Филиппова Анастасия

## Домашнее задание 5

(1) (a) **Сколькими способами можно раскрасить вершин тетраэдра в три цвета, с точностью до вращений?**

Пронумеруем вершины тетраэдра: $A-1, B-2, C-3, D-4$.Группа вращений тетраэдра состоит из поворотов относительно оси, проходящей через вершину и центр противоположной грани - 8(4 поворота в 2 стороны), поворотов относительно оси, соединяющей середины противоположных ребер - 3 и тождественного преобразования - 1. Всего 12.

Тождественные :$3^4$, повороты относительно, оси, проходящей через вершину: $8 \cdot 3^2$, повороты относительно оси, соединыющей середины: $3 \cdot 3^2$. Найдем количество орбит по лемме Бернсайда: $(3^4 + 3^2 \cdot 8 + 3 \cdot 3^2)/12 = 15$.

Ответ: 15.

(b) **Сколькими способами можно раскрасить ребра куба в три цвета, с точностью до вращений?**

Аналогично первому пункту промумеруем все ребра куба от 1 до 12. Группа вращений куба состоит из поворотов относительно оси, проходящей через центр грани - 3 оси и 3 поворота для каждой $(\pi/2, \pi, 3\pi/2)$, то есть 9 поворотов; 4 симметрии относительно главных диагоналей (по 2 поворота относительно каждой); повороты относительно осей, соединяющих середины противоположных ребер - 6 и тождественное преобразование. Всего в группе 24 элемента.

Посчитаем количество орбит: тождественных перестановок $3^{12}$, поворотов относительно оси, проходящей через центр грани : на $\pi/2$ и $-\pi/2$ по $3 \cdot 3^3$, то есть $3^3 \cdot 6$, на $3\pi/2$ : $3^4 \cdot 3$. Поворотов, относительно главной диагонали - $8 \cdot 3^4$ (показано на рисунке 1, куда переходят вершины при повороте). Повороты относительно оси, соединяющей противоположные ребра: 2 ребра переходят сами в себя (те, через которые проходит ось), остальные составляют пары, получаем $2 \cdot 3 \cdot 3 \cdot 3^5 = 6 \cdot 3^7$.

По лемме Бернсайда найдем число орбит: $\frac{3^7+3^4 \cdot 2+3^4 \cdot 8+3^{12}+6 \cdot 3^7}{24} = \frac{547560}{24} = 22815$

Ответ :22815.

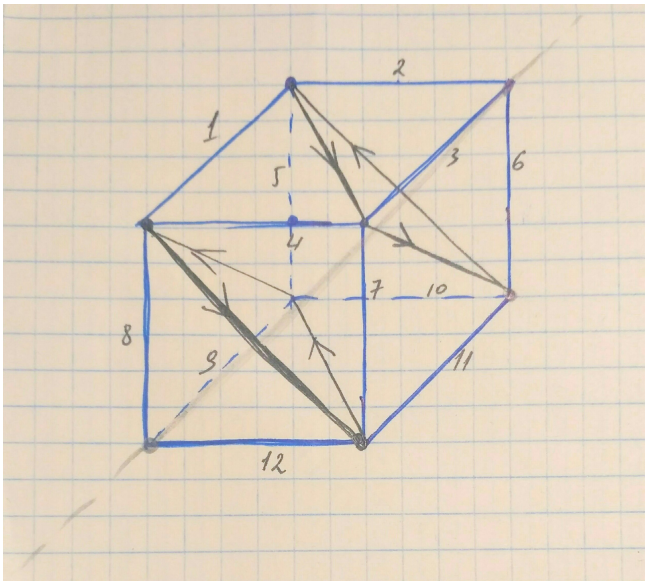


Рис. 1

(2) **Пусть циклы перестановки $\sigma$ в цикловом разложении имеют длины $l_1, l_2 \ldots l_k$**

(a) **Найдите количество сопряженных с ней перестановок.**

Перестановки сопряжены тогда и только тогда, когда они имеют одинаковое цикловое разложение$\Rightarrow$ перестановка $\pi$, сопряженная с исходной должна содержать циклы такой же длины. В первый цикл длины $l_1$ можем "набрать"элементы $\frac{(n)\ldots(n-l_1+1)}{l_1}$ способами, во второй длины $l_2$: $\frac{(n-l_1)\ldots(n-l_1-l_2+1)}{l_2}$.

И так далее. В итоге получаем, что сопряженных перестановок $\frac{n!}{l_1 \ldots l_k}$

(b) **Найдите количествоэлементов в нормализаторе этой перестановки.**
В предыдущем домашнем задании доказано, что индекс группы по нормализатору элемента равен количеству элементов в классе эквивалентности, содержащим этот элемент. То есть $|G : N(a)| = |A|$ (A - класс эквивалентности, содержащий a). Получаем: $|A| = \frac{n!}{\frac{n!}{l_1 \dots l_k}} = l_1 \dots l_k$

(c) **Докажите, что в $S_{11}$ все перестановки порядка 11 сопряжены.**
Число 11 - простое, следовательно, все перестановки из этой группы имеют в цикловом разложении только один цикл длины 11, следовательно, все перестановки из этой группы сопряжены.

(3) (a) **Для каких простых чисел p остаток $-1$ является квадратичным вычетом по модулю p?**
$a^{\frac{(p-1)}{2}} \equiv 1 \ mod \ p \Rightarrow -1$ - квадратичный вычет, если $p = 4k + 1$, где $k$ - натуральное число.

(b) **Является ли 25000000 квадратичным вычетом по модулю $67^{66^{65^{\cdots}}}$?**
Воспользуемся символом Лежандра: $(25000000, 67^{66^{65^{\cdots}}}) = 1$, $\frac{25000000}{67^{66^{65^{\cdots}}}} = (\frac{5000}{67^{66^{65^{\cdots}}}})^2 = 1 \Rightarrow$ да.
Ответ: да.

(c) **Является ли 998 квадратичным вычетом по модулю 199?**
$(\frac{998}{199}) = (\frac{2}{199})(\frac{499}{199}) = (\frac{101}{199})(-1)^{(199^2-1)/8} = (\frac{199}{101})(-1)^{(99)(50)} = (\frac{98}{199}) = (\frac{2}{199})(\frac{7}{199})^2 = (-1)^{(199^2-1)/2} = 1 \Rightarrow$да.
Ответ: да.

(4) **Даны натуральные числа $a$ и $n$ такие, что $(a, n) = 1$ и $a^{n-1} \neq 1 \ mod \ n$. Докажите, что тогда по краней мере для половины чисел $b$ из промежутка $1 \leqslant b < n$ выполнено $b^{n-1} \neq 1 \ mod \ n$.**
Сначала рассмотрим такие $b$ из данного промежутка, что $(b, n) > 1 \Rightarrow b^{n-1} = qn + 1$. Но тогда $b^{n-1} \neq 1 \ mod \ n \Rightarrow$ для всех $b$ из промежутка не взаимопростых с $n$ выполнено нужное утверждение. Всего таких $b$: $n - 1 - \varphi(n)$.
Теперь рассмотрим $b$, такие что $(b, n) = 1$. Множество таких элементов с операцией умножения составляют мультипликативную группу вычетов по модулю $n$. Построим следующий гомоморфизм:$\varphi : x \to x^{n-1}$. $Ker(\varphi) = (x | x^{n-1} = 1)$. Индекс группы $Z_n^*$ по ядру гомоморфизм как минимум 2, так как точно найдется элемент, не содержащийся в ядре. Следовательно, мощность группы без ядра гомоморфизма $\geqslant \frac{\varphi(n)}{2}$. Следовательно, $k_b \geqslant n - 1 - \varphi(n) + \frac{\varphi(n)}{2} = n - 1 - \frac{\varphi(n)}{2}$, где $k_b$ количество элементов $b$, удовлетворяющих условию. Так как $(n-1) \geqslant \varphi(n) \Rightarrow n - 1 - \frac{\varphi(n)}{2} > (n-1)/2$. Следовательно, по краней мере для половины чисел $b$ из промежутка $1 \leqslant b < n$ выполнено $b^{n-1} \neq 1 \ mod \ n$. Доказано.

(5) (a) **Доказать, что если $x$ - нечетно, то при $n > 2$ выполнено $x^{2^{n-2}} \equiv 1 \ mod \ 2^n$.** $\varphi(2^n) = 2^{n-1}$
$(x, 2^n) = 1$. По теореме Эйлера: $x^{2^{n-1}} = (x^{2^{n-2}})^2 \equiv 1 \ mod \ 2^n \Rightarrow (x^{2^{n-2}}) \equiv 1 \ mod \ 2^n$ или $(x^{2^{n-2}}) \equiv (-1) \ mod \ 2^n$. Если $n > 2$, то $4 | 2^n$. Посмотрим, какие остатки может давать полный квадрат при делении на 4: 0 и 1. $(x^{2^{n-2}})$ при $n > 2$ является квадратом, следовательно, $(x^{2^{n-2}}) \equiv 2^n \ mod \ 2^n$. Что и требовалось доказать.

(b) **Доказать , что мультипликативная группа по модулю $2^n$ не циклическая.**
По теорема Гаусса первообразные корни существуют только по следующим модулям: $2, 4, p^n, 2 \cdot p^n, p$ - простое нечетное. Следовательно, в мультипликативной группе по модулю $2^n$ нет первообразного, следовательно, она не является циклической, так как нет порождающего элемента.

(6) (a) **Доказательство:**
1) $\Rightarrow$ Пусть $g$ - первообразный, следовательно, $Z_n^* =< g > \Rightarrow ord(g) = \varphi(n) \Rightarrow g^{\varphi(n)/p_i} \neq 1 \ mod \ n$, что и требовалось доказать.
2) $\Leftarrow g \in Z_n^*, n = p_1^{l_1} \dots p_k^{l_k}, g^{\frac{\varphi(n)}{p_i}} \neq 1$. Докажем, что $g$ - первообразный.
Группа является конечной, следовательно, каждый элемент имеет конечный порядок. Пусть $ord(g) = f$. $f \neq$. Так как порядок элемента делит порядок группы, следовательно, $f | \varphi(n)$. Но по условию $g$ ни в какой степени вида $\varphi(n)/p_i$ не дает единичный элемент, следовательно, $f = \varphi(n)$.

(b) **Найти первообразный по модулю 31.**
$\varphi(31) = 30 = 3 \cdot 2 \cdot 5.3^6 = 729 \neq 1 \ mod \ 31$
$3^{15} = 14348907 \neq 1 \ mod \ 31$
$3^{10} = 59049 \neq 1 \ mod \ 31 \Rightarrow Z_{31}^* =< 3 >$.

(c) **Найти количество первообразных группы $Z_{31}^*$.**
1)Докажем, что в группе $Z_p^*$ ровно $\varphi(\varphi(p))$ первообразных корней и все первообразные - степени наименьшего первообразного корня. Для это докажем, что $g^l$- первообразный тогда и только тогда, когда $(l, p-1) = 1$.
$< g >= Z_p^*$. Пусть $g^l$ - первообразный и $(l, \varphi(p)) = k \neq 1$.
$g^{l \cdot \varphi(p)} = e \Rightarrow \ q < \varphi(p) \hookrightarrow g^q = e$ - противоречие, так как $ord(g) = \varphi(p)$. Всего возможных $l$ - $\varphi(\varphi(p))$.

2) Пусть $(l, \varphi(p)) = 1$ и $g$ - первообразный. Докажем, что $g^l$ - первообразный.
Группа $Z_p^*$ - циклическая, следовательно в ней $\varphi(\varphi(p))$ первообразных корней. Но в пункте 1) мы доказати, что элементов вида $g^l$, где $g$ первообразный, $(l, p-1)$ ровно $\varphi(\varphi(p))$ и все они являются первообразными. Следовательно, только элементы такого вида являются первообразными в группе.
В группе $Z_{31}^*$ первообразные: $3^1, 3^7, 3^{11}, 3^{13}, 3^{17}, 3^{19}, 3^{23}, 3^{29}$.

(7) (a) **Сопряжены ли перестановки?**
Очевидно, нет, так как имеют разное цикловое разложение.

(b) **Сопряжены ли перестановки?**
Да, так как имеют одинаковое цикловое разложение.
$a = (147)(5)(236)$
$b = (145)(627)(3)$
Перестановки сопряжены посредством элемента $g$: $\begin{pmatrix} 1 & 3 & 5 & 4 & 7 & 2 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix} = (1)(32675)(4)$
Найдем количество таких элементов: (5) однозначно ставим в соответсвие (3) (так как единственные простые циклы длины 1), для 1 выбираем из 6 элементов, затем из 3. В итоге получаем: $3 \cdot 6 = 18$.
Ответ: 18.