Основные задачи

Задача 1

Условие: Корни уравнения $x^n = 1$, как действительные, так и комплексные, называются корнями n-й степени из единицы. Проверить, что корни n-й степени образуют группу по умножению. (а) Верно ли, что всякий корень 35-й степени из единицы является кубом некоторого корня 35-й степени из единицы? (б) Тот же вопрос про корни 36-й степени из единицы.

Пусть $X_n = \{\, x \mid x^n = 1 \,\}$. Проверим, является ли X_n группой по умножению. Для этого проверим выполнение аксиом группы:
1. *Ассоциативность.*
Если $x_1^n = 1$, $x_2^n = 1$, $x_3^n = 1$, то очевидно $(x_1^n x_2^n)x_3^n = x_1^n(x_2x_3)^n = (x_1x_2x_3)^n = 1$.
2. *Аксиома единицы.*
$\exists\ e = 1 \in X_n\ \forall x \in X_n : x * \boldsymbol{e} = \boldsymbol{e} * x = x$
3. *Обратный элемент.*
Если $x_1^n = 1$, то $\dfrac{1}{x_1^n} = \left(\dfrac{1}{x_1}\right)^n = 1$. Значит, для x_i обратным элементом является $\dfrac{1}{x_i}$.
4. *Коммутативность.*
Если $x_1^n = 1$, $x_2^n = 1$, то $(x_1x_2)^n = (x_2x_1)^n = 1$.
Итак, выполнены аксиомы группы, а также свойство коммуникативности. Значит,
X_n — **абелева группа**.

а) $x^{35} = 1$
Решения этого уравнения: $x_k = \boldsymbol{e}^{i\varphi}$, где $\varphi = \frac{2\pi k}{35}, k = 0, 1, \ldots, 34$.
Положим, $x_k = x_m^3$. Тогда $\boldsymbol{e}^{\frac{2i\pi k}{35}} = (\boldsymbol{e}^{\frac{2i\pi m}{35}})^3 = \boldsymbol{e}^{\frac{6\pi m}{35}} = 1 \Rightarrow \boldsymbol{e}^{\frac{2i\pi(3m-k)}{35}} = 1 \Rightarrow$
$3m - k = 35p, p \in \mathbb{Z}$
Значит, $(35p + k) \vdots 3$.
1) $p = 3s \Rightarrow k = 3l$.
2) $p = 3s + 1 \Rightarrow k = 3l + 1$.
3) $p = 3s + 2 \Rightarrow k = 3l + 2$.
То есть k может принимать любые значения от 0 до 34. А значит, всякий корень уравнения $x^{35} = 1$ является кубом для некоторого другого корня этого уравнения.

Ответ: верно.

б) $x^{36} = 1$
Положим, $x_k = x_m^3$. Тогда $\boldsymbol{e}^{\frac{2i\pi k}{36}} = (\boldsymbol{e}^{\frac{2i\pi m}{36}})^3 = \boldsymbol{e}^{\frac{6\pi m}{36}} = 1 \Rightarrow \boldsymbol{e}^{\frac{2i\pi(3m-k)}{36}} = 1 \Rightarrow$
$3m - k = 6p, p \in \mathbb{Z}$
Откуда получим, что $k = 3l$. А значит, не все корни уравнения $x^{36} = 1$ являются кубами некоторого другого корня этого уравнения.

Ответ: неверно.

Задача 2

Условие: C_{360} — цикличекая группа порядка 360. Найти число решений уравнения $x^k = \boldsymbol{e}$ и количество элементов порядка k в группе C_{360} при а) $k = 7$; б) $k = 12$; в) $k = 48$. Сколько в C_{360} порождающих элементов?

а) Порядок элемента — делитель порядка группы, а значит элементов порядка 7 нет. $(7, 360) = 1$, значит уравнение $x^7 = \boldsymbol{e}$ имеет единственное решение: $x = \boldsymbol{e}$.

б) Количество элементов порядка 12 равно: $\varphi(12) = 4$. Т. к. $x^{12} = (x^2)^6 = (x^3)^4 = (x^4)^3 = (x^6)^2$, то количество решений уравнения $x^{12} = \boldsymbol{e}$ равно количеству элементов порядка 1, 2, 3, 4, 6, 12. Тогда число решений равно $1 + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12) = 12$.

в) Количество элементов порядка 48 равно 0, т. к. 360 не делится на 48. Аналогично пункту б) количество решений уравнения $x^{48} = \boldsymbol{e}$ равно:
$1 + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(8) + \varphi(12) + \varphi(24) = 24$.

Количество порождающих элементов — количество элементов порядка 360:
$\varphi(360) = \varphi(72) \cdot \varphi(5) = \varphi(8) \cdot \varphi(9) \cdot \varphi(5) = 96$.

Ответ: а) 1; б) 12; в) 24; порождающих элементов 96.

Задача 3

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ

Задача 4

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ

Задача 5

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ

Задача 6

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ

Задача 7

Условие: Порождают ли перестановки порядка 11 группу S_{11}?

Как известно, любая перестановка разбиватся на циклы. Если это циклы длин $a_1, a_2, \ldots, a_k$, то порядком перестановки будет $(a_1, a_2, \ldots, a_k)$. Отсюда следует, что элементы порядка 11 в S_{11} - это циклы длины 11. Каждый такой цикл представляется в виде 10 композиций: цикл $(b_1, b_2, \ldots, b_{11})$ представляется как $(b_1, b_2) \circ (b_2, b_3) \circ \ldots \circ (b_{10}, b_{11})$. Таким образом, данные перестановки порождают лишь перестановки, выражающиеся четным количеством транспозиций, и, например, траспозиция $(1, 2)$ не может быть получена.

Ответ: не порождают.

Задача 8

Условие: Построить некоммутативную группу группу минимального порядка.

Рассмотрим различные значения порядков.

$n = 1$: Очевидно, что это группа из одной единицы. Такая группа абелева.

$n = 2$: Пусть a — элемент группы. Тогда $a * \boldsymbol{e} = \boldsymbol{e} * a = \boldsymbol{e}$ и получаем, что группа абелева.

$n = 3$: Пусть $G = \{\boldsymbol{e}, a, b\}$. Чтобы доказать что группа абелева достаточно показать что $a * b = b * a$. Посмотрим чему может быть равно $a * b$. Если $a * b = a$, то $b = \boldsymbol{e}$. Аналогично, если $a * b = b$, то $a = \boldsymbol{e}$. Получаем, что $a * b = \boldsymbol{e}$. Аналогично, $b * a = \boldsymbol{e}$ и группа абелева.

$n = 4$: Пусть $G = \{\boldsymbol{e}, a, b, c\}$. Посмотрим чему может быть равен порядок элементов. Порядок элемента должен делить порядок группы, то есть он равен или 2 или 4. Если порядок равен 4 (порядку группы), то группа циклическая, а этот элемент — порождающий. Циклическая группа является абелевой. Порядок равный единице означает, что элемент равен $\boldsymbol{e}$. Получаем, что порядок любого элемента равен 2. Тогда

$$(ab)^2 = \boldsymbol{e} \Rightarrow (ab)(ab) = \boldsymbol{e}$$
$$(ab)(ba) = ab^2a = a^2 = \boldsymbol{e} = (ab)(ab) \Rightarrow$$
$$(ab)(ba) = (ab)(ab) \Rightarrow ab = ba$$

Получили, что группа абелева.

$n = 5$: Порядок элемента делит порядок группы, то есть порядок элемента в группе порядка 5 может быть равен только 5, что означает, что группа всегда циклическая и абелева.

$n = 6$: Пример группы из 6 элементов это S_3. (Число элементов равно $3! = 6$)

Ответ: S_3

Задача 9

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ

Задача 10

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ

Задача 11

Условие: Доказать, что группа вращений трехмерного куба изоморфна группе S_4.

Каждому вращению куба соответствует перестановка его четырех диагоналей. Композиции вращений соответствует композиция перестановок. Разным вращениям a и b соответствуют различные перестановки, т. к. в ином случае нетождественному вращению ab^{-1} соответствовала бы тождественная перестановка. Каждой перестановке соответствует только одно вращение.

Таким образом, установлен установлен изоморфизм вращения группе S_4.

Задача 12

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ

Задача 13

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ

Задача 14

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ

Задача 15

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ

Задача 16

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ

Задача 17

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ

Задача 18

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ

Задача 19

Условие: Является ли кольцом главных идеалов кольцо $\mathbb{Z}_{72}$?

Пусть I — произвольный идеал кольца R. Нужно доказать, что I имеет вид $n\mathbb{Z}_{72}$.

Если $I = \{0\}$, то $I = 0\mathbb{Z}_{72}$. Пусть $I \neq \{0\}$. Тогда пусть n — наименьший элемент из I.

$n\mathbb{Z} \subseteq I$ в силу определения идеала.

Пусть $a \in I$. Разделим a на n. $r = a - qn, r \in I$. Если $a \notin n\mathbb{Z}$, то $r > 0$ и $r < n$. Получаем противоречие (n — наименьший элемент идеала) и $a \in n\mathbb{Z}$. Значит $I = n\mathbb{Z}$, то есть все идеалы главные.

Ответ: является.

Задача 20

Условие: Решить диофантово уравнение: $33x + 23y = 4$.

$33x + 23y = 4$
$23(x + y) + 10x = 4$
Замена: $x + y = z$
$23z + 10x = 4$
$10(2z + x) + 3z = 4$
Замена: $2z + x = a$
$10a + 3z = 4$
$3(3a + z) + a = 4$
Замена: $3a + z = b$
$3b + a = 4$
Заметим, что $\begin{cases} 3b \equiv 0 \pmod 3 \\ 4 \equiv 1 \pmod 3 \end{cases} \implies a \equiv 1 \pmod 3$.
Откуда $\begin{cases} a = 3n + 1 \\ b = 1 - n \end{cases}$
Проведя ряд обратных замен, выразим x и y через n: $\begin{cases} x = 23n + 5 \\ y = -33n - 7 \end{cases}$, где $n \in \mathbb{Z}$

Ответ: $x = 23n - 5, y = -33n - 7, n \in \mathbb{Z}$.

Задача 21

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ

Задача 22

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ

Задача 23

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ

Задача 24

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ

Задача 25

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ

Задача 26

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ

Задача 27

Условие: Многочлен $f(x)$ над полем F_5 степени 2 принимает значение 1 в точке 1, значение 2 в точке 3 и значение 3 в точке 4. Найти $f(x)$.

$f(x) = ax^2 + bx + c, \quad a, b, c \in F_5$

$x = 1: \quad a + b + c \equiv 1 \pmod 5;$

$x = 3: \quad 9a + 3b + c \equiv 2 \pmod 5;$

$x = 4: \quad 16a + 4b + c \equiv 3 \pmod 5;$

$$\begin{cases} a+b+c \equiv 1 \pmod 5; \\ 9a+3b+c \equiv 2 \pmod 5; \\ 16a+4b+c \equiv 3 \pmod 5. \end{cases} \Leftrightarrow \begin{cases} a+b+c \equiv 1 \pmod 5; \\ 9a+3b+c \equiv 2 \pmod 5; \\ 7a+b \equiv 1 \pmod 5. \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} a+b+c \equiv 1 \pmod 5; \\ a+b \equiv 0 \pmod 5; \\ 7a+b \equiv 1 \pmod 5. \end{cases} \Leftrightarrow \begin{cases} c \equiv 1 \pmod 5; \\ a+b \equiv 0 \pmod 5; \\ 6a \equiv 1 \pmod 5. \end{cases} \Leftrightarrow \begin{cases} a = 1; \\ b = 4; \\ c = 1. \end{cases}$$

Ответ: 1, 4, 1.

Задача 28

Условие: а) Найти сумму всех квадратичных вычетов по модулю 73. б) Найти произведение всех квадратичных невычетов по модулю 103.

а) По Малой теореме Ферма любой элемент группы является решением уравнения $x^{72} = 1$.
$(x^{72} - 1 = 0) \Rightarrow (x^{36} - 1)(x^{36} + 1) = 0$

Заметим, что все квадратичные вычеты удовлетворяют уравнению $x^{36} - 1 = 0$, т. к. если a — квадратичный вычет, то $a = x^2$, где x — элемент группы. Тогда все корни, которые содержатся в первой скобке уравнения — квадратичные вычеты. Докажем что все кв. вычеты являются корнями уравнения $x^{36} - 1 = 0$. Для этого покажем, что квадратичных вычетов по модулю 73 ровно 36 (не считая 0).

Рассмотрим всевозможные остатки по модулю 73. Очевидно, что элементы a и $(-a)$ образуют один квадратичный вычет. Тогда всего квадратичных вычетов не больше чем $(73 - 1)/2 = 36$. Но их хотя бы 36, а значит их ровно 36. Тогда все корни, которые содержатся в первой скобке — квадратичные вычеты, все корни второй скобки — квадратичные невычеты. Тогда по теореме Виета сумма квадратичных вычетов равна 0.

б) Из пункта а) следует, что все квадратичные невычеты содержатся во второй скобке, а их произведение по теореме Виета равно (-1).

Ответ: а) 1; б) -1.

Задача 29

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ

Задача 30

Условие: Решить уравнение $1 + x + x^2 + \ldots + x^6 \equiv 0 \pmod{29}$.

$1 + x + x^2 + \ldots + x^6 \equiv 0 \pmod{29}$
$(1 + x + x^2 + \ldots + x^6)(1 - x) \equiv 0 \pmod{29}$
$1 - x^7 \equiv 0 \pmod{29}$
$x^7 \equiv 1 \pmod{29}$

Заметим, что $\forall x : x^{28} \equiv 1 \pmod{29}$, так что все вычеты 4 степени будут решениями. Их можно получить простым подсчетом: квадратичными вычетами будут числа 1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28. Вычетами 4 степени будут тогда все различные квадраты данных чисел — 1, 7, 16, 20, 23, 24, 25. Поскольку уравнение 7 степени — больше решений нет. Для изначального же уравнения 1 является посторонним корнем (это решение появилось в результате умножения на $1 - x$).

Ответ: 7, 16, 20, 23, 24, 25.

Задача 31

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ

Дополнительные задачи

Дополнительная задача 1

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ

Дополнительная задача 2

Условие: C_{360} — цикличекая группа порядка 360. Найти число решений уравнения $x^k = \boldsymbol{e}$ и количество элементов порядка k в группе C_{360} при а) $k = 7$; б) $k = 12$; в) $k = 48$. Сколько в C_{360} порождающих элементов?

Ответ: а) 1; б) 12; в) 24; порождающих элементов 96.

Дополнительная задача 3

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ

Дополнительная задача 4

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ

Дополнительная задача 5

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ

Дополнительная задача 6

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ

Дополнительная задача 7

Условие: Порождают ли перестановки порядка 11 группу S_{11}?

Ответ: не порождают.

Дополнительная задача 8

Условие: Построить некоммутативную группу группу минимального порядка.

Ответ: S_3

Дополнительная задача 9

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ

Дополнительная задача 10

Условие: Построить некоммутативную группу порядка 8, все подгрупы которой нормальны.

Всего 2 некоммутативных групп порядка 8. Рассмотрим группу симметрий четырехугольника D_4 и покажем что она удовлетворяет условию.

Таблица Кэли:

e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	e	a	a^2	a^3b	b	ab	a^2b
b	a^3b	a^2b	ab	e	a^3	a^2	a^2
ab	b	a^3b	a^2b	a^2	e	a^3	a^2
a^2b	ab	b	a^3b	a^2	a^2	e	a^3
a^3b	a^2b	ab	b	a^3	a^2	a^2	e

Очевидно, что группа не является абелевой. Рассмотрим возможные подгруппы этой группы.

Пусть порядок подгруппы равен 4. Тогда нужно выбрать 3 элемента (кроме единичного). Ни один из них не может содержать b, так как в этом случае при умножении на степень элемента без b получим все элементы, содержащие b. Тогда все элементы, содержащие b, должны быть в подгруппе, но элементов с b 4, а не единичных элементов подгруппы 3, поэтому существует только одна подгруппа порядка 4. $H_4 = \{\boldsymbol{e}, a, a^2, a^3\}$.

Теперь нужно построить смежные классы. Построить левый смежный класс означает, что мы должны взять элементы на пересечении первых четырех столбцов и одной строки. Для правого нужно взять 4 первых строки и 1 столбец. В силу симметрии таблицы строки и столбцы равнозначны, то есть левые и правые смежные классы совпадают, то есть H_4 — нормализатор.

Пусть теперь порядок подгруппы равен 2. Таких подгрупп 7. Проводя аналогичные рассуждения, получаем что подгруппы порядка 2 тоже нормализаторы.

Дополнительная задача 11

Условие: Доказать, что группа вращений трехмерного куба изоморфна группе S_4.

Ответ: А тут будет ответ

Дополнительная задача 12

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ

Дополнительная задача 13

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ

Дополнительная задача 14

Условие: Доказать, что если порядок абелевой группы G равен nm, где $(n, m) = 1$, то G изоморфна прямому произведению групп порядков n и m.

Требуется доказать, что в условиях теоремы G изоморфна прямому произведению некоторых групп. В качестве этих групп возьмем подгруппы G' и G'' группы G_{mn}. *Прямым произведением групп* G' и G'' называется множество, состоящее из всевозможных элементов вида (g'_1, g''_1). Заметим, что если в произведении $G'_n \times G''_m$ элементов меньше, чем mn, то построить изоморфизм G_{mn} и $G'_n \times G''_m$ невозможно.

Покажем, что в нашем случае $|G_{mn}| = |G'_n \times G''_m|$.

Пусть $G'_n = \{e, a_1 ... a_{n-1}\}$, $G''_m = \{e, b_1 .. b_{m-1}\}$. Запишем эти элементы в таблицу. На (i, j) месте этой таблицы стоит элемент (g'_i, g''_j) группы $G'_n \times G''_m$.

	$\boldsymbol{e}$	$\boldsymbol{a}$	$\boldsymbol{a}_2$	..	$\boldsymbol{a}_i$	..	$\boldsymbol{a}_{n-1}$
$\boldsymbol{e}$	(e, e)	(a, e)	(a_2, e)	..	(a_i, e)	..	(a_{n-1}, e)
$\boldsymbol{b}$	(e, b)	(a, b)	(a_2, b)	..	(a_i, b)	..	(a_{n-1}, b)
$\boldsymbol{b}_2$	(e, b_2)	(a, b_2)	(a_2, b_2)	..	(a_i, b_2)	..	(a_{n-1}, b_2)
..	..	..	..	..	..	..	..
$\boldsymbol{b}_j$	(e, b_j)	(a, b_j)	(a_2, b_j)	..	(a_i, b_j)	..	(a_{n-1}, b_j)
..	..	..	..	..	..	..	..
$\boldsymbol{b}_{m-1}$	(e, b_{m-1})	(a, b_{m-1})	(a^2, b_{m-1})	..	(a_i, b_{m-1})	..	(a_{n-1}, b_{m-1})

Предположим, что элемент $a_i \neq \boldsymbol{e}$ группы G'_n равен элементу $b_j \neq \boldsymbol{e}$ группы G''_m. Тогда, как видно из таблицы, в группе $G'_n \times G''_m$ будут повторяющиеся элементы, а значит, $|G'_n \times G''_m| < mn$. Однако, так как $a_i \in G^{'}_n$, порядок этого элемента делит n, с другой стороны $a_i = b_j \in G'_m$, а значит порядок этого элемента делит m. По условию $(n, m) = 1$, то есть порядок нашего элемента может быть равен только 1, что неверно. Получили противоречие $\Rightarrow$ в G''_m и G'_n нет равных элементов, кроме $\boldsymbol{e} \Rightarrow |G'_n \times G''_m| = |G_{mn}| = mn$.

Построим изоморфизм следующим образом: $(a_i, b_j) \in G'_n \times G''_m \longrightarrow a_i * b_j$, где $a_i, b_i \in G_{mn}$. При этом среди $a_i * b_j$ есть все элементы группы, отображение биективно и групповая операция сохраняется по свойствам прямого произведения: $(a_i, b_j) * (a_{i2}, b_{j2}) = (a_i * a_{i2}, b_j * b_{j2})$.

Таким образом мы доказали, что если порядок абелевой группы G равен nm, где $(n, m) = 1$, то G изоморфна прямому произведению групп порядков n и m, ч. т. д. ■

Дополнительная задача 15

Условие: Группа называется p-группой, если ее порядок является степенью простого числа p. Центром группы называется множество элементов, коммутирующих со всеми элементами группы. Доказать, что центр p-группы состоит не только из единичного элемента.

Пусть конечная группа G — нетривиальная p-группа, т. е. $|G| = p^n$ и ее центр Z состоит не только из единичного элемента. Множество $G \setminus Z$ разбивается на нетривиальные классы сопряженных элементов, число элементов в каждом из которых, согласно формуле $|C(x)| = \frac{|G|}{|Z(x)|}$, делится на p. Следовательно, число элементов центра также делится на p. Таким образом, центр p-группы состоит не только из единичного элемента.

Дополнительная задача 16

Условие: Доказать, что всякая группа порядка p^2 абелева.

Пусть G — группа порядка p^2, а Z — ее центр. Предположим тогда, что $Z \neq G$, что и будет означать существование неабелевой группы порядка p^2.

Покажем, что число элементов центра делится на p. Разобьем G на классы сопряженных элементов. Каждый из элементов центра образовывает класс из одного элемента, поскольку $a^{-1}z_i a = a^{-1}az_i = z_i$.

Каждый из элементов вне центра образует класс с количеством элементов, больше 1. Рассмотрим сопряжение как действие G на себя. Тогда для каждого $g \in G$ стабилизатором будет служить множество сопряжений $s^{-1}gs$ таких, что $gs = sg$. По лемме Бернсайда получаем, что $|C(x)| = \dfrac{|G|}{|Z(x)|}$, где $C(x)$ — орбита x относительно сопряжений, $Z(x)$ — стабилизатор по сопряжениям. Заметим, что количество элементов в классе совпадает с количеством элементов в орбите любого элемента по сопряжениям. Итак, для любого класса сопряженных элементов $|S_i| = |C(x)| = \dfrac{|G|}{|Z(x)|} \vdots p$.

Итак, пусть в центре элементов t, тогда, поскольку вся группа разбивается на непересекающиеся классы сопряженных элементов, $p^n = t + pk_1 + p_2^k + \ldots + p_m^k$, откуда следует, что $t \vdots p$, что и требовалось.

До этого момента было написано понадобившееся более полное и громоздкое решение Д15.

Итак, теперь мы знаем, что $|Z| \vdots p$, и значит, по предположению, $|Z| = p$. Тогда $|G/Z| = p$, так что группа G/Z является циклической. Пусть тогда aZ — ее порождающий элемент. Тогда любой элемент из G представляется в виде $g = a^k z_i$. Но любые два элемента такого вида коммутируют, что противоречит предположению.

Итак, центр такой группы совпадает со всей группой, что и требовалось.

Дополнительная задача 17

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ

Дополнительная задача 18

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ

Дополнительная задача 19

Условие: Является кольцом главных идеалов кольцо $\mathbb{Z}_{72}$?

Ответ: Является.

Дополнительная задача 20

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ

Дополнительная задача 21

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ

Дополнительная задача 22

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ

Дополнительная задача 23

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ

Дополнительная задача 24

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ

Дополнительная задача 25

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ

Дополнительная задача 26

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ

Дополнительная задача 27

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ

Дополнительная задача 28

Условие: а) Найти сумму всех квадратичных вычетов по модулю 73. б) Найти произведение всех квадратичных невычетов по модулю 103.

Ответ: а) 1; б) -1.

Дополнительная задача 29

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ

Дополнительная задача 30

Условие: Решить уравнение $1 + x + x^2 + \ldots + x^6 \equiv 0 \pmod{29}$.

Ответ: 7, 16, 20, 23, 24, 25.

Дополнительная задача 31

Условие: Найти наибольший порядок элемента мультипликативной группы кольца $\mathbb{Z}_{72}$

Мультипликативная группа кольца вычетов по модулю 72 — это множество чисел, взаимно простых с 72, с введенной операцией умножения (той же, что и в кольце вычетов по модулю 72). Заметим, что число 67 взаимно просто с 72, поэтому оно в мультикативной группе. Заметим так же, что по модулю 72 верны равенства

$67 * 67 = 25;$

$25 * 25 = 49;$

$49 * 49 = 25;$

$25 * 25 = 49;$

$49 * 49 = 25;$

$\ldots$

Ясно, что на 25 и 49 мы зациклились, поэтому порядок элемента 67 равен бесконечности.

Ответ: бесконечность.

Дополнительная задача 32

Условие: Найти количество нильпотентных элементов в кольце $F_7[x]/(x^{14}+x^7+2)$

$0 = x^{14}+x^7+2 = x^{14}+8x^7+16 = (x^7+4)^2$. Заметим теперь, что по МТФ $x^7 \equiv x \pmod 7$, так что 3 является корнем x^7+4, т.е. $(x^7+4) \vdots (x-3) = (x+4)$. Проверим, действительно ли $(x+4)^7 = x^7+4$. Действительно, $(x+4)^7 = x^7 + \binom{7}{1}4x^6 + \binom{7}{2}4^2x^5 + \ldots + \binom{7}{6}4^6x + 4^7$. Все коэффициенты, кроме первого и последнего, делятся на 7, и по МТФ $4^7 \equiv 4 \pmod 7$, так что $(x+4)^7 = x^7 + 4^7 = x^7 + 4$.

Итак, $0 = x^{14}+x^7+2 = (x^7+4)^2 = (x+4)^{14}$. Таким образом, все элементы, делящиеся на $x+4$, являются нильпотентами. Все эти элементы вида $(x+4)P(x)$, где $P(x)$ - многочлен из данного кольца степени не выше 12.

Покажем теперь, что среди многочленов, неделящихся на $x+4$, нет нильпотентов. Предоположим, что такой многочлен $R(x) = (x+4)Q(x)+b$, где $b \neq 0$ — число из F_7. Возведем его в 14 степень, по предположению должно получаться 0:

$\big((x+4)Q(x)+b\big)^{14} = \big(Q(x)\big)^{14}(x+4)^{14} + \binom{14}{1}\big(Q(x)\big)^{13}(x+4)^{13}b + \binom{14}{2}\big(Q(x)\big)^{12}(x+4)^{12}b^2 + \ldots + \binom{14}{13}(x+4)Q(x)b^{13} + b^{14} = 0\cdot\big(Q(x)\big)^{14} + 0\cdot\big(Q(x)\big)^{13}(x+4)^{13}b + 0\cdot\big(Q(x)\big)^{12}(x+4)^{12}b^2 + \ldots + 0\cdot(x+4)Q(x)b^{13} + b^{14} = b^{14}$.

Итак, получили, что $b^{14} = 0$, что равносильно тому, что $b = 0$, что противоречит предположению.

Итак, все нильпотенты вида $(x+4)P(x)$, и их количество есть 7^{13}.

Ответ: 7^{13}.

Дополнительная задача 33

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ

Дополнительная задача 34

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ

Дополнительная задача 35

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ

Дополнительная задача 36

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ

Дополнительная задача 37

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ

Дополнительная задача 38

Условие: Указать степени неприводимых делителей многочленов а) $x^5 - 2$ из кольца $F_{67}[x]$; б) $x^{28} - 1$ из кольца $F_3[x]$.

Обозначения. $f_5(x)$ — исходный многочлен. $f_i(x)$ — неприводимый многочлен степени i.

а) Заметим, что только число 41 является корнем многочлена (перебор). Значит $x^5 - 2 = (x-41)f_4(x)$, где $f_4(x)$ — многочлен 4 степени. Он может раскладываться как произведение 2 неприводимых многочленов степени 2, или сам f_4 является неприводимым. Разделим исходный многочлен на $x - 41$. Получим $x^4 - 26x^3 + 6x^2 - 22x + 65$. С помощью метода неопределенных коэффициентов находим разложение $(x^2-14x-6)(x^2-12x-22)$. Значит степени неприводимых многочленов равны 1, 2, 2.

б) $x^{28} - 1 = (x-1)(x+1)(x^2+1)(...)$. Посмотрим, какие степени могут быть у неприводимых многочленов. Нужно проверить, делится ли $x^{(3^n-1,28)} - 1$ на наш многочлен. Для $n \neq 6, 12, 18, 24$ получаем, что $(3^n - 1, 28)$ меньше чем n. Так как $x^{28} - 1 = (x^7-1)(x^7+1)(x^{14}+1)$, то можно исключить случаи со степенью неприводимых многочленов 24, 18 и 6, 12 и 12. Значит остается два случая для степеней неприводимых многочленов: 12 и 6 и 6, 6 и 6 и 6 и 6. Многочлен 12 степени это $(x^{14}+1)/(x^2+1) = x^{12} - x^{10} + x^8 - x^6 + x^4 - x^2 + 1$. Заметим, что неприводимый многочлен степени 6 это $(x^7+1)/(x+1) = x^6 - x^5 + x^4 - x^3 + x^2 - x^1 + 1$. Так как этот многочлен неприводим, что многочлен $(x^6)^2 - (x^5)^2 + (x^4)^2 - (x^3)^2 + (x^2)^2 - (x^1)^2 + 1 = x^{12} - x^{10} + x^8 - x^6 + x^4 - x^2 + 1$. Значит степени неприводимых многочленов равны 1, 1, 2, 6, 6, 12.

Ответ: а) 1, 2, 2; б) 1, 1, 2, 6, 6, 12.

Дополнительная задача 39

Условие: veni vidi vici

Здесь будет написано решение

Ответ: А тут будет ответ