циклическая группа изоморфна либо $\mathbb{Z}$, либо $\mathbf{U_n}$.

Задача 3. Пусть $\varepsilon_1, \ldots, \varepsilon_n$ — все корни степени n из 1. Докажите, что

$$\varepsilon_1^k + \ldots + \varepsilon_n^k = \begin{cases} n, \text{ если } k \text{ делится на } n, \\ 0, \text{ иначе.} \end{cases}$$

Задача 4. Представьте $\cos 72^\circ$ в виде $a + b\sqrt{5}$, где $a, b \in \mathbb{Q}$. *Подсказка:* рассмотрите $n = 5$, $k = 1$ в предыдущей задаче.

Напомним, что через $\mathbb{Z}_n^*$ обозначается группа обратимых (по умножению) элементов кольца вычетов $\mathbb{Z}_n$. Каждый порождающий элемент этой группы называется *первообразным корнем по модулю* n. В курсе теории чисел доказывается, что первообразные корни существуют для любого простого $n = p$.

Задача 5. Найти все первообразные корни по модулю 7 и 17 (другими словами, найдите порождающие элементы в группах $\mathbb{F}_7^*$ и $\mathbb{F}_{17}^*$).

3. Линейная алгебра над конечным полем. Метод Гаусса, теория определителей, правило Крамера без существенных изменений переносятся на случай поля положительной характеристики.

Задача 6. Для каждого простого числа p найдите над полем $\mathbb{F}_p$ все решения однородной системы $Ax = 0$ с матрицей

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ -10 & 13 & 14 & 15 \\ 12 & -9 & 14 & 15 \\ 12 & 13 & -8 & 15. \end{pmatrix}$$

Подсказка: для выяснения совместности этой системы, начните с вычисления определителя (это даст вам понимание того, какие p следует рассматривать отдельно).

Задача 7. Сколько элементов содержит n-мерное векторное пространство над полем $\mathbb{F}_p$?

Задача 8. Рассмотрим целочисленную матрицу $A \in \mathrm{Mat}_n(\mathbb{Z})$ и обозначим через $A \pmod p$ матрицу из $\mathrm{Mat}_n(\mathbb{F}_p)$, полученную заменной каждого матричного элемента a_{ij} на $a_{ij} \pmod p$. Докажите, что при такой редукции по модулю p ранг не может увеличиться:

$$\mathrm{rk}(A \pmod p) \leqslant \mathrm{rk}(A).$$

Напомним, что *общей линейной группой* над полем $\mathbb{K}$ называется группа всех невырожденных квадратных матриц

$$\mathrm{GL}_n(\mathbb{K}) = \{A \in \mathrm{Mat}_n(\mathbb{K}) :\ \det A \neq 0\},$$

а *специальной линейной группой* называется группа матриц с определителем равным 1:

$$\mathrm{SL}_n(\mathbb{K}) = \{A \in \mathrm{Mat}_n(\mathbb{K}) :\ \det A = 1\}.$$

Задача 9. Найдите число элементов в группах $\mathrm{GL}_n(\mathbb{F}_p)$ и $\mathrm{SL}_n(\mathbb{F}_p)$, где p — простое число.