Филиппова Анастасия

Домашнее задание 2

(1) 1)Ассоциативность очевидна:
$\forall\ a,b,c \in Z_m^* \hookrightarrow (ab\ mod\ m)\cdot c)\ mod\ m = (a\cdot(cb\ mod\ m))\ mod\ m$
2) Существование обратного:
$\forall\ a \in Z_m^*\ \exists\ a^{-1} \hookrightarrow aa^{-1} = e$
$ax \equiv 1\ mod\ m$(из 1-го домашнего задания доказано, что есть целые решения тогда и только тогда, когда $(a,m) = 1$.А так как по условию это верно$\Rightarrow$ для каждого a существует обратный.
3)Нейтральный элемент:
$\exists\ e = 1:\ \forall\ a \in Z_m* \hookrightarrow a \cdot e = a$
Z_m^* - группа.

(2) $(R;+)$ - коммутативная, но не является циклической.
Предположим противное: является иклической, следовательно, так как бесконечная, изоморфна группе целых чисел по сложению.Но это не так, ведь множество целых чисел счетно, а множество рациональных нет, значит не можем задать взаимооднозначное соответствие.

(3) $H = (h|h \in G)$
$\forall\ h_1,h_2 \in H, h_1h_2 \in H$ Является ли H подгруппой G?
Множество замкнуто относительно группово операции, поэтому можем представить все элементы, как $a, a^2...a^k...$, так как конечно, в какой-то момент $a^m = a^k$(то есть мы попадем в уже полученный элемент).Тогда отсюда следует,что $a^{m-k} = e$, отсюда следует, что в множестве лежит групповая единица.Но тогда $a^l \cdot a^{(m-k-l)} = e, m,k,l \in Z$.Из этого следует существование обратного.Получаем, что конечное замкнутое множество относительно групповой операции является подгруппой.

(4) Доказать, что группа простого порядка всегда циклическая.
$|G| = p$, p простое. Порядок любого элемента группы делит порядок группы. Получается, что в группе G единичный элемент порядка 1 (групповая единица) и $p-1$ элементов порядка p.$\forall\ a \in G \hookrightarrow a^p = e$
Пусть $b \in H,\ b^p = e = a^p \Rightarrow b = a^m, m \in Z$
Очевидно, что группа является циклической, так как существует порождающий элемент.

(5)
(a) В группе вращений $2n$- угольника $2n$ элементов:$2n-1$ поворот и 1 тождественное преобразование.Теперь рассмотрим группу симметрий n-угольника. Если n - четное, то оси симметрии будут проходить через середины противоположных сторон и через противолежащие вершины.Получаем n осей.Если n нечетное, то оси симметрии проходят через вершину и середину противолежащей стороны, тоже получаем n осей симметрии.Занумеруем вершины от 0 до n - 1.Далее каждому элементу (повороту относительно осей симметрии или вращению) из группы симметрий n-угольника будем ставить в соответствие различные элементы из группы вращени $2n$-угольника.Множества равномощны, мы получим взаимооднозначное соответствие.Группы изоморфны.
(b) $C_{18} \times C_2 \cong C_{36}$?
$C_{18} \times C_2 \cong C_9 \times C_2 \times C_2$
$C_{36} \cong C_9 \times C_4$, группы не изоморфны по спектральному признаку: в группе C_{36} будет элемент порядка 12, как НОК элементов порядка 3 и 4, а в группе $C_{18} \times C_2$ нет элемента такого порядка.
(c) Нумеруем вершины треугольника и строим биекцию между группой симметрий и группой перестановок S_3. Тождественная перестановка соответсвует 3-м поворотам вокруг оси C_3, перестановка $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ - одному, $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ - двум. Транспозиции $(12),(23),(13)$ - повороту относительно одной из осей, проходящих через вершину треугольника и центр противолежащей стороны.К примеру, транспозиция (12) меняет местами 1 и 2 вершины.Мы получили биекцию.Группы изоморфны.
(d) Контр-пример: $C_4 \times C_2$ и C_8
Группы не изоморфны по спектральному признаку: в группе C_8 есть элемент порядка 8, а в группе $C_4 \times C_2$ нет, так порядок не выше 4(НОК 4 и 2).
(e) $C_{12} \times C_{45} \cong C_3 \times C_4 \times C_9 \times C_5$
$C_{15} \times C_{36} \cong C_3 \times C_5 \times C_9 \times C_4$
По мощностному признаку группы изоморфны.

(6)
(a) $\varphi(n)$ - функция равная количеству натуральных чисел, меньших либо равных n и взаимопростых с ним.
$\varphi(1) = 1$ - полагают равной 1.
$\varphi(2) = 1$, (2), $\varphi(3) = 2, (2,3)$, $\varphi(4) = 2, (3,4)$, $\varphi(6) = 2, (4,5)$
(b) Если p - простое, то среди чисел от 0 до p^k, p^{k-1} чисел, которые не взаимопросты с p^k (числа вида mp, где $m \in Z, 1 <= m <= p^{k-1}$)
Получаем, $\varphi(p^k) = p^k - p^{k-1}$

(c) Доказать: $\varphi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})...(1 - \frac{1}{p_n})$
Сначала найдем все числа, кратные $p_i, i \in [1, n]$.Для этого рассмотрим ряд чисел от 1 до n.Выделим из этого ряда только числа кратные p_i: $p_i ... \frac{n}{p_i} \cdot p_i$ - $\frac{n}{p_i}$ чисел.
Числа кратные p_i и p_j: из ряда чисел $p_i ... \frac{n}{p_i}$ вычеркнем числа, кратные p_j (вида kp_2, где k - целое).Получаем $\frac{n}{p_j \cdot p_i}$ чисел.Также действуем для 3-х и большего количества.
E_i - множество чисел меньших либо равных n, кратных $p_i,\ i \in [1, t]$.$|E_i \cap E_j \cap E_k = \frac{n}{p_j \cdot p_i^{\cdot} p_k}$, По формуле включений и исключений:
E_i - множество чисел меньших либо равных n, кратных $p_i,\ i \in [1, t]$.
$\varphi(n) = n - |E_1 \cup E_2 \cup ... \cup E_t| = n - \sum\limits_{i=1}^{t} |E_i| + \sum\limits_{i<j} |E_i \cap E_j| + \sum\limits_{i<j<k} |E_i \cap E_j \cap E_k| - ...(-1)^t |E_i \cap E_j \cap E_k \cap ... \cap E_t| = n - \sum\limits_{i=1}^{t} \frac{n}{p_i} + \sum\limits_{i<j} \frac{n}{p_j \cdot p_i} - \sum\limits_{i<j<k} \frac{n}{p_j \cdot p_i^{\cdot} p_k} ...(-1)^t \frac{n}{p_i p_j p_k ... p_t} = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})...(1 - \frac{1}{p_n})$, что и требовалось доказать

(d) Доказать, что $\varphi(mn) = \varphi(n) \cdot \varphi(m), (m, n) = 1$
Чтобы числа были взаимопростые с mn необходимо и достаточно, чтобы они были взаимопростые с m и с n, так как $(m, n) = 1$. Число, взаимопростое с m представим в виде: $mq + r, q \in Z_+, r \in N$.Очевидно, что $(m, r) = 1$, тогда получаем, что число возможных остатков равно $\varphi(m)$.Зафиксируем произвольный остаток r_1 и посмотрим, какие значения может принимать целая часть q.Числа взаимопростые с n представимы в виде: $m+r_1, 2m+r_1 ... (n-1)m+r_1$.Получаем, что при фиксированном остатке количество чисел: $\varphi(n)$. Получаем, что всего чисел взаимопростых с mn и меньших либо равных mn:$\varphi(mn) = \varphi(m) \cdot \varphi(n)$, что и требовалось доказать.

(7) (a) Сколько элементов порядка k в циклической группе C_n, если $k|n$?
Пусть a - порождающий элемент группы.Пусть $b \in C_n, b^k = e, \exists\ m \in Z : b = a^m$
$b^k = a^{mk} = e \Rightarrow nq = mk, q \in Z$.Какие числа q подходят?
Порядок элемента делит порядок группы, следовательно, в группе будут элементы, порядок которых - делитель n. Предположим, что $(q, k) \neq 1$, тогда $mlu = lny, l, u, y \in Z$, тогда $mu = ny$.Получаетмя, k - не минимальная степень, то есть порядок элемента не k, противоречие, то есть $(q, k) = 1$.Если $q > k, (q, k) = 1 : mk = n(jk + h)$, h - остаток, поэтому $0 < h < k$, а так как $(q, k) = 1 \Rightarrow (h, k) = 1, j, h \in Z$.Получаем: $b = a^{nj} a^{hn/k} = a^{hn/k}$.Но тогда $b^k = a^{hn}$, и $h < k$, то есть мы попали в уже разобранный выше случай.
Получаем, что число подходящих q: числа меньшие либо равные k взаимопростые с ним, то есть $\varphi(k)$.

(b) Доказательство пункта b следует из пнкта a: порядок элемента делит порядок группы, следовательно в группе C_n будут элементы порядков, которые являются делителями числа n. При этом количество элементов порядка $d : \varphi(d)$. Получаем, $\sum \varphi(d) = n$.Что и требовалось доказать.

(8) Пусть C_n - циклическая группа из n элементов,a - порождающий элемент.Каждый элемен $b \in C_n$ порождает подгруппу $< b >$ порядка $ord(b)$.В подгруппе циклической группы порядка n число элементов может быть равно делителю числа n, так как порядок подгруппы делит порядок группы.В циклической группе есть ровно одна подгруппа порядка $ord(b)$, так как подгруппа будет одназначно задаваться числом элементов, то есть элементы группы одного порядка порождают эквивалентные подгруппы.Получается, количество подгрупп циклическо группы $C_n :< e >, < a^k >$, где k - делитель n.Количество подгрупп - количество делителей.

(9) Пусть G - подгруппа $(Z, +), x \in (Z, +), c, d \in G\ a = x + c, b = x + d$. Не умаляя общности предположим, что $(a > b)$.
$-d \in G$ как обратный к d.Тогда $(c-d) \in G \Rightarrow (a-b) \in G$.Тогда числа вида $k(a-b) \in G, k \in Z$(применяем групповую операцию к числу $(a - b)$ при $k > 0$ и находим обратный элемент при $k < 0, 0 \in G$, так как это групповая единица.
Ответ:числа вида $k(a - b), k \in Z$.

(10) Чтобы левы и правый смежный класс совпадали необходимо :$gH = Hg$, $H = ((), (12))$.Очевидно, что $\forall a \in S_3 : a \cdot () = () \cdot a$, проверим для транспозиции (12).
$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \xrightarrow{(12)} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$
$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \xrightarrow{(231)} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$
Получаем: $(231)(12) = (12)(231)$.
Аналогично проверяем остальные случаи и получаем:$(13)(12) = (12)(13), (23)(12) = (12)(23), (123)(12) = (12)(123), (321)(12) = (12)(321)$.Правый и левый смежные классы совпадают.