Конспект по миникурсу С.А. Игонина "Применение групп преобразований в комбинаторике и теории чисел"

Этот конспект основан на миникурсе из двух лекций для студентов и школьников, прочитанных в ЯрГУ в октябре 2019 года.

Видео лекций доступно на сайте `https://cis.uniyar.ac.ru/event/214`

Задачи тестирования по миникурсу приведены на странице 12.

Вопросы можно задавать Сергею Александровичу Игонину <s-igonin@yandex.ru>.

1. Группы преобразований, лемма Бернсайда и их применения в комбинаторике

Используемые обозначения:

- Для конечного множества Z количество элементов в нем обозначается $|Z|$.
- $\varnothing$ – пустое множество.
- Для множества X и множества Y символом $X \times Y$ обозначается их прямое произведение, состоящее из упорядоченных пар (x, y) для всех $x \in X$, $y \in Y$. То есть,

$$X \times Y = \{(x, y) \mid x \in X,\ \ y \in Y\}.$$

Определение 1. Пусть $F\colon X \to Y$ – отображение из множества X в множество Y.

- Отображение F называется *сюръективным*, если для любого $y \in Y$ существует элемент $x \in X$ такой, что $F(x) = y$.
- F называется *инъективным*, если для любых различных элементов $x_1, x_2 \in X$ имеем $F(x_1) \neq F(x_2)$.

Отображение F является *биективным*, если оно сюръективно и инъективно. Биективное отображение $F\colon X \to Y$ устанавливает взаимно однозначное соответствие между элементами множеств X и Y.

Определение 2. Множество G с операцией

$$*\colon G \times G \to G, \qquad (a, b) \mapsto a * b, \qquad a, b \in G,$$

называется *группой*, если

- операция $*$ *ассоциативна*: для любых $a, b, c \in G$ выполнено равенство $a * (b * c) = (a * b) * c$,
- существует *нейтральный элемент* e, т.е. такой, что для любого $a \in G$ выполнены равенства $a * e = e * a = a$,
- все *элементы обратимы*: для каждого $a \in G$ существует элемент $a^{-1} \in G$ такой, что $a^{-1} * a = a * a^{-1} = e$.

Тогда говорят, что $*$ является *групповой операцией*.

Нейтральный элемент e также называется *единичным элементом* группы G. Для данного $a \in G$ элемент $a^{-1} \in G$ называется *обратным к* a.

Определение 3. *Подгруппой* группы G с операцией $*$ называется подмножество $H \subset G$, являющееся группой относительно операции $*$, т.е. обладающее свойствами:

- подмножество H содержит единичный элемент e;
- для любых $a, b \in H$ выполнено $a * b \in H$;
- для любого элемента $a \in H$ его обратный a^{-1} также принадлежит подмножеству H.

Определение 4. Пусть X – множество. Для отображений $f\colon X \to X$ и $g\colon X \to X$ определена их композиция

$$f \circ g\colon X \to X, \qquad (f \circ g)(a) = f(g(a)), \qquad a \in X.$$

Преобразование множества X – это взаимно однозначное (биективное) отображение $f\colon X \to X$. Это значит, что существует *обратное* отображение f^{-1} такое, что

$$f\big(f^{-1}(a)\big) = f^{-1}\big(f(a)\big) = a \qquad \forall\, a \in X.$$

Рассмотрим *тождественное отображение* $\mathrm{Id}\colon X \to X$, задаваемое формулой $\mathrm{Id}(a) = a$ для всех $a \in X$. Тогда для любого преобразования $f\colon X \to X$ имеем $f \circ f^{-1} = \mathrm{Id}$ и $f^{-1} \circ f = \mathrm{Id}$.

Преобразования множества X образуют группу относительно операции композиции отображений. Единичным элементом в этой группе служит тождественное преобразование Id.

Пусть G – группа с операцией $*$. В дальнейшем для любых $g_1, g_2 \in G$ элемент $g_1 * g_2 \in G$ будем писать просто как $g_1 g_2$.

Лемма 1. *Пусть G – группа с единичным элементом $e \in G$. Пусть $a, g \in G$.*

- *Если $ga = a$ или $ag = a$, то $g = e$.*
- *Если $ga = e$ или $ag = e$, то $g = a^{-1}$.*
- *Для любых $g_1, g_2 \in G$ имеем $(g_1 g_2)^{-1} = g_2^{-1} g_1^{-1}$.*

Доказательство. Пусть $ga = a$. Тогда имеем $g = ge = g(aa^{-1}) = (ga)a^{-1} = aa^{-1} = e$.
Остальные утверждения леммы доказываются аналогично. □

Определение 5. Пусть G – группа с единичным элементом $e \in G$, а X – множество.
Будем говорить, что *группа G действует на множестве X*, если для каждого элемента $g \in G$ задано преобразование $T_g \colon X \to X$ множества X так, что

$$T_{g_1 g_2} = T_{g_1} \circ T_{g_2} \qquad \forall\, g_1, g_2 \in G. \tag{1}$$

Согласно лемме 2 ниже из свойства (1) следует, что $T_e = \mathrm{Id}$, то есть,

$$T_e(x) = x \qquad \forall\, x \in X. \tag{2}$$

Применяя (1) для $g_1 = g \in G,\ g_2 = g^{-1}$ и используя равенство $T_e = \mathrm{Id}$, получаем

$$T_g \circ T_{g^{-1}} = T_{gg^{-1}} = T_e = \mathrm{Id}. \tag{3}$$

По лемме 1 из (3) следует равенство $T_{g^{-1}} = (T_g)^{-1}$ для любого $g \in G$.
Орбитой элемента $x \in X$ под действием группы G называется множество

$$Gx = \{\, T_g(x) \mid g \in G \,\}.$$

Согласно лемме 3 на странице 3 множество X разбивается в объединение непересекающихся орбит.
Стабилизатором элемента $x \in X$ при действии группы G называется множество

$$\mathrm{St}_G(x) = \{\, g \in G \mid T_g(x) = x \,\}.$$

Легко проверить, что $\mathrm{St}_G(x)$ является подгруппой в G.
Для $g \in G$ и $x \in X$ элемент $T_g(x)$ иногда пишут просто как gx.

Лемма 2. *Пусть группа G с единичным элементом e действует на множестве X. Тогда из свойства (1) имеем $T_e = \mathrm{Id}$.*

Доказательство. Применяя (1) в случае $g_1 = g_2 = e$, получаем

$$T_e = T_e \circ T_e. \tag{4}$$

Поскольку T_e является преобразованием множества X, определено обратное преобразование $T_e^{-1} \colon X \to X$, удовлетворяющее

$$T_e^{-1} \circ T_e = \mathrm{Id}. \tag{5}$$

Из (4), (5) получаем

$$\mathrm{Id} = T_e^{-1} \circ T_e = T_e^{-1} \circ (T_e \circ T_e) = (T_e^{-1} \circ T_e) \circ T_e = \mathrm{Id} \circ T_e = T_e.$$

□

Пример 1. Модуль (абсолютную величину) комплексного числа $z \in \mathbb{C}$ будем обозначать $|z|$. Рассмотрим группу

$$G = \{\, z \in \mathbb{C} \mid |z| = 1 \,\}$$

с операцией умножения комплексных чисел. Определим действие группы G на множестве $X = \mathbb{C}$ следующим образом

$$T_g \colon \mathbb{C} \to \mathbb{C}, \qquad T_g(x) = gx \in \mathbb{C}, \qquad g \in G \subset \mathbb{C}, \quad x \in \mathbb{C},$$

где gx – произведение комплексных чисел $g, x \in \mathbb{C}$.
Для любого ненулевого числа $x \in \mathbb{C}$ орбита Gx и стабилизатор $\mathrm{St}_G(x)$ таковы

$$Gx = \{\, z \in \mathbb{C} \mid |z| = |x| \,\}, \qquad \mathrm{St}_G(x) = \{1\} \subset G.$$

Для нуля $0 \in \mathbb{C}$ имеем орбиту $G0 = \{0\}$ и стабилизатор $\mathrm{St}_G(0) = G$.

Пример 2. Рассмотрим группу G и подгруппу $\tilde{G} \subset G$. Определим действие группы $\tilde{G}$ на множестве $X = G$ следующим образом

$$T_g \colon G \to G, \qquad T_g(a) = ag^{-1} \in G, \qquad g \in \tilde{G}, \quad a \in G,$$

где ag^{-1} – произведение элементов a и g^{-1} в группе G. Свойство $T_{g_1 g_2} = T_{g_1} \circ T_{g_2}$ для элементов $g_1, g_2 \in \tilde{G}$ следует из формулы $(g_1 g_2)^{-1} = g_2^{-1} g_1^{-1}$.

Орбита элемента $a \in G$ под действием группы $\tilde{G}$ совпадает с множеством

$$a\tilde{G} = \{\, ag \mid g \in \tilde{G} \,\}. \tag{6}$$

Множество (6) называется *левым смежным классом* группы G по подгруппе $\tilde{G}$.

Если $ag_1 = ag_2$ для каких-то элементов $g_1, g_2 \in \tilde{G}$, то, умножая равенство $ag_1 = ag_2$ на элемент a^{-1} слева, получаем $g_1 = g_2$. Следовательно, если группа $\tilde{G}$ конечна, $|a\tilde{G}| = |\tilde{G}|$.

Множество всех левых смежных классов группы G по подгруппе $\tilde{G}$ обозначается $G/\tilde{G}$. То есть,

$$G/\tilde{G} = \{\, a\tilde{G} \mid a \in G \,\}.$$

Другими словами, $G/\tilde{G}$ – это множество орбит описанного действия группы $\tilde{G}$ на множестве G.

Предположим, что G конечно. Тогда $\tilde{G}$ и $G/\tilde{G}$ тоже конечны, и $|G/\tilde{G}|$ равно количеству орбит. Согласно лемме 3 ниже множество G разбивается в объединение непересекающихся орбит относительно действия группы $\tilde{G}$. Поскольку имеется $|G/\tilde{G}|$ таких орбит и количество элементов в каждой орбите равно $|\tilde{G}|$, получаем

$$|G/\tilde{G}| \cdot |\tilde{G}| = |G|. \tag{7}$$

Пусть $a_1, a_2 \in G$. Рассмотрим левые смежные классы $a_1\tilde{G}$ и $a_2\tilde{G}$. Имеем $a_1\tilde{G} = a_2\tilde{G}$ тогда и только тогда, когда $a_2^{-1} a_1 \in \tilde{G}$.

Вернемся к рассмотрению общей ситуации из определения 5, когда группа G действует на множестве X преобразованиями $T_g \colon X \to X$, $g \in G$. В дальнейшем для $g \in G$ и $x \in X$ элемент $T_g(x)$ будем писать как gx.

Тогда свойства (1), (2) можно записать так

$$(g_1 g_2)x = g_1(g_2 x) \qquad \forall\, g_1, g_2 \in G, \quad \forall\, x \in X, \tag{8}$$

$$ex = x \qquad \forall\, x \in X. \tag{9}$$

Для каждого $x \in X$ имеем орбиту $Gx \subset X$ и стабилизатор $\mathrm{St}_G(x) \subset G$

$$Gx = \{\, gx \mid g \in G \,\}, \qquad \mathrm{St}_G(x) = \{\, g \in G \mid gx = x \,\}.$$

Для элемента $g \in G$ обозначим

$$X^g = \{\, x \in X \mid gx = x \,\}.$$

Таким образом, $X^g \subset X$, и для любого $y \in X^g$ имеем $gy = y$.

Замечание 1. Предположим, что группа G конечна. Количество пар $(g, x) \in G \times X$, для которых $gx = x$, можно вычислить двумя способами, которые указаны в разных частях следующего равенства

$$\sum_{x \in X} |\,\mathrm{St}_G(x)| = \sum_{g \in G} |X^g|. \tag{10}$$

Это равенство понадобится нам в доказательстве леммы Бернсайда на странице 4.

Лемма 3. *Пусть группа G действует на множестве X. Рассмотрим элементы $x_1, x_2 \in X$ и их орбиты*

$$Gx_1 = \{\, gx_1 \mid g \in G \,\}, \qquad Gx_2 = \{\, gx_2 \mid g \in G \,\}.$$

- *Если $x_1 \in Gx_2$, то $Gx_1 = Gx_2$.*
- *Если $x_1 \notin Gx_2$, то $Gx_1 \cap Gx_2 = \varnothing$, т.е. множества Gx_1 и Gx_2 не пересекаются.*

Таким образом, множество X разбивается в объединение непересекающихся орбит.

Доказательство. Рассмотрим случай $x_1 \in Gx_2$. Поскольку $Gx_2 = \{\, gx_2 \mid g \in G \,\}$, существует элемент $\hat{g} \in G$ такой, что $x_1 = \hat{g}x_2$. Тогда по свойствам (8), (9) для любого $g \in G$ имеем

$$gx_1 = g(\hat{g}x_2) = (g\hat{g})x_2 \in Gx_2,$$
$$gx_2 = g(ex_2) = g(\hat{g}^{-1}\hat{g})x_2 = (g\hat{g}^{-1})(\hat{g}x_2) = (g\hat{g}^{-1})x_1 \in Gx_1.$$

Следовательно, $Gx_1 = Gx_2$.

Теперь рассмотрим случай $x_1 \notin Gx_2$. Предположим, что $Gx_1 \cap Gx_2 \neq \varnothing$, и рассмотрим произвольный элемент $y \in Gx_1 \cap Gx_2$. Тогда существуют элементы $g_1, g_2 \in G$ такие, что $y = g_1x_1 = g_2x_2$. По свойствам (8), (9) имеем

$$x_1 = ex_1 = \big((g_1)^{-1}g_1\big)x_1 = (g_1)^{-1}(g_1x_1) = (g_1)^{-1}(g_2x_2) = \big((g_1)^{-1}g_2\big)x_2 \in Gx_2,$$

что противоречит предположению $x_1 \notin Gx_2$. Следовательно, $Gx_1 \cap Gx_2 = \varnothing$. □

Лемма 4. *Пусть конечная группа G действует на множестве X. Для любого элемента $x \in X$ имеем*

$$|Gx| \cdot |\operatorname{St}_G(x)| = |G|. \tag{11}$$

Доказательство. Пусть $x \in X$. Применяя формулу (7) для подгруппы $\tilde{G} = \operatorname{St}_G(x) \subset G$, получаем

$$|G/\operatorname{St}_G(x)| \cdot |\operatorname{St}_G(x)| = |G|, \tag{12}$$

где

$$G/\operatorname{St}_G(x) = \{\, a \operatorname{St}_G(x) \mid a \in G \,\}$$

– множество левых смежных классов группы G по подгруппе $\operatorname{St}_G(x)$.

Пусть $a, \hat{a} \in G$ таковы, что $a \operatorname{St}_G(x) = \hat{a} \operatorname{St}_G(x)$. Тогда $a^{-1}\hat{a} \in \operatorname{St}_G(x)$, т.е. $(a^{-1}\hat{a})x = x$, и, следовательно, $\hat{a}x = ax$.

Это наблюдение позволяет нам определить отображение $f\colon G/\operatorname{St}_G(x) \to Gx$ с помощью формулы $f\big(a \operatorname{St}_G(x)\big) = ax$.

Докажем, что отображение f биективно. Сюръективность сразу следует из определения орбиты Gx элемента $x \in X$. Пусть $a_1, a_2 \in G$ таковы, что $f\big(a_1 \operatorname{St}_G(x)\big) = f\big(a_2 \operatorname{St}_G(x)\big)$, т.е. $a_1x = a_2x$. Тогда $(a_2^{-1}a_1)x = x$, откуда $a_2^{-1}a_1 \in \operatorname{St}_G(x)$, а из этого получаем $a_1 \operatorname{St}_G(x) = a_2 \operatorname{St}_G(x)$. Следовательно, отображение f инъективно.

Таким образом, f биективно отображает множество $G/\operatorname{St}_G(x)$ на множество Gx, а это возможно только если $|G/\operatorname{St}_G(x)| = |Gx|$. Подставляя $|G/\operatorname{St}_G(x)| = |Gx|$ в (12), получаем (11). □

Лемма Бернсайда. *Количество орбит действия конечной группы G на множестве X равно*

$$\frac{1}{|G|} \sum_{g \in G} |X^g|. \tag{13}$$

Доказательство. Обозначим число орбит через N. Каждый элемент $x \in X$ лежит в орбите Gx. Сопоставим ему число $\dfrac{1}{|Gx|}$. Сумма этих чисел по всем x из данной орбиты $\mathcal{O} \subset X$ очевидно равна 1, поскольку мы просто $|\mathcal{O}|$ раз складываем число $\dfrac{1}{|\mathcal{O}|}$ с самим собой. Поэтому количество орбит можно вычислить по формуле

$$N = \sum_{x \in X} \frac{1}{|Gx|}. \tag{14}$$

Из (11) имеем $|Gx| = \dfrac{|G|}{|\operatorname{St}_G(x)|}$. Подставляя $|Gx| = \dfrac{|G|}{|\operatorname{St}_G(x)|}$ в (14), получаем

$$N = \sum_{x \in X} \frac{|\operatorname{St}_G(x)|}{|G|} = \frac{1}{|G|} \sum_{x \in X} |\operatorname{St}_G(x)|. \tag{15}$$

Из (10) и (15) получаем

$$N = \frac{1}{|G|} \sum_{g \in G} |X^g|.$$

□

Лемма Бернсайда используется для решения многих комбинаторных задач, которые можно свести к вычислению количества орбит при действии какой-то конечной группы.

Пример 3. Рассмотрим следующую задачу.

Квадратная таблица размера 3×3 заполнена крестиками и ноликами так, что крестиков 3, а ноликов 6. Ясно, что существует $\frac{9 \cdot 8 \cdot 7}{3 \cdot 2 \cdot 1} = 84$ способа заполнить таблицу, поскольку для крестиков мы можем выбрать любые 3 из 9 клеток таблицы.

Два способа заполнения считаются эквивалентными, если один можно получить из другого такими преобразованиями:

- поворот вокруг центра таблицы на угол $\dfrac{k\pi}{2}$, где $k = 0, 1, 2, 3$;
- отражение относительно горизонтальной оси, проходящей через центр;
- отражение относительно вертикальной оси, проходящей через центр;
- отражения относительно двух диагоналей таблицы.

Например, способ $\begin{array}{|ccc|}\hline 0 & \times & \times \\ \times & 0 & 0 \\ 0 & 0 & 0 \\ \hline \end{array}$ эквивалентен следующим способам:

$$\begin{array}{|ccc|}\hline 0 & \times & \times \\ \times & 0 & 0 \\ 0 & 0 & 0 \\ \hline \end{array} \quad \begin{array}{|ccc|}\hline \times & 0 & 0 \\ \times & 0 & 0 \\ 0 & \times & 0 \\ \hline \end{array} \quad \begin{array}{|ccc|}\hline 0 & 0 & 0 \\ 0 & 0 & \times \\ \times & \times & 0 \\ \hline \end{array} \quad \begin{array}{|ccc|}\hline 0 & \times & 0 \\ 0 & 0 & \times \\ 0 & 0 & \times \\ \hline \end{array} \quad \begin{array}{|ccc|}\hline 0 & 0 & 0 \\ \times & 0 & 0 \\ 0 & \times & \times \\ \hline \end{array} \quad \begin{array}{|ccc|}\hline \times & \times & 0 \\ 0 & 0 & \times \\ 0 & 0 & 0 \\ \hline \end{array} \quad \begin{array}{|ccc|}\hline 0 & \times & 0 \\ \times & 0 & 0 \\ \times & 0 & 0 \\ \hline \end{array} \quad \begin{array}{|ccc|}\hline 0 & 0 & \times \\ 0 & 0 & \times \\ 0 & \times & 0 \\ \hline \end{array}$$

Сколько существует неэквивалентных способов заполнения? Рассматриваются только заполнения, содержащие 3 крестика и 6 ноликов.

Рассмотрим группу, состоящую из 8 преобразований таблицы

$$G = \big\{\, p_0, \quad p_1, \quad p_2, \quad p_3, \quad s_{\text{hor}}, \quad s_{\text{ver}}, \quad s_{\text{diag1}}, \quad s_{\text{diag2}} \,\big\}. \tag{16}$$

Здесь

- p_k – поворот вокруг центра таблицы на угол $\dfrac{k\pi}{2}$, $k = 0, 1, 2, 3$;
- s_{hor}, s_{ver} – отражения относительно горизонтальной и вертикальной осей, проходящих через центр;
- s_{diag1} – отражение относительно главной диагонали, проходящей через верхний левый и нижний правый углы таблицы;
- s_{diag2} – отражение относительно другой диагонали, проходящей через нижний левый и верхний правый углы.

Преобразование $p_0 = \mathrm{Id}$ является единичным элементом этой группы.

Пусть X – множество способов заполнения. Как объяснено выше, $|X| = 84$.

Группа G действует на множестве X. Например, применяя преобразования p_1, p_2, s_{hor}, s_{diag1}, s_{diag2} к элементу $x = \begin{array}{|ccc|}\hline 0 & \times & \times \\ \times & 0 & 0 \\ 0 & 0 & 0 \\ \hline \end{array} \in X$, получаем

$$p_1 x = \begin{array}{|ccc|}\hline \times & 0 & 0 \\ \times & 0 & 0 \\ 0 & \times & 0 \\ \hline \end{array}, \quad p_2 x = \begin{array}{|ccc|}\hline 0 & 0 & 0 \\ 0 & 0 & \times \\ \times & \times & 0 \\ \hline \end{array}, \quad s_{\text{hor}} x = \begin{array}{|ccc|}\hline 0 & 0 & 0 \\ \times & 0 & 0 \\ 0 & \times & \times \\ \hline \end{array}, \quad s_{\text{diag1}} x = \begin{array}{|ccc|}\hline 0 & \times & 0 \\ \times & 0 & 0 \\ \times & 0 & 0 \\ \hline \end{array}, \quad s_{\text{diag2}} x = \begin{array}{|ccc|}\hline 0 & 0 & \times \\ 0 & 0 & \times \\ 0 & \times & 0 \\ \hline \end{array}.$$

Количество неэквивалентных способов заполнения равно количеству орбит этого действия G на множестве X. Найдем количество орбит с помощью леммы Бернсайда по формуле (13), где $X^g = \{\, x \in X \mid gx = x \,\}$ для $g \in G$.

Для $g = p_0 = \mathrm{Id}$ имеем $X^g = X$, так что $|X^g| = 84$.

Для преобразования $g = p_2$ (поворота на угол π) множество X^g состоит из следующих элементов: $\begin{array}{|ccc|}\hline \times & 0 & 0 \\ 0 & \times & 0 \\ 0 & 0 & \times \\ \hline \end{array}$, $\begin{array}{|ccc|}\hline 0 & 0 & \times \\ 0 & \times & 0 \\ \times & 0 & 0 \\ \hline \end{array}$, $\begin{array}{|ccc|}\hline 0 & 0 & 0 \\ \times & \times & \times \\ 0 & 0 & 0 \\ \hline \end{array}$, $\begin{array}{|ccc|}\hline 0 & \times & 0 \\ 0 & \times & 0 \\ 0 & \times & 0 \\ \hline \end{array}$. Следовательно, $|X^g| = 4$.

Для преобразования $g = s_{\text{hor}}$ (отражения относительно горизонтальной оси) имеем

$$X^g = \left\{ \begin{array}{|ccc|}\hline 0 & 0 & 0 \\ \times & \times & \times \\ 0 & 0 & 0 \\ \hline \end{array}, \quad \begin{array}{|ccc|}\hline \times & 0 & 0 \\ \times & 0 & 0 \\ \times & 0 & 0 \\ \hline \end{array}, \quad \begin{array}{|ccc|}\hline \times & 0 & 0 \\ 0 & \times & 0 \\ \times & 0 & 0 \\ \hline \end{array}, \quad \begin{array}{|ccc|}\hline \times & 0 & 0 \\ 0 & 0 & \times \\ \times & 0 & 0 \\ \hline \end{array}, \quad \begin{array}{|ccc|}\hline 0 & \times & 0 \\ \times & 0 & 0 \\ 0 & \times & 0 \\ \hline \end{array}, \quad \begin{array}{|ccc|}\hline 0 & \times & 0 \\ 0 & \times & 0 \\ 0 & \times & 0 \\ \hline \end{array}, \quad \begin{array}{|ccc|}\hline 0 & \times & 0 \\ 0 & 0 & \times \\ 0 & \times & 0 \\ \hline \end{array}, \quad \begin{array}{|ccc|}\hline 0 & 0 & \times \\ \times & 0 & 0 \\ 0 & 0 & \times \\ \hline \end{array}, \quad \begin{array}{|ccc|}\hline 0 & 0 & \times \\ 0 & \times & 0 \\ 0 & 0 & \times \\ \hline \end{array}, \quad \begin{array}{|ccc|}\hline 0 & 0 & \times \\ 0 & 0 & \times \\ 0 & 0 & \times \\ \hline \end{array} \right\},$$

поэтому $|X^g| = 10$.

Аналогично, для $g = s_{\text{ver}}$ получаем $|X^g| = 10$.

Для преобразования $g = s_{\text{diag1}}$ (отражения относительно главной диагонали) имеем

$$X^g = \left\{ \begin{smallmatrix} \times & 0 & 0 \\ 0 & \times & 0 \\ 0 & 0 & \times \end{smallmatrix}, \begin{smallmatrix} \times & \times & 0 \\ \times & 0 & 0 \\ 0 & 0 & 0 \end{smallmatrix}, \begin{smallmatrix} 0 & \times & 0 \\ \times & \times & 0 \\ 0 & 0 & 0 \end{smallmatrix}, \begin{smallmatrix} 0 & \times & 0 \\ \times & 0 & 0 \\ 0 & 0 & \times \end{smallmatrix}, \begin{smallmatrix} \times & 0 & \times \\ 0 & 0 & 0 \\ \times & 0 & 0 \end{smallmatrix}, \begin{smallmatrix} 0 & 0 & \times \\ 0 & \times & 0 \\ \times & 0 & 0 \end{smallmatrix}, \begin{smallmatrix} 0 & 0 & \times \\ 0 & 0 & 0 \\ \times & 0 & \times \end{smallmatrix}, \begin{smallmatrix} \times & 0 & 0 \\ 0 & 0 & \times \\ 0 & \times & 0 \end{smallmatrix}, \begin{smallmatrix} 0 & 0 & 0 \\ 0 & \times & \times \\ 0 & \times & 0 \end{smallmatrix}, \begin{smallmatrix} 0 & 0 & 0 \\ 0 & 0 & \times \\ 0 & \times & \times \end{smallmatrix} \right\},$$

поэтому $|X^g| = 10$.

Аналогично, для $g = s_{\text{diag2}}$ получаем $|X^g| = 10$.

По формуле (13) количество орбит равно $\frac{1}{8}(84+0+4+0+10+10+10+10) = 16$. Таким образом, количество неэквивалентных способов заполнения таблицы 3 крестиками и 6 ноликами равно 16.

Пример 4. На второй лекции миникурса `https://cis.uniyar.ac.ru/event/214` лемма Бернсайда применялась для вычисления количества ожерелий, составленных из 4 бусинок, каждая из которых может быть одного из 3 цветов.

При решении этой задачи на лекции использовалось действие группы (16), которую можно отождествить с группой симметрий квадрата, состоящей из 8 элементов:

- p_k – поворот вокруг центра квадрата на угол $\frac{k\pi}{2}$, $k = 0, 1, 2, 3$;
- s_{hor}, s_{ver} – отражения относительно горизонтальной и вертикальной осей симметрии квадрата;
- s_{diag1}, s_{diag2} – отражения относительно двух диагоналей квадрата.

Четыре бусинки ожерелья можно расположить в вершинах квадрата. Два ожерелья считаются одинаковыми, если одно получается из другого с помощью описанных преобразований (симметрий) квадрата. Количество разных ожерелий равно количеству орбит действия группы (16), которое можно вычислить по формуле (13). Это вычисление подробно описано на видео второй лекции `https://cis.uniyar.ac.ru/event/214`

Аналогично, для любых натуральных чисел m, n можно вычислить количество ожерелий, составленных из m бусинок, каждая из которых может быть одного из n цветов. Информацию об этом легко найти в интернете по ключевым словам “задача об ожерельях”.

2. Применения групп в теории чисел

Выберем произвольным образом и зафиксируем натуральное число $n > 1$. Тогда для каждого целого числа m однозначно определено представление

$$m = nq + r, \qquad q, r \in \mathbb{Z}, \qquad 0 \le r \le n-1. \tag{17}$$

Процедура, ставящая в соответствие целому числу m такое представление, называется *делением с остатком* числа m на n. Число r называется *остатком* от деления m на n.

Определение 6. Целые числа a и b *сравнимы по модулю* n (обозначение: $a \equiv b \mod n$), если a и b дают равные остатки при делении на n.

Напомним, что ненулевое целое число d является *делителем* целого числа m, если существует $k \in \mathbb{Z}$ такое, что $m = dk$.

Заметим, что $a \equiv b \mod n$ тогда и только тогда, когда n является делителем числа $a-b$. Например, $7 \equiv 25 \mod 6$, поскольку 6 является делителем числа $7 - 25 = -18$.

Легко проверить следующее утверждение.

Предложение 1. *Если целые числа* $a, \tilde{a}, b, \tilde{b}$ *удовлетворяют* $a \equiv b \mod n$, $\tilde{a} \equiv \tilde{b} \mod n$, *то*

$$a + \tilde{a} \equiv b + \tilde{b} \mod n, \qquad a\tilde{a} \equiv b\tilde{b} \mod n.$$

Для любого натурального числа i *из* $a \equiv b \mod n$ *следует* $a^i \equiv b^i \mod n$.

Из процедуры деления с остатком получаем

Предложение 2. *Отношение сравнимости по модулю* n *разбивает все множество целых чисел на* n *непересекающихся классов, каждый из которых состоит из всех чисел, имеющих остаток, равный* r; $r = 0, 1, \ldots, n-1$.

Определение 7. Классы, указанные в предложении 2, называются *классами вычетов по модулю* n.

Класс вычетов целого числа m по модулю n обозначается $(m \bmod n)$. То есть, $(m \bmod n)$ – это класс чисел вида $m + nk$ для всех целых k. Другими словами, подмножество $(m \bmod n) \subset \mathbb{Z}$ состоит из чисел вида $m + nk$ для всех целых k.

Предложение 2 можно переформулировать так. Для любого $m \in \mathbb{Z}$ существует единственное число $r \in \{0, 1, \ldots, n-1\}$ такое, что $(m \bmod n) = (r \bmod n)$. Для целых m и $\tilde{m}$ имеем

$$(m \mod n) = (\tilde{m} \mod n)$$

тогда и только тогда, когда $m \equiv \tilde{m} \mod n$.

Множество классов вычетов по модулю n обозначается $\mathbb{Z}_n$. По предложению 2 получаем

$$\mathbb{Z}_n = \big\{(0 \mod n),\ (1 \mod n),\ (2 \mod n),\ \ldots,\ (n-1 \mod n)\big\}.$$

Поскольку $(r \bmod n) = (r + an \bmod n)$ для любых $r, a \in \mathbb{Z}$, имеем также

$$\mathbb{Z}_n = \big\{(an \mod n),\ (1+an \mod n),\ (2+an \mod n),\ \ldots,\ (n-1+an \mod n)\big\}.$$

Классы вычетов по модулю n можно складывать и умножать друг на друга следующим образом

$$(m_1 \mod n) + (m_2 \mod n) = (m_1 + m_2 \mod n),$$
$$(m_1 \mod n) \cdot (m_2 \mod n) = (m_1 m_2 \mod n), \qquad m_1, m_2 \in \mathbb{Z}.$$

Легко убедиться, что это определение сложения и умножения корректно.

Очевидно, что операции сложения и умножения классов вычетов ассоциативны и коммутативны, т.е. для любых $m_1, m_2, m_3 \in \mathbb{Z}$ имеем

$$\big((m_1 \mod n) \cdot (m_2 \mod n)\big) \cdot (m_3 \mod n) = (m_1 \mod n) \cdot \big((m_2 \mod n) \cdot (m_3 \mod n)\big),$$
$$\big((m_1 \mod n) + (m_2 \mod n)\big) + (m_3 \mod n) = (m_1 \mod n) + \big((m_2 \mod n) + (m_3 \mod n)\big),$$
$$(m_1 \mod n) \cdot (m_2 \mod n) = (m_2 \mod n) \cdot (m_1 \mod n),$$
$$(m_1 \mod n) + (m_2 \mod n) = (m_2 \mod n) + (m_1 \mod n).$$

Отметим также, что для любого $m \in \mathbb{Z}$

$$(m \mod n) + (0 \mod n) = (m \mod n), \qquad (m \mod n) \cdot (1 \mod n) = (m \mod n).$$

Определение 8. Пусть $m \in \mathbb{Z}$. Элемент $(m \bmod n) \in \mathbb{Z}_n$ называется *обратимым*, если существует число $\tilde{m} \in \mathbb{Z}$ такое, что

$$(m \mod n) \cdot (\tilde{m} \mod n) = (1 \mod n). \tag{18}$$

Равенство (18) означает, что n является делителем числа $m\tilde{m} - 1$.

Тогда элемент $(\tilde{m} \bmod n) \in \mathbb{Z}_n$ называется *обратным* к элементу $(m \bmod n) \in \mathbb{Z}_n$ и обозначается как $(m \bmod n)^{-1}$. Можно писать $(\tilde{m} \bmod n) = (m \bmod n)^{-1}$.

Напомним, что два целых числа называются *взаимно простыми*, если они не имеют никаких общих делителей, кроме ± 1.

Лемма 5. *Числа $a, b \in \mathbb{Z}$ взаимно просты тогда и только тогда, когда существуют $m_1, m_2 \in \mathbb{Z}$ такие, что $m_1 a + m_2 b = 1$.*

Доказательство. Пусть $m_1 a + m_2 b = 1$. Тогда любой общий делитель d чисел a и b также является делителем числа 1, т.е. $d = \pm 1$. Следовательно, a и b взаимно просты.

Если $a, b \in \mathbb{Z}$ взаимно просты, то существование требуемых чисел $m_1, m_2 \in \mathbb{Z}$ следует из применения алгоритма Евклида для вычисления наибольшего общего делителя чисел a и b. □

Предложение 3. *Пусть $a \in \mathbb{Z}$. Элемент $(a \bmod n)$ обратим в $\mathbb{Z}_n$ тогда и только тогда, когда число a взаимно просто с n.*

Доказательство. Пусть $(a \bmod n)$ обратим. Это значит, что существует число $\tilde{a} \in \mathbb{Z}$ такое, что

$$(a \mod n) \cdot (\tilde{a} \mod n) = (1 \mod n). \tag{19}$$

Другими словами, $(\tilde{a} \bmod n) = (a \bmod n)^{-1}$.

Поскольку $(a \bmod n) \cdot (\tilde{a} \bmod n) = (a\tilde{a} \bmod n)$, равенство (19) говорит, что $a\tilde{a} \equiv 1 \mod n$. То есть, существует $k \in \mathbb{Z}$ такое, что

$$a\tilde{a} - 1 = nk. \tag{20}$$

Из (20) следует, что, если d – делитель чисел a и n, то d также является делителем числа 1, т.е. $d = \pm 1$. Таким образом, числа a и n взаимно просты.

Теперь докажем, что, если a и n взаимно просты, то элемент $(a \bmod n)$ обратим. По лемме 5, если a и n взаимно просты, то существуют $m_1, m_2 \in \mathbb{Z}$ такие, что

$$m_1 a + m_2 n = 1. \tag{21}$$

Из (21) получаем $(m_1 \bmod n) \cdot (a \bmod n) = (m_1 a \bmod n) = (1 \bmod n)$, т.е. $(a \bmod n)$ обратим и

$$(m_1 \bmod n) = (a \bmod n)^{-1}.$$

□

Определение 9. *Функция Эйлера* $n \mapsto \varphi(n)$ определена на множестве натуральных чисел следующим образом.

- Если $n > 1$, то $\varphi(n)$ – количество натуральных чисел, меньших n и взаимно простых с n.
- Для $n = 1$ полагают $\varphi(1) = 1$.

Например, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$. Из предложения 3 следует, что

(22) при $n > 1$ количество обратимых элементов в $\mathbb{Z}_n$ равно $\varphi(n)$.

Обозначим $U(\mathbb{Z}_n) \subset \mathbb{Z}_n$ подмножество обратимых элементов. Из (22) имеем $|U(\mathbb{Z}_n)| = \varphi(n)$. Например, применяя предложение 3 для $n = 5, 6$, получаем

$$U(\mathbb{Z}_5) = \big\{(1 \bmod 5),\ (2 \bmod 5),\ (3 \bmod 5),\ (4 \bmod 5)\big\},$$
$$U(\mathbb{Z}_6) = \big\{(1 \bmod 6),\ (5 \bmod 6)\big\}.$$

Предложение 4. *Пусть* $m_1, m_2 \in \mathbb{Z}$ *таковы, что* $(m_1 \bmod n)$ *и* $(m_2 \bmod n)$ *обратимы в* $\mathbb{Z}_n$. *То есть,* $(m_i \bmod n) \in U(\mathbb{Z}_n)$ *для* $i = 1, 2$.

Тогда элемент $(m_1 \bmod n) \cdot (m_2 \bmod n) = (m_1 m_2 \bmod n)$ *тоже обратим в* $\mathbb{Z}_n$.

Множество $U(\mathbb{Z}_n)$ *с операцией умножения является группой. Единичным элементом в этой группе служит* $(1 \bmod n) \in U(\mathbb{Z}_n)$.

Доказательство. Поскольку $(m_1 \bmod n)$ и $(m_2 \bmod n)$ обратимы, существуют $\tilde{m}_1, \tilde{m}_2 \in \mathbb{Z}$ такие, что

$$(m_1 \bmod n) \cdot (\tilde{m}_1 \bmod n) = (1 \bmod n), \qquad (m_2 \bmod n) \cdot (\tilde{m}_2 \bmod n) = (1 \bmod n).$$

Тогда имеем

$$\big((m_1 \bmod n) \cdot (m_2 \bmod n)\big) \cdot \big((\tilde{m}_2 \bmod n) \cdot (\tilde{m}_1 \bmod n)\big) = (m_1 m_2 \tilde{m}_2 \tilde{m}_1 \bmod n) =$$
$$= (m_1 \bmod n) \cdot \big((m_2 \bmod n) \cdot (\tilde{m}_2 \bmod n)\big) \cdot (\tilde{m}_1 \bmod n)\big) =$$
$$= (m_1 \bmod n) \cdot (1 \bmod n) \cdot (\tilde{m}_1 \bmod n)\big) = (m_1 \bmod n) \cdot (\tilde{m}_1 \bmod n) = (1 \bmod n).$$

Следовательно, элемент $(m_1 \bmod n) \cdot (m_2 \bmod n) = (m_1 m_2 \bmod n)$ обратим, и обратным к нему является элемент $(\tilde{m}_2 \bmod n) \cdot (\tilde{m}_1 \bmod n) = (\tilde{m}_2 \tilde{m}_1 \bmod n)$.

Таким образом, для любых двух элементов $(m_1 \bmod n)$ и $(m_2 \bmod n)$ из множества $U(\mathbb{Z}_n)$ их произведение $(m_1 \bmod n) \cdot (m_2 \bmod n)$ тоже лежит в $U(\mathbb{Z}_n)$. То есть, операция умножения определена на $U(\mathbb{Z}_n)$.

Легко проверить, что $U(\mathbb{Z}_n)$ является группой с единичным элементом $(1 \bmod n)$. □

Пусть G – группа с единичным элементом e.

Определение 10. Если число элементов группы G конечно, то оно называется *порядком* группы G и обозначается как $|G|$. Если множество элементов группы G бесконечно, то говорят, что группа G *имеет бесконечный порядок.*

Из (22) получаем, что

(23) при $n > 1$ порядок группы $U(\mathbb{Z}_n)$ дается функцией Эйлера: $|U(\mathbb{Z}_n)| = \varphi(n)$.

Пусть $g \in G$. Для каждого $k \in \mathbb{Z}$ определим *k-ю степень* g^k элемента g следующим образом.

- Если $k > 0$, то
$$g^k = \underbrace{gg\dots g}_{k \text{ множителей}}.$$
В частности, $g^1 = g$.
- Если $k < 0$, то $g^k = \underbrace{(g^{-1})(g^{-1})\dots(g^{-1})}_{-k \text{ множителей}}$.
- При $k = 0$ положим $g^0 = e$.

Для любых $k, l \in \mathbb{Z}$ имеем $g^k g^l = g^{k+l}$. Следовательно, множество всех степеней g^k, $k \in \mathbb{Z}$, элемента g является подгруппой группы G. Она обозначается
$$\langle g \rangle = \left\{ g^k \;\middle|\; k \in \mathbb{Z} \right\}$$
и называется *циклической подгруппой, порожденной элементом* g. В зависимости от строения группы G и выбора элемента g в ней, циклическая подгруппа $\langle g \rangle$ может оказаться как конечной, так и бесконечной.

Определение 11. *Порядком* элемента g группы G называется порядок циклической подгруппы $\langle g \rangle$, порожденной им в группе G.

Пример 5. Покажем, что порядок элемента $(4 \mod 7)$ в группе $U(\mathbb{Z}_7)$ равен 3. Имеем
$$(4 \mod 7)^2 = (4 \mod 7) \cdot (4 \mod 7) = (16 \mod 7) = (2 \mod 7),$$
$$(4 \mod 7)^3 = (4 \mod 7)^2 \cdot (4 \mod 7) = (2 \mod 7) \cdot (4 \mod 7) = (8 \mod 7) = (1 \mod 7).$$
Следовательно, для любого $m \in \mathbb{Z}$ имеем
$$(4 \mod 7)^{3m} = \left((4 \mod 7)^3\right)^m = (1 \mod 7)^m = (1 \mod 7),$$
$$(4 \mod 7)^{3m+1} = (4 \mod 7)^{3m} \cdot (4 \mod 7) = (1 \mod 7) \cdot (4 \mod 7) = (4 \mod 7),$$
$$(4 \mod 7)^{3m+2} = (4 \mod 7)^{3m} \cdot (4 \mod 7)^2 = (1 \mod 7) \cdot (2 \mod 7) = (2 \mod 7).$$
Таким образом, циклическая подгруппа, порожденная элементом $(4 \mod 7) \in U(\mathbb{Z}_7)$, состоит из трех элементов: $(1 \mod 7)$, $(4 \mod 7)$, $(2 \mod 7)$. То есть, порядок этой циклической подгруппы равен 3.

Из определения порядка элемента группы легко вывести

Предложение 5. *Если элемент g группы G имеет конечный порядок m, то m является наименьшим натуральным числом таким, что $g^m = e$, где e – единичный элемент группы G.*

В этом случае циклическая подгруппа $\langle g \rangle$ состоит из элементов g^i, $i = 0, 1, \dots, m-1$. Для $a, b \in \mathbb{Z}$ имеем $g^a = g^b$ тогда и только тогда, когда $a \equiv b \mod m$.

Следующий результат имеет многочисленные приложения.

Теорема 1. **(Теорема Лагранжа)** *Если G – конечная группа, то порядок любой ее подгруппы является делителем порядка группы G. В частности, порядок любого элемента группы G является делителем порядка группы G.*

Доказательство. Рассмотрим конечную группу G и подгруппу $\tilde{G} \subset G$. В примере 2 мы доказали равенство (7), где $G/\tilde{G}$ – множество всех левых смежных классов группы G по подгруппе $\tilde{G}$. Из (7) получаем, что $|\tilde{G}|$ является делителем $|G|$. □

Следствие 1. *Для любого элемента g конечной группы G с единичным элементом e справедливо равенство $g^{|G|} = e$.*

Доказательство. Обозначим через m порядок элемента $g \in G$. По теореме 1 существует натуральное число k такое, что $|G| = mk$. Тогда имеем $g^{|G|} = g^{mk} = (g^m)^k = e^k = e$. □

Теорема 2. **(Теорема Эйлера)** *Если целое число a взаимно просто с натуральным $n > 1$, то $a^{\varphi(n)} \equiv 1 \mod n$.*

Доказательство. Пусть $a \in \mathbb{Z}$ взаимно просто с натуральным $n > 1$. Тогда по предложению 3 имеем $(a \bmod n) \in U(\mathbb{Z}_n)$. Поскольку $|U(\mathbb{Z}_n)| = \varphi(n)$, применяя следствие 1 к $G = U(\mathbb{Z}_n)$ и $g = (a \bmod n)$, получаем $(a \bmod n)^{\varphi(n)} = (1 \bmod n)$, т.е. $a^{\varphi(n)} \equiv 1 \mod n$. □

Напомним, что *простое число* – это натуральное число, больше единицы, имеющее ровно два натуральных делителя: 1 и само себя.

Число 2 простое и четное. Все другие простые числа – нечетные.

Поскольку для любого простого числа p имеем $\varphi(p) = p - 1$, применяя теорему 2 для $n = p$, получаем

Теорема 3. **(Малая теорема Ферма)** *Если целое a не делится на простое p, то $a^{p-1} \equiv 1 \bmod p$.*

При исследовании групп очень полезной оказывается конструкция так называемого *прямого произведения*. Пусть даны группы G и H с операциями $*_G$ и $*_H$ соответственно и единичными элементами e_G и e_H соответственно. В каждой группе – своя групповая операция и свой единичный элемент; это отражено в обозначениях. Таким образом, для любых $g, g' \in G$ и $h, h' \in H$

$$g *_G g' \in G, \qquad h *_H h' \in H, \qquad e_G *_G g = g *_G e_G = g, \qquad e_H *_H h = h *_H e_H = h.$$

Определение 12. *Прямым произведением* групп $(G, *_G)$ и $(H, *_H)$ называется множество

$$G \times H = \{(g, h) \mid \ g \in G, \ \ h \in H\}$$

с операцией

$$(g, h) \star (g', h') = (g *_G g',\, h *_H h').$$

Предложение 6. *Прямое произведение групп является группой относительно операции $\star$ с единичным элементом $(e_G, e_H) \in G \times H$.*

Доказательство. Легко проверить, что множество $G \times H$ с операцией $\star$ удовлетворяет всем свойствам группы, перечисленным в определении 2. Для элемента $(g, h) \in G \times H$ обратным является элемент $(g^{-1}, h^{-1}) \in G \times H$. □

Некоторые группы, будучи заданными по-разному, обладают аналогичной структурой. Пусть $(G, *_G)$ и $(H, *_H)$ – группы.

Определение 13. Отображение $f\colon G \to H$ называется *изоморфизмом групп*, если оно биективно и сохраняет групповую операцию, т.е. $f(g *_G g') = f(g) *_H f(g')$ для любых $g, g' \in G$.

Группы, между которыми существует изоморфизм, называются *изоморфными*. Изоморфизм часто обозначают символом $\cong$.

Нетрудно убедиться в том, что изоморфизм $f\colon G \to H$ переводит единичный элемент группы G в единичный элемент группы H, и для любого элемента $a \in G$ имеем $f(a^{-1}) = f(a)^{-1}$.

Пусть $a > 1$ и $b > 1$ – натуральные числа. Если целые числа r, r' удовлетворяют $r \equiv r' \bmod ab$, то $r \equiv r' \bmod a$ и $r \equiv r' \bmod b$. Следовательно, можно рассмотреть отображение

$$F_{a,b}\colon \mathbb{Z}_{ab} \to \mathbb{Z}_a \times \mathbb{Z}_b, \qquad (r \bmod ab) \mapsto \big((r \bmod a), (r \bmod b)\big), \qquad r \in \mathbb{Z}. \tag{24}$$

Рассмотрим произвольные элементы $g = (m \bmod ab)$ и $g' = (m' \bmod ab)$ множества $\mathbb{Z}_{ab}$. Легко проверить, что

$$F_{a,b}(g + g') = F_{a,b}(g) + F_{a,b}(g'), \tag{25}$$

$$F_{a,b}(gg') = F_{a,b}(g) \cdot F_{a,b}(g') \qquad \forall\, g, g' \in \mathbb{Z}_{ab}. \tag{26}$$

Пусть натуральные числа $a > 1$ и $b > 1$ взаимно просты. Поскольку $U(\mathbb{Z}_a) \subset \mathbb{Z}_a$ и $U(\mathbb{Z}_b) \subset \mathbb{Z}_b$, имеем $U(\mathbb{Z}_a) \times U(\mathbb{Z}_b) \subset \mathbb{Z}_a \times \mathbb{Z}_b$. По предложению 3 элемент $g \in U(\mathbb{Z}_{ab})$ имеет вид $g = (r \bmod ab)$, где r взаимно просто с ab. Тогда число r взаимно просто с a и взаимно просто с b. По предложению 3 имеем $(r \bmod a) \in U(\mathbb{Z}_a)$ и $(r \bmod b) \in U(\mathbb{Z}_b)$. Таким образом,

$$\forall\, g \in U(\mathbb{Z}_{ab}) \qquad F_{a,b}(g) \in U(\mathbb{Z}_a) \times U(\mathbb{Z}_b) \subset \mathbb{Z}_a \times \mathbb{Z}_b. \tag{27}$$

Предложение 7. *Пусть натуральные числа $a > 1$ и $b > 1$ взаимно просты. Тогда отображение* (24) *биективно.*

Доказательство. Вначале докажем, что отображение $F_{a,b}\colon \mathbb{Z}_{ab} \to \mathbb{Z}_a \times \mathbb{Z}_b$ сюръективно. Рассмотрим произвольные элементы $(r_1 \bmod a) \in \mathbb{Z}_a$ и $(r_2 \bmod b) \in \mathbb{Z}_b$. Чтобы доказать сюръективность $F_{a,b}$, нам нужно найти число $q \in \mathbb{Z}$ такое, что

$$F_{a,b}\big((q \bmod ab)\big) = \big((r_1 \bmod a), (r_2 \bmod b)\big). \tag{28}$$

По лемме 5 существуют $m_1, m_2 \in \mathbb{Z}$, удовлетворяющие $m_1 a + m_2 b = 1$. Тогда для числа $q = r_2 m_1 a + r_1 m_2 b$ имеем

$$q \equiv r_1 \mod a, \qquad q \equiv r_2 \mod b, \tag{29}$$

поскольку

$$q - r_1 = r_2 m_1 a + r_1 m_2 b - r_1(m_1 a + m_2 b) = a(r_2 m_1 - r_1 m_1),$$
$$q - r_2 = r_2 m_1 a + r_1 m_2 b - r_2(m_1 a + m_2 b) = b(r_1 m_2 - r_2 m_1).$$

Из (29) получаем (28).

Поскольку $|\mathbb{Z}_{ab}| = ab = |\mathbb{Z}_a \times \mathbb{Z}_b|$, сюръективность отображения $F_{a,b}$ влечет его биективность. □

Теорема 4. *Пусть натуральные числа $a > 1$ и $b > 1$ взаимно просты. Тогда ограничение отображения (24) на подмножество $U(\mathbb{Z}_{ab}) \subset \mathbb{Z}_{ab}$ задает изоморфизм между группой $U(\mathbb{Z}_{ab})$ и группой $U(\mathbb{Z}_a) \times U(\mathbb{Z}_b)$.*

Доказательство. По предложению 7 отображение (24) биективно. По свойствам (27), (26) ограничение отображения (24) на подмножество $U(\mathbb{Z}_{ab}) \subset \mathbb{Z}_{ab}$ задает биективное отображение $U(\mathbb{Z}_{ab}) \to U(\mathbb{Z}_a) \times U(\mathbb{Z}_b)$, являющееся изоморфизмом групп. □

Теорема 5. *Функция Эйлера мультипликативна в следующем смысле: если $n = n_1 \cdot n_2 \cdot \ldots \cdot n_s$, где натуральные числа $n_1, n_2, \ldots, n_s$ попарно взаимно просты, то $\varphi(n) = \varphi(n_1) \cdot \varphi(n_2) \cdot \ldots \cdot \varphi(n_s)$.*

Доказательство. Поскольку $\varphi(1) = 1$, достаточно рассмотреть случай, когда $n_i > 1$ для всех $i = 1, \ldots, s$.

Докажем утверждение теоремы индукцией по s, предполагая $n_i > 1$ для всех $i = 1, \ldots, s$.

Вначале рассмотрим случай $s = 2$, $n = n_1 n_2$, где $n_1 > 1$ и $n_2 > 1$ взаимно просты. По теореме 4 группа $U(\mathbb{Z}_n)$ изоморфна группе $U(\mathbb{Z}_{n_1}) \times U(\mathbb{Z}_{n_2})$. Следовательно, $|U(\mathbb{Z}_n)| = |U(\mathbb{Z}_{n_1}) \times U(\mathbb{Z}_{n_2})|$. Поскольку $|U(\mathbb{Z}_n)| = \varphi(n)$ и $|U(\mathbb{Z}_{n_1}) \times U(\mathbb{Z}_{n_2})| = \varphi(n_1) \cdot \varphi(n_2)$, получаем $\varphi(n) = \varphi(n_1) \cdot \varphi(n_2)$.

Пусть утверждение теоремы верно при $s = k$ для некоторого натурального $k \geq 2$. Докажем его для $s = k + 1$. Пусть натуральные числа $n_i > 1$, $i = 1, \ldots, k+1$, попарно взаимно просты.

По предположению индукции имеем $\varphi(n_1 \cdot \ldots \cdot n_k) = \varphi(n_1) \cdot \ldots \cdot \varphi(n_k)$. Поскольку числа $n_1 \cdot \ldots \cdot n_k$ и n_{k+1} взаимно просты, для $n = n_1 \cdot \ldots \cdot n_k \cdot n_{k+1}$ имеем $\varphi(n) = \varphi(n_1 \cdot \ldots \cdot n_k) \cdot \varphi(n_{k+1})$. Следовательно, $\varphi(n) = \varphi(n_1) \cdot \ldots \cdot \varphi(n_k) \cdot \varphi(n_{k+1})$. □

Из определения функции Эйлера легко вывести

Предложение 8. *Для простого числа p и натурального числа k имеем $\varphi(p^k) = (p-1)p^{k-1}$.*

Если натуральное n разложено в произведение простых чисел, теорема 5 и предложение 8 позволяют вычислить значение функции Эйлера $\varphi(n)$. Например,

$$\varphi(540) = \varphi(2^2 \cdot 3^3 \cdot 5) = \varphi(2^2) \cdot \varphi(3^3) \cdot \varphi(5) = 2 \cdot 2 \cdot 3^2 \cdot 4 = 144.$$

Полученные свойства функции Эйлера можно применять для вычисления остатков при делении натуральных чисел.

Пример 6. Найдем две последние цифры в десятичной записи числа 23^{123}, т.е. остаток при делении 23^{123} на 100. Заметим, что числа 23 и 100 взаимно просты, и применим теорему Эйлера:

$$23^{\varphi(100)} \equiv 1 \mod 100.$$

Вычислив $\varphi(100) = \varphi(4) \cdot \varphi(25) = 40$, получаем

$$23^{40} \equiv 1 \mod 100. \tag{30}$$

Имеем

$$23^{123} = 23^{120} \cdot 23^3 = (23^{40})^3 \cdot 23^3 \equiv 23^3 \mod 100, \tag{31}$$

так как из (30) получаем $(23^{40})^3 \equiv 1 \mod 100$. Следовательно,

$$23^{123} = 23^{120} \cdot 23^3 = (23^{40})^3 \cdot 23^3 \equiv 23^3 \equiv 23^2 \cdot 23 \equiv 29 \cdot 23 \equiv 67 \mod 100, \tag{32}$$

т.е. искомый остаток равен 67. В вычислении (32) мы использовали свойство $23^2 \equiv 29 \mod 100$.

Задачи тестирования

При решении задач можно пользоваться всеми утверждениями этого конспекта, не доказывая их.

Задача 1. (2 балла) Рассмотрим элементы $(8 \bmod 15)$, $(7 \bmod 15)$, $(-4 \bmod 15)$, $(16 \bmod 15)$ группы $U(\mathbb{Z}_{15})$. Докажите равенство

$$(8 \mod 15) \cdot (7 \mod 15) = (-4 \mod 15) \cdot (16 \mod 15).$$

Задача 2. (3 балла) Покажите, что порядок элемента $(5 \bmod 16)$ в группе $U(\mathbb{Z}_{16})$ равен 4.

Задача 3. (4 балла) Вычислите $\varphi(14850)$, где φ – функция Эйлера.

Задача 4. (6 баллов) Используя теорему Эйлера, найдите остаток от деления числа 2717^{2019} на 270.
(*Подсказка*: можно рассуждать аналогично примеру 6 со страницы 11.)

Задача 5. (12 баллов) Назовем *рисунком* правильный 6-угольник, каждая сторона которого окрашена в один из четырех цветов. Существует $4^6 = 4096$ таких рисунков, поскольку для каждой из 6 сторон мы можем выбрать один из 4 цветов.

Два рисунка считаются эквивалентными, если один можно получить из другого поворотом на угол $\dfrac{k\pi}{3}$, $k = 0, 1, 2, 3, 4, 5$, вокруг центра 6-угольника.

Сколько существует неэквивалентных рисунков?

Другими словами, на множестве рисунков действует группа $G = \{p_0,\ p_1,\ p_2,\ p_3,\ p_4,\ p_5\}$, где p_k – поворот на угол $\dfrac{k\pi}{3}$, и нужно найти количество орбит этого действия.

Задача 6. (12 баллов)

Квадратная таблица размера 3×3 заполнена крестиками и ноликами так, что крестиков 4, а ноликов 5. Существует $\frac{9 \cdot 8 \cdot 7 \cdot 6}{4 \cdot 3 \cdot 2 \cdot 1} = 126$ способов заполнить таблицу, поскольку для крестиков мы можем выбрать любые 4 из 9 клеток таблицы.

Два способа заполнения считаются эквивалентными, если один можно получить из другого такими преобразованиями:

- поворот вокруг центра таблицы на угол $\dfrac{k\pi}{2}$, где $k = 0, 1, 2, 3$;
- отражение относительно горизонтальной оси, проходящей через центр;
- отражение относительно вертикальной оси, проходящей через центр;
- отражения относительно двух диагоналей таблицы.

Например, способ $\begin{array}{|ccc|}\hline 0 & \times & \times \\ \times & 0 & 0 \\ 0 & \times & 0 \\ \hline\end{array}$ эквивалентен следующим способам:

$$\begin{array}{|ccc|}\hline 0 & \times & \times \\ \times & 0 & 0 \\ 0 & \times & 0 \\ \hline\end{array} \quad \begin{array}{|ccc|}\hline \times & 0 & 0 \\ \times & 0 & \times \\ 0 & \times & 0 \\ \hline\end{array} \quad \begin{array}{|ccc|}\hline 0 & \times & 0 \\ 0 & 0 & \times \\ \times & \times & 0 \\ \hline\end{array} \quad \begin{array}{|ccc|}\hline 0 & \times & 0 \\ \times & 0 & \times \\ 0 & 0 & \times \\ \hline\end{array} \quad \begin{array}{|ccc|}\hline 0 & \times & 0 \\ \times & 0 & 0 \\ 0 & \times & \times \\ \hline\end{array} \quad \begin{array}{|ccc|}\hline \times & \times & 0 \\ 0 & 0 & \times \\ 0 & \times & 0 \\ \hline\end{array} \quad \begin{array}{|ccc|}\hline 0 & \times & 0 \\ \times & 0 & \times \\ \times & 0 & 0 \\ \hline\end{array} \quad \begin{array}{|ccc|}\hline 0 & 0 & \times \\ \times & 0 & \times \\ 0 & \times & 0 \\ \hline\end{array}$$

Сколько существует неэквивалентных способов заполнения? Рассматриваются только заполнения, содержащие 4 крестика и 5 ноликов.

Задача 7. (11 баллов) Пусть p, q – нечетные простые числа, $p \neq q$. Докажите, что

$$p^{2q-1} \equiv p \mod 8q.$$

То есть, нужно доказать, что число $8q$ является делителем числа $p^{2q-1} - p$.

Вопросы по конспекту и условиям задач можно задавать Сергею Александровичу Игонину <s-igonin@yandex.ru>.