Филиппова Анастасия

Домашнее задание 3

(1) (a) $2^{23542} = 2^{23541}2 = 8^{7847}2$
$8^{7847}2 \equiv (1)^{7847}2 \equiv 2 \ mod \ 7$
Ответ: 2.

(b) $(13, 17) = 1 \Rightarrow 13^{2^{2009}} \equiv 13^{(2^{(2009 \ mod \ \varphi(\varphi(17)))} \ mod \varphi(17))} \ mod \ 17$
$\varphi(\varphi(17)) = 8, 2009 \ mod \ 8 = 1$
$13^2 \equiv (-4)^2 \equiv 16 \ mod \ 17$
Ответ:16.

(c) $(4, 49) = 1 \Rightarrow$ аналогично пункту 1 : $\varphi(\varphi(\varphi(49))) = \varphi(\varphi(42)) = \varphi(12) = \varphi(3)\varphi(4) = 4$
$2009 \ mod \ 4 = 1, 2009 \ mod \ 12 = 5, 37^5 \equiv (-5)^5 \equiv (-125)25 \equiv 25 \ mod \ 42$
$4^{25} \equiv 64^8 \cdot 4 \equiv 15^8 \cdot 4 \equiv 225^4 \cdot 4 \equiv 29^4 \cdot 4 \equiv (-20)^4 \cdot 4 \equiv (400^2) \cdot 4 \equiv 8^2 \cdot 4 \equiv 11 \ mod \ 49$
Ответ:11

(2) $a^n \equiv 1 \ mod \ m, a^k \equiv 1 \ mod \ m, (a, m) = 1$, доказать, что $a^{(n,k)} \equiv 1 \ mod \ m,$ причем $Ord_m|(n, k)$
Д-во:
$a^n \equiv 1 \ mod \ m, a^k \equiv 1 \ mod \ m \Rightarrow Ord_m(a)|n, Ord_m(a)|k \Rightarrow n = ord \cdot l_1, k = ord \cdot l_2, \ l_1, l_2 \in Z \Rightarrow\Rightarrow Ord_m(a)|(n, k) \Rightarrow a^{(n,k)} \equiv 1 \ mod \ m$. Что и требовалось доказать.

(3) 1) $\Rightarrow$:
Пусть все p_i различны, $(p_1^{k_1}...p_n^{k_n}) = 1$ и $(a_1, ..., a_n)^l = e$,тогда $a_i^l = e$ и l =НОК$(p_i^{k_i}) \Rightarrow |G_m| = l$. Действительно, очевидно, что прямое произведение $C_{p_1^{k_1}} \times C_{p_2^{k_2}} \times ... \times C_{p_n^{k_n}} \cong C_{p_1^{k_1} p_2^{k_2} ... p_n^{k_n}}$, порождающий элемент: $(a_1, a_2, ..., a_n)$, где a_i: порождающий элемент в группе $C_{p_i^{k_i}}$.
В обратную сторону:2) $\Leftarrow$
Группа циклическая, докажем, что все p_i различны.
Пусть $(p_i^{k_i}, p_j^{k_j}) = p > 1$, тогда НОК$(p_1^{k_1}...p_i^{k_i}...p_j^{k_j}..p_n^{k_n}) < |C_m|$, то есть в группе $C_{p_1^{k_1}} \times C_{p_2^{k_2}} \times ... \times C_{p_n^{k_n}}$ не будет элемента порядка $m = (p_1^{k_1}...p_n^{k_n}) = |C_{p_1^{k_1} p_2^{k_2} ... p_n^{k_n}}|$. Следовательно, группа не будет являться циклической. Что и требовалось доказать.

(4) Доказать, что пересечение подгрупп взаимопростых порядков тривиально (содержит только e).
Д - во:
Пусть $|H_1| = m, |H_2| = n, (n, m) = 1$. Предположим, что $H_1 \cap H_2$ не тривиально, т.е $\exists \ h \neq e \hookrightarrow H_1 \cap H_2$ Тогда $h \cdot h \in H_1 \cap H_2$.Так как подгруппы конечные: $\exists k \in Z \hookrightarrow h^k = e$.Но $H_1 \cap H_2 < H_1$ и $H_1 \cap H_2 < H_2$, а так как порядок подгруппы делит порядок группы:$k|m, k|n$.Противоречие, так как по условию $(m, n) = 1$.Из этого следует, что $H_1 \cap H_2$ содержит только e.

(5) Может ли в коммутативной группе быть 14 решений уравнения $x^{12} = e$?
Покажем, что все решения уравнения составляют подгруппу $(H = (a|a^{12} = e))$:
1) $a^{12}b^{12} = e = a...a \cdot b...b =$ (по св-ву коммутативности) $= (ab)^{12} \Rightarrow$множество решений замкнуто относительно групповой операции.
2) $(a \cdot a^{-1})^12 = e = a^{12} \cdot (a^{-1})^{12} = e = (a^{-1})^{12} \Rightarrow \forall \ a \in H \exists \ a^{-1} \in H \hookrightarrow a^{-1}a = aa^{-1} = e$
3)Очевидно, что ассоциативность выполняется.
Следовательно, H - подгруппа коммутативной группы, то есть H также является подгруппой.По теореме о конечнопорожденных абелевых группах любая абелева группа может быть представлена как прямое произведение простых циклических групп: $H_14 \cong C_2 \times C_7$. В группе есть элементы порядка 1, 2, 7, 14. Но $(12, 7) = 1$, следовательно получаем противоречие, то есть в коммутативной группе не может быть 14 решений данного уравнения.

(6) (a) $C_{100} \times C_{10} \times C_1 \cong C_{25} \times C_4 \times C_2 \times C_5$
$C_{50} \times C_{20} \cong C_{25} \times C_2 \times C_4 \times C_5$
Из разложений видно, что группы изоморфны.

(b) $C_6 \times C_{18} \times C_{100} \times C_{36} \times C_{40} \cong C_3 \times C_2 \times C_9 \times C_2 \times C_{25} \times C_4 \times C_9 \times C_4 \times C_8 \times C_5$
$C_{60} \times C_{36} \times C_{36} \times C_{200} \cong C_8 \times C_{25} \times C_9 \times C_4 \times C_4 \times C_9 \times C_4 \times C_3 \times C_5 \times C_4$
Из разложений видно, что группы не изоморфны.
Ответ:a) да, b) нет.

(7) (a) Пусть G - абелева группа, докажем, что любая ее подгруппа нормальная.
Пусть $H < G$.H - нормальная подгруппа, если $\forall \ a \in G \hookrightarrow Ha = aH$.
Очевидно, что $\forall a \in G, h \in H \hookrightarrow ah = ha$, так как h тоже лежит в группе G. То есть левый и правый смежные классы по подгруппе H совпадают, следовательно, она нормальная.

(b) Индекс группы G по подгруппе H равен 2. Следовательно, группа разбивается на 2 левых смежных класса :H и $xH, x \in G$.С другой стороны, группа по подгруппе H разбивается тоже на 2 смежных класса:H и Hx. В обоих случаях, все элементы группы разбиваются на 2 класса: элементы подгруппы H и все остальные. Из сделенного вывода, следует, что $xH = Hx$.То есть подгруппа индекса 2 всегда нормальная.

(8) (a) Перестановки делятся на 2 класса: четные и нечетные. Докажем, что количесвто четных перестановок в группе S_n равно количеству нечетных.($|A_n| = |S_n/A_n|$)
Для этого построим взаимооднозначное соответствие между множествами. Построим следующее отображение $\varphi : A_n \to S_n/A_n$.Пусть $\pi^+ \in A_n, \varphi(\pi^+) = \pi^+ \cdot \alpha, \alpha$ - транспозиция. Так как любая транспозиция меняет четность перестановки, тогда $\pi^+ \cdot \alpha = \pi^-, \pi^- \in S_n/A_n$. Тогда $\forall\ \pi^+ \in A_n \exists\ \pi^- \hookrightarrow \varphi(\pi^+) = \pi^+ \cdot \alpha = \pi^-$. Также справедливо обратное: домножем выражение на обратную транспозицию: $pi^+ \cdot \alpha \cdot \alpha^{-1} = \pi^+ = \pi^- \cdot \alpha^{-1} \Rightarrow \forall\ \pi^- \in S_n/A_n \exists\ \pi^+ \in A_n \hookrightarrow pi^- = \varphi(\pi^+)$. Построили биекцию, следовательно множества равномощны.$|S_n| = n!$, тогда $|A_n| = \frac{n!}{2}$. Левые смежные классы по этой подгруппе: $x \cdot A_n = (x \cdot \pi | x \in S_n/A_n, \pi \in A_n) \Rightarrow$ 2 смежных класса: класс четных перестановок(сама подгруппа) и класс нечетных.

(b) Четность перестановки определяется количеством транспозиций, на которые может быть разложена данная перестановка.(четное число транспозиций - четная, нечетное - нечестная).Из этого можно сделать вывод, что композиция любых нечетных и четных перестановок будет нечетной перестановкой, так как $(l + k) \equiv 1\ mod\ 2$, l - число транспозиций в разложении четной перестановки, k - в разложении нечетной перестановки. Получается, индекс группы S_n по подгруппе A_n равен 2, потому что группа разбивается на 2 класса: четные перестановки (сама подгруппа A_n) и нечетные перестановки.В пункте 7) доказано, что любая подгруппа индекса 2 всегда нормальная. Что и требовалось доказать.

(9) (a) $Z < (R, +)$
Очевидно, что подгруппа нормальная, так как групп действительных чисел по сложению коммутативнаб то есть: $\forall a \in R \hookrightarrow a + Z = Z + a$.
Фактор-группа - группа, составленная из классов смежности по данной подгруппе. Каждому классу смежности мы можем поставить в соответвие число $z \in T, T = (z||z| = 1)$.То есть можем построить следующую биекцию:$f : R/Z \to T, f(r+Z) = \cos 2\pi r + i \sin 2\pi r$.Фактор-группа действительных чисел по сложению по подгруппе елых чисел изоморфна мультипликативной группе комплексных чисел, модуль которых равен 1.

(b) Очевидно, что группа нормальная, так как операция сложения коммутативна.Каждому вектору ставим в соответствие пару чисел x и y - координаты по осям Ox и Oy соответственно.Тогда для векторов параллельных оси $Ox : (x', 0), x' \in R$. Смежные классы по данной подгруппе: $(x_0, y_0) + h = h + (x_0, y_0) = (x_0 + x, y_0)$.То есть к одному смежному классу принадлежат векторы, координаты которых по оси x совпадают, а по оси Oy принимают все действительные значения. Тогда каждому классу смежности можем поставить в соответствие действительное число y_0.Таким образом мы получили взаимооднозначное соответствие между фактор-группой $(R^2; +)$ по подгруппе векторов, параллельных оси Ox и группой $(R, +)$,которое сохраняет операцию: $\varphi(x + x_0, y_0) = y_0, \varphi((x_0, y_0) + (x, 0)) = \varphi(x_0, y_0) + \varphi(x, 0) = y_0 = \varphi(x + x_0, y_0)$

(c) $R < (C/0, \cdot)$
Очевидно, что подгруппа нормальная, так как группа $(C/0, *)$ коммутативная: $\forall a + bi, c + di \in C \hookrightarrow (a + bi)(c + di) = (c + di)(a + bi)$.Смежные классы по данной подгруппе:$xH = xh | h \in R$.Представим комплексные числа на комплексной плоскости: $|c|(\cos\varphi + \sin\varphi \cdot i)$. При домножении на действительное число h, угол поворота не меняется, меняет модуль числа в h раз.Получается, к одному классу смежности относятся векторы с одинаковым углом наклона, проходящие через начала координат, модули которых принимают все действительные значения.Тогда каждому смежному классу можем поставить в соответствие комплексное число, модуль которго равен 1, а угол равен углу комплексных чисел, принадлежащих данному классу смежности, то есть:
$f : (c/0, \cdot)/R \to T, c = |c|(\cos\varphi + i\sin\varphi), f(c \cdot R) = \cos\varphi + i\sin\varphi$.Данное отображение сохраняет операцию: $f((c \cdot r_1) \cdot (c \cdot r_2)) = \cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2) = (\cos\varphi_1 + i\sin\varphi_1)(\cos\varphi_2 + i\sin\varphi_2) = f(c \cdot r_1) \cdot f(c \cdot r_2)$. Получаем, что фактор-группа $(C/0, \cdot)/R$ изоморфна мультипликативной группе комплексных чисел, модуль которых равен 1.

(d) Аддитивная группа действительнозначных функций $f : [0, 1] \to R$ по подгруппе функций, таких, что $f(0) = f(1) = 0$.
Подгруппа нормальная, так как группа коммутативна: $\forall f_1, f_2 \in G \hookrightarrow f_1 + f_2 = f_2 + f_1$
$f + F = F + f, f \in G, F < G$, тогда в точках 0 и 1 :$f + 0 = f$, то есть значению функции в данной точке.Следовательно, можем построить следующую биекцию: $\varphi(f(0) + F(0)) = f(0), \varphi(f(1) + F(1)) = f(1)$, тогда каждому смежному классу данной группы по подгруппе F ставим в соответсвие пару точек $(f(0), f(1))$ - значения функции в данной точке.$\varphi((f_1(0) + F(0)) + (f_2(0) + F(0)) = \varphi(f_1(0)) + \varphi(f_2(0)) = f_1(0) + f_2(0) \Rightarrow$отображение сохраняет операцию.Фактор-группа изоморфна группе $(R^2, +)$.

(10) (a) Каждая перестановка может быть представлена в виде произведения простых (непересекающихся) циклов. Пусть есть перестановка $\pi = (i_1 ... i_l)$. Очевидно, что порядок $Ord(\pi) = l$.Тогда очевидно, что порядок перестановки, состоящей из нескольких простых циклов, равен НОК длины этих циклов. Действительно, НОК длины циклов - наименьшее необходимое количество композиций перестановки с собой, дающее тривиальную перестановку. Что и требовалось доказать.

(b) $\begin{pmatrix} 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10 \\ 2\ 1\ 3\ 6\ 4\ 7\ 5\ 10\ 8\ 9 \end{pmatrix} = (1\ 2)(3)(6\ 7\ 5\ 4)(8\ 10\ 9)$
НОК$(2,4,3) = 12 \Rightarrow Ord(\pi) = 12$
Четность:$(10-4) \equiv 0\ mod\ 2 \Rightarrow$перестановка четная.

(c) $i \in [0, n-1] \Rightarrow i < n \Rightarrow (i+k)\ mod n = i + (k\ mod\ n)$
То есть в результате перестановки каждый элемент сдвинется на равное количство мест.Пусть $k = zn + s, z, s \in Z, n > s > 0$, тогда перестановку можно представить в виде $(1...n)^{k\ mod\ n} = (1...n)^s = (1...n)^{zn+s} = (1...n)^k$.
Очевидно, что порядок такой перестановки: $Ord(\pi) = (n, k\ mod\ n)$, исходя из алгоритма Евклида:$(n, k\ mod\ n) = (k, n) \Rightarrow Ord(\pi) = \frac{n}{(k,n)}$. Такую перестановку можно представить как композицию $k\ mod\ n$ циклов длины n. Каждый из циклов можно представить в виде $(n-1)$ транспозиции. Получаем $k\ mod\ n \cdot (n-1)$ транспозицию. Если n - нечетное, то перестановка четная.Если n - четное, $k \equiv zn + s \equiv s\ mod\ 2 \Rightarrow k\ mod\ n$ и k дают одинаковые остатки при делении на 2, если n четное. В результате получаем:если n - нечетное - перестановка четная, если n - четное, при четном k перестановка четная, при нечетном - нечетная.

(11) (a) $Ord(\pi) = 8 \Rightarrow$НОК длины простых циклов, на которые расскладывется перестановка = 8. Но минимальное количество элементов, необходимых для того, чтобы НОК был равен 8 это 8. А элементов всего 5 $\Rightarrow$в группе нет элемента порядка 8.

(b) $Ord(\pi) = 60 \Rightarrow$НОК = 60. Минимальное количество элементов, необходимых, чтобы НОК = 60 это 12 (простые циклы длины $3, 4, 5; 3 + 4 + 5 = 12$, но в перестановке может быть только 11 элементов.Ответ: нет.

(12) (a) Любую перестановку можно разложить на простые циклы, а любой цикл на транспозиции. Следовательно, любую перестановку можно представить в виде композиции транспозиций, поэтому перестановка S_n порождается множеством транспозиций $(1, i), i \in [1, n]$

(b) $(i, j, k) = (i, k)(i, j) \Rightarrow$ любой цикл вида (i, j, k) раскладывается в четное число транспозиций. А так как в разложении четной перестановки по транспозициям транспозиций четное число, то обЪеденив 2 транспозиции, получаем цикл длины 3. Следовательно, множество четных перестановок A_n порождается множеством циклов вида (i, j, k).

(13) Порождают ли перестановки порядка p группу S_p?
Порядок перестановки $p \Rightarrow$ НОК длин простых циклов, на которые раскладывается перестановка - p. Но так как p простое - такие перестановки будут состоять только из цикла длины p.Каждый тако цикл можно представить в виде $(p-1)$ транспозиции.$2|(p-1)$. То есть из циклов длины p мы получим только четные перестановки, следовательно множество перестановок порядка p на порождает группу перестановок S_p.