Геометрия и алгебра, весенний семестр 2020 г.

Семинар 13. Приложения групп

факультет математики, НИУ ВШЭ

Задача 1. Пусть $p > 2$ — простое число. Рассмотрим множество X всех раскрасок вершин правильного p-угольника в a цветов. На множестве X действует группа G вращений правильного p-угольника.

(а) Сколько раскрасок не меняются при поворотах многоугольника? (Выражаясь научно, сколько неподвижных точек у действия группы G на X?)

(б) Есть ли орбиты, порядок которых отличен от 1 и p?

(в) Сколько орбит порядка p при действии группы G на X?

(г) Используя результаты пунктов (а)–(в) докажите малую теорему Ферма.

> Малая теорема Ферма: Если p простое, то $a^p - a$ делится на p для всех натуральных a.

Задача 2. (а) Докажите "формулу сокращённого умножения ленивого школьника":

$$(x + y)^p \equiv x^p + y^p \pmod{p},$$

если p — простое число.

(б) Останется ли формула из пункта (а) верной, если p — составное?

(в) Докажите малую теорему Ферма с помошью формулы из пункта (а).

Задача 3. Пусть n — произвольное натуральное число, а $(\mathbb{Z}/n\mathbb{Z})^*$ — множество всех вычетов по модулю n, которые взаимно просты с n.

(а) Проверьте, что $(\mathbb{Z}/n\mathbb{Z})^*$ является группой относительно умножения (она называется мультипликативной группой вычетов).

(б) Найдите порядок группы $(\mathbb{Z}/n\mathbb{Z})^*$ для всех $n \leq 10$ (порядок обозначается $\varphi(n)$ и называется функцией Эйлера).

(в) Используя теорему Лагранжа для группы $(\mathbb{Z}/n\mathbb{Z})^*$, докажите теорему Эйлера.

> Теорема Эйлера: Если натуральное число a взаимно просто с n, то $a^{\varphi(n)} - 1$ делится на n.

(г) Проверьте, что если n — простое, то теорема Эйлера превращается в малую теорему Ферма.

Задача 4. Пусть p — простое число, а S_p — группа перестановок множества $\{1, 2, \ldots, p\}$.

(а) Опишите все элементы порядка p в S_p.

> Указание: Для перестановки σ порядка p найдите первой последовательности $1 \overset{\sigma}{\to} \sigma(1) \overset{\sigma}{\to} \cdots$

(б) Найдите количество подгрупп порядка p в S_p.

(в) Пусть $\sigma = (1\ 2\ \ldots\ p)$ — цикл длины p, а g — произвольная перестановка. Проверьте, что $g\sigma g^{-1}$ — это тоже цикл длины p, а именно

$$g(1\ 2 \ldots\ p)g^{-1} = (g(1)\ g(2) \ldots g(p)\ ).$$

(г) Пусть X — множество всех подгрупп порядка p в S_p, а G — какая-нибудь подгруппа порядка p. Определим действие группы G на множестве X сопряжениями:

$$g(H) := gHg^{-1}, \text{ где } g \in G,\ H \in X.$$

Найдите все неподвижные точки этого действия.

(д) Используя пункты (б),(в), докажите теорему Вильсона.

> Теорема Вильсона: Если p простое, то $(p-1)! + 1$ делится на p.