ПРАКТИЧЕСКИЕ ЗАНЯТИЯ

Оглавление

Раздел I. Основы теории чисел

1.1. Делимость целых чисел

№1. Найти частные и остатки от деления a на b

а)

$a = 0,\ b \neq 0.$

Решение:

$0 = 0 \cdot b + 0$

Ответ: $q = r = 0.$

б)

$a = 119,\ b = -852.$

Решение:

$119 = 0 \cdot (-852) + 119$

Ответ: $q = 0,\ r = 119.$

в)

$a = 4357,\ b = 38.$

Решение:

Метод деления "уголком".

$$\begin{array}{r|l} 4357 & 38 \\ \underline{38} & 114 \\ 55 & \\ \underline{38} & \\ 177 & \\ \underline{152} & \\ 25 & \end{array}$$

Ответ: $q = 144,\ r = 25.$

г)

$a = -2023,\ b = 116.$

Решение:

$2023 = 116 \cdot 17 + 51.$

$-2023 = 116 \cdot (-17) - 51 = 116 \cdot (-18) + 65$

$-116 + x = -51$

$x = 116 - 51$

$x = 65.$

Ответ: $q = 18,\ r = 65.$

д)

$a = -11078,\ b = -311.$

Решение:

$11078 = 31 \cdot 357 + 11.$

$-11078 = (-31) \cdot 357 - 11$

$-11 = -31 + x$

$x = 31 - 11$

$x = 20$

$-11078 = (-31) \cdot 358 + 20.$

Ответ: $q = 358,\ r = 20.$

№2. Доказать признаки делимости

а) на 2:

$2 \mid a_n a_{n-1} \ldots a_1 a_0 \ \Leftrightarrow\ 2 \mid a_0,\ n = 0,\ 1,\ 2,\ \ldots$

Решение:

$\alpha = a_n a_{n-1} \ldots a_1 a_0 = a_n \cdot 10^n + \ldots + a_1 \cdot 10 + a_0 = \beta + a_0.$

$2 \mid \beta,\ 2 \mid \alpha \Leftrightarrow 2 \mid a_0$ (делимость линейной комбинации).

б) на 4:

$4 \mid a_n a_{n-1} \ldots a_1 a_0 \Leftrightarrow 4 \mid a_1 a_0,\ \mathrm{n} = 1,\ 2,\ \ldots$

Решение:

$\alpha = \mathrm{a_n} \cdot 10^n + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 = \beta + a_1 \cdot 10 + a_0.$

$4 \mid \beta.\ \ \alpha \vdots 4 \Leftrightarrow a_1 a_0 \vdots 4.$

в) на 3:

$3 \mid a_n a_{n-1} \ldots a_1 a_0 \Leftrightarrow 3 \mid a_n + a_{n-1} + \ldots + a_1 + a_0.$

Решение:

$\alpha = a_n \cdot 10^n + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 = a_n (9+1)^n + \ldots + a_2 (9+1)^2 +$

$+ a_1 (9+1) + a_0$ (бином Ньютона) $= \beta + (a_n + \ldots + a_2 + a_1 + a_0).$

$3 \mid \beta,\ \ 3 \mid \alpha \Leftrightarrow 3 \mid (\mathrm{a_n} + \ldots + a_1 + a_0).$

г) на 11:

$11 \mid a_n a_{n-1} \ldots a_1 a_0 \Leftrightarrow 11 \mid a_n (-1)^n + a_{n-1} (-1)^{n-1} + \ldots - a_1 + a_0.$

Решение:

$\alpha = a_n 10^n + \ldots + a_1 10 + a_0 = a_n (11-1)^n + \ldots + a_1 (11-1) + a_0 =$

$= \beta + a_n (-1)^n + a_{n-1} (-1)^{n-1} + a_1 (-1) + a_0.$

$11 \mid \beta,\ \ 11 \mid \alpha \Leftrightarrow 11 \mid a_n (-1)^n + a_{n-1} (-1)^{n-1} + \ldots - a_1 + a_0.$

д) на 8:

$8 \mid a_n a_{n-1} ... a_1 a_0 \Leftrightarrow 8 \mid a_2 a_1 a_0.$

Решение:

$\alpha = a_n 10^n + a_{n-1} 10^{n-1} + ... + a_1 10 + a_0 = \beta + a_2 \cdot 100 + a_1 \cdot 10 + a_0.$

$8 \mid \beta, \;\; 8 \mid \alpha \Leftrightarrow 8 \mid a_2 a_1 a_0.$

№3. Доказать утверждения.

а)

$\mathrm{ab} - \mathrm{ba} \vdots 9.$

Решение:

$\mathrm{ab} - \mathrm{ba} = 10 \cdot \mathrm{a} + \mathrm{b} - (10 \cdot \mathrm{b} + \mathrm{a}) = 10(\mathrm{a} - \mathrm{b}) + \mathrm{b} - \mathrm{a} = 9(\mathrm{a} - \mathrm{b}).$

$9 \mid 9(\mathrm{a} - \mathrm{b}), \;\; 0 \le \mathrm{a}, \mathrm{b} \le 9.$

б)

$\mathrm{nnn} \vdots 37, \;\; 0 \le \mathrm{n} \le 9.$

Решение:

$\mathrm{nnn} = \mathrm{n} \cdot 10^2 + \mathrm{n} \cdot 10 + \mathrm{n} = 100\mathrm{n} + 10\mathrm{n} + \mathrm{n} = 111\mathrm{n}.$

$111 : 37 = 3.$

в) Среди трех последовательных чисел n–1, n, n+1 одно и только одно из них делится на 3, $n \in \mathbf{Z}$.

Решение:

1. Пусть $n - 1 = 3q + 0$, тогда $n = 3q + 1, \;\; n + 1 = 3q + 2.$
2. Пусть $n - 1 = 3q + 1$, тогда $n = 3q + 2, \;\; n + 1 = 3q + 3, \;\; 3 \mid n + 1.$
3. Пусть $n - 1 = 3q + 2$, тогда $n = 3q + 3 \;\; (3 \mid n), \;\; n + 1 = 3(q + 1) + 1.$

Обобщение: среди k последовательных целых чисел одно и только одно из них делится на натуральное число k.

г)

$7^n - 1 \vdots 6, \;\; n \in N \cup \{0\}$

Решение:

1) $7^n - 1 = (7 - 1)(7^{n-1} + 7^{n-2} + ... + 7 + 1) - 6(7^{n-1} + 7^{n-2} + ... + 7 + 1)$

$\Rightarrow 6 \mid 7^n - 1, \;\; \forall n \in N.$

2) $n = 1, \;\; 7 - 1 = 6, \;\; 6 \mid 6.$ Делаем предположение индукции: $6 \mid 7^n - 1.$

$7^{n+1} - 1 = 7(7^n - 1) + 6 = 7^{n+1} - 7 + 6 = 7^{n+1} - 1.$

$6 \mid 7^n - 1, \;\; 6 \mid 6 \Rightarrow 6 \mid 7(7^n - 1) + 6$ (линейная комбинация).

1.2. НОД и его нахождение по алгоритму Евклида

№1. Найти НОД целых чисел и записать соотношения Безу для него.
а) (831, 2022).
Решение:

$$
\begin{array}{rl|l}
 & 2022 & 831 \\
- & 1662 & 2 \\
\hline
 & 360 & \text{r1} \\
- & 831 & 2 \\
\hline
 & 111 & \text{r2} \\
- & 360 & 3 \\
\hline
 & 27 & \text{r3} \\
- & 111 & 4 \\
\hline
 & 3 & \text{r4} \\
- & 27 & 9 \\
\hline
 & 0 &
\end{array}
$$

$$(831, 2022) = r_4 = 3.$$

$$3 = 111 - 27 \cdot 4 = 111 - (360 - 111 \cdot 3) \cdot 4 =$$

$$= 831 \cdot 13 - 360 \cdot 30 = 831 \cdot 13 - (2022 - 831 \cdot 2) \cdot 30 = 831 \cdot 73 + 2022 \cdot (-30).$$

Ответ: (831, 2022)=3, u=73, v= –30.
б) (–2584, 1824, –171).

Решение:

$$(-2584,\ 1824,\ 171) = ((-2584,\ 1824),\ -171).$$

$$
\begin{array}{rl|l}
 & 2584 & 1824 \\
- & 1824 & 1 \\
\hline
 & 760 & \text{r1} \\
- & 1824 & 760 \\
\hline
 & 1520 & 2 \\
\hline
 & 304 & \text{r2} \\
- & 760 & 2 \\
\hline
 & 668 & 2 \\
\hline
 & 152 & \text{r3} \\
- & 304 & 2 \\
\hline
 & 304 & 2 \\
\hline
 & 0 &
\end{array}
$$

$$(-2584, 1824) = r_3 = 152.$$

$$
\begin{array}{rl|l}
 & 171 & 152 \\
- & 152 & 1 \\
\hline
 & 19 & \text{r1} \\
- & 152 & 8 \\
\hline
 & 0 &
\end{array}
$$

$$19 = 171 - 152 = (-171)\cdot(-1) - (760 - 304\cdot 2) =$$
$$= (-171)\cdot(-1) - (2584 - 1824 - (1824 - 760\cdot 2)\cdot 2) =$$
$$= (-171)\cdot(-1) - 2584 + 3\cdot 1824 - (2584 - 1824)\cdot 4 =$$
$$= (-171)\cdot(-1) + 5\cdot(-2584) + 1824\cdot 7.$$

Ответ: (–2584, 1824, –171)=19, *u*=5, *v*=7, *w*= –1.

№2. Найти НОК целых чисел.

а)

[831, 2022].

Решение:

$$[831,\ 2022] = \frac{1680282}{3} = 560094.$$

Ответ: 560094.

б)

$[-2584, 1824, -171]$.

Решение:

$$[-2584, 1824, -171] = [[-2584, 1824], -171] = \left[\frac{2584\cdot 1824}{152}, -171\right] =$$

$$= \frac{2584\cdot 1824\cdot 171}{152\cdot\left(\frac{2584\cdot 1824}{152}, 171\right)} = \frac{31008\cdot 171}{(31008, 171)} = \frac{31008\cdot 171}{57} = 93024.$$

Ответ: 93024.

в)

$[-2057, -1496, 451]$.

Решение:

$$[-2057, -1496, 451] = [[-2057, -1496], 451] = \frac{2057\cdot 1496\cdot 451}{187\cdot\left(\frac{2057\cdot 1496}{187}, 451\right)} =$$

$$= \frac{16456\cdot 451}{(16456, 451)} = \frac{16456\cdot 451}{11} = 674696.$$

Ответ: 674696.

Домашнее задание

№1. Найти (–2057, –1496, 451) и записать для него соотношение Безу.

Решение:

$$\begin{array}{r|l} 2057 & 1496 \\ \hline 1496 & 1 \\ \hline 561 - r1 & \end{array} \qquad \begin{array}{r|l} 1496 & 561 - r1 \\ \hline 1122 & 2 \\ \hline 374 - r2 & \end{array} \qquad \begin{array}{r|l} 561 & 374 - r2 \\ \hline 374 & 1 \\ \hline 187 - r3 & \end{array}$$

$$\begin{array}{r|l} 451 & 187 \\ \hline 374 & 2 \\ \hline 77 - r1 & \end{array} \qquad \begin{array}{r|l} 187 & 77 - r1 \\ \hline 154 & 2 \\ \hline 33 - r2 & \end{array} \qquad \begin{array}{r|l} 77 & 33 - r2 \\ \hline 66 & 2 \\ \hline 11 - r3 & \end{array} \qquad \begin{array}{r|l} 33 & 11 - r3 \\ \hline 33 & 3 \\ \hline 0 & \end{array}$$

$$\begin{array}{r|l} 374 & 187 \\ \hline 374 & 2 \\ \hline 0 & \end{array}$$

$(2057, 1496) = 187;\ (187, 451) = 11 \Rightarrow (-2057, -1496, 451) = 11.$

$187 = (561 - 74) = 2057 - 1496 - (1496 - 561 \cdot 2) =$

$= 2057 - 1496 - (1496 - (2057 - 1496) \cdot 2) = 2057 \cdot 3 - 1496 \cdot 4 =$

$= (-2057) \cdot (-3) + (-1496) \cdot 4$

$11 = 77 - 33 \cdot 2 = 451 - 187 \cdot 2 - (187 - 77 \cdot 2) \cdot 2 = 451 - 187 \cdot 4 +$

$+ (451 - 187 \cdot 2) \cdot 4 = 451 \cdot 5 - 187 \cdot 12 = 451 \cdot 5 - ((-2057)(-3) +$

$+ (-1496) \cdot 4) \cdot 12 = 451 \cdot 5 + (-2057) \cdot 36 + (-1496) \cdot (-48).$

Ответ: (–2057, –1496, 451)=11, *u*=36, *v*= –48, *w*=5.

№2. Найти частные и остатки от деления *a* на *b*.

а) $a = 13677,\ \ b = -189.$

$$\begin{array}{r|l} 13677 & 189 \\ \hline 1323 & 72 \\ \hline 447 & \\ 378 & \\ \hline 69 & \end{array}$$

$13677 = 189 \cdot 72 + 69 = (-189) \cdot (-72) + 69.$

Ответ: $q = -72,\ \ r = 69.$

б)

$a = -3198,\ b = 7293$

Решение:

$-3198 = 7293 \cdot (-1) + 3095$

Ответ: $q = -1,\ \ r = 3095.$

в)

$a = -1958,\ \ b = -2275.$

Решение:

$-1958 = (-2275) \cdot 1 + 317$

Ответ: $q = 1,\ \ r = 317.$

1.3. Простые числа и их свойства. Основная теорема арифметики

№1. Проверить на простоту числа.

а)

179.

Решение:

$13 < \sqrt{179} < 14$

Рассмотрим простые числа в пределах от 2 до 13.

$2 \nmid 9,\ 1+7+9 = 17 \nmid 3$

$5 \nmid 9,\ \ 9-7+1 = 2+1 \nmid 11,$

$10^n = (7+3)^n = C_n + 3^n$

$1 \cdot 3^2 + 7 \cdot 3 + 1 \cdot 3^2 = 9 + 21 + 9 = 39 \nmid 7,$

$1 \cdot 10^2 + 7 \cdot 10 + 9 = 1 \cdot (7+3)^2 + 7 \cdot (7+3) + 7 + 2$

$9 - 7 \cdot 3 + 1 \cdot 3^2 = 9 - 21 + 9 = -3 \nmid 13.$

$10^n = (13-3)^n = C_n \cdot (-3)^n$

Ответ: число 179 – простое.

б)

719.

Решение:

$26 < \sqrt{719} < 27$

$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23$ – простые числа

$2 \nmid 9,\ \ 7+1+9 = 17 \nmid 3,\ \ 5 \nmid 9,\ 7 \cdot 3^2 + 1 \cdot 3 + 9 = 63 + 3 + 9 = 66 + 9 = 75 \nmid 7,$

$9 - 1 + 7 = 15 \nmid 11,\ \ 9 - 3 + 7 \cdot 3^2 = 6 + 63 = 69 \nmid 13,$

$719 \nmid 17,\ \ 719 \nmid 19,\ \ 719 \nmid 23$

Ответ: 719 – простое число.

№2. Выписать все простые числа указанного диапазона.

а)

от 200 до 225.

Решение:

$14 < \sqrt{225} = 15,\ \ 13 -$ последнее простое число.

Ответ: $223,\ 211$ – простые числа.

б)

от 2320 до 2350.

Решение:

$48 < \sqrt{2350} < 49$, 13 – последнее простое число.

Ответ: 2333, 2339, 2341, 2347 – простые числа.

в)

от 1300 до 1350.

Решение:

$36 < \sqrt{1350} < 37$, 31 – последнее простое число.

Сразу не выписываем четные числа и числа, кратные 5.

Ответ: 1301, 1303, 1307, 1319, 1321, 1327 – простые числа.

№3. Найти каноническое разложение числа 8279848.

Решение:

$2877^2 = 8277129$, $2878^2 = 8282884$.

Находим наименьший делитель: $q_0 = 2$.

Наибольший делитель будет $8279848:2 = 4139924 = Z$

$2034^2 < Z < 2035^2$, $2033^2 = 4133089$.

Делим число на $q_i^{k_i}$, ищем проостые делители полученного числа.

Ответ: $2^3 \cdot 29 \cdot 89 \cdot 401$.

№4. Доказать, что для $\forall n \in \mathbf{N}$, $n > 2$, между n и $n!$ Содержится, по меньшей мере, одно простое число.

Решение:

Пусть $n > 2$, $n \in \mathbf{N}$. Рассмотрим число $n!-1 > 1$.

$n!-(n!-1) = 1$ (критерий взаимной простоты).

Числа $n!$ и $n!-1$ взаимно просты. Пусть $d = (n!, n!-1)$.

$d \mid n!$, $d \mid n!-1 \Rightarrow d \mid n!-(n!-1) \Rightarrow d \mid 1 \Rightarrow d = 1$.

$n! = 2 \cdot 3 \cdot 4 \cdot \ldots \cdot (n-1) \cdot n$.

Делителями n! являются все делители чисел от 2 до n. Простыми делителями $n!$ являются все простые числа от 2 до n включительно.

$n < n!-1 < n!$ $\forall n > 2$.

$n < n \cdot (n-1)!-1 \Leftrightarrow 1 < (n-1)! < 1$.

Потому либо $n!-1$ – простое число ($n = 3$, $2 - \frac{1}{3} > 1$), либо составное и имеет простые делители, большие n, естественно, меньшие $n!$ Пэтому существует простое $p \mid n < p < n!$.

№5. Доказать, что для всякого $n \in \mathbf{N}$ $\exists k \in \mathbf{N}|$ все натуральные числа из отрезка $[\mathrm{k}, \mathrm{k}+\mathrm{n}]$ составные.

Решение:

Пусть $k = (n+2)!+2$. Тогда $k+1 = (n+2)!+3, \ldots,\ k+n = (n+2)!+n+2$.

$k = 2 \cdot (3 \cdot 4 \cdot \ldots \cdot (n+1)(n+2)+1)$ – составное число

$k+1 = 3 \cdot (2 \cdot 4 \cdot 5 \cdot \ldots \cdot (n+1)(n+2)+1)$ – составное число

$k+n = (n+2)(2 \cdot 3 \cdot 4 \cdot \ldots \cdot (n+1)+1)$ – составное число.

№6. С помощью канонического разложения чисел найти их НОД и НОК.

а)

$a = 244604911,\ \ b = 61875907.$

Решение:

$a = 31 \cdot 53^4,\ \ b = 31^4 \cdot 67.$

Ответ: $(a,b) = 31;\ [a,b] = 31^4 \cdot 53^4 \cdot 67.$

б)

$a = -356216713,\ \ b = 312380651,\ c = -2212339679.$

Решение:

$a = -47^4 \cdot 73,\ \ b = 11 \cdot 73^4,\ \ c = -11^2 \cdot 47 \cdot 73^3.$

Ответ: $(a,b,c) = 73,\ \ [a,b,c] = 11^2 \cdot 47^4 \cdot 79^4 = 16767497201975641.$

в)

$a = -16254559,\ \ b = -44250139,\ \ c = 1643534754511.$

Решение:

$a = -43^2 \cdot 59 \cdot 149,\ \ b = -43 \cdot 97 \cdot 103^2,\ c = 13^3 \cdot 43^3 \cdot 97^2.$

Ответ: $(a,b) = 43,\ \ [a,b] = 13^3 \cdot 43^3 \cdot 59 \cdot 97^2 \cdot 103^2 \cdot 149 = 15342024172900399.$

1.4. Диофантовы линейные уравнения

№1. Решить диофантовы линейные уравнения.

а)

$66x + 80y = 440.$ (1.4.1)

Решение:

$(60,\ 80) = 20,\quad 60 = 20 \cdot 3,\ \ 80 = 20 \cdot 4;\ \ 20|440.$

$3x + 4y = 22.$ (1.4.2)

$(3,\ 4) = 1,\ \ 3x + 4y = 1.$ (1.4.3)

Тогда $3 \cdot 22x_0 + 4 \cdot 22y_0 = 22.$

Найдем x_0 и y_0 по расширенному алгоритму Евклида.

$4 = 31 + 1,\ \ r_1 = 4 - 3;$

$3 = 1 \cdot 3 + 0,\ \ r_2 = 0.$

$d = 1 = 4 - 3,\ \ x_0 = -1,\ \ y_0 = 1$ – решение уравнения (1.4.3).

$x_1 = -22,\ \ y_1 = 22$ – частное решение уравнения (1.4.2).

Ответ: $\{(-22 - 4t, 22 + 3t) \mid t \in \mathbf{Z}\}$.

б)

$39x - 22y = 10.$ (1.4.4)

Решение:

$(39, 22) = 1,\ \ 1|10.$

$39x - 22y = 1.$ (1.4.5)

$39 = 22 \cdot 1 + 17,\quad 17 = 39 - 22,$

$22 = 17 \cdot 1 + 5,\quad 5 = 22 - 17 = 22 - (39 - 22) = 2 \cdot 22 - 39,$

$17 = 5 \cdot 3 + 2,\quad 2 = 17 - 5 \cdot 3 = 17 - (2 \cdot 22 - 39) \cdot 3 =$

$= 39 - 22 - 6 \cdot 22 + 3 \cdot 39 = -7 \cdot 22 + 4 \cdot 39,$

$5 = 2 \cdot 2 + 1,\quad 1 = 5 - 2 \cdot 2 = 2 \cdot 22 - 39 - 2(-7 \cdot 22 + 4 \cdot 39) =$

$= 16 \cdot 22 - 9 \cdot 39 = (-16) \cdot (-22) + (-9) \cdot 39.$

$x_0 = -9,\quad y_0 = -16$ – частное решение (1.4.5).

$x_1 = -90,\quad y_1 = -160$ – частное решение (1.4.4).

Ответ: $\{(-90 + 22t, -160 + 39t) \mid t \in \mathbf{Z}\}$.

в)

$7x - 19y = 23.$ (1.4.6)

Решение:

$(7, 19) = 1,\ 1|23.$

$7x - 19y = 1$ (1.4.7)

$19 = 7 \cdot 2 + 5,\ \ 5 = 19 - 7 \cdot 2,$

$7 = 5 \cdot 1 + 2,\ \ 2 = 7 - 5 \cdot 1 = 7 - 19 + 7 \cdot 2 - 2(73 - 19) = 19 \cdot 3 - 7 \cdot 8 =$

$= (-3)(-19) + (-8) \cdot 7,$

$2 = 1 \cdot 2 + 0.$

$x_0 = -8,\ \ y_0 = -3$ – частное решение (1.4.7)

$x_1 = -184,\ \ y_1 = -69$ – частное решение (1.4.6)

Ответ: $\{(-184 + 19t, -69 + 7t) \mid t \in \mathbf{Z}\}$.

1.5. Сравнения целых чисел

№1. С каким числом $0 \le r \le 5$ по модулю 6 сравнимо число $a = 1001 \cdot 23^{10} \cdot 19^{13} \cdot 51^2$?

Решение:

$1001 = 6 \cdot 166 + 5 \Rightarrow 1001 \equiv 5 (\mathrm{mod}\, 6)$

$23 \equiv -1 (\mathrm{mod}\, 6) \Rightarrow 23^{10} \equiv 1 (\mathrm{mod}\, 6)$

$19 \equiv 1 (\mathrm{mod}\, 6) \Rightarrow 19^{13} \equiv 1 (\mathrm{mod}\, 6)$

$51 = 48 + 3 \equiv 3 (\mathrm{mod}\, 6)$

$51^2 \equiv 3^2 = 9 \equiv 3 (\mathrm{mod}\, 6)$

$a \equiv 5 \cdot 3 = 15 \equiv 3 (\mathrm{mod}\, 6).$

Ответ: $a \equiv 3 (\mathrm{mod}\, 6)$.

№2. Показать, что если n – нечетное число, то $n^2 - 1 \equiv 0 (\mathrm{mod} 8)$.

Решение:

$n = 2m + 1,\ \ m \in \mathbf{Z},\ \ n^2 - 1 = (2m+1)^2 - 1 = (2m+2) \cdot 2m = 4m(m+1)$

$n^2 = 4m^2 + 4m + 1,\ \ n^2 - 1 = 4m^2 + 4m$

Если m – четное число, то $m = 2k,\ k \in \mathbf{Z},$ и $4m^2 + 4m = 4 \cdot 4k^2 + 8k =$

$= 8(2k^2 + k) \equiv 0 (\mathrm{mod} 8).$

Если $m = 2k + 1,\ k \in \mathbf{Z},$ то $4m^2 + 4m = 4(4k^2 + 4k + 1) + 8k + 4 =$

$= 8(2k^2 + 3 + 1) \equiv 0 (\mathrm{mod} 8).$

№3. Доказать, что если $3^n \equiv -1 (\mathrm{mod} 10)$, то $3^{n+4} \equiv -1 (\mathrm{mod} 10),\ \ n \in \mathbf{N}.$

Решение:

$3^4 = 81 \equiv 1 (\mathrm{mod} 10) \Rightarrow 3^n \cdot 3^4 \equiv -1 \cdot 1 (\mathrm{mod} 10) \Rightarrow 3^{n+4} \equiv -1 (\mathrm{mod} 10).$

№4. Доказать, что $2^{11 \cdot 31} \equiv 2(11 \cdot 31)$.

Решение:

$(2, 11) = 1,\ \ (2, 31) = 1.$

$2^5 = 32 \equiv -1 (\mathrm{mod} 11),\ \ 2^{11} = (2^5)^2 \cdot 2 \equiv (-1)^2 \cdot 2 \equiv 2 (\mathrm{mod} 11),$ т.к.

$2^{10} \equiv 1 (\mathrm{mod} 11)$ (малая теорема Ферма).

$(2^{11})^{31} \equiv 2^{31} (\mathrm{mod}\, 11)$, $2^{31} = (2^5)^6 \cdot 2 \equiv 2 (\mathrm{mod}\, 11) \Rightarrow$

$2^{11 \cdot 31} \equiv 2 (\mathrm{mod}\, 11).$

$(2^{31})^{11} \equiv 2^{11} (\mathrm{mod}\, 31)$, $2^{11} = (2^5)^2 \cdot 2 \equiv 2 (\mathrm{mod}\, 31) \Rightarrow$

$2^{31 \cdot 11} \equiv 2 (\mathrm{mod}\, 31).$

$2^{11 \cdot 31} = 2 + 11q = 2 + 31m \Rightarrow 11q = 31m,$ т.к. $(11, 31) = 1,$

то $11|\mathrm{m}$, $31|\mathrm{q} \Rightarrow 2^{11 \cdot 31} \equiv 2 (\mathrm{mod}\, 11 \cdot 31).$

№5. Проверить, что $3^{14} \equiv -1 (\mathrm{mod}\, 29).$

Решение:

$3^3 = 27 \equiv -2 (\mathrm{mod}\, 29),$

$3^{14} = 3^{12} \cdot 3^2 = (3^3)^4 \cdot 3^2 \equiv (-2)^4 \cdot 3^2 = 48 \cdot 3 \equiv 19 \cdot 3 = 57 \equiv -1 (\mathrm{mod}\, 29).$

№6. Найти остаток от деления числа $1532^5 - 1$ на 9.

Решение:

$1532 = 2^2 \cdot 383 \equiv 4 \cdot 5 = 20 \equiv 2 (\mathrm{mod}\, 9),$

$1532^5 - 1 \equiv 2^5 - 1 = 31 \equiv 4 (\mathrm{mod}\, 9).$

Ответ: 4.

№7. По утверждению Ферма, число $2^{2^n} + 1$ – простое число при $\forall n \in \mathbf{N}$. Проверить, что при $n = 5$ получается число, кратное 641.

Решение:

$2^9 = 512 \equiv -129, \quad 2^{10} = 1024 \equiv 383 (\mathrm{mod}\, 641),$

$2^{32} + 1 = 2^{30} \cdot 2^2 - 1 = (2^{10})^3 \cdot 4 - 1,$

$2^{32} + 1 = 125 \cdot 125 \cdot 383 + 1 \equiv -16 \cdot 25 \cdot 383 + 1 = -400 \cdot 383 + 1 =$

$= -200 \cdot 766 + 1 \equiv -200 \cdot 125 + 1 = -40 \cdot 625 + 1 \equiv -40 \cdot (-16) + 1 \equiv$

$\equiv 640 + 1 = 641 \equiv 0 (\mathrm{mod}\, 641).$

1.6. Множество классов вычетов. Функция Эйлера

№1. Составить таблицы Кэли сложения и умножения в $\mathbf{Z}/n\mathbf{Z}$, $n \in \mathbf{N}$. Найти противоположные и обратные элементы, если они существуют. Проверить обратимость элементов по критерию обратимости классов вычетов.

а) $\mathrm{n} = 7.$

Решение:

Противоположные и обратные элементы находим по таблицами Кэли сложения и умножения классов вычетов (таблица 1.6.1). $-\bar{i} = \overline{7 - i}, \quad i = \overline{0,6}.$ Все ненулевые классы обратимы, поскольку 7 – простое число.

$$1^{-1}=1,\ 2^{-1}=4,\ 3^{-1}=5,\ 4^{-1}=2,\ 5^{-1}=3,\ 6^{-1}=6.$$

Таблица 1.6.1

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{6}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$

×	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{1}$	$\bar{3}$	$\bar{5}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{2}$	$\bar{5}$	$\bar{1}$	$\bar{4}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{1}$	$\bar{5}$	$\bar{2}$	$\bar{6}$	$\bar{3}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{3}$	$\bar{1}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{6}$	$\bar{0}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Ответ: обратимые классы – $\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}$.

б) $n=9$.

Решение:

Противоположные и обратные элементы находим по таблицам Кэли сложения и умножения классов вычетов (таблица 1.6.2). $-\bar{i}=\overline{9-i},\ i=\overline{0,8}$. Обратимыми являются только те классы вычетов, представители которых взаимно просты с 9.

$$1^{-1}=1,\ 2^{-1}=5,\ 4^{-1}=7,\ 5^{-1}=2,\ 7^{-1}=4,\ 8^{-1}=8.$$

Таблица 1.6.2

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{6}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{7}$	$\bar{7}$	$\bar{8}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{8}$	$\bar{8}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$

×	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{8}$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{0}$	$\bar{3}$	$\bar{0}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{8}$	$\bar{3}$	$\bar{7}$	$\bar{2}$	$\bar{6}$	$\bar{1}$	$\bar{5}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{1}$	$\bar{6}$	$\bar{2}$	$\bar{7}$	$\bar{3}$	$\bar{8}$	$\bar{4}$
$\bar{6}$	$\bar{0}$	$\bar{6}$	$\bar{3}$	$\bar{0}$	$\bar{6}$	$\bar{3}$	$\bar{0}$	$\bar{6}$	$\bar{3}$
$\bar{7}$	$\bar{0}$	$\bar{7}$	$\bar{5}$	$\bar{3}$	$\bar{1}$	$\bar{8}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{8}$	$\bar{0}$	$\bar{8}$	$\bar{7}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Ответ: $\bar{1},\ \bar{2},\ \bar{4}, \bar{5}, \bar{7}, \bar{8}$ – обратимые классы.

в) $n=12$.

Решение:

Противоположные и обратные элементы находим по таблицам Кэли сложения и умножения классов вычетов (таблицы 1.6.3, 1.6.4). $-\bar{i}=\overline{12-i},\ i=\overline{0,11}$. Обратимыми являются только те классы вычетов, представители которых взаимно просты с 12.

$$1^{-1}=1,\ 5^{-1}=5,\ 7^{-1}=7,\ 11^{-1}=11.$$

Таблица 1.6.3

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$1\,\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{6}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{7}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{8}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{9}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$
$\overline{10}$	$\overline{10}$	$\overline{11}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$
$\overline{11}$	$\overline{11}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$

Таблица 1.6.4

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{8}$	$\overline{10}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{8}$	$\overline{10}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{9}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{9}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{9}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{8}$	$\overline{0}$	$\overline{4}$	$\overline{8}$	$\overline{0}$	$\overline{4}$	$\overline{8}$	$\overline{0}$	$\overline{4}$	$\overline{8}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{10}$	$\overline{3}$	$\overline{8}$	$\overline{1}$	$\overline{6}$	$\overline{11}$	$\overline{4}$	$\overline{9}$	$\overline{2}$	$\overline{7}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{0}$	$\overline{6}$
$\overline{7}$	$\overline{0}$	$\overline{7}$	$\overline{2}$	$\overline{9}$	$\overline{4}$	$\overline{11}$	$\overline{6}$	$\overline{1}$	$\overline{8}$	$\overline{3}$	$\overline{10}$	$\overline{5}$
$\overline{8}$	$\overline{0}$	$\overline{8}$	$\overline{4}$	$\overline{0}$	$\overline{8}$	$\overline{4}$	$\overline{0}$	$\overline{8}$	$\overline{4}$	$\overline{0}$	$\overline{8}$	$\overline{4}$
$\overline{9}$	$\overline{0}$	$\overline{9}$	$\overline{6}$	$\overline{3}$	$\overline{0}$	$\overline{9}$	$\overline{6}$	$\overline{3}$	$\overline{0}$	$\overline{9}$	$\overline{6}$	$\overline{3}$
$\overline{10}$	$\overline{0}$	$\overline{10}$	$\overline{8}$	$\overline{6}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{10}$	$\overline{8}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{11}$	$\overline{0}$	$\overline{11}$	$\overline{10}$	$\overline{9}$	$\overline{8}$	$\overline{7}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Ответ: обратимые классы – $\overline{1}, \overline{5}, \overline{7}, \overline{11}$.

№2. В **Z**/*n***Z** найти обратные элементы к $\bar{k}_1, \bar{k}_2, \bar{k}_3$ или доказать, что их нет.

а) $n = 236,\ \bar{k}_1 = \overline{100},\ \bar{k}_2 = \overline{71},\ \bar{k}_3 = \overline{185}.$

Решение:

$(236,\ 100) = 4 > 1 \Rightarrow \overline{100}$ не обратим в **Z**/236**Z**.

$(236,\ 71)=1 \Rightarrow \overline{71}$ обратим в **Z**/236**Z**.

Из соотношения Безу находим, что

$\overline{71}^{-1} = \overline{-113} = \overline{236-113} = \overline{123}.$

$(236,\ 185)=1 \Rightarrow \overline{185}$ обратим в **Z**/236**Z**.

Из соотношения Безу находим, что $\overline{185}^{-1} = \overline{37}.$

б) $n = 318,\ \bar{k}_1 = \overline{273},\ \bar{k}_2 = \overline{59},\ \bar{k}_3 = \overline{126}.$

№3. Найти значение функции Эйлера $\varphi(x)$.

а) n=480.

Решение:

$480=2^5\cdot 3\cdot 5$, $\varphi(480)=(2^5-2^4)\cdot 2\cdot 4=16\cdot 8=128$.

б) n=697.

Решение:

$697=17\cdot 41$, $\varphi(697)=16\cdot 40=640$.

№4. С помощью функции Эйлера решить сравнение, находя $\bar{a}^{-1}$.

а) $256x \equiv 179 \pmod{337}$.

Решение:

$256=2^8$, 179 – простое число, 337 – простое число. $\varphi(337)=336=2^4\cdot 3\cdot 7$.

$\bar{x} = \overline{179}\cdot \overline{256}^{335}$,

$\bar{a}^{-1} = \overline{256}^{335} = (\overline{-81})^{338} = (\overline{-3}^4)^{338} = \overline{104}$.

$x \equiv 179\cdot 104 = 169\cdot 2\cdot 52 + 10\cdot 104 \equiv 52 + 10\cdot 104 \equiv 52 + 29 = 81 \pmod{337}$.

Ответ: $\bar{x} = \overline{81}$.

б) $114x \equiv 42 \pmod{87}$.

Решение:

$87=3\cdot 29$, $114=2\cdot 3\cdot 19$, $42=2\cdot 3\cdot 7$. Значит, $(87, 114, 42)=3$.

Разделим обе части сравнения и модуль на 3. Получим следующее сравнение:

$38x \equiv 14 \pmod{29}$.

Разделив обе части сравнения на 2, получим следующее сравнение:

$19x \equiv 7 \pmod{29}$.

$x \equiv 7\ (-10)^{27} = 7\cdot 4\cdot (-5)^{27}\ 2^{25} = (-1)\cdot(-5)^{27}\cdot 2^{25} = 5^{27}\cdot 2^{25} = (5^2)^{13}\cdot 2^{25}\cdot 5 \equiv$

$\equiv (-4)^{13}\cdot 2^{25}\cdot 5 = 2^{26+25}\cdot 5 \equiv -2^{23}\cdot 5 \pmod{29}$;

$5^2 = 25 \equiv -4 \pmod{29}$;

$2^5 = 32 \equiv 3 \pmod{29}$;

$2^{23} = (2^5)^4\cdot 2^3 \equiv 81\cdot 2^3 \equiv -6\cdot 2^3 = -48 \equiv -19 \pmod{29}$;

$29\cdot 3 = 87$; $29\cdot 2 = 58$;

$10\cdot5=50\equiv-8(\mathrm{mod}\ 29)$; $-10\cdot5\equiv8(\mathrm{mod}\ 29)$.

Итак, $x\equiv8(\mathrm{mod}\ 29)$.

Тогда (поскольку 8+29=37, 8+27·2=66) $\bar{8}$, $\overline{37}$, $\overline{66}$ – решения в **Z**/87**Z**.

$19^{27}\equiv(-10)^{27}=(-5)^{27}\cdot2^{27}=$

$=-(5^2)^{13}\cdot5\cdot2^{27}\equiv4^{13}\cdot5\cdot2^{27}=2^{26}\cdot5\cdot2^{27}\equiv2^{25}\cdot5\equiv3^5\cdot5=81\cdot3\cdot5\equiv$

$\equiv(5^2)^{13}\cdot5\cdot2^{27}\equiv4^{13}\cdot5\cdot2^{27}=2^{26}\cdot5\cdot2^{27}\equiv2^{25}\cdot5\equiv3^5\cdot5=81\cdot3\cdot5\equiv$

$\equiv-6\cdot3\cdot5\equiv-18\cdot5\equiv11\cdot5=55\equiv-3\equiv26(\mathrm{mod}\ 29)$.

$19\cdot(-3)=-57\equiv-(-1)=1(\mathrm{mod}\ 29)$, $-3\cdot7=-21\equiv8(\mathrm{mod}\ 29)$.

$7\cdot(-3)=-21\equiv8(\mathrm{mod}\ 29)$,

Ответ: $\bar{x}=\bar{8}$, $\overline{37}$, $\overline{66}$ в **Z**/87**Z**.

Раздел II. Отображения и их свойства

2.1. Соответствия, отображения функции

№1. Выписать все соответствия между множествами X и Y. Какие из соответствий являются отображениями? Какие из отображений являются функциями? Указать инъективные, сюръективные и биективные функции.

а) X={1, 2}, Y={3}.

Решение:

X×Y={(1, 3), (2, 3)}. Это множество дает возможность получить $2^2=4$ различных соответствия. Графики соответствий: $Q_0=\{(\,)\}=\varnothing$, $Q_1=\{(1, 3)\}$, $Q_2=\{(2, 3)\}$, $Q_3=\{(1, 3), (2, 3)\}=X\times Y$. Обозначим q_i соответствие с графиком Q_i, $i=\overline{0, 3}$. Отображением является соответствие q_3, оно же является функцией. q_3 – неинъективная, сюръективная, небиективная функция.

б) X={1}, Y={3, 4}.

Решение:

X×Y={(1, 3), (1, 4)}. Это множество дает возможность получить $2^2=4$ различных соответствия. Графики соответствий: $Q_0=\{(\,)\}=\varnothing$, $Q_1=\{(1, 3)\}$, $Q_2=\{(1, 4)\}$, $Q_3=\{(1, 3), (1, 4)\}=X\times Y$. Обозначим q_i соответствие с графиком Q_i, $i=\overline{0, 3}$. Отображениями являются соответствия q_1–q_3. Функциями являются отображения q_1, q_2. q_1, q_2 – инъективные, несюръективные, небиективные функции.

№2. Представить в виде композиций следующие функции.

а) $f(x)=\left(1+\left(\frac{x}{1-x}\right)^2\right)^{\frac{1}{2}}$.

Решение:

$f_1(x)=\dfrac{x}{1-x}$, D(f_1)=**R**\{1}, E(f_1)=**R**\{–1}, т.к. уравнение $\dfrac{x}{1-x}=y$ разрешимо относительно x и $x=\dfrac{y}{1+y}$ для любого $y\in$**R**\{–1}.

$f_2(x)=x^2$, D(f_2)=**R**, E(f_2)=$\mathbf{R}_{\geq 0}$, E(f_2f_1)=$\mathbf{R}_{\geq 0}$.

$f_3(x)=1+x$, D(f_3)=**R**, E(f_3)=**R**, E($f_3f_2f_1$)=$\mathbf{R}_{\geq 1}$.

$f_4(x)=x^{\frac{1}{2}}$, D(f_4)=$\mathbf{R}_{\geq 0}$, E(f_4)=$\mathbf{R}_{\geq 0}$, E($f_4f_3f_2f_1$)=$\mathbf{R}_{\geq 1}$.

Видно, что E(f_i)$\subset$D(f_{i+1}), $i=\overline{1,3}$.

Итак, $f(x)=f_4(f_3(f_2(f_1(x))))=f_4f_3f_2f_1(x)$, D($f$)=D($f_1$)=**R**\{1}, E($f$)=$\mathbf{R}_{\geq 1}$.

б) $f(x)=(1-e^{2x})^3$.

Решение:

$f_1(x)=2x$, D(f_1)=**R**, E(f_1)=**R**.

$f_2(x)=e^x$, D(f_2)=**R**, E(f_2)=$\mathbf{R}_{>0}$, E(f_2f_1)=$\mathbf{R}_{>0}$.

$f_3(x)=1-x$, D(f_3)=**R**, E(f_3)=**R**, E($f_3f_2f_1$)=$\mathbf{R}_{<1}$.

$f_4(x)=x^3$, D(f_4)=**R**, E(f_4)=**R**, E($f_4f_3f_2f_1$)=$\mathbf{R}_{<1}$.

Видно, что E(f_i)$\subset$D(f_{i+1}), $i=\overline{1,3}$.

Итак, $f(x)=f_4(f_3(f_2(f_1(x))))=f_4f_3f_2f_1(x)$, D($f$)=D($f_1$)=**R**, E($f$)=$\mathbf{R}_{<1}$.

№3. Исследовать свойства функции φ:**Z**/n**Z**$\to$**Z**/n**Z**, $n\in$**N**. $\varphi(\bar{a})=\overline{m\cdot a}$, $\forall\, a\in$**Z**/n**Z**, фиксированное $\bar{m}\in$**Z**/n**Z**.

Решение:

1) Если (m, n)=1, то при $\bar{a}\neq\bar{b}$ $\varphi(\bar{a})\neq\varphi(\bar{b})$.

Действительно, $m\cdot a\not\equiv m\cdot b(\mathrm{mod}\ n)$, т.к. иначе $m\cdot(a-b)\vdots n$, но $0<m<n$, $0\leq a-b<n\Rightarrow|a-b|<n$, поэтому $m\cdot(a-b)\not\vdots n$. Итак, φ – инъекция, а по теореме 1.2.1 сюръекция и, следовательно, биекция.

2) Если (m, n)$\neq$1, пусть (m, n)=d>1. Тогда $m=m_1\cdot d$, $n=n_1\cdot d$, (m_1, n_1)=1.

$\varphi(\bar{0})=\bar{0}$, $\varphi(\overline{n_1})=\overline{m_1\cdot n_1\cdot d}=\overline{m_1\cdot n}=\bar{0}\Rightarrow\varphi$ – не инъекция. Значит, по теореме 1.2.1 φ – не сюръекция и, следовательно, не биекция.

№4. Исследовать свойства отображения φ:**Z**/p**Z**$\to$**Z**/p**Z**, p – простое число, $\varphi(\bar{a})=\bar{a}^{\,p}$. Вывести формулы бинома Ньютона $(\bar{a}+\bar{b})^{n1}$, $(\bar{a}+\bar{b})^{n2}$, $(\bar{a}+\bar{b})^{n3}$.

а) p=11, n_1=28, n_2=44, n_3=75.

б) p=17, n_1=51, n_2=38, n_3=155.

Решение:

$\bar{a}^{\,p-1}=\bar{1}\ \forall\,\bar{a}\neq\bar{0}$, т.к. ($a$, p)=$\bar{1}$, выполняется теорема Ферма.

$\bar{0}^{\,p}=\bar{0}$, $\bar{a}^{\,p}=\bar{a}\ \forall\,\bar{a}\neq\bar{0}$.

Поэтому φ – тождественное отображение на **Z**/p**Z**. Значит, $\varphi(\bar{a}+\bar{b})=\bar{a}+\bar{b}$.

а) $(\bar{a}+\bar{b})^{28}=(\bar{a}+\bar{b})^{22+6}=((\bar{a}+\bar{b})^{11})^2(\bar{a}+\bar{b})^6=(\bar{a}+\bar{b})^2\cdot(\bar{a}+\bar{b})^6=(\bar{a}+\bar{b})^8=$

$$=\bar{a}^{8}+\bar{8}\,\bar{a}^{7}\bar{b}+\overline{\frac{8\cdot 7}{2}}\,\bar{a}^{6}\bar{b}^{2}+\overline{\frac{8\cdot 7\cdot 6}{6}}\,\bar{a}^{5}\bar{b}^{3}+\overline{\frac{8\cdot 7\cdot 6\cdot 5}{6\cdot 4}}\,\bar{a}^{4}\bar{b}^{4}+\overline{\frac{8\cdot 7\cdot 6}{6}}\,\bar{a}^{3}\bar{b}^{5}+$$

$$+\overline{\frac{8\cdot 7}{2}}\,\bar{a}^{2}\bar{b}^{6}+\bar{8}\,\bar{a}\,\bar{b}^{7}+\bar{b}^{8}=\bar{a}^{8}+\bar{8}\,\bar{a}^{7}\bar{b}+\bar{6}\,\bar{a}^{6}\bar{b}^{2}+\bar{a}^{5}\bar{b}^{3}+\bar{4}\,\bar{a}^{4}\bar{b}^{4}+\bar{a}^{3}\bar{b}^{5}+$$

$$+\bar{6}\,\bar{a}^{2}\bar{b}^{6}+\bar{8}\,\bar{a}\,\bar{b}^{7}+\bar{b}^{8}.$$

$$(\bar{a}+\bar{b})^{44}=((\bar{a}+\bar{b})^{11})^{4}=(\bar{a}+\bar{b})^{4}=\bar{a}^{4}+\bar{4}\,\bar{a}^{3}\bar{b}+\overline{\frac{4\cdot 3}{2}}\,\bar{a}^{2}\bar{b}^{2}+\bar{4}\,\bar{a}\,\bar{b}^{3}+\bar{b}^{4}.$$

$$(\bar{a}+\bar{b})^{75}=(\bar{a}+\bar{b})^{66}(\bar{a}+\bar{b})^{9}=(\bar{a}+\bar{b})^{6}(\bar{a}+\bar{b})^{9}=(\bar{a}+\bar{b})^{15}=(\bar{a}+\bar{b})^{11}(\bar{a}+\bar{b})^{4}=$$

$$=(\bar{a}+\bar{b})^{5}=\bar{a}^{5}+\bar{5}\,\bar{a}^{4}\bar{b}+\overline{10}\,\bar{a}^{3}\bar{b}^{2}+\overline{10}\,\bar{a}^{2}\bar{b}^{3}+\bar{5}\,\bar{a}\,\bar{b}^{4}+\bar{b}^{5}.$$

б) $(\bar{a}+\bar{b})^{51}=((\bar{a}+\bar{b})^{17})^{3}=(\bar{a}+\bar{b})^{3}=\bar{a}^{3}+3\bar{a}^{2}\bar{b}+3\bar{a}\,\bar{b}^{2}+\bar{b}^{3}.$

$$(\bar{a}+\bar{b})^{38}=(\bar{a}+\bar{b})^{34}\,(\bar{a}+\bar{b})^{4}=(\bar{a}+\bar{b})^{2}\cdot(\bar{a}+\bar{b})^{4}=(\bar{a}+\bar{b})^{6}=$$

$$=\bar{a}^{6}+\bar{6}\,\bar{a}^{5}\bar{b}+\overline{\frac{6\cdot 5}{2}}\,\bar{a}^{4}\bar{b}^{2}+\overline{\frac{6\cdot 5\cdot 4}{6}}\,\bar{a}^{3}\bar{b}^{3}+\overline{\frac{6\cdot 5}{2}}\,\bar{a}^{2}\bar{b}^{4}+\bar{6}\,\bar{a}\,\bar{b}^{5}+\bar{b}^{6}=$$

$$=\bar{a}^{6}+\bar{6}\,\bar{a}^{5}\bar{b}+\overline{15}\,\bar{a}^{4}\bar{b}^{2}+\bar{3}\,\bar{a}^{3}\bar{b}^{3}+\overline{15}\,\bar{a}^{2}\bar{b}^{4}+\bar{6}\,\bar{a}\,\bar{b}^{5}+\bar{b}^{6}.$$

$$(\bar{a}+\bar{b})^{155}=((\bar{a}+\bar{b})^{17})^{5}(\bar{a}+\bar{b})^{15}=(\bar{a}+\bar{b})^{15+5}=(\bar{a}+\bar{b})^{17}(\bar{a}+\bar{b})^{3}=(\bar{a}+\bar{b})^{4}=$$

$$=\bar{a}^{4}+\bar{4}\,\bar{a}^{3}\bar{b}+\bar{6}\,\bar{a}^{2}\bar{b}^{2}+\bar{4}\,\bar{a}\,\bar{b}^{3}+\bar{b}^{4}.$$

№5. Доказать что композиция функций не коммутативна.

а) $f(x)=\sin x$, $g(x)=\sqrt{x^2-5x+9}$.

Решение:

$X=Y=Z=\mathbf{R}$, $f: X\to Y$, $g: Y\to Z$, где $f(x)=\sin x$, $g(x)=\sqrt{x^2-5x+9}$.

Поскольку $D=25-36=-11<0 \Rightarrow x^2-5x+9>0 \ \forall x\in R$, функция g всюду на $\mathbf{R}$ определена. Построим композиции функций gf и fg. Очевидно, что $D(gf)=D(fg)=\mathbf{R}$.

$$gf(x)=\sqrt{\sin^2 x-5\sin x+9},\ \text{при } x=0\ gf(0)=3;$$

$$fg(x)=\sin\sqrt{x^2-5x+9},\ \text{при } x=0\ fg(0)=\sin 3\neq 3\ (|\sin x|\le 1).$$

Итак, $gf\neq fg$.

б) $f(x)=\log_2 x$, $g(x)=\log_3 x$.

Решение:

$f, g: \mathbf{R}_{>0}\to\mathbf{R}$, $f(x)=\log_2 x$, $g(x)=\log_3 x$. f и g – биекции. $D(fg)=D(gf)=\mathbf{R}_{>1}$.

$fg(2)=\log_2(\log_3 2)<0$, т.к. $\log_3 2<1$.

$gf(2)=\log_3(\log_2 2)=\log_3 1=0$.

Т.к. $fg(2)\neq gf(2)$, то не может быть равенства композиций функций $fg=gf$ во всей области определения $\mathbf{R}_{>1}$.

№6. Заданы три вещественных функции $f, g, h: \mathbf{R}\to\mathbf{R}$.

1) Найти заданные композиции функций: fgh, hfg, ffg.

2) Являются ли f, g, h инъекциями, сюръекциями, биекциями на $\mathbf{R}$?

3) Найти обратные функции к f, g, h. Если функции со своими областями определения обратных не имеют, то найти обратные функции к их сужениям.

а) $f(x)=2x-3$, $g(x)=x^3+7x-8$, $h(x)=2^{x^2+16x}$.

Решение:

1) $D(f)=D(g)=D(h)=\mathbf{R}$, поэтому все три указанные композиции функций определены на **R**.

$gh(x)=(2^{x^2+16x})^3+7\cdot 2^{x^2+16x}-8=2^{3x^2+48x}+7\cdot 2^{x^2+16x}-8$.

$fgh(x)=2\cdot(2^{3x^2+48x}+7\cdot 2^{x^2+16x}-8)-3=2\cdot 2^{3x^2+48x}+14\cdot 2^{x^2+16x}-19$.

$hfg(x)=2^{(2x^2+14x-19)^2+16*(2x^3+14x-19)}\ \forall x\in\mathbf{R}$.

$fg(x)=2\cdot(x^3+7x-8)-3=2x^3+14x-19\ \forall x\in\mathbf{R}$.

$ffg(x)2\cdot(x^3+7x-8)-3=4x^3+28x-41\ \forall x\in\mathbf{R}$.

2) $2x-3=y$, $x, y\in\mathbf{R}$, $\forall y\in\mathbf{R}$.

$2x=y+3$,

$x=\frac{y+3}{2}=\frac{y}{2}+\frac{3}{2}\ \Rightarrow f$ – сюръекция на **R**.

Пусть $x_1\neq x_2$, если $2x_1-3=2x_2-3$, то приходим к противоречию: $x_1=x_2$. Следовательно, f – инъекция.

Таким образом, f – биекция на **R**.

Функция g непрерывна на **R**. $\lim\limits_{x\to-\infty}g(x)=-\infty$ и $\lim\limits_{x\to+\infty}g(x)=+\infty$. Поэтому g является сюръекцией на **R**.

$g'(x)=3x^2+7>0$ для всех $x\in\mathbf{R}$, поэтому g является строго возрастающей функцией на **R**. Поэтому f инъективна.

Таким образом, g – биекция на **R**.

Т.к. $2^{x^2+16x}>0\ \forall x\in\mathbf{R}$ то h не является сюръекцией на **R**.

$x_1\neq x_2$.

$2^{x_1^2+16x_1}=2^{x_2^2+16x_2}\ \Leftrightarrow x_1^2+16x_1=x_2^2+16x_2$.

$x^2+16x=x(x+16)$.

$x=0$: $x^2+16x=0$

$x=-16$: $x^2+16x=0$

$h(0)=2^0=1$, $h(16)=2^0=1\ \Rightarrow$h не является инъекцией.

Таким образом, h – не биекция на **R**.

3) f: $2x-3=y$, $x=\frac{y+3}{2}=\frac{1}{2}y+\frac{3}{2}$; $f^{-1}(x)=\frac{1}{2}x+\frac{3}{2}\ \forall x\in\mathrm{R}$.

h: $2^{x^2+16x}=y$

$x^2+16x=\log_2 y$

$x^2+16x-\log_2 y=0$

$\frac{D}{4}=8^2+\log_2 y=64+\log_2 y\geq 0$

$\log_2 y\geq -64$

$y\geq 2^{-64}$

$x_1 = -8 - \sqrt{64 + \log_2 y}$;

$x_2 = -8 + \sqrt{64 + \log_2 y}$.

$h_1^{-1}(x) = -8 - \sqrt{64 + \log_2 x}$, $h_2^{-1}(x) = -8 + \sqrt{64 + \log_2 x}$, $x \in \left[2^{-64}, +\infty\right)$.

h_1^{-1}–обратная к функции h_1, $D(h_1) = (-\infty; -8]$, h_2– обратная к функции h_2^{-1}, $D(h_2) = [-8; +\infty)$.

g: $g(x) = x^3 + 7x - 8$, g – биекция на **R**.

$x^3 + 7x - 8 = y$

$x^3 + 7x - (8 + y) = 0$.

Формула Кордано решения в **R** кубического уравнения $x^3 + px + q = 0$:

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}\ .$$

При p=7, q= –8–y получаем

$$x = \sqrt[3]{\frac{8+y}{2} + \sqrt{\frac{8+y^2}{4} + \frac{343}{27}}} + \sqrt[3]{\frac{8+y}{2} - \sqrt{\frac{8+y^2}{4} + \frac{343}{27}}} \quad \forall y \in \mathbf{R}.$$

$$g^{-1}(x) = \sqrt[3]{\frac{8+y}{2} + \sqrt{\frac{8+y^2}{4} + \frac{343}{27}}} + \sqrt[3]{\frac{8+y}{2} - \sqrt{\frac{8+y^2}{4} + \frac{343}{27}}} \quad \forall x \in \mathbf{R}, \ D(g^{-1}) = \mathbf{R}.$$

б) $f(x)=2x^9-7$, $g(x)=5arctg(4x)+2$, $h(x)=e^{5^x} - 17$.

1) $D(f)=D(g)=D(h)=\mathbf{R}$, поэтому все три указанные композиции функций определены на **R**.

$$fgh(x)=f(gh(x))=2(gh(x))^9-7=2(5arctg(4h(x))+2)^9-7=2(5arctg(4(e^{5^x}-17))+2)^9-7=$$
$$=2(5arctg(4e^{5^x}-68)+2)^9-7.$$

$$hfg(x)=hf(g(x))=hf(5arctg(4x)+2)=h(2(5arctg(4x)+2)^9-7)=e^{5^{2(5arctg(4x)+2)^9-7}}-17.$$

$$ffg(x)=f(fg(x))=f(2(5arctg(4x)+2)^9-7)=2(2(5arctg(4x)+2)^9-7)^9-7.$$

2) Рассмотрим функцию $f(x)=2x^9-7$. Производная функции $f'(x)=18x^8>0$ для всех $x \in \mathbf{R}\setminus\{0\}$, поэтому f является строго возрастающей функцией на $(-\infty,0)\cup(0,+\infty)$. $f'(0)=0$, $f(0)=-7\neq f(\xi)$ для $\forall \xi \neq 0$. Поэтому f инъективна.

Функция f непрерывна на **R**. $\lim\limits_{x\to-\infty} f(x) = -\infty$ и $\lim\limits_{x\to+\infty} f(x) = +\infty$. Поэтому f является сюръекцией на **R**. Итак, f: $\mathbf{R}\to\mathbf{R}$ – биекция.

Рассмотрим функцию $g(x)=5arctg(4x)+2$. Производная функции g $g'(x) = \dfrac{20}{1+16x^2} > 0$ для любого $x \in \mathbf{R}$. Следовательно, функция строго возрастает на всей области определения **R**. Поэтому g – инъекция. Поскольку $-\pi/2<arctg(4x)<\pi/2$ для всех $x \in \mathbf{R}$, то $-5\pi/2+2<g(x)<5\pi/2+2$ для всех $x \in \mathbf{R}$. Значит, g не является сюръекцией на **R**. Итак, g: $\mathbf{R}\to\mathbf{R}$ не является биекцией.

Рассмотрим функцию $h(x)=e^{5^x}-17$. $h=h_3h_2h_1$, где $h_1(x)=5^x$, $h_2(x)=e^x$, $h_3(x)=x-17$, $D(h_i)=\mathbf{R}$, $i=1, 2, 3$. $h_1'(x) = \ln 5 \cdot 5^x > 0$ для $\forall x \in \mathbf{R}$, следовательно, h_1

строго возрастает на **R**, значит, h_1 – инъекция $h_2'(x)=e^x>0$ для $\forall x\in\mathbf{R}$, следовательно, h_2 строго возрастает на **R**, значит, h_2 – инъекция. Пусть $x_1\neq x_2$; из равенства $x_1-17=x_2-17$ следует, что $x_1=x_2$, поэтому h_3 – инъекция. h является инъективной функцией, как композиция инъекций, по свойству 2 композиции функций. $0<5^x<+\infty$ для всех $x\in\mathbf{R}$, $1<e^{5^x}<+\infty$ для всех $x\in\mathbf{R}$, $-16<e^{5^x}-17<+\infty$ для всех $x\in\mathbf{R}$. Значит, h не является сюръекцией на **R**. Итак, h: $\mathbf{R}\to\mathbf{R}$ не является биекцией.

3) Поскольку f: $\mathbf{R}\to\mathbf{R}$ – биекция, то по теореме 2.1.1 на **R** существует обратная функция к f – f^{-1}: $\mathbf{R}\to\mathbf{R}$.

$$2x^9-7=y;$$
$$x^9=\frac{y+7}{2};$$
$$x=\sqrt[9]{\frac{y+7}{2}}.$$

Итак, $f^{-1}(x)=\sqrt[9]{\frac{x+7}{2}}$, $x\in\mathbf{R}$.

E(g)=(–5π/2+2, 5π/2+2). Поскольку g – инъекция на **R**, то g: $\mathbf{R}\to$E(g) – биекция. Поэтому, по теореме 2.1.1 на E(g) существует обратная функция к g – g^{-1}: E(g)$\to\mathbf{R}$.

$$5arctg(4x)+2=y;$$
$$5arctg(4x)=y-2;$$
$$arctg(4x)=\frac{y-2}{5};$$
$$4x=tg\left(\frac{y-2}{5}\right);$$
$$x=\frac{1}{4}tg\left(\frac{y-2}{5}\right).$$

Итак, $g^{-1}(x)=\frac{1}{4}tg\left(\frac{x-2}{5}\right)$, $x\in(-5\pi/2+2,\ 5\pi/2+2)$.

E(h)=(–16;+∞). Поскольку h – инъекция на **R**, то h: $\mathbf{R}\to$E(h) – биекция. Тогда по теореме 3.1 для функции h существует обратная функция h^{-1}: E(h)$\to\mathbf{R}$.

$$e^{5^x}-17=y;$$
$$e^{5^x}=y+17;$$
$$5^x=ln(y+17);$$
$$x=log_5(ln(y+17)).$$

Итак, $h^{-1}(x)=log_5(ln(x+17))$, $x\in(-16;+\infty)$.

№7. Обратима ли функция f? В случае положительного ответа найти обратную функцию f^{-1}. $f(\bar{c})=A\cdot\bar{c}$ (mod 26), где $\bar{c}\in\left(\mathbf{Z}/26\mathbf{Z}\right)^3$.

а) $A=\begin{pmatrix} \overline{11} & \overline{2} & \overline{19} \\ \overline{5} & \overline{23} & \overline{25} \\ \overline{22} & \overline{7} & \overline{1} \end{pmatrix}$.

Решение:

$$\det A=11\cdot 23\cdot 1+5\cdot 7\cdot 19+2\cdot 25\cdot 22-19\cdot 23\cdot 22-7\cdot 25\cdot 11-5\cdot 2\cdot 1\equiv$$
$$\equiv 11(-3)+9\cdot 19-44+19\cdot 3\cdot 22+7\cdot 11-10\equiv 75\cdot 19-10\equiv(-3)\cdot 19-10\equiv(-3)\cdot(-7)-10=$$
$$=21-10=11(\mathrm{mod}\ 26)\Rightarrow \exists A^{-1}\ \det A^{-1}=11^{-1};$$
$$26=11\cdot 2+4;\ 4=26-11\cdot 2;$$
$$11=4\cdot 2+3;\ 3=11-4\cdot 2=11-26\cdot 2+11\cdot 4=(-2)\cdot 26+5\cdot 11;\ 4=3\cdot 1+1;$$
$$1=4-3=26-11\cdot 2+2\cdot 26-5\cdot 11=3\cdot 26-7\cdot 11;\ 11^{-1}\equiv -7\equiv 19(\mathrm{mod}\ 26).$$

$$A^{-1}=\overline{19}\begin{pmatrix} \begin{vmatrix} \overline{29} & \overline{25} \\ \overline{7} & \overline{1} \end{vmatrix} & -\begin{vmatrix} \overline{2} & \overline{19} \\ \overline{7} & \overline{1} \end{vmatrix} & \begin{vmatrix} \overline{2} & \overline{19} \\ \overline{23} & \overline{25} \end{vmatrix} \\ -\begin{vmatrix} \overline{5} & \overline{25} \\ \overline{22} & \overline{1} \end{vmatrix} & \begin{vmatrix} \overline{11} & \overline{19} \\ \overline{22} & \overline{1} \end{vmatrix} & -\begin{vmatrix} \overline{11} & \overline{19} \\ \overline{5} & \overline{25} \end{vmatrix} \\ \begin{vmatrix} \overline{5} & \overline{23} \\ \overline{22} & \overline{7} \end{vmatrix} & -\begin{vmatrix} \overline{11} & \overline{2} \\ \overline{22} & \overline{7} \end{vmatrix} & \begin{vmatrix} \overline{11} & \overline{2} \\ \overline{5} & \overline{23} \end{vmatrix} \end{pmatrix}=$$ в $Z/26Z=$

$$=\overline{19}\begin{pmatrix} \overline{-3+7} & \overline{-(2+49)} & \overline{-2-3\cdot 7} \\ \overline{-(5+22)} & \overline{11-28} & \overline{-(-11+35)} \\ \overline{35-12} & \overline{-(77+8)} & \overline{-33-10} \end{pmatrix}=\overline{19}\begin{pmatrix} \overline{4} & \overline{1} & \overline{3} \\ \overline{-1} & \overline{-17} & \overline{2} \\ \overline{-3} & \overline{-7} & \overline{9} \end{pmatrix}=$$

$$=\overline{-7}\begin{pmatrix} \overline{4} & \overline{1} & \overline{3} \\ \overline{-1} & \overline{9} & \overline{2} \\ \overline{-3} & \overline{-7} & \overline{9} \end{pmatrix}=\begin{pmatrix} \overline{-2} & \overline{-7} & \overline{-21} \\ \overline{7} & \overline{-11} & \overline{-14} \\ \overline{21} & \overline{13} & \overline{-11} \end{pmatrix}=\begin{pmatrix} \overline{24} & \overline{19} & \overline{5} \\ \overline{7} & \overline{15} & \overline{12} \\ \overline{21} & \overline{23} & \overline{15} \end{pmatrix}.$$

Ответ: $\det A=\overline{11}$, $\det A^{-1}=\overline{19}$, $A^{-1}=\begin{pmatrix} \overline{24} & \overline{19} & \overline{5} \\ \overline{7} & \overline{15} & \overline{12} \\ \overline{21} & \overline{23} & \overline{15} \end{pmatrix}$.

б) $A=\begin{pmatrix} \overline{1} & \overline{2} & \overline{3} \\ \overline{4} & \overline{5} & \overline{6} \\ \overline{7} & \overline{8} & \overline{0} \end{pmatrix}$.

Решение:

$$\det A=\overline{18}+\overline{84}-\overline{105}-\overline{48}=\overline{102}-\overline{153}=-\overline{51}=-(\overline{-1})=\overline{1},\ \det A^{-1}=\overline{1}.$$

$$A^{-1}=\begin{pmatrix} \overline{\begin{vmatrix}5&6\\8&0\end{vmatrix}} & \overline{-\begin{vmatrix}2&3\\8&0\end{vmatrix}} & \overline{\begin{vmatrix}2&3\\5&6\end{vmatrix}} \\ \overline{-\begin{vmatrix}4&6\\7&0\end{vmatrix}} & \overline{\begin{vmatrix}1&3\\7&0\end{vmatrix}} & \overline{-\begin{vmatrix}1&3\\4&6\end{vmatrix}} \\ \overline{\begin{vmatrix}4&5\\7&8\end{vmatrix}} & \overline{-\begin{vmatrix}1&2\\7&8\end{vmatrix}} & \overline{\begin{vmatrix}1&2\\4&5\end{vmatrix}} \end{pmatrix}=\begin{pmatrix} \overline{-48} & \overline{24} & \overline{-3} \\ \overline{42} & \overline{-21} & \overline{6} \\ \overline{-3} & \overline{6} & \overline{-3} \end{pmatrix}=\begin{pmatrix} \bar{4} & \overline{24} & \overline{23} \\ \overline{16} & \bar{5} & \bar{6} \\ \overline{23} & \bar{6} & \overline{23} \end{pmatrix}.$$

Ответ: $\det A=\bar{1},\ \det A^{-1}=\bar{1},\ A^{-1}=\begin{pmatrix} \bar{4} & \overline{24} & \overline{23} \\ \overline{16} & \bar{5} & \bar{6} \\ \overline{23} & \bar{6} & \overline{23} \end{pmatrix}$.

2.2 Взаимно однозначное соответствие. Мощность множества. Счетные и континуальные множества

№ 1. Задает ли функция f взаимно однозначное соответствие между множествами?

1) A={множество людей в аудитории}, B={$x\in\mathbf{R}$ | $1{,}5\le x\le 2$}, f: A→B, где функция f ставит в соответствие каждому человеку его рост в метрах.

2) X=Y=**R**, f: X→Y, где $f(x)=\sin x$. В случае отрицательного ответа как нужно изменить множества, чтобы функция f задавала взаимно однозначное соответствие между ними?

№ 2. Пусть A и B – конечные множества. Доказать следующие утверждения:

1) $|A\cap B|=|A|-|A\setminus B|$;

2) $|A\cup B|=|A|+|B|-|A\cap B|$;

3) $|A\Delta B|=|A|+|B|-2|A\cap B|$;

4) $|A\times B|=|A|\cdot|B|$;

5) $|A^n|=|A|^n,\ \forall n\in\mathbf{N}$.

№ 3. Показать, что множества $\mathbf{R}^2$ и A×B, где A={$(x, y)\in\mathbf{R}^2$ | $2x+y=1$}, B={$(x, y)\in\mathbf{R}^2$ | $x-y=0$}, равномощны.

Решение:

Нетрудно видеть, что $\mathbf{R}^2$ равномощно множеству всех точек на действительной плоскости, A равномощно множеству всех точек прямой $2x+y=1$, B – множеству всех точек прямой $x-y=0$ на действительной плоскости. Поскольку коэффициенты при x и y у данных двух прямых не пропорциональны, прямые пересекаются на плоскости в единственной точке с координатами (1/3, 1/3). Для доказательства равномощности $\mathbf{R}^2$ и A×B достаточно показать равномощность множеств всех точек действительной плоскости и всех упорядоченных пар точек на прямых $2x+y=1$ и $x-y=0$.

Каждой точке M на плоскости поставим в соответствие пару точек (A_M, B_M) на прямых $2x+y=1$ и $x-y=0$, являющихся точками пересечения этих прямых с прямыми, проходящими через данную точку и параллельными $x-y=0$ и $2x+y=1$ соответственно. Если точка N принадлежит прямой $2x+y=1$ либо $x-y=0$, то первым (вторым) элементом пары точек на прямых будет сама данная точка, а вторым (первым) элементом пары – точка (1/3, 1/3) (см. рис. 2.2.1).

Согласно утверждениям планиметрии, данное правило задает взаимно однозначное соответствие между множеством всех точек на действительной плоскости ($\mathbf{R}^2$) и множеством всех упорядоченных пар точек на прямых $2x+y=1$ и $x-y=0$ (A×B).

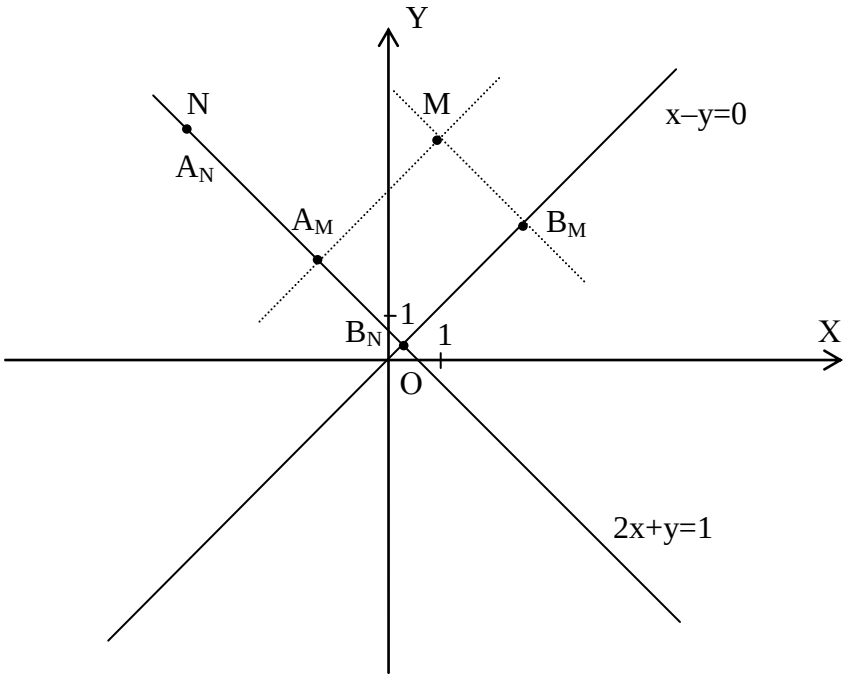


Рис. 2.2.1

№ 4. Доказать, что множество $\mathbf{N}^2$ счетно.

Решение:

$\mathbf{N}^2=\{(m, n) \mid m, n\in\mathbf{N}\}$. Разобьем $\mathbf{N}^2$ на классы. К первому классу N_2 отнесем все пары чисел с минимальной суммой, равной 2. Таким образом, $N_2=\{(1, 1)\}$. Ко второму классу N_3 отнесем все пары чисел с суммой 3: $N_3=\{(1, 2), (2, 1)\}$. Тогда $N_4=\{(1, 3), (2, 2), (3, 1)\}$. В общем случае $N_i = \{(1, i-1), (2, i-2), (3, i-3),\ldots, (i-1, 1)\}$, $i=2, 3,\ldots$ Каждый класс содержит ровно $i-1$ пару. Упорядочим классы по возрастанию индексов i, а пары внутри класса – по возрастанию первого элемента и занумеруем получившуюся последовательность пар номерами 1, 2, 3,… Легко видеть, что если $m+n=i+1$, то пара (m, n) получит номер $0+1+2+\ldots+(i-1)+m=\frac{(i-1)\cdot i}{2}+m$. Эта нумерация задает взаимно однозначное соответствие $\mathbf{N}^2 \leftrightarrow \mathbf{N}$ и доказывает счетность $\mathbf{N}^2$.

№ 5. Доказать, что бесконечное множество равносторонних треугольников, в котором вершинами каждого треугольника являются

середины сторон уже построенного треугольника (рис. 2.2.2), является счётным.

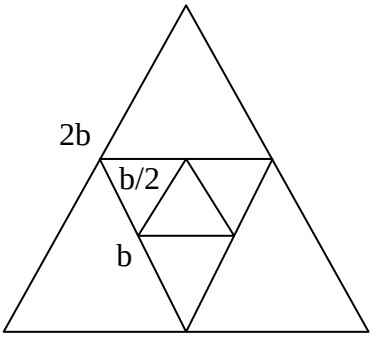


Рис. 2.2.2

Решение:

Докажем, что это бесконечное множество равносторонних треугольников является счётным. Каждому равностороннему треугольнику поставим в соответствие длину его стороны. Если длина стороны фиксированного треугольника равна b, то длина стороны предыдущего треугольника равна $2b$, а последующего – $b/2$. Итак, существует взаимно однозначное соответствие между данным бесконечным множеством равносторонних треугольников и множеством чисел $T_b=\{2^n b \mid n\in\mathbf{Z}\}$. Покажем, что $T_b\leftrightarrow\mathbf{N}$.

$$\begin{array}{lccccccccc} T_b\colon & \dots & 2^{-n}b & \dots & 2^{-2}b & 2^{-1}b & b & 2b & 4b & \dots 2^n b \quad \dots \\ & & \downarrow & & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ \mathbf{N}\colon & \dots & 2n+1 & \dots & 5 & 3 & 1 & 2 & 4 & \dots 2n \quad \dots \end{array}$$

$$f\left(2^n b\right)=\begin{cases} 2n, & n\in\mathbf{N}; \\ 2|n|+1, & n\in\mathbf{Z}_{\le 0}. \end{cases}$$

f задает взаимно однозначное соответствие между множествами T_b и $\mathbf{N}$. Следовательно, рассмотренное бесконечное множество равносторонних треугольников является счетным.

№ 6. Построить взаимно однозначные соответствия между множествами:

1) $[0, 1]$ и $[0, 1]\cup[3, 4]$;

2) $[0, 1]$ и $[10, 11]\cup\{12\}$;

3) $[0, 1]$ и $[0, 1]\cup\{3\}\cup\{4\}$.

№ 7. Показать, что множество всех вещественных чисел интервала $(0,+\infty)$ – континуальное множество.

Решение:

Известно, что $\mathbf{R}$ – континуальное множество. Рассмотрим соответствие $f\colon \mathbf{R}\to(0,+\infty)$, $f(x)=e^x$, $\forall x\in\mathbf{R}$. Тогда для $\forall y\in(0,+\infty)$ существует единственное $x\in\mathbf{R}$, такое что $f(x)=y$, $x=\ln y$. Итак, $\mathbf{R}\leftrightarrow(0,+\infty)$.

№ 8. Доказать, что множество точек гиперболы $y=1/x$ на действительной плоскости имеет мощность континуум.

Решение:

Представим множество точек гиперболы в следующем виде: $\Gamma=\{(x,\ 1/x)\mid x\in\mathbf{R}\backslash\{0\}\}$. Установим взаимно однозначное соответствие между множествами Γ и $\mathbf{R}$.

$$f((x,\ 1/x))=\begin{cases}x,\ x\in\mathbf{R}\backslash\mathbf{Z}_{\geq 0};\\ x-1,\ x\in\mathbf{N}.\end{cases}$$

$f\colon \Gamma\to\mathbf{R}$ действительно является взаимно однозначным соответствием (рис. 2.2.3). Итак, $\Gamma\leftrightarrow\mathbf{R}$. Поскольку $\mathbf{R}$ – континуальное множество, Γ – также континуальное множество.

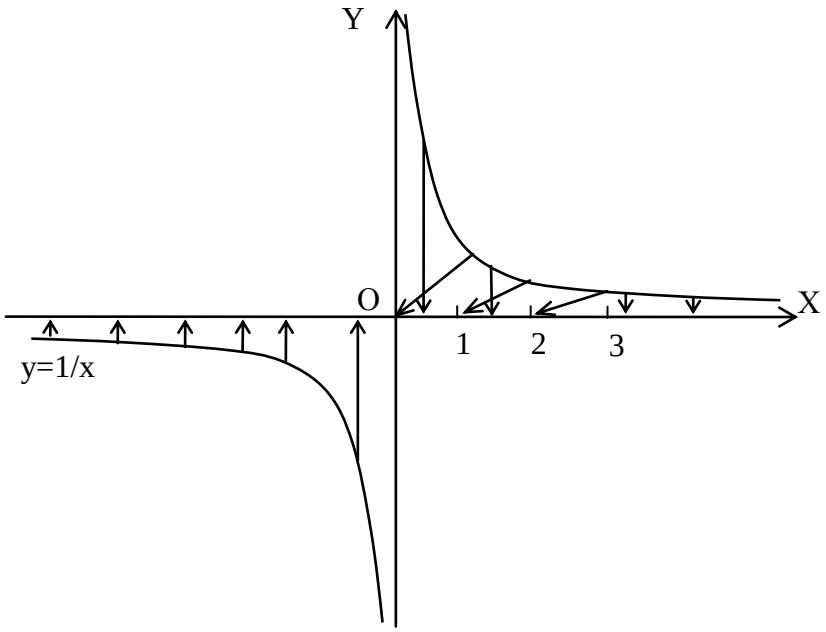


Рис. 2.2.3

№9. Доказать, что равномощны множества $C\backslash\{0\}$ и $(0,+\infty)\times(-2\pi,\pi)$.

Решение:

$(-2\pi,\ \pi)\leftrightarrow[0,\ 2\pi)$, $f(x)=\dfrac{x+2\pi}{3\pi}\cdot 2\pi=\dfrac{2}{3}(x+2\pi)$, f – биекция.

$(0,\ 2\pi)\leftrightarrow[0,\ 2\pi)$;

$g(x)=x$, $x\neq 0{,}5,\ 0{,}55,\ldots$

$g(0{,}5)=0$;

$g(0{,}55)=0{,}5$ и т.д.

$gf\colon (-2\pi,\ \pi)\leftrightarrow[0,\ 2\pi)\Rightarrow(0,+\infty)\times(-2\pi,\ \pi)\leftrightarrow(0,+\infty)\times[0,\ 2\pi)$.

$h(z)=\rho e^{i\varphi}$, $\rho\in(0,+\infty)$, $\varphi\in[0,\ 2\pi)$, – показательная форма записи.

h – биекция $C\backslash\{0\}$ на $(0,+\infty)\times(-2\pi,\pi)$.

2.3. Классические шифры

№1. Зашифровывание фразы на латинском языке осуществляется в два этапа. На первом этапе каждая буква текста заменяется на следующую в алфавитном порядке (Z заменяется на A). На втором этапе применяется шифр

простой замены с неизвестным ключом. Его применение заключается в замене каждой буквы шифрованного текста буквой того же алфавита, при этом разные буквы заменяются разными буквами. Ключом такого шифра является таблица, в которой указано, какой буквой надо заменить каждую букву алфавита. По данному шифртексту

OSZJX FXRF YOQJSZ RAYFJ

восстановить отправленное сообщение, если известно, что для использованного (неизвестного) ключа результат шифрования не зависит от порядка выполнения указанных этапов для любого отправленного сообщения. Пробелы разделяют слова, при зашифровывании пробел остается пробелом. Известно также, что в результате зашифровывания $\mathrm{A} \to \mathrm{F}$.

Решение:

Таблица 2.3.1

Порядковый номер	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Латинский алфавит	A	B	C	D	E	F	G	H	I	J	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z

Занумеруем буквы латинского алфавита от 0 до 23, как указано в таблице 2.3.1. Пусть $x \in [0,\ 23]$ – некоторое число, $f(x)$ – число, в которое переходит x на втором этапе. Тогда перестановочность этапов можно записать в виде: $f(x+1) = f(x)+1$, то есть $f(x+1) - f(x) = 1$, значит, соседние числа x и x+1 на втором этапе переходят в соседние числа $f(x)$ и $f(x)+1$, отсюда следует, что второй этап – тоже циклический сдвиг. Последовательное применение $f(x)+1$ двух сдвигов – сдвиг. Итак, мы имеем классический шифр Цезаря. Остаётся рассмотреть 24 варианта различных сдвигов. Но поскольку в условии указано, что в результате зашифровывания $\mathrm{A} \to \mathrm{F}$, то получаем, что зашифровывание представляет собой циклический сдвиг на 5 позиций вправо. Осложнения, связанные с переходом Z в A, устраняются либо переходом к остаткам при делении на 24, либо выписыванием после буквы Z второй раз алфавита AB…Z, т.е. операции выполняются в $\mathbf{Z}/24\mathbf{Z}$. Итак, для расшифровывания фразы нужно каждую букву полученного сообщения сдвинуть циклически на 5 позиций влево, а пробелы оставить на месте.

Итак, получаем следующее исходное сообщение:

INTER ARMA SILENT MUSAE (´интэр ´арма с´илент м´узэ – когда гремит оружие, музы молчат).

Ответ: INTER ARMA SILENT MUSAE.

№2. Пусть x_1, x_2 – корни многочлена x^2+3x+1. К порядковому номеру каждой буквы в стандартном русском алфавите (33 буквы) прибавляется значение многочлена $f(x) = x^6 + 3x^5 + x^4 + x^3 + 4x^2 + 4x + 3$, вычисленного либо при $x=x_1$, либо при $x=x_2$ (в неизвестном порядке), а затем получают число, замененное соответствующей ему буквой. Нужно расшифровать сообщение

ФВМЁЖТИВФЮ.

Решение:

Занумеруем буквы русского алфавита от 0 до 32. Все операции будут выполняться в **Z**/33**Z.** Легко видеть, что $f(x)=(x^2+3x+1)(x^4+x+1)+2$. Отсюда $f(x_1)=f(x_2)=2$, где x_1, x_2 – корни x^2+3x+1. Итак, мы имеем классический шифр Цезаря с циклическим сдвигом на 2 позиции вправо. Для расшифровывания сообщения нужно каждую букву циклически сдвинуть на 2 позиции влево. Смотрите таблицу 2.3.2.

Таблица 2.3.2

Буква ш. с.	Ф	В	М	Ё	Ж	Т	И	В	Ф	Ю
Порядковый номер буквы ш. с.	21	2	13	6	7	19	9	2	21	31
Порядковый номер буквы и. с.	19	0	11	4	5	17	7	0	19	29
Буква и. с.	Т	А	К	Д	Е	Р	Ж	А	Т	Ь

Ответ: ТАКДЕРЖАТЬ.

№3. Зашифровывание сообщения на русском языке в алфавите без букв Ё, Й, Ъ осуществляется следующим образом. Пусть сообщение состоит из *n* букв. Выбирается ключ *K* – некоторая последовательность из *n* букв приведенного выше алфавита. Зашифровывание каждой буквы сообщения состоит в сложении ее номера в таблице с номером соответствующей буквы ключевой последовательности и замене полученной суммы на букву алфавита, номер которой имеет тот же остаток от деления на 30, что и эта сумма. Фактически, это шифр Виженера.

Прочитайте РБЫНПТСИТСРРЕЗОХ, если известно, что ключевая последовательность не содержит никаких букв, кроме Б, В, Г.

Решение:

Каждая буква шифрованного сообщения расшифровывается в трех вариантах, предполагая последовательно, что соответствующая буква шифрованной последовательности есть Б, В или Г.

Таблица 2.3.3

Шифрованное сообщение	Р	Б	Ы	Н	П	Т	С	И	Т	С	Р	Р	Е	З	О	Х
вариант Б	П	А	Щ	М	О	С	Р	З	С	Р	П	П	Д	Ж	Н	Ф
вариант В	О	Я	Ш	Л	Н	Р	П	Ж	Р	П	О	О	Г	Е	М	У
вариант Г	Н	Ю	Ч	К	М	П	О	Е	П	О	Н	Н	В	Д	Л	Т

Выбирая из каждой колонки полученной таблицы 2.3.3 ровно по одной букве, находим осмысленное сообщение НАШКОРРЕСПОНДЕНТ, которое и является искомым.

Можно было найти НАШМОРОЗПОПОВЕМУ. Если предположить искажение в шифрованном сообщении (в качестве одиннадцатой буквы была бы принята не Р, а П), то получим НАШМОРОЗПОМОГЕМУ. Число всех

различных вариантов сообщений без ограничений на осмысленность равно 3^{16} или 43046721, то есть более 40 миллионов!

Ответ: НАШКОРРЕСПОНДЕНТ.

№4. Зашифровывание сообщения на русском языке в алфавите без букв Ё, Й, Ъ и с добавлением знака пробел _ осуществляется следующим образом. Пусть сообщение состоит из *n* букв. Выбирается ключ *K* – некоторая периодическая последовательность из *n* букв приведенного выше алфавита с периодом 3, в периоде которой все буквы различны. Зашифровывание каждой буквы сообщения состоит в сложении ее номера в таблице с номером соответствующей буквы ключевой последовательности и замене полученной суммы на букву алфавита, номер которой имеет тот же остаток от деления на 31, что и эта сумма. Это также шифр Виженера.

Прочитайте РБЫВЛРУСЗФРРРЕЗРУ, если известно, что ключевая последовательность не содержит никаких букв кроме Б, В, Г.

Решение:

Количество различных вариантов ключевых периодических последовательностей равно 3!=6. Выбирая из каждой колонки таблицы 2.3.4, построенной как и в предыдущей задаче, выбираем ровно по одной букве, учитывая вид ключевой периодической последовательности.

Таблица 2.3.4

Шифрованное сообщение	Р	Б	Ы	В	Л	Р	У	С	З	Ф	Р	Р	Р	Е	З	Р	У
вариант Б	П	А	Щ	Б	К	П	Т	Р	Ж	У	П	П	П	Д	Ж	П	Т
вариант В	О	_	Ш	А	И	О	С	П	Е	Т	О	О	О	Г	Е	О	С
вариант Г	Н	Я	Ч	_	З	Н	Р	О	Д	С	Н	Н	Н	В	Д	Н	Р

Далее совершаем перебор 6-ти вариантов, чтобы в результате получилось выражение, имеющее смысл, в качестве исходного сообщения.

Если БВГ: П_ЧБИН… – нет смысла.

Если БГВ: ПЯШБЗО… – нет смысла.

Если ВБГ: ОАЧАКНСРД… – нет смысла.

Если ГБВ: НАШ_КОРРЕСПОНДЕНТ… - есть смысл.

Если ВГБ: ОЯЩАЗПСОЖТНПОВ… – нет смысла.

Если ГБВ: Н_Щ_ИП … – нет смысла.

Ответ: ключевая последовательность ГБВ, исходное сообщение НАШ_КОРРЕСПОНДЕНТ.

Раздел III. Элементы теории групп

3.1. Группы и их свойства. Подгруппы. Смежные классы. Нормальные подгруппы

№1. Образуют ли группы множества с указанными операциями? Если нет, то какими алгебраическими системами они являются? Являются ли эти системы абелевыми?

а) $\left\{\frac{m}{2^k} \mid m,k \in \mathbf{Z}\right\}$ относительно операции сложения.

Решение:

$T = \left\{\frac{m}{2^k} \mid m,k \in \mathbf{Z}\right\} \subset \mathbf{Q}$.

<Q, +> –абелева группа.

Проверим по критерию подгруппы, будет ли <T, +> подгруппой <Q, +>.

Рассмотрим $\forall m_1, k_1, m_2, k_2 \in \mathbf{Z}$. Тогда

$$\frac{m_1}{2^{k_1}} - \frac{m_2}{2^{k_2}} = \frac{m_1 \cdot 2^{k_2} - m_2 \cdot 2^{k_1}}{2^{k_1+k_2}},\ k_1, k_2 \in \mathbf{Z}.$$

Если $k_1 \le 0$, $k_2 \le 0$, то $\frac{m_1}{2^{k_1}} - \frac{m_2}{2^{k_2}} = \frac{M_2}{2^0} \in \mathbf{Z} \subset T$.

Итак, $T \le Q \Rightarrow$ <T, +> – абелева группа. Это можно было также проверить по определению.

Ответ: <T, +> – абелева группа.

б) подмножества непустого множества относительно операции пересечения.

Решение:

$V \neq \varnothing \Rightarrow P(V) \neq \varnothing$ 1. $\forall A, B \subseteq V$ $A \cap B \subseteq V \Rightarrow A \cap B \in P(V)$ определена бинарная алгебраическая операция на множестве P(V).

2. $(A \cap B) \cap C = A \cap (B \cap C)$ – ассоциативность из свойства операции $\cap$.

3. $A \cap V = V \cap A = V \Rightarrow$ V – нейтральный элемент.

4. $\forall A \subseteq V$, найти $B \subseteq V \mid A \cap B = B \cap A = V$. Но если $A \subset V$, $A \neq V$, то $\forall B \subseteq V$ $A \cap B \subseteq A \subset V$, $A \cap B \neq V \Rightarrow$ нет обратных элементов у элементов, отличных от V.

5. $A \cap B = B \cap A$ по свойству операции $\cap$.

Итак, (V, $\cap$) – коммутативный (абелев) моноид, но не группа.

Ответ: (V, $\cap$) – абелев моноид.

в) $\mathbf{R}_{>0}$ относительно операции $a * b = a^2 \cdot b^2$, где $\cdot$ – обычное умножение.

Решение:

1. $\forall a,b \in R_{>0}$ $a^2 \cdot b^2 \in R_{>0} \Rightarrow$определена бинарная алгебраическая операция $*$ на $\mathbf{R}_{>0}$.

2. $a * (b * c) = a^2 \cdot (b * c)^2 = a^2 \cdot \left(b^2 \cdot c^2\right)^2 = a^2 \cdot b^4 \cdot c^4$;

$(a*b)*c=\left(a*b\right)^2\cdot c^2=\left(a^2\cdot b^2\right)^2\cdot c^2=a^4\cdot b^4\cdot c^2$.

Пусть $a=b=1,\ c=2$, тогда $1*\left(1*2^2\right)^2=2^4=16$, $\left(1*1\right)^2*2^2=4\neq 16\ \Rightarrow$ операция $*$ не ассоциативна.

Операция $*$ коммутативна, т.к. коммутативно умножение в **R**.

Нет нейтрального элемента: $\forall\, a\in\mathbf{R}_{>0}\quad a^2\cdot h^2=a\ \Leftrightarrow a\cdot h^2=1,\ h^2=\frac{1}{a}$, то есть в каждом случае зависимость нейтрального элемента от элемента *a*. Поэтому нет и обратного элемента.

Итак, $<\mathbf{R}_{>0},\ *>$ – не группа, а коммутативный (абелев) группоид.

Ответ: $<\mathbf{R}_{>0},\ *>$ – абелев группоид.

г) Z относительно операции $m*n=m+n+n\cdot m$, где $+$ и $\cdot$ – обычные операции сложения и умножения в **Z**.

Решение:

1. $\forall m,n\in\mathbf{Z}\ \ m+n+m\cdot n\in\mathbf{Z}\ \Rightarrow$ определена бинарная алгебраическая операция $*$ на **Z**.

2.

$$\left(m*n\right)*p=(m+n+m\cdot n)*p=m+n+m\cdot n+p+(m+n+m\cdot n)\cdot p=m+n+$$
$$+m\cdot n+p+m\cdot p+n\cdot p+m\cdot n\cdot p;$$
$$m*\left(n*p\right)=m*\left(n+p+n\cdot p\right)=m+n+p+n\cdot p+m\cdot\left(n+p+n\cdot p\right)=m+n+$$
$$+p+n\cdot p+m\cdot n+m\cdot p+m\cdot n\cdot p.$$

То есть $\left(m*n\right)*p=m*\left(n*p\right)\ \forall m,n,p\in\mathbf{Z}\ \Rightarrow$ операция $*$ ассоциативна.

3. $m*o=o*m=m\ \ \forall m\in\mathbf{Z}\ \ \exists o\in\mathbf{Z}$. Найдем *o*.

$$m*0=m+0+0\cdot m=m,$$
$$0*m=0+m+m\cdot 0=m.$$

Итак, $m*0=0*m=m,\ 0\in\mathbf{Z}\Rightarrow 0$ – нейтральный элемент.

4. $\forall m\in\mathbf{Z}\quad \exists m^{-1}\in\mathbf{Z}\ \mid\ m*m^{-1}=m^{-1}*m=0$.

$$m+n+m\cdot n=0\quad m+\left(1+m\right)\cdot n=0,$$

$n=-\frac{m}{1+m}$, но такое число не всегда принадлежит **Z**. Например, пусть *m*=1. Тогда $1+n+n=0$, откуда $1+2n=0,\ n=-\frac{1}{2}\notin\mathbf{Z}$. Поэтому не для всякого элемента из **Z** существует обратный элемент относительно операции $*$.

5. $m*n=n*m\ \forall m,n\in\mathbf{Z}$, т.к. $+$ и $\cdot$ коммутативны в **Z**, следовательно, операция $*$ коммутативна.

Итак, $<\mathbf{Z},\ *>$ – коммутативный (абелев) моноид, но не группа.

Ответ: $<\mathbf{Z},\ *>$ – абелев моноид.

№2. Является ли *H* подгруппой группы *G*?

а) $<G,\ *>$ – абелева группа, $H=\left\{g^2=g*g\mid g\in G\right\}$.

Решение:

Пусть $g_1 * g_1,\ g_2 * g_2 \in H,\ \ \forall g_1, g_2 \in G$. Тогда

$$(g_1 * g_1) * (g_2 * g_2)^{-1} = g_1 * g_1 * g_2^{-1} * g_2^{-1} = g_1 * g_2^{-1} * g_1 * g_2^{-1} = \left(g_1 * g_2^{-1}\right) * \left(g_1 * g_2^{-1}\right) \in H,$$

поскольку $g_1 * g_2^{-1} \in G$, а $(g_2 * g_2)^{-1} = g_2^{-1} * g_2^{-1}$:

$$(g_2 * g_2) * \left(g_2^{-1} * g_2^{-1}\right) = g_2 * \left(g_2 * g_2^{-1}\right) * g_2^{-1} = g_2 * e * g_2^{-1} = e.$$

Итак, по критерию подгруппы H подгруппа группы G.

Ответ: $H \le G$.

б) $|G|$=2000, $|H|$=127.

Решение:

$$|G| = 2000, \quad |H| = 127. \quad 2000 = 2 \cdot 10^3 = 2 \cdot (2 \cdot 5)^3 = 2^4 \cdot 5^3,$$

$$11 < \sqrt{127} < 12, \quad 2,3 \nmid 127,\ 5 \nmid 127,\ 7 \nmid 127,\ 11 \nmid 127 \ \Rightarrow$$

127 – простое число, $127 \nmid 2000 \ \Rightarrow$ H подгруппой группы G не может быть, т.к. по теореме Лагранжа должно быть $|H| \mid |G|$.

Ответ: $H \not\le G$.

в) $H_1, H_2 \le G$, $H = H_1 \setminus H_2$.

Решение:

Пусть H_1, H_2 – подгруппы группы G. $e \in H_1 \cap H_2$, e – нейтральный элемент группы G.

$e \notin H_1 \setminus H_2 \Rightarrow H_1 \setminus H_2$ – не подгруппа группы G, т.к. любая подгруппа содержит нейтральный элемент группы, который является ее нейтральным элементом.

Ответ: $H \not\le G$.

г) $H_1, H_2 \le G,\ H = \{h_1 * h_2 \mid h_1 \in H_1,\ h_2 \in H_2\}$.

Решение:

Рассмотрим $\forall h_1 \cdot h_2,\ g_1 \cdot g_2 \in H,$ где $\forall g_1, h_1 \in H_1,\ g_2, h_2 \in H_2$. Тогда

$$(g_1 \cdot g_2)^{-1} = g_2^{-1} \cdot g_1^{-1}, \text{ где } g_1^{-1} \in H_1,\ \ g_2^{-1} \in H_2.$$

Если G – абелева группа, то $H \le G$, поскольку

$$g_2^{-1} \cdot g_1^{-1} = g_1^{-1} \cdot g_2^{-1} \in H,\ h_1 \cdot h_2 \cdot g_2^{-1} \cdot g_1^{-1} = \left(h_1 \cdot g_1^{-1}\right) \cdot \left(h_2 \cdot g_2^{-1}\right) \in H.$$

Теперь рассмотрим пример неабелевой группы. Пусть

$$G = GL_2(\mathbf{R}),\ \ H_1 = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid a \in \mathbf{R} \right\}, \quad H_2 = \left\{ \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} \mid b \in \mathbf{R} \right\}.$$

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b+a \\ 0 & 1 \end{pmatrix} \in H_1, \quad \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix} \in H_1 \ \Rightarrow\ H_1 < G.$$

$$\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ b+a & 1 \end{pmatrix} \in H_2, \quad \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ -a & 1 \end{pmatrix} \in H_2 \ \Rightarrow\ H_2 < G.$$

$$H = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} = \begin{pmatrix} 1+ab & a \\ b & 1 \end{pmatrix} \mid a, b \in \mathbf{R} \right\}, \text{ т.е. } a_{22} = 1 \text{ всегда.}$$

$$\begin{pmatrix} 1+ab & a \\ b & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ -b & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -a \\ -b & ab+1 \end{pmatrix}.$$

Должно быть $ab+1=1$. Но если, например, $a=b=1$, то $ab+1=2$ и получаем, что в этом случае $\begin{pmatrix} 1+ab & a \\ b & 1 \end{pmatrix}^{-1} \notin H$. Итак, в данном примере $H \not\leq G$.

Итак, не всегда $(h_1 \cdot h_2)^{-1} = h_2^{-1} \cdot h_1^{-1} \in H \Rightarrow H$ – не подгруппа группы G в общем случае.

Ответ: $H \not\leq G$.

№3. а) $A = \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{2} \end{pmatrix}$, $A \in GL_2(\mathbf{Z}/3\mathbf{Z})$. Выписать <A>, найти $Ord(A)$. Является ли $< A > \lhd GL_2(\mathbf{Z}/3\mathbf{Z})$?

Решение:

$$A = \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{2} \end{pmatrix},\ A \in GL_2(Z/3Z).\ E = \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix}.$$

$$A \neq E,\quad A^2 = \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{2} \end{pmatrix} \cdot \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{2} \end{pmatrix} = \begin{pmatrix} \bar{1} & \bar{2} \\ \bar{2} & \bar{2} \end{pmatrix},\ A^3 = \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{2} \end{pmatrix} \cdot \begin{pmatrix} \bar{1} & \bar{2} \\ \bar{2} & \bar{2} \end{pmatrix} = \begin{pmatrix} \bar{2} & \bar{2} \\ \bar{2} & \bar{0} \end{pmatrix},$$

$$A^4 = \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{2} \end{pmatrix} \cdot \begin{pmatrix} \bar{2} & \bar{2} \\ \bar{2} & \bar{0} \end{pmatrix} = \begin{pmatrix} \bar{2} & \bar{0} \\ \bar{0} & \bar{2} \end{pmatrix},\quad A^8 = A^4 \cdot A^4 = \begin{pmatrix} \bar{2} & \bar{0} \\ \bar{0} & \bar{2} \end{pmatrix} \cdot \begin{pmatrix} \bar{2} & \bar{0} \\ \bar{0} & \bar{2} \end{pmatrix} = \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix} = E.$$

Если $Ord\ (A)<8$, например, $Ord(A)=5, 6, 7$, то должно быть $8 \vdots Ord\ (A)$, но $8 \not\vdots 5, 6, 7$. Поэтому, $Ord\ (A)=8$.

$$A^5 = \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{2} \end{pmatrix} \cdot \begin{pmatrix} \bar{2} & \bar{0} \\ \bar{0} & \bar{2} \end{pmatrix} = \begin{pmatrix} \bar{0} & \bar{2} \\ \bar{2} & \bar{1} \end{pmatrix},\ A^6 = \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{2} \end{pmatrix} \cdot \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{2} \end{pmatrix} = \begin{pmatrix} \bar{2} & \bar{1} \\ \bar{1} & \bar{1} \end{pmatrix},$$

$$A^7 = \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{2} \end{pmatrix} \cdot \begin{pmatrix} \bar{2} & \bar{1} \\ \bar{1} & \bar{1} \end{pmatrix} = \begin{pmatrix} \bar{1} & \bar{1} \\ \bar{0} & \bar{1} \end{pmatrix},\quad A^8 = \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{2} \end{pmatrix} \cdot \begin{pmatrix} \bar{1} & \bar{1} \\ \bar{0} & \bar{1} \end{pmatrix} = \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix}.$$

Итак, $< A >= \{A, A^2, A^3, A^4, A^5, A^6, A^7, E\}$.

$$B = \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{2} \end{pmatrix},\ B^{-1} = 2^{-1} \cdot \begin{pmatrix} \bar{2} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix} = \bar{2} \cdot \begin{pmatrix} \bar{2} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix} = \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{2} \end{pmatrix} = B,$$

$$B \cdot A \cdot B^{-1} = \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{2} \end{pmatrix} \cdot \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{2} \end{pmatrix} \cdot \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{2} \end{pmatrix} = \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{2} & \bar{1} \end{pmatrix} \cdot \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{2} \end{pmatrix} = \begin{pmatrix} \bar{0} & \bar{2} \\ \bar{2} & \bar{2} \end{pmatrix} \notin < A >.$$

Значит, $< A > \not\lhd GL_2(\mathbf{Z}/3\mathbf{Z})$ согласно критерию нормальной подгруппы.

Ответ: $Ord\ (A)=8$, $< A > \not\lhd GL_2(\mathbf{Z}/3\mathbf{Z})$.

б) $A=\begin{pmatrix} \bar{1} & \bar{1} & \bar{0} \\ \bar{0} & \bar{1} & \bar{1} \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix}$, $A \in GL_3(\mathbf{Z}/2\mathbf{Z})$. Выписать <A>, найти *Ord*(*A*). Является ли $< A > \lhd GL_3(\mathbf{Z}/2\mathbf{Z})$?

Ответ: *Ord* (*A*)=4, $< A > \not\lhd GL_3(\mathbf{Z}/2\mathbf{Z})$.

№4. Пусть $< G, \circ >$ – группа. Доказать, что если $a^2 = e$, $\forall a \in G$, то G – абелева группа.

Решение:

Рассмотрим $\forall a, b \in G$. Тогда

$(a \circ b) \circ (b \circ a) = a \circ (b \circ b) \circ a = a \circ e \circ a = a \circ a = e$, т.е. $b \circ a = (a \circ b)^{-1}$, но с другой стороны, $(a \circ b)^{-1} = a \circ b$. Поэтому получаем, что $a \circ b = b \circ a$.

Итак, $a \circ b = b \circ a \quad \forall a, b \in G \Rightarrow G$ – абелева группа.

№5. Доказать, что любая бесконечная группа имеет бесконечное число подгрупп.

Решение:

1) Если $\forall a \in G \quad Ord(a) < +\infty$, то можно рассмотреть все <a>, причем взять все различные циклические подгруппы. Таких подгрупп будет бесконечно много, иначе бы *H* была конечна, т.к. *H* представляет собой объединение всех таких подгрупп. Поэтому, *H* содержит бесконечно много подгрупп.

2) В группе H есть элемент бесконечного порядка $a \in H$, $Ord(a) = +\infty$. Тогда можно брать подгруппы $< a >, < a^2 >, < a^3 >, < a^4 >, \ldots, < a^n >, n \in \mathbf{N}$. Таких подгрупп бесконечно много, т.к. если (m, n)=1, то $< a^m > \neq < a^n >$, $a^m \notin < a^n >$, $a^n \notin < a^m >$. Поэтому, *H* содержит бесконечно много подгрупп.

№6. Найти все подгруппы группы и указать их включения.

а) Циклической группы порядка 6.

Решение:

$G = < a > = \{e, a, a^2, a^3, a^4, a^5\}$. Все подгруппы являются циклическими.

Порядок подгруппы делит порядок группы. 1, 2, 3, 6 | 6.

$|H| = 1 \Rightarrow H = \{e\} = < e >$.

$|H| = 2 \Rightarrow H = \{b, e\}, Ord(b) = 2, \; Ord(a^3) = 2 \Rightarrow H = \{a^3, e\} = < a^3 >$.

$|H| = 3, Ord(a^2) = Ord(a^4) = 3 \Rightarrow H = \{a^2, a^4, e\} = < a^2 > = < a^4 >$.

$|H| = 6, Ord(a) = Ord(a^5) = 1 \Rightarrow H = G = < a > = < a^5 >$.

Имеем следующие включения подгрупп:

$$< e > \subset < a^2 > \subset < a >,$$
$$< e > \subset < a^3 > \subset < a >.$$

б) Циклической группы порядка 24.

Решение:

Все подгруппы являются циклическими. Порядок подгруппы делит порядок группы. 1, 2, 3, 4, 6, 8, 12, 24 | 24.

$|H|=1,\ H=\{e\}=<e>.$

$|H|=2,\ Ord(a^{12})=2, H=\{a^{12},e\}<a^{12}>.$

$|H|=3,\ Ord(a^8)=Ord(a^{16})=2,\ H=\{a^8,a^{16},e\}=<a^8>=<a^{16}>.$

$|H|=4,\ Ord(a^6)=Ord(a^{18})=4,\ H=\{a^6,a^{12},a^{18},e\}=<a^6>=<a^{18}>.$

$|H|=6,\ Ord(a^4)=Ord(a^{16})=6,\ H=\{a^4,a^8,a^{12},a^{16},a^{20},e\}=<a^4>=<a^{16}>.$

$|H|=8,\ Ord(a^3)=Ord(a^9)=Ord(a^{15})=Ord(a^{21})=8,$

$H=\{a^3,a^6,a^9,a^{12},a^{15},a^{18},a^{21},a^{24}=e\}=<a^3>=<a^9>=<a^{15}>=<a^{21}>.$

$|H|=12,\ Ord(a^2)=Ord(a^{10})=Ord(a^{14})=Ord(a^{22})=12,$

$H=\{a^2,a^4,a^6,a^8,a^{10},a^{12},a^{14},a^{16},a^{18},a^{20},a^{22},e\}=<a^2>=<a^{10}>=<a^{14}>=<a^{22}>.$

$|H|=24,\ Ord(a)=Ord(a^5)=Ord(a^7)=Ord(a^{11})=Ord(a^{13})=Ord(a^{17})=$

$=Ord(a^{19})=Ord(a^{23})=24,$

$H=\{a,a^2,a^3,...,\ a^{23},e\}=<a>=<a^5>=<a^7>=<a^{11}>=<a^{13}>=<a^{17}>=<a^{19}>=<a^{23}>.$

Имеем следующие включения подгрупп:

$$<e>\subset<a^{12}>\subset<a^6>\subset<a^3>\subset<a>,$$

$$<e>\subset<a^8>\subset<a^4>\subset<a^2>\subset<a>,$$

$$<a^6>\subset<a^2>,\ <a^{12}>\subset<a^4>.$$

$$<e>\subset<a^3>\subset<a>.$$

№7. Доказать, что $H\lhd G$.

а) H – произвольная подгруппа индекса 2 группы G.

Решение:

$G=H\cup aH,\ a\in G\setminus H$, с другой стороны, $G=H\cup Ha,\ a\in G\setminus H$.

Следовательно, $H\cup Ha=H\cup aH\Leftrightarrow Ha=aH\ \ \forall a\in G$, по определению $H\lhd G$.

б) H – центр группы G, $H=\{h\in G\mid\forall a\in G\ \ a\cdot h=h\cdot a\}$.

Решение:

Для $\forall a\in G$ рассмотрим левый и правый смежные классы с этим представителем. $aH=\{a\cdot h\mid h\in H\}$, но $a\cdot h=h\cdot a\Rightarrow aH=\{h\cdot a\mid h\in H\}=Ha$, т.е. $aH=Ha$, значит, по определению $H\lhd G$.

№8. Найти смежные классы группы по подгруппе.

а) $<\mathbf{Z},+>$ по $n\mathbf{Z},\ n\in\mathbf{N}$.

Решение:

$1+n\mathbf{Z}=\overline{1},\ 2+n\mathbf{Z}=\overline{2},\ldots,\ (n-1)+n\mathbf{Z}=\overline{n-1},\ n+n\mathbf{Z}=n\mathbf{Z}$.

$i+n\mathbf{Z}\neq j+n\mathbf{Z},$ если $i\not\equiv j(\mathrm{mod}\,n)$, $\forall k\in\mathbf{Z}$ попадает в один из классов $i+n\mathbf{Z}, i=\overline{0,n-1}$. Поэтому $\mathbf{Z}=\bigcup_{i=0}^{n-1}(i+n\mathbf{Z})=\bigcup_{i=0}^{n-1}\bar{i}$. Таким образом, смежные классы – классы вычетов по модулю n.

Ответ: классы вычетов по модулю n.

б) $<\mathbf{R},+>$ по $<\mathbf{Z},+>$.

Решение:

Для $\forall r\in\mathbf{R}\quad r=[r]+\{r\},\ [r]\in\mathbf{Z},\ 0\le\{r\}<1$. Поэтому $r\in\{r\}+\mathbf{Z}$.

$$r_1\neq r_2,\ 0\le r_1,r_2<1,\Rightarrow r_1+\mathbf{Z}\neq r_2+\mathbf{Z}:$$

$$r_1+m_1=r_2+m_2\Rightarrow r_1-r_2=m_2-m_1,$$

$$\text{но}\ \ r_1-r_2\notin\mathbf{Z},\ \text{а}\ \ m_2-m_1\in\mathbf{Z}.$$

Поэтому можно рассмотреть в качестве представителей смежных классов числа $0\le r<1,\ r\in\mathbf{R}$. Итак, $\mathbf{R}=\bigcup_{0\le r<1}(r+\mathbf{Z}),\ r\in\mathbf{R}$.

Ответ: $r+\mathbf{Z}$, где $0\le r<1,\ r\in\mathbf{R}$.

в) $<\mathbf{C}^*,\cdot>$ по $H=\{z\in\mathbf{C}^*\mid |z|=1\}$.

Решение:

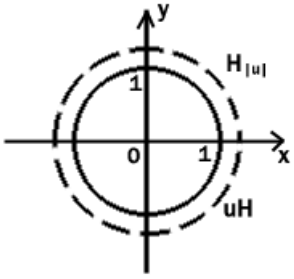


Рис. 3.1.1

$\forall u\in\mathbf{C}^*\ \ u=|u|e^{i\varphi},\quad |u|\in\mathbf{R}_{>0},\ |e^{i\varphi}|=1.$

$H=\{z\in\mathbf{C}^*\mid z=e^{i\varphi},0\le\varphi<2\pi\}.$

$u=|u|e^{i\varphi}\in|u|H,\quad |u|H=\{|u|e^{i\varphi}\mid 0\le\varphi<2\pi\}.$

$$|u_1|\neq|u_2|\Rightarrow|u_1|H\neq|u_2|H.$$

$\mathbf{C}^*=\bigcup_{|u|\in\mathbf{R}_{>0}}|u|H$ (см. рис. 3.1.1).

Ответ: $|u|H,\ |u|\in\mathbf{R}_{>0}$.

г) $<\mathbf{C}^*,\cdot>$ по $<\mathbf{R}^*,\cdot>$.

Решение:

$z=a+ib,\ a,b\in\mathbf{R}$.

$z\neq0\Leftrightarrow a^2+b^2>0\Leftrightarrow z\in\mathbf{R}^*$.

$i\mathbf{R}^*$ – смежный класс всех мнимых чисел.

$(1+ib)\mathbf{R}^*=\{r+ibr\mid r\in\mathbf{R}^*\},\quad b\in\mathbf{R}^*.$

$r_1+ib_1r_1=r_2+ib_2r_2\Leftrightarrow i(b_1r_1-b_2r_2)=r_2-r_1.$

Если $r_1\neq r_2$, то слева стоит 0 или чисто мнимое число, а справа – действительное, отличное от 0. Такого равенства быть не может. Если $r_1=r_2=r$, то получаем равенство:

$ir(b_1 - b_2) = 0 \Leftrightarrow b_1 = b_2 \quad \forall r \in \mathbf{R}^*.$

$$\forall z \in \mathbf{C}^* \quad z = a + ib = \begin{cases} a(1 + i\frac{b}{a}) \in (1 + i\frac{b}{a})\mathbf{R}^*, \ a \neq 0; \\ ib \in i\mathbf{R}^*, \ a = 0. \end{cases}$$

Итак, $\mathbf{C}^* = \bigcup\limits_{b \in \mathbf{R}} (1 + ib)\mathbf{R}^* \cup i\mathbf{R}^*$.

Ответ: $(1 + ib)\mathbf{R}^*, \ b \in \mathbf{R}, \ i\mathbf{R}^*$.

3.2. Симметрическая группа. Фактор группа

№1. Найти произведение подстановок fg и gf

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 6 & 3 & 4 & 7 & 5 \end{pmatrix}, \quad g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 5 & 7 & 1 & 2 & 3 & 4 \end{pmatrix}.$$

Решение:

$$fg = f(g) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 4 & 5 & 2 & 1 & 6 & 3 \end{pmatrix}, \quad gf = g(f) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 6 & 3 & 7 & 1 & 4 & 2 \end{pmatrix}.$$

$$fg \neq gf.$$

№2. Найти f^{-1} и g^{-1} для подстановок из предыдущей задачи.

Решение:

$$f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 4 & 5 & 7 & 3 & 6 \end{pmatrix}, \quad g^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 5 & 6 & 7 & 2 & 1 & 3 \end{pmatrix}.$$

Меняются местами 1-я и 2-я строки, затем столбцы упорядочиваются по возрастанию элементов 1-ой строки.

№3. Разложить подстановку f в произведение независимых циклов и транспозиций. Является ли f четной или нечетной?

а) $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 6 & 3 & 4 & 7 & 5 \end{pmatrix}$.

Решение:

$f = (12)(36754)$ – произведение циклов,

$f = (12)(34)(35)(37)(36)$ – произведение транспозиций.

f – нечетная подстановка, поскольку в разложении в произведение транспозиций количество транспозиций равно 5.

б) $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 1 & 2 & 3 & 6 & 5 & 7 \end{pmatrix}$.

Решение:

$f = (1432)(56)$ – произведение циклов,

$f = (12)(13)(14)(56)$ – произведение транспозиций.

f – четная подстановка, поскольку в разложении в произведение транспозиций количество транспозиций равно 4.

№4. Найти $< f >$ из задачи №3. Определить $Ord(f)$ *в* S_7. Является ли $< f > \lhd S_7$?

а) Решение:

$$f = (12)(36754) \Rightarrow Ord(f) = [2,\ 5] = 10.$$

$$f = t_1 t_2,\ (12) = t_1,\ (36754) = t_2.$$

$$\begin{pmatrix} 3 & 6 & 7 & 5 & 4 \\ 6 & 7 & 5 & 4 & 3 \end{pmatrix}^2 = \begin{pmatrix} 3 & 6 & 7 & 5 & 4 \\ 7 & 5 & 4 & 3 & 6 \end{pmatrix} \text{ и т.д.}$$

$$Ord(t_1) = 2, \quad Ord(t_2) = 5.$$

$$(36754)^2 = (37465),\ (36754)^3 = (35647),\ (37465)^4 = (34576),\ (36754)^5 = e.$$

$$< f >= \{e, f, f^2, f^3, f^4, f^5, f^6, f^7, f^8, f^9\} = \{e,\ (12)(36754),\ (37465),$$

$$(12)(35647),\ (34576),\ (12),\ (36754),\ (12)(37465),$$

$$(35647),\ (12)(34576)\} = \{e, t_1t_2, t_2^2, t_1t_2^3, t_2^4, t_1, t_2, t_1t_2^2, t_2^3, t_1t_2^4\}.$$

Пусть g=$(35) \notin < f >$. Проверим выполнение критерия нормальной подгруппы для $< f >$.

$$g^{-1} = (35), \quad gt_2g^{-1} = (35)(36754)(35) = (35)(34)(567) =$$

$$= (345)(567) = (56734) \notin < f >.$$

Значит, $< f > \not\lhd S_7$.

Ответ: $Ord(f) = 10,\ < f > \not\lhd S_7$.

б) Решение:

$$f = (1432)(56) \Rightarrow Ord(f) = [4,\ 2] = 4.$$

$$f = t_1t_2, \quad t_1 = (1432), \quad t_2 = (56).$$

$$< f >= \{e,\ t_1t_2,\ t_1^2,\ t_1^3t_2\} = \{e,\ (1432)(56),\ (13)(42),\ (4123)(56)\}.$$

$$g = (16) \notin < f >, \quad g^{-1} = (16), \quad gt_1^2g^{-1} = (16)(13)(42)(16) = (16)(13)(16)(42) =$$

$$= (16)(163)(42) = (63)(42) \notin < f >.$$

Значит, $< f > \not\lhd S_7$.

Ответ: $Ord(f) = 4,\ < f > \not\lhd S_7$.

№5. Найти фактор-группы.

а) $< \mathbf{Z}, + >$ по $< n\mathbf{Z}, + >,\ n \in \mathbf{N}$.

Решение:

$< \mathbf{Z}, + >$ – абелева группа $\Rightarrow n\mathbf{Z} \lhd \mathbf{Z}$.

Как было показано в задаче №8 из 3.1, фактор-множеством является множество классов вычетов по модулю n $\mathbf{Z}/n\mathbf{Z}$.

$\mathbf{Z} = \bigcup_{i=0}^{n-1} (i + n\mathbf{Z}) = \bigcup_{i=0}^{n-1} \overline{i}, \quad \overline{i} + \overline{j} = \overline{i+j}, \ \ i, j = \overline{0, n-1}.$

$(i + n\mathbf{Z}) \oplus (j + n\mathbf{Z}) = (i + j) + n\mathbf{Z}$ – сложение классов вычетов.

$< \mathbf{Z}/n\mathbf{Z}, \oplus >$ – абелева и циклическая группа порядка n, поскольку $< \mathbf{Z}, + >$ – абелева и циклическая группа. $\overline{1} = 1 + n\mathbf{Z}$ – образующий элемент. Количество образующих элементов равно $\varphi(n)$, где φ – функция Эйлера.

Ответ: $< \mathbf{Z}/n\mathbf{Z}, \oplus >$ – абелева и циклическая группа порядка n, количество образующих элементов равно $\varphi(n)$.

б) $< 3\mathbf{Z}, + >$ по $< 15\mathbf{Z}, + >$.

Решение:

$\forall 15m, \ 15n \in 15\mathbf{Z} \ \Rightarrow \ 15m - 15n = 15(m-n) \in 15\mathbf{Z} \ \Rightarrow \ 15\mathbf{Z} < 3\mathbf{Z}.$

$< 3\mathbf{Z}, + >$ – абелева группа $\Rightarrow 15\mathbf{Z} \lhd 3\mathbf{Z}$.

$3\mathbf{Z}/15\mathbf{Z} = \{15\mathbf{Z}, \ 3+15\mathbf{Z}, \ 6+15\mathbf{Z}, \ 9+15\mathbf{Z}, \ 12+15\mathbf{Z}\} = \{\overline{0}, \ \overline{3}, \ \overline{6}, \ \overline{9}, \ \overline{12}\}$ – все фактор-множество. $< 3\mathbf{Z}/15\mathbf{Z}, \oplus >$ – абелева и циклическая группа порядка 5, поскольку $< 3\mathbf{Z}, + >$ – абелева и циклическая группа. Количество образующих равно $\varphi(5) = 4$, образующими элементами являются все ненулевые смежные классы. Сложение смежных классов задается на представителях по модулю 15, его можно задать таблицей Кэли. Например, $-\overline{3} = \overline{12}, \ -\overline{6} = \overline{9}$.

Ответ: $< 3\mathbf{Z}/15\mathbf{Z}, \oplus >$ – абелева и циклическая группа порядка 5, количество образующих элементов равно 4, образующими элементами являются все ненулевые смежные классы.

в) $< 4\mathbf{Z}, + >$ по $< 24\mathbf{Z}, + >$.

Решение:

$\forall 24m, \ 24n \in 24\mathbf{Z} \ \Rightarrow \ 24m - 24n = 24(m-n) \in 24\mathbf{Z} \ \Rightarrow \ 24\mathbf{Z} < 4\mathbf{Z}.$

$< 4\mathbf{Z}, + >$ – абелева группа $\Rightarrow 24\mathbf{Z} \lhd 4\mathbf{Z}$.

$4\mathbf{Z}/24\mathbf{Z} = \{24\mathbf{Z}, \ 4+24\mathbf{Z}, \ 8+24\mathbf{Z}, \ 12+24\mathbf{Z}, \ 16+24\mathbf{Z}, \ 20+24\mathbf{Z}\} = \{\overline{0}, \ \overline{4}, \ \overline{8}, \ \overline{12}, \ \overline{16}, \ \overline{20}\}$ – все фактор-множество. $< 4\mathbf{Z}/24\mathbf{Z}, \oplus >$ – абелева и циклическая группа порядка 6, поскольку $< 4\mathbf{Z}, + >$ – абелева и циклическая группа. Количество образующих равно $\varphi(6) = 2$, образующими элементами являются смежные классы $\overline{4}, \ \overline{20}$, для представителей n которых $(n, \ 24) = 4$. Сложение смежных классов задается на представителях по модулю 24, его можно задать таблицей Кэли. Например, $\overline{4} + \overline{8} = \overline{12}, \ -\overline{4} = \overline{20}, \ -\overline{8} = \overline{16}, \ -12 = \overline{12}$.

Ответ: $< 4\mathbf{Z}/24\mathbf{Z}, \oplus >$ – абелева и циклическая группа порядка 6, образующими элементами являются смежные классы $\overline{4}, \ \overline{20}$.

г) $< \mathbf{R}^*, \cdot >$ по $< \mathbf{R}_{>0}, \cdot >$.

Решение:

$\forall r_1, r_2 \in \mathbf{R}_{>0} \ \ r_1 \cdot r_2^{-1} \in \mathbf{R}_{>0} \ \Rightarrow \ \mathbf{R}_{>0} < \mathbf{R}^*.$

$< \mathbf{R}^*, \cdot >$ – абелева группа $\Rightarrow \ \mathbf{R}_{>0} \lhd \mathbf{R}^*.$

$\forall r = |r| \cdot sign(r),\ r \neq 0,\ \Rightarrow \mathbf{R}^* = \mathbf{R}_{>0} \cup \mathbf{R}_{<0} = \mathbf{R}_{>0} \cup (-1)\mathbf{R}_{>0}.$

Если $r_1 \in \mathbf{R}_{>0}$, а $r_2 \in \mathbf{R}_{<0}$, то $r_1 \neq r_2$.

Значит, $\mathbf{R}^* / \mathbf{R}_{>0} = \{\mathbf{R}_{>0},\ \mathbf{R}_{<0}\}$ – все фактор-множество. $< \mathbf{R}^* / \mathbf{R}_{>0}, \square >$ – абелева и циклическая группа порядка 2, поскольку $< \mathbf{R}^*, \cdot >$ – абелева группа, и порядок фактор-группы – простое число. В данном случае $< \mathbf{R}^*, \cdot >$ – не циклическая группа. Количество образующих равно $\varphi(2) = 1$, образующим элементом является смежный класс $\mathbf{R}_{<0}$. Умножение смежных классов задается на представителях, его можно задать следующей таблицей Кэли (см. таблицу 3.2.1).

Таблица 3.2.1

$\square$	$\mathbf{R}_{>0}$	$\mathbf{R}_{<0}$
$\mathbf{R}_{>0}$	$\mathbf{R}_{>0}$	$\mathbf{R}_{<0}$
$\mathbf{R}_{<0}$	$\mathbf{R}_{<0}$	$\mathbf{R}_{>0}$

Ответ: $< \mathbf{R}^* / \mathbf{R}_{>0}, \square >$ – абелева и циклическая группа порядка 2, образующим элементом является смежный класс $\mathbf{R}_{<0}$.

3.3. Гомоморфизмы групп. Криптосистема RSA

№1. Доказать, утверждения.

а) Группа $<\mathbf{R}_{>0}, \cdot>$ изоморфна группе $<\mathbf{R}, +>$.

Решение:

$\forall r \in \mathbf{R}_{>0}$ можно представить в виде $r = e^{\alpha},\ \alpha \in \mathbf{R}$.

Построим отображение $\varphi : \mathbf{R}_{>0} \to \mathbf{R},\quad \varphi(e^{\alpha}) = \alpha.$

Тогда $\varphi(e^{\alpha_1} \cdot e^{\alpha_2}) = \varphi(e^{\alpha_1 + \alpha_2}) = \alpha_1 + \alpha_2 = \varphi(e^{\alpha_1}) + \varphi(e^{\alpha_2}).$

$\varphi(a) = ln(a)\ \ \forall a \in \mathbf{R},\ \varphi -$ гомоморфизм групп.

$Im\varphi = \mathbf{R}$, т.к. $\forall \alpha \in \mathbf{R}\ \ \exists e^{\alpha} = \varphi^{-1}(\alpha) \in \mathbf{R}_{>0}$, т.е. φ – эпиморфизм.

$Ker\varphi = \{e^{\alpha} \mid \alpha = 0\} = \{1\} \Rightarrow \varphi$ – мономорфизм.

Итак, φ – изоморфизм. Поэтому $\mathbf{R}_{>0} \cong \mathbf{R}$.

б) Группа $< \mathbf{Q}_{>0}, \cdot >$ не изоморфна группе $< \mathbf{Q}, + >$.

Решение:

Пусть $\varphi : \mathbf{Q}_{>0} \to \mathbf{Q}$ – изоморфизм.

Тогда $\exists \varphi^{-1} : \mathbf{Q} \to \mathbf{Q}_{>0}$ – изоморфизм.

$3 = \varphi^{-1}(\varphi(3)) = \varphi^{-1}(\varphi(3)/2 + \varphi(3)/2) = \varphi^{-1}(\varphi(3)/2) \cdot \varphi^{-1}(\varphi(3)/2) =$

$= (\varphi^{-1}(\varphi(3)/2))^2 = r^2,\ \ r \in \mathbf{Q}_{>0}$, что не возможно, $\Rightarrow \varphi$ нельзя построить.

№2. Найти все гомоморфизмы групп.

а) $Ord(a)=n$, найти все эндоморфизмы группы <a>. Какие из них являются автоморфизмами?

Решение:

$\varphi_0(a)=e,\quad \varphi_1(a)=a,\quad \varphi_1=e_{<a>},\quad \varphi_2(a)=a^2,\ldots,\quad \varphi_{n-1}(a)=a^{n-1}$ – всего можно построить n различных отображений, таких что $\varphi(a^i)=\varphi(a)^i,\ i=\overline{0,n-1}$. Вид эндоморфизма определяется образом элемента a.

$\varphi_k(a)=a^k,\ k=\overline{0,n-1}$.

$\varphi_k(a^i\cdot a^j)=\varphi_k(a^{i+j})=(a^k)^{i+j}=a^{ki}\cdot a^{kj}=\varphi_k(a^i)\cdot\varphi_k(a^j),\quad \forall i,j=\overline{0,n-1}$.

Всего существует n различных эндоморфизмов. Автоморфизмами являются только те, при которых $Im\varphi_k=<a>$, т.е. $|Im\varphi_k|=n$. Если $(m,\ n)=1$, то a^m – другая образующая <a>, и φ_m – автоморфизм, их количество равно $\varphi(n)$, где φ – функция Эйлера. Если a^S не является образующей, то $Ord(a^S)<n,\quad |\varphi_S(<a>)|=|Ord(a^S)|$, не будет инъекции и сюръекции $\Rightarrow \varphi_S$ – не автоморфизм.

Ответ: Эндоморфизмы – $\varphi_k(a)=a^k,\ k=\overline{0,n-1}$, автоморфизмы – $\varphi_m(a)=a^m,\ (m,\ n)=1$.

б) $Ord(a)=6,\ Ord(b)=18,\ \varphi:<a>\to<b>$.

Решение:

$\varphi(<a>)\le<b>$. Подгруппами <b> могут быть только подгруппы <b> порядка 18, $<b^2>$ порядка 9, $<b^3>=<b^{15}>$ порядка 6, $<b^6>=<b^{12}>$ порядка 3, $<b^9>$ порядка 2, <e> порядка 1. При этом $1\le|\varphi(<a>)|\le 6$, и $\varphi(e_1)=e_2$, $\varphi(a^k)=\varphi(a)^k,\ \forall k\in\mathbf{Z}$, поэтому должно выполняться $|<a>|\vdots|\varphi(<a>)|$. Поэтому $|\varphi(<a>)|$ может быть равно 1, 2, 3, 6. Перечислим все гомоморфизмы, они задаются образом элемента a, который является образующим элементом подгруппы соответствующего порядка в <b>.

1) $\varphi_0:a\to e$; 2) $\varphi_1:a\to b^9$; 3) $\varphi_{21}:a\to b^6,\ \varphi_{22}:a\to b^{12}$; 4) $\varphi_{31}:a\to b^3,\ \varphi_{32}:a\to b^{15}$.

Ответ: $\varphi_0:a\to e;\ \varphi_1:a\to b^9;\ \varphi_{21}:a\to b^6,\ \varphi_{22}:a\to b^{12};\ \varphi_{31}:a\to b^3,\ \varphi_{32}:a\to b^{15}$.

в) $Ord(a)=18,\ Ord(b)=6,\ \varphi:<a>\to<b>$.

Решение:

$|\varphi(<a>)|$ может быть равно 1, 2, 3, 6. Перечислим все гомоморфизмы, они задаются образом элемента a, который является образующим элементом подгруппы соответствующего порядка в <b>.

1) $\varphi_0:a\to e$; 2) $\varphi_1:a\to b^3$; 3) $\varphi_{21}:a\to b^2,\ \varphi_{22}:a\to b^4$; 4) $\varphi_{31}:a\to b,\ \varphi_{32}:a\to b^5$.

Ответ: $\varphi_0:a\to e;\ \varphi_1:a\to b^3;\ \varphi_{21}:a\to b^2,\ \varphi_{22}:a\to b^4;\ \varphi_{31}:a\to b,\ \varphi_{32}:a\to b^5$.

г) $Ord(a)=12,\ Ord(b)=15,\ \varphi:<a>\to<b>$.

Решение:

$|\varphi(<a>)|\ |\ 12$ и $|\varphi(<a>)|\ |\ 15,\ \Rightarrow\ |\varphi(<a>)|$ может быть равно 1, 3.

Перечислим все гомоморфизмы, они задаются образом элемента *a*, который является образующим элементом подгруппы соответствующего порядка в <b>.

$$1)\ \varphi_0 : a \to e; \quad 2)\ \varphi_{11} : a \to b^5,\ \ \varphi_{12} : a \to b^{10}.$$

Ответ: $\varphi_0 : a \to e; \quad \varphi_{11} : a \to b^5,\ \ \varphi_{12} : a \to b^{10}.$

д) $Ord(a) = 6,\ Ord(b) = 25,\ \varphi : < a > \to < b >$.

Решение:

$|\varphi(< a >)|$ | 6 и $|\varphi(< a >)|$ | 25, $\Rightarrow$ $|\varphi(< a >)|$ может быть равно только 1. Поэтому $\varphi : a \to e$ – единственный гомоморфизм.

Ответ: $\varphi : a \to e$.

№3. Доказать, что группу <**Q**,+> нельзя гомоморфно отобразить на <**Z**,+>.

Решение:

Опишем вид гомоморфизмов из первой группы во вторую.

$\varphi : \mathbf{Q} \to \mathbf{Z},\ \varphi(a+b) = \varphi(a) + \varphi(b).$

$$\varphi(1) = \varphi(\sum_{k=1}^{q} \frac{1}{q}) = q \cdot \varphi\left(\frac{1}{q}\right) \ \Rightarrow\ \varphi\left(\frac{1}{q}\right) = \frac{\varphi(1)}{q} \in \mathbf{Z},\ \forall q \in \mathbf{N} \Rightarrow$$

$$\varphi(1) = 0,\ \varphi\left(\frac{1}{q}\right) = 0 \quad \forall q \in \mathbf{N}.$$

$$\forall q \in \mathbf{N} \quad q \mid \varphi(1) \Rightarrow \varphi(1) = 0.$$

$$\forall \frac{p}{q} \in \mathbf{Q}\ \ \varphi\left(\frac{p}{q}\right) = p \cdot \varphi\left(\frac{1}{q}\right) = 0,\ \text{т.е. } Im\varphi = \{0\} \neq \mathbf{Z}.$$

Итак, существует единственный гомоморфизм, не являющийся эпиморфизмом.

№4. Доказать изоморфность групп $S_n / A_n \cong < \mathbf{Z}/2\mathbf{Z}, + >$ при *n*>1.

Решение:

$$f : S_n \to \mathbf{Z}/2\mathbf{Z}, \quad f(g) = \begin{cases} \bar{0}, \text{ если } g \in A_n; \\ \bar{1}, \text{ если } g \notin A_n. \end{cases}$$

$$f(g_1 g_2) = \overline{\delta(g_1)} + \overline{\delta(g_2)}, \quad f(g) = \overline{\delta(g)},$$

где δ определяет характер четности подстановки, $\delta(g) = \begin{cases} 1,\ g \in A_n; \\ 0,\ g \notin A_n. \end{cases}$

g_1 *и* g_2 разлагаются в произведение транспозиций, произведение подстановок одинаковой четности – четная подстановка, произведение подстановок различной четности – нечетная подстановка.

$$\delta(g_1 g_2) = \delta(g_1) + \delta(g_2).$$

Поэтому f – гомоморфизм групп. f – эпиморфизм, т.к. при *n*>1 в S_n есть как четные, так и нечетные подстановки.

$Ker(f) = A_n \Rightarrow$ по 2-й теореме о гомоморфизме групп $S_n / A_n \cong < \mathbf{Z}/2\mathbf{Z}, + >$.

№5. Доказать следующие утверждения.

а) $GL_n(\mathbf{R}) / SL_n(\mathbf{R}) \cong < \mathbf{R}^*, \cdot >$.

Решение:

$f : GL_n(\mathbf{R}) \to \mathbf{R}^*, \quad f(A) = \det A.$

$f(A \cdot B) = \det(A \cdot B) = \det A \cdot \det B = f(A) \cdot f(B) \Rightarrow f -$ гомоморфзм.

$$\forall a \in \mathbf{R}^* \ \exists A = \begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & 1 & 0 & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 \end{pmatrix} \in GL_n(\mathbf{R}), \ \det A = a, \ \Rightarrow f - \text{эпиморфизм.}$$

$Ker(f) = SL_n(\mathbf{R})$.

По 2-ой теореме о гомоморфизмах групп $GL_n(\mathbf{R}) / SL_n(\mathbf{R}) \cong < \mathbf{R}^*, \cdot >$.

б) $GL_n(\mathbf{R}) / H \cong < \mathbf{R}_{>0}, \cdot >, \ H = \{A \in GL_n(\mathbf{R}) \mid \det A = \pm 1\}$.

Решение:

$f : GL_n(\mathbf{R}) \to \mathbf{R}_{>0}, \quad f(A) = |\det A|$.

$f(A \cdot B) = |\det(A \cdot B)| = |\det A \cdot \det B| = |\det A| \cdot |\det B| = f(A) \cdot f(b) \Rightarrow$

$f -$ гомоморфизм групп.

$f -$ эпиморфизм, поскольку для $\forall a \in R_{>0} \ \exists A \in GL_n(\mathbf{R}) \mid f(A) = a$, матрица A строится также, как в задаче а).

$Ker(f) = H \Rightarrow GL_n(\mathbf{R}) / H \cong < \mathbf{R}_{>0}, \cdot >$ по 2-ой теореме о гомоморфизмах групп.

в) $GL_n(\mathbf{R}) / H \cong < \mathbf{Z}/2\mathbf{Z}, + >, \ H = \{A \in GL_n(\mathbf{R}) \mid \det A > 0\}$.

Решение:

$$f : GL_n(\mathbf{R}) \to \mathbf{Z}/2\mathbf{Z}, \ f(A) = \begin{cases} \bar{0}, & \det A > 0; \\ \bar{1}, & \det A < 0. \end{cases}$$

$$f(A \cdot B) = \begin{cases} \bar{0}, & \det(A \cdot B) > 0 \\ \bar{1}, & \det(A \cdot B) < 0 \end{cases} = f(A) + f(B).$$

Следовательно, $f -$ гомоморфизм групп. $f -$ эпиморфизм, поскольку для $\forall a \in R^* \ \exists A \in GL_n(\mathbf{R}) \mid \det(A) = a, \ f(A) = \begin{cases} \bar{0}, & a > 0; \\ \bar{1}, & a < 0. \end{cases}$. Матрица A строится также, как в задаче а).

$Ker(f) = H \ \Rightarrow GL_n(\mathbf{R}) / H \cong < \mathbf{Z}/2\mathbf{Z}, + >$ по 2-ой теореме о гомоморфизмах групп.

г) $GL_n(\mathbf{C}) / H \cong < U, \cdot >, \ H = \{A \in GL_n(\mathbf{C}) \mid \det A > 0\}, \ U = \{z \in \mathbf{C} \mid |z| = 1\}$.

Решение:

$$f: GL_n(\mathbf{C}) \to U,\ \ f(A) = \frac{\det A}{|\det A|}.$$

$$f(A \cdot B) = \frac{\det(A \cdot B)}{|\det(A \cdot B)|} = \frac{\det A \cdot \det B}{|\det A \cdot \det B|} = \frac{\det A}{|\det A|} \cdot \frac{\det B}{|\det B|} = f(A) \cdot f(B).$$

Следовательно, f – гомоморфизм групп. f – эпиморфизм, поскольку для $\forall a \in U \ \ \exists A \in GL_n(\mathbf{C}) \mid \det A = a \ \Rightarrow\ f(A) = \frac{a}{|a|} = \frac{a}{1} = a.$ Матрица A строится также, как в задаче а).

$$Ker(f) = \{A \in GL_n(\mathbf{C}) \mid \ \frac{\det A}{|\det A|} = 1 \Leftrightarrow \det A = |\det A| \Leftrightarrow \det A \in R_{>0}\} = H.$$

Следовательно, $GL_n(\mathbf{C}) / H \cong < U, \cdot >$ по 2-ой теореме о гомоморфизмах групп.

№6. Построить подгруппу в $S(G)$, изоморфную указанной группе G, используя теорему Кэли.

а) $< \mathbf{Z}, + >$.

Решение:

Построим согласно доказательству теоремы Кэли функцию $\varphi: \mathbf{Z} \to S(\mathbf{Z})$, $Ker\varphi = \{0\}$, $\mathrm{Im}\,\varphi \cong < \mathbf{Z}, + >$, где $\varphi(a) = \varphi_a$, $\varphi_a(z) = a + z$, $\forall\, z \in \mathbf{Z}$. φ_a представляет собой сдвиг на постоянную целочисленную величину a во множестве $\mathbf{Z}$. $\varphi(0) = e_{\mathbf{Z}}$ – тождественное отображение.

$$\varphi(a+b) = \varphi(b+a) = \varphi_a \circ \varphi_b = \varphi_b \circ \varphi_a.$$

$Im\varphi \le S(\mathbf{Z})$, $Im\varphi$ – абелева бесконечная циклическая группа (как изоморфная $< \mathbf{Z}, + >$) сдвигов множества $\mathbf{Z}$ на постоянные целочисленные величины.

Ответ: абелева бесконечная циклическая группа сдвигов множества $\mathbf{Z}$ на постоянные целочисленные величины.

б) $< a >,\ Ord(a) = 4$.

Решение:

$< a > = \{e,\ a,\ a^2,\ a^3\},\ a^4 = e.$

$\varphi: < a > \to S_4,\ \varphi(a^i) = \varphi_{a^i},\ i = \overline{0,3},\ \forall\ g \in < a >\ \varphi_{a^i}(g) = a^i \cdot g$.

$\varphi_e(g) = g\ \ \forall g \in < a >\ \Rightarrow\ \varphi_e = e_{<a>}$.

$\varphi_a = (1\ 2\ 3\ 4)$, поскольку $\varphi_a(g) = a \cdot g\ \ \forall g \in < a >$, и $\varphi_a(e) = a$, $\varphi_a(a) = a^2$, $\varphi_a(a^2) = a^3$, $\varphi_a(a^3) = e$.

$\varphi_{a^2}(g) = a^2 \cdot g\ \ \forall g \in < a >$, и $\varphi_{a^2}(e) = a^2$, $\varphi_{a^2}(a) = a^3$, $\varphi_{a^2}(a^2) = e$, $\varphi_{a^2}(a^3) = a$, поэтому $\varphi_{a^2} = \begin{pmatrix} 1\,2\,3\,4 \\ 3\,4\,1\,2 \end{pmatrix} = (1\,3) \cdot (2\,4)$.

$\varphi_{a^3}(g) = a^3 \cdot g \quad \forall g \in < a >$, и $\varphi_{a^3}(e) = a^3$, $\varphi_{a^3}(a) = e$, $\varphi_{a^3}(a^2) = a$, $\varphi_{a^3}(a^3) = a^2$,

поэтому $\varphi_{a^3} = \begin{pmatrix} 1\,2\,3\,4 \\ 4\,1\,2\,3 \end{pmatrix} = (1\,4\,3\,2)$.

$< a > \cong Im\varphi = < (1\,2\,3\,4) >$, $< 1\,2\,3\,4 > < S_4$.

Ответ: $< (1\,2\,3\,4) >$.

№7. Задан открытый ключ (n, e) и сообщение x. Найти секретный ключ и дешифровать сообщение.

а) n=2021, e=5, x=415.

Решение:

Разложим $n = p \cdot q$. Ищем минимальное простое число p, $p \mid n$. Используем «решето» Эратосфена, $p \le [\sqrt{n}]$. Получаем, что p=43, q=47.

$\varphi(n) = (p-1)(q-1) = 1932$.

Далее ищем секретный ключ d.

$e \cdot d \equiv 1 (\mathrm{mod}\, \varphi(n))$. Ищем d как e^{-1} в $\mathbf{Z}/\varphi(n)\mathbf{Z}$.

$2 = 1992 - 5 \cdot 386;$

$1 = 5 - 2 \cdot 2 = 5 - 1932 \cdot 2 + 5 \cdot 772 = 5 \cdot 773 - 1932 \cdot 2;$

$d = 773.$

Далее возводим x в степень d модулю n. Для этого удобно использовать двоичное представление числа d.

$773 = 2^9 + 261 = 2^9 + 2^8 + 2^2 + 2^0.$

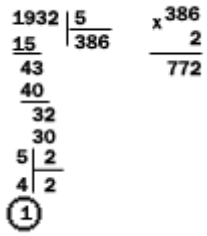
$c = 415^{773} = 415^{2^9+2^8+2^2+2^0} =$

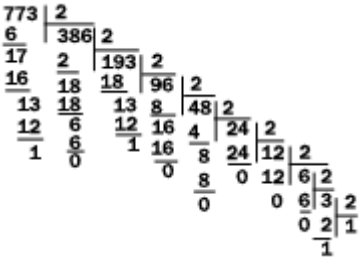
$= 415^{2^0} \cdot 415^{2^2} \cdot 415^{2^8} \cdot 415^{2^9} =$

$= 415 \cdot 415^{2^2} \cdot (415^{2^2})^{2^6} \cdot (415^{2^8})^2.$

$a_0 = 415, \quad a_1 = a_0^{\,2^2}, \quad a_2 = a_0 \cdot a_1,$

$a_3 = a_1^{\,2^6}, \quad a_4 = a_2 \cdot a_3, \quad a_5 = a_3^{\,2}, \quad a_6 = a_4 \cdot a_5.$





Для удобства возведения в степень можно использовать также каноническое разложение числа x.

$415 = 5 \cdot 83$ – каноническое разложение.

$c = 415^{773} \equiv 1078 \ (\mathrm{mod}\, 2021).$

Ответ: d=773, c=1078.

б) n=2491, e=11, x=85.

Решение:

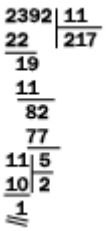
$p = 47, \quad q = 53; \quad \varphi(n) = 46 \cdot 52 = 2392.$

$5 = 2392 - 11 \cdot 217;$

$1 = 11 - 2 \cdot 5 = 11 - 2 \cdot 2392 + 11 \cdot 434 = -2 \cdot 2392 + 435 \cdot 11;$

$d = 435.$

$c = 85^{435} \equiv 1110 \pmod{2491}.$



Ответ: d=435, c=1110.

№8. Выберите открытый ключ (n, e) так, чтобы n>1300. Вычислите секретный ключ d. Убедитесь, что вы нашли правильный ключ – зашифруйте и расшифруйте сообщение.

Раздел IV. Элементы теории колец и полей

4.1. Кольца и их идеалы

№1. Выяснить, какие из следующих множеств являются кольцами, коммутативными кольцами (но не полями) и какие полями относительно указанных операций. Если операции не указаны, то подразумеваются сложение и умножение чисел.

а) $\{a + b\sqrt{2} \mid a,b \in \mathbf{Z}\}$.

Ответ: коммутативное кольцо.

б) $\{a + b\sqrt{3} \mid a,b \in \mathbf{Q}\}$.

Ответ: поле.

в) $\left\{ \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \mid a,b \in \mathbf{Q}\ (\mathbf{R}) \right\}$ относительно обычных сложения и умножения матриц.

Ответ: поле при $a,b \in \mathbf{Q}$, коммутативное кольцо при $a,b \in \mathbf{R}$.

г) $\left\{ \begin{pmatrix} a_1 & 0 & 0 & \cdots & 0 \\ 0 & a_2 & 0 & \cdots & 0 \\ 0 & 0 & a_3 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & a_n \end{pmatrix} \mid a_i \in \mathbf{R},\ i = \overline{1,n},\ n \geq 2 \right\}$ относительно обычных сложения и умножения матриц.

Ответ: коммутативное кольцо.

№2. Доказать, что в кольце квадратных матриц порядка $n \in \mathbf{N}$ с элементами из некоторого поля вырожденные матрицы, и только они, являются делителями нуля.

№3. Показать, что множество $\mathrm{K} = \{(a,b) \mid a,b \in \mathbf{Z}\}$ относительно операций, заданных равенствами

$$(a_1,\ b_1) \oplus (a_2,\ b_2) = (a_1 + a_2,\ b_1 + b_2),\ \ (a_1,\ b_1) \square\ (a_2,\ b_2) = (a_1 \cdot a_2,\ b_1 \cdot b_2),$$

где + и · – обычные операции сложения и умножения в **Z**, образуют ассоциативное и коммутативное кольцо с единицей. Найти все делители нуля этого кольца.

Ответ: $\{(a,\ 0) \mid a \in Z \setminus \{0\}\} \cup \{(0,\ b) \mid b \in Z \setminus \{0\}\}$ – множество всех делителей нуля.

№4. Будут ли следующие множества подгруппами аддитивной группы, подкольцами или идеалами указанных ниже коммутативных колец?

а) $n\mathbf{Z}[x]$ – множество многочленов, коэффициенты которых кратны числу $n \in \mathbf{N}_{>1}$, в кольце $\mathbf{Z}[x]$ целочисленных многочленов.

Ответ: идеал.

б) Множество $\mathbf{N}$ в кольце $< \mathbf{Z}, +, \cdot >$.

Ответ: не является подгруппой аддитивной группы.

в) Множество $\mathbf{Z}$ в кольце целых гауссовых чисел $< \mathrm{A}, +, \cdot >,\ \mathrm{A} = \{a + bi \mid a,b \in \mathbf{Z},\ i^2 = -1\}$.

Ответ: подкольцо.

г) Множество $\mathrm{B} = \{a + bi \mid a,b \in \mathbf{Z},\ i^2 = -1,\ a = b\}$ в кольце целых гауссовых чисел.

Ответ: подгруппа аддитивной группы.

д) Множество $\mathbf{Z}[x]$ целочисленных многочленов в кольце $\mathbf{Q}[x]$ многочленов над полем рациональных чисел.

Ответ: подкольцо.

е) Множество I многочленов, не содержащих членов с x^k для всех $k < n$, где $n \in \mathbf{N}_{>1}$, в кольце $\mathbf{Z}[x]$ целочисленных многочленов.

Ответ: идеал.

№5. Является ли идеалом кольца (левым, правым, двусторонним) следующее множество *I*?

а) $I_1,\ I_2$ – идеалы кольца (одновременно левые или правые, или двусторонние). $I = I_1 \setminus I_2$.

Ответ: не является.

б) J – идеал кольца (левые или правый, или двусторонний). $I = J^2 = \{j^2 \mid j \in J\}$.

Ответ: не является.

в) $I_1,\ I_2$ – идеалы кольца (одновременно левые или правые, или двусторонние). $I = I_1 \cup I_2$.

Ответ: не является.

г) I_1, I_2 – идеалы кольца (одновременно левые или правые, или двусторонние). $I = I_1 \cap I_2$.

Ответ: является (соответственно левым или правым, или двусторонним) идеалом.

д) I_1, I_2 – идеалы кольца (одновременно левые или правые, или двусторонние). $I = I_1 + I_2 = \{i_1 + i_2 \mid i_1 \in I_1,\ i_2 \in I_2\}$.

Ответ: является (соответственно левым или правым, или двусторонним) идеалом.

4.2. Кольцо полиномов и его свойства

№1. Найти НОД полиномов.

а) $f(x) = x^3 + x^2 + 2x + 2,\ \ g(x) = x^2 + 2x + 1$ над $\mathbf{Z}/3\mathbf{Z}$ и над $\mathbf{Q}$.

Ответ: $x + \bar{2}$ и 1 соответственно.

б) $f(x) = 5x^3 + x^2 + 5x + 1,\ \ g(x) = 5x^2 + 21x + 4$ над $\mathbf{Z}/5\mathbf{Z}$ и над $\mathbf{Q}$.

Ответ: $\bar{1}$ и $5x + 1$ соответственно.

№2. Разложить полином на неприводимые множители над полем.

а) $x^5 + x^3 + x^2 + \bar{1}$ над $\mathbf{Z}/2\mathbf{Z}$.

Ответ: $(x + \bar{1})^3 \cdot (x^2 + x + \bar{1})$.

б) $x^4 + x^3 + x + \bar{2}$ над $\mathbf{Z}/3\mathbf{Z}$.

Ответ: $(x^2 + \bar{1}) \cdot (x^2 + x + \bar{2})$

№3. Разложить полиномы на неприводимые множители над полем.

а) Все полиномы второй степени от x над $\mathbf{Z}/2\mathbf{Z}$.

Ответ: $f_1(x) = x^2,\ \ f_2(x) = x^2 + 1 = (x+1)^2,\ \ f_3(x) = x^2 + x = x \cdot (x+1),$

$f_4(x) = x^2 + x + 1.$

б) Все полиномы третьей степени от x над $\mathbf{Z}/2\mathbf{Z}$.

Ответ: $f_1(x) = x^3,\ \ f_2(x) = x^3 + 1 = (x+1) \cdot (x^2 + x + 1),$

$f_3(x) = x^3 + x = x \cdot (x+1)^2,\ \ f_4(x) = x^3 + x^2 = x^2 \cdot (x+1),$

$f_5(x) = x^3 + x + 1,\ \ f_6(x) = x^3 + x^2 + 1,$

$f_7(x) = x^3 + x^2 + x = x \cdot (x^2 + x + 1),\ \ f_8(x) = x^3 + x^2 + x + 1 = (x+1)^3.$

№4. Максимален ли идеал в кольце полиномов?

а) $< x^4 + 1 >$ в $\mathbf{R}[x]$, $\mathbf{C}[x]$, $\mathbf{Q}[x]$.

Решение:

Т.к. $\deg f = 4$, то $f(x)$ приводим над $\mathbf{R}$ и $\mathbf{C} \Leftrightarrow$

$< f(x) >$ не максимален в $\mathbf{R}[x]$ и $\mathbf{C}[x]$.

$x^4 = -1$, найдем все $\sqrt[4]{-1}$:

$$\omega_k = cos\frac{\pi + 2k\pi}{4} + isin\frac{\pi + 2k\pi}{4}, \quad k = \overline{0,3}.$$

$$\omega_0 = cos\frac{\pi}{4} + isin\frac{\pi}{4} = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2},$$

$$\omega_1 = cos\frac{\pi + 2\pi}{4} + isin\frac{\pi + 2\pi}{4} = -\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2},$$

$$\omega_2 = cos\frac{\pi + 4\pi}{4} + isin\frac{\pi + 4\pi}{4} = -\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2},$$

$$\omega_3 = cos\frac{\pi + 6\pi}{4} + isin\frac{\pi + 6\pi}{4} = \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}.$$

$$f(x) = \left(x - \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}\right)\cdot\left(x - \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right)\cdot\left(x + \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}\right)\cdot\left(x + \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right) =$$

$$= \left(\left(x - \frac{\sqrt{2}}{2}\right)^2 - \left(i\frac{\sqrt{2}}{2}\right)^2\right)\cdot\left(\left(x + \frac{\sqrt{2}}{2}\right)^2 - \left(i\frac{\sqrt{2}}{2}\right)^2\right) = \left(x^2 - \sqrt{2}x + \frac{1}{2} + \frac{1}{2}\right)\times$$

$$\times\left(x^2 + \sqrt{2}x + \frac{1}{2} + \frac{1}{2}\right) = \left(x^2 - \sqrt{2}x + 1\right)\cdot\left(x^2 + \sqrt{2}x + 1\right).$$

$f(x) = f_1(x)\cdot f_2(x)$, f приводим над $\mathbf{C}$ и $\mathbf{R}$, f_1, f_2 не приводимы над $\mathbf{R}$.

В то же время, $f(x)$ не приводим над $\mathbf{Q}$. Если бы $f(x)$ был приводим над $\mathbf{Q}$, то разложение было бы другим и над $\mathbf{R}$, чего быть не может. Каноническое разложение на множители со старшим коэффициентом 1 определяется однозначно.

Итак, $< x^4 + 1 >$ не является максимальным идеалом в $\mathbf{R}[x]$ и $\mathbf{C}[x]$, но является максимальным идеалом в $\mathbf{Q}[x]$.

Ответ: не максимальный идеал в $\mathbf{R}[x]$ и $\mathbf{C}[x]$, максимальный идеал в $\mathbf{Q}[x]$.

б) $< x^6 + x^5 + x^4 + x + 1 >$ в $\mathbf{Z}/2\mathbf{Z}[x]$.

Решение:

$\overline{0}$ и $\overline{1}$ не являются корнями $f(x)$.

$x^2 + x + 1$ – единственный неприводимый многочлен 2-ой степени в $\mathbf{Z}/2\mathbf{Z}[x]$.

$$\begin{array}{l} x^6 + x^5 + x^4 + x + 1 \\ x^6 + x^5 + x^4 \\ \qquad\quad x + 1 \end{array} \left| \begin{array}{l} x^2 + x + 1 \\ \hline x^4 \end{array} \right. \qquad \left(x^2 + x + 1\right) \nmid f(x).$$

Неприводимыми многочленами степени 3 над $\mathbf{Z}/2\mathbf{Z}$ являются x^3+x+1 и x^3+x^2+1.

$$\begin{array}{r|l} x^6+x^5+x^4+x+1 & x^3+x+1 \\ \hline x^6+x^4+x^3 & x^3+x^2 \\ \hline x^5+x^3+x+1 & \\ x^5+x^3+x^2 & \\ \hline x^2+x+1 & \end{array} \qquad \begin{array}{r|l} x^6+x^5+x^4+x+1 & x^3+x^2+1 \\ \hline x^6+x^5+x^3 & x^3+x \\ \hline x^4+x^3+x+1 & \\ x^4+x^3+x & \\ \hline 1 & \end{array}$$

$(x^3+x+1) \nmid f(x)$. $\qquad x^3+x^2+1 \nmid f(x)$.

Значит, $f(x)$ не приводим над $\mathbf{Z/2Z} \Rightarrow < f(x) >$ максимален в $\mathbf{Z/2Z}[x]$ (и $\mathbf{Z}/2\mathbf{Z}[x]/ < f(x) >$ – поле).

Ответ: максимальный идеал.

в) $< x^4+1 >$ в $\mathbf{Z}/2\mathbf{Z}[x]$.

Решение:

$\overline{1}$ – корень x^4+1, $x^4+1=(x+1)^4$, т.к. $\mathbf{Z}/2\mathbf{Z}$ – поле характеристики 2.

x^4+1 приводим над $\mathbf{Z}/2\mathbf{Z} \Rightarrow < x^4+1 >$ – не максимальный идеал.

Ответ: не максимальный идеал.

г) $< x^4+4 >$ в $\mathbf{Q}[x]$.

Решение:

$$x^4+2\cdot 2\cdot x^2+2^2-4\cdot x^2=(x^2+2)^2-(2x)^2=(x^2+2-2x)\cdot(x^2+2+2x)=$$

$$=(x^2-2x+2)(x^2+2x+2).$$

$f(x)$ приводим над $\mathbf{Q} \Rightarrow < x^4+4 >$ не является максимальным в $\mathbf{Q}[x]$.

x^2-2x+2 и x^2+2x+2 уже не приводимы над $\mathbf{R}$,

т.к. $\frac{D}{4}=1-2=-1<0 \Rightarrow$ не приводимы и над $\mathbf{Q}$.

Ответ: не максимальный идеал.

д) $< x^3+x+1 >$ в $\mathbf{Q}[x]$, $\mathbf{Z}/2\mathbf{Z}[x]$.

Решение:

Если полином третьей степени приводим над полем, то среди его делителей будет хотя бы один полином первой степени.

x^3+x+1 имеет ли корни в $\mathbf{Q}$?

Такие корни могут быть только в $\mathbf{Z}$ и являются делителями 1.

$1+1+1=3\neq 0 \Rightarrow 1$ – не корень $f(x)$,

$-1-1+1=-1\neq 0 \Rightarrow -1$ – не корень $f(x)$.

Т.к. $f(x)$ не имеет корней в $\mathbf{Q}$, то $f(x)$ не приводим над $\mathbf{Q}$,

следовательно, $< f(x) >$ максимален в $\mathbf{Q}[x]$.

Ответ: максимальный идеал.

е) $< 2x^5 + 3x^2 - 9x + 15 >$ в $\mathbf{Q}[x]$.

Решение:

3 – простое число,

$3 \mid 15, \quad 3 \mid -9, \quad 3 \mid 3,$ но $3 \nmid 2, \quad 3^2 = 9 \nmid 15.$

Значит, по признаку Эйзенштейна $f(x)$ не приводим над $\mathbf{Q}$, следовательно, $< f(x) >$ – максимальный идеал в $\mathbf{Q}[x]$.

Ответ: максимальный идеал.

4.3. Фактор-кольца. Гомоморфизмы колец

№1. Построить фактор-кольцо P[*x*]/<*f*(*x*)>. Является ли оно полем? В случае положительного ответа найти характеристику поля.

а) $\mathbf{Z}/2\mathbf{Z}[x]/< x^3 + x^2 + 1 >$.

Решение:

$g(x) = x^3 + x^2 + 1$ не приводим над $\mathbf{Z}/2\mathbf{Z} \Rightarrow \mathbf{Z}/2\mathbf{Z}[x]/< f(x) >$ – поле. Это конечное поле из $2^3 = 8$ элементов характеристики 2. Сложение и умножение в данном поле задаются таблицами Кэли (таблицы 4.2.1 и 4.2.2 соответственно).

Таблица 4.2.1

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$	$\overline{x^2}$	$\overline{x^2+1}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$	$\overline{x^2}$	$\overline{x^2+1}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	$\bar{x}$	$\overline{x^2+1}$	$\overline{x^2}$	$\overline{x^2+x+1}$	$\overline{x^2+x}$
$\bar{x}$	$\bar{x}$	$\overline{x+1}$	$\bar{0}$	$\bar{1}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$	$\overline{x^2}$	$\overline{x^2+1}$
$\overline{x+1}$	$\overline{x+1}$	$\bar{x}$	$\bar{1}$	$\bar{0}$	$\overline{x^2+x+1}$	$\overline{x^2+x}$	$\overline{x^2+1}$	$\overline{x^2}$
$\overline{x^2}$	$\overline{x^2}$	$\overline{x^2+1}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\overline{x^2+1}$	$\overline{x^2+1}$	$\overline{x^2}$	$\overline{x^2+x+1}$	$\overline{x^2+x}$	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	$\bar{x}$
$\overline{x^2+x}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$	$\overline{x^2}$	$\overline{x^2+1}$	$\bar{x}$	$\overline{x+1}$	$\bar{0}$	$\bar{1}$
$\overline{x^2+x+1}$	$\overline{x^2+x+1}$	$\overline{x^2+x}$	$\overline{x^2+1}$	$\overline{x^2}$	$\overline{x+1}$	$\bar{x}$	$\bar{1}$	$\bar{0}$

Обозначим α примитивный элемент данного поля, α – корень полинома $g(x)$, тогда выполняется соотношение $\alpha^3 + \alpha^2 + 1 = 0$. Откуда находим выражения степеней элемента α.

$\alpha^3 = \alpha^2 + 1,$

$\alpha^4 = \alpha^3 + \alpha = \alpha^2 + \alpha + 1,$

$\alpha^5 = \alpha^3 + \alpha^2 + \alpha = \alpha + 1,$

$\alpha^6 = \alpha^2 + \alpha,$

$\alpha^7 = \alpha^3 + \alpha^2 = 1.$

Таблица 4.2.2

$\otimes$	$0:\ \bar{0}$	$1:\ \bar{1}$	$\alpha:\ \bar{x}$	$\alpha^5:\ \overline{x+1}$	$\alpha^2:\ \overline{x^2}$	$\alpha^3:\ \overline{x^2+1}$	$\alpha^6:\ \overline{x^2+x}$	$\alpha^4:\ \overline{x^2+x+1}$
$0:\ \bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$1:\ \bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$	$\overline{x^2}$	$\overline{x^2+1}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$
$\alpha:\ \bar{x}$	$\bar{0}$	$\bar{x}$	$\overline{x^2}$	$\overline{x^2+x}$	$\overline{x^2+1}$	$\overline{x^2+x+1}$	$\bar{1}$	$\overline{x+1}$
$\alpha^5:\ \overline{x+1}$	$\bar{0}$	$\overline{x+1}$	$\overline{x^2+x}$	$\overline{x^2+1}$	$\bar{1}$	$\bar{x}$	$\overline{x^2+x+1}$	$\overline{x^2}$
$\alpha^2:\ \overline{x^2}$	$\bar{0}$	$\overline{x^2}$	$\overline{x^2+1}$	$\bar{1}$	$\overline{x^2+x+1}$	$\overline{x+1}$	$\bar{x}$	$\overline{x^2+x}$
$\alpha^3:\ \overline{x^2+1}$	$\bar{0}$	$\overline{x^2+1}$	$\overline{x^2+x+1}$	$\bar{x}$	$\overline{x+1}$	$\overline{x^2+x}$	$\overline{x^2}$	$\bar{1}$
$\alpha^6:\ \overline{x^2+x}$	$\bar{0}$	$\overline{x^2+x}$	$\bar{1}$	$\overline{x^2+x+1}$	$\bar{x}$	$\overline{x^2}$	$\overline{x+1}$	$\overline{x^2+1}$
$\alpha^4:\ \overline{x^2+x+1}$	$\bar{0}$	$\overline{x^2+x+1}$	$\overline{x+1}$	$\overline{x^2}$	$\overline{x^2+x}$	$\bar{1}$	$\overline{x^2+1}$	$\bar{x}$

Ответ: поле из 8 элементов характеристики 2.

б) $\mathbf{Z}/3\mathbf{Z}[x]/<x^2+2x+2>$.

Решение:

$f(x)=x^2+2x+2$ не имеет корней в $\mathbf{Z}/3\mathbf{Z} \Rightarrow \mathbf{Z}/3\mathbf{Z}[x]/f(x)$ – конечное поле из $3^2=9$ элементов характеристики 3. Сложение и умножение в данном поле задаются таблицами Кэли (таблицы 4.2.3 и 4.2.4 соответственно).

Таблица 4.2.3

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{x}$	$\overline{x+1}$	$\overline{x+2}$	$\overline{2x}$	$\overline{2x+1}$	$\overline{2x+2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{x}$	$\overline{x+1}$	$\overline{x+2}$	$\overline{2x}$	$\overline{2x+1}$	$\overline{2x+2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$	$\overline{x+1}$	$\overline{x+2}$	$\bar{x}$	$\overline{2x+1}$	$\overline{2x+2}$	$\overline{2x}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$	$\overline{x+2}$	$\bar{x}$	$\overline{x+1}$	$\overline{2x+2}$	$\overline{2x}$	$\overline{2x+1}$
$\bar{x}$	$\bar{x}$	$\overline{x+1}$	$\overline{x+2}$	$\overline{2x}$	$\overline{2x+1}$	$\overline{2x+2}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\overline{x+1}$	$\overline{x+1}$	$\overline{x+2}$	$\bar{x}$	$\overline{2x+1}$	$\overline{2x+2}$	$\overline{2x}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\overline{x+2}$	$\overline{x+2}$	$\bar{x}$	$\overline{x+1}$	$\overline{2x+2}$	$\overline{2x}$	$\overline{2x+1}$	$\bar{2}$	$\bar{0}$	$\bar{1}$
$\overline{2x}$	$\overline{2x}$	$\overline{2x+1}$	$\overline{2x+2}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{x}$	$\overline{x+1}$	$\overline{x+2}$
$\overline{2x+1}$	$\overline{2x+1}$	$\overline{2x+2}$	$\overline{2x}$	$\bar{1}$	$\bar{2}$	$\bar{0}$	$\overline{x+1}$	$\overline{x+2}$	$\bar{x}$
$\overline{2x+2}$	$\overline{2x+2}$	$\overline{2x}$	$\overline{2x+1}$	$\bar{2}$	$\bar{0}$	$\bar{1}$	$\overline{x+2}$	$\bar{x}$	$\overline{x+1}$

Обозначим α примитивный элемент данного поля, α – корень полинома $g(x)$, тогда выполняется соотношение $\alpha^2+2\alpha+2=0$. Откуда находим выражения степеней элемента α.

$\alpha^2=\alpha+1,$
$\alpha^3=\alpha^2+\alpha=2\alpha+1,$
$\alpha^4=\alpha^2+2\alpha+1=2,$
$\alpha^5=2\alpha,$
$\alpha^6=2\alpha^2=2\alpha+2,$
$\alpha^7=2\alpha^2+2\alpha=\alpha+2,$
$\alpha^8=1.$

Таблица 4.2.4

$\otimes$	$0:\ \bar{0}$	$1:\ \bar{1}$	$\alpha^4:\ \bar{2}$	$\alpha:\ \bar{x}$	$\alpha^2:\ \overline{x+1}$	$\alpha^7:\ \overline{x+2}$	$\alpha^5:\ \overline{2x}$	$\alpha^3:\ \overline{2x+1}$	$\alpha^6:\ \overline{2x+2}$
$0:\ \bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$1:\ \bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{x}$	$\overline{x+1}$	$\overline{x+2}$	$\overline{2x}$	$\overline{2x+1}$	$\overline{2x+2}$
$\alpha^4:\ \bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$	$\overline{2x}$	$\overline{2x+2}$	$\overline{2x+1}$	$\bar{x}$	$\overline{x+2}$	$\overline{x+1}$
$\alpha:\ \bar{x}$	$\bar{0}$	$\bar{x}$	$\overline{2x}$	$\overline{x+1}$	$\overline{2x+1}$	$\bar{1}$	$\overline{2x+2}$	$\bar{2}$	$\overline{x+2}$
$\alpha^2:\ \overline{x+1}$	$\bar{0}$	$\overline{x+1}$	$\overline{2x+2}$	$\overline{2x+1}$	$\bar{2}$	$\bar{x}$	$\overline{x+2}$	$\overline{2x}$	$\bar{1}$
$\alpha^7:\ \overline{x+2}$	$\bar{0}$	$\overline{x+2}$	$\overline{2x+1}$	$\bar{1}$	$\bar{x}$	$\overline{2x+2}$	$\bar{2}$	$\overline{x+1}$	$\overline{2x}$
$\alpha^5:\ \overline{2x}$	$\bar{0}$	$\overline{2x}$	$\bar{x}$	$\overline{2x+2}$	$\overline{x+2}$	$\bar{2}$	$\overline{x+1}$	$\bar{1}$	$\overline{2x+1}$
$\alpha^3:\ \overline{2x+1}$	$\bar{0}$	$\overline{2x+1}$	$\overline{x+2}$	$\bar{2}$	$\overline{2x}$	$\overline{x+1}$	$\bar{1}$	$\overline{2x+2}$	$\bar{x}$
$\alpha^6:\ \overline{2x+2}$	$\bar{0}$	$\overline{2x+2}$	$\overline{x+1}$	$\overline{x+2}$	$\bar{1}$	$\overline{2x}$	$\overline{2x+1}$	$\bar{x}$	$\bar{2}$

Ответ: поле из 9 элементов характеристики 3.

в) $\mathbf{Z}/2\mathbf{Z}[x]/<x^2+1>.$

Решение:

$f(x)=x^2+1$ приводим над $\mathbf{Z}/2\mathbf{Z}$, т.к. $x^2+1=(x+1)^2$. Поэтому $\mathbf{Z}/2\mathbf{Z}[x]/<x^2+1>$ – не поле, а кольцо с делителями нуля. Сложение и умножение в данном кольце задаются таблицами Кэли (таблицы 4.2.5 и 4.2.6 соответственно).

Таблица 4.2.5

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	$\bar{x}$
$\bar{x}$	$\bar{x}$	$\overline{x+1}$	$\bar{0}$	$\bar{1}$
$\overline{x+1}$	$\overline{x+1}$	$\bar{x}$	$\bar{1}$	$\bar{0}$

Таблица 4.2.6

$\otimes$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{x}$	$\bar{0}$	$\bar{x}$	$\bar{1}$	$\overline{x+1}$
$\overline{x+1}$	$\bar{0}$	$\overline{x+1}$	$\overline{x+1}$	$\bar{0}$

$\bar{1},\ \bar{x}$ – обратимые элементы кольца, $\bar{1}^{-1}=\bar{1},\quad \bar{x}^{-1}=\bar{x}$.

$\overline{x+1}$ – делитель нуля.

$<\bar{0}>\subset<\overline{x+1}>\subset \mathbf{Z}/2\mathbf{Z}[x]/<f(x)>$ – идеалы кольца.

Ответ: не поле.

№2. Найти все идеалы кольца $\mathbf{Z}/n\mathbf{Z}$, расположить их в порядке включения, указать максимальные идеалы.

а) $\mathbf{Z}/29\mathbf{Z}$.

Решение:

29 – простое число $\Rightarrow$ $29\mathbf{Z}$ – максимальный идеал в $\mathbf{Z}$ и $\mathbf{Z}/29\mathbf{Z}$ – поле. В поле каждый отличный от нуля элемент обратим. Поэтому единственными идеалами в $\mathbf{Z}/29\mathbf{Z}$ будут $\{0\}$ и $\mathbf{Z}/29\mathbf{Z}$. Собственных максимальных идеалов не будет.

Ответ: $\{0\}\subset\mathbf{Z}/29\mathbf{Z}$; максимальных идеалов нет.

б) $\mathbf{Z}/8\mathbf{Z}$.

Решение:

Рассмотрим канонический гомоморфизм $f:\mathbf{Z}\to\mathbf{Z}/8\mathbf{Z},\quad f(z)=\bar{z}$, $Kerf=8\mathbf{Z}$.

$\mathbf{Z}/8\mathbf{Z}=\{\bar{0},\ \bar{1},\ \bar{2},\ \bar{3},\ \bar{4},\ \bar{5},\ \bar{6},\ \bar{7}\}$.

Собственные идеалы не могут содержать обратимых элементов. Т.к. $\mathbf{Z}$ – кольцо главных идеалов, то в $\mathbf{Z}/8\mathbf{Z}$ любой идеал является главным и является образом идеала из $\mathbf{Z}$.

Не взаимно простыми с 8 являются 2, 4, 6: $(2, 8)=2\neq 1$, $(4, 8)=4\neq 1$, $(6, 8)=2\neq 1$.

$\left|<\bar{k}>\right|=\dfrac{n}{(k,\ n)}$; $8=2^3$, $n=p_1^{s_1}\cdot\ldots\cdot p_k^{s_k}$; $<\overline{p_i}>$ – максимальные идеалы.

$<\bar{2}>=\{\bar{0},\ \bar{2},\ \bar{4},\ \bar{6}\}$, $<\bar{6}>=\{\bar{0},\ \bar{6},\ \bar{4},\ \bar{2}\}$, $<\bar{4}>=\{\bar{0},\ \bar{4}\}$,

$<\bar{2}>=<\bar{6}>$ – максимальный идеал.

$<\bar{0}>\subset<\bar{4}>\subset<\bar{2}>\subset \mathbf{Z}/8\mathbf{Z}$.

Ответ: $<\bar{0}>\subset<\bar{4}>\subset<\bar{2}>\subset \mathbf{Z}/8\mathbf{Z}$; $<\bar{2}>=<\bar{6}>$ – максимальный идеал.

в) $\mathbf{Z}/24\mathbf{Z}$.

Решение:

Рассмотрим канонический гомоморфизм $f:\mathbf{Z}\to\mathbf{Z}/24\mathbf{Z}$, $f(z)=\bar{z}$, $Kerf=24\mathbf{Z}$.

Собственные идеалы не могут содержать обратимых элементов. Т.к. $\mathbf{Z}$ – кольцо главных идеалов, то в $\mathbf{Z}/24\mathbf{Z}$ любой идеал является главным и является образом идеала из $\mathbf{Z}$.

$1, 2, 3, 4, 6, 8, 12 \mid 24$, $\mathbf{Z}/24\mathbf{Z}=\{\bar{0},\ \bar{1},\ \bar{2},\ \bar{3},...,\ \overline{22},\ \overline{23}\}$,

$24=2^3\cdot 3$,

максимальные идеалы $<\bar{2}>$ и $<\bar{3}>$.

$<\bar{2}>=\{\bar{0},\ \bar{2},\ \bar{4},\ \bar{6},\ \bar{8},\ \overline{10},\ \overline{12},\ \overline{14},\ \overline{16},\ \overline{18},\ \overline{20},\ \overline{22}\}$,

$|<\bar{2}>|=12$, $\varphi(12)=\varphi(2^3\cdot 3)=(2^2-2)\cdot 2=2\cdot 2=4$,

$<\bar{2}>=<\overline{10}>=<\overline{14}>=<\overline{22}>$.

$<\bar{3}>=\{\bar{0},\ \bar{3},\ \bar{6},\ \bar{9},\ \overline{12},\ \overline{15},\ \overline{18},\ \overline{21}\}$,

$|<\bar{3}>|=\frac{24}{3}=8$, $\varphi(8)=\varphi(2^3)=2^3-2^2=4$,

$<\bar{3}>=<\bar{9}>=<\overline{15}>=<\overline{21}>$.

$<\bar{4}>=\{\bar{0},\ \bar{4},\ \bar{8},\ \overline{12},\ \overline{16},\ \overline{20}\}$,

$|<\bar{4}>|=\frac{24}{4}=6$, $\varphi(6)=2$, $<\bar{4}>=<\overline{20}>$.

$<\bar{6}>=\{\bar{0},\ \bar{6},\ \overline{12},\ \overline{18}\}$, $<\bar{6}>=<\overline{18}>$, $|<\bar{6}>|=\frac{24}{6}=4$, $\varphi(4)=2$.

$<\bar{8}>=\{\bar{0},\ \bar{8},\ \overline{16}\}$, $<\bar{8}>=<\overline{16}>$, $|<\bar{8}>|=\frac{24}{8}=3$, $\varphi(3)=2$.

$<\overline{12}>=\{\bar{0},\ \overline{12}\}$, $|<\overline{12}>|=\frac{24}{12}=2$, $\varphi(2)=1$.

$<\bar{0}>\subset<\overline{12}>\subset<\bar{6}>\subset<\bar{3}>\subset \mathbf{Z}/24\mathbf{Z}$,

$<\bar{0}>\subset<\bar{8}>\subset<\bar{4}>\subset<\bar{2}>\subset \mathbf{Z}/24\mathbf{Z}$,

$<\overline{12}>\subset<\bar{4}>$, $<\bar{6}>\subset<\bar{2}>$.

Ответ: $<\overline{12}>\subset<\bar{4}>$, $<\bar{6}>\subset<\bar{2}>$, $<\bar{0}>\subset<\overline{12}>\subset<\bar{6}>\subset<\bar{3}>\subset \mathbf{Z}/24\mathbf{Z}$, $<\bar{0}>\subset<\bar{8}>\subset<\bar{4}>\subset<\bar{2}>\subset \mathbf{Z}/24\mathbf{Z}$; $<\bar{2}>=<\overline{10}>=<\overline{14}>=<\overline{22}>$, $<\bar{3}>=<\bar{9}>=<\overline{15}>=<\overline{21}>$ – максимальные идеалы.

№3. $f: P \to R$ – гомоморфизм, P – поле, R – кольцо. Доказать, что либо f – изоморфизм P на некоторое поле $P_1 \subset R_1$ как подкольцо (вложение), либо $Imf = \{0\}$.

Решение:

$Kerf \lhd P$. Идеалами поля P могут быть только $\{0\}$ и само P.

1) $Kerf = \{0\}$, тогда f – мономорфизм.

$P/\{0\} \cong Imf = P_1$ – поле, $P_1 \subset R$, т.к. $Imf \le R$ то $P_1 \le R$.

2) $Kerf = P$, тогда $Imf = \{0\}$.

№4. Доказать, что $\mathbf{R}[x]/ < x^2 + 1 > \cong < \mathbf{C}, +, \cdot >$.

Решение:

$\varphi: \mathbf{R}[x] \to \mathbf{C}$, $\varphi(f(x)) = f(i)$, где $i^2 = -1$, $\forall f(x) \in \mathbf{R}[x]$.

$\varphi(f(x) + g(x)) = \varphi(F(x)) = f(i) + g(i) = \varphi(f(x)) + \varphi(g(x))$,

$\varphi(f(x) \cdot g(x)) = \varphi(G(x)) = G(i) = f(i) \cdot g(i) = \varphi(f(x)) \cdot \varphi(g(x))$.

φ – гомоморфизм колец.

$\mathrm{Im}\,\varphi = \mathbf{C}$, т.к. для $\forall\ a + bi \in \mathbf{C}\ \ \exists\, b \cdot x + a \mid \varphi(b \cdot x + a) = bi + a$, $a,\ b \in \mathbf{R}$.

φ – эпиморфизм колец.

$Ker\varphi = \{ f(x) \in R[x] \mid f(i) = 0 \}$,

$i \notin \mathbf{R}$, минимальный многочлен (нормированный), корнем которого является i, будет $x^2 + 1$.

$Ker\varphi \lhd \mathbf{R}[x]$ – двусторонний идеал, $Ker\varphi = < h(x) >$, $Ker\varphi = < x^2 + 1 >$.

$h(x)$ выбираем минимальной степени так, чтобы корень $h(x)$ был равен $i \Rightarrow \deg h = 2, \quad h(x) = x^2 + 1$.

По 2-ой теореме о гомоморфизмах колец $\mathbf{R}[x]/ < x^2 + 1 > \cong < \mathbf{C}, +, \cdot >$.

№5. Доказать, что $\mathbf{Z}[x]/ < n > \cong \mathbf{Z}/n\mathbf{Z}[x]$, $n \in \mathbf{N}$.

Решение:

$\varphi: \mathbf{Z}[x] \to \mathbf{Z}/n\mathbf{Z}[x]$, $\varphi(f(x)) = \overline{f(x)}$, коэффициенты приводим по $\mathrm{mod}\, n$.

$< n > = \{ a_0 \cdot x^n + \ldots + a_{m-1} \cdot x + a_m \mid a_i \in \mathbf{Z},\ n \mid a_i,\ i = \overline{0, m} \}$,

$\varphi(f(x) + g(x)) = \varphi(f(x)) + \varphi(g(x))$, $\quad \varphi(f(x) \cdot g(x)) = \varphi(g(x)) \cdot \varphi(g(x))$.

φ – гомоморфизм колец.

Для $\forall\ \overline{f(x)}\ \ \exists\, f(x)$ с такими же коэффициентами в $\mathbf{Z}$, как представители классов вычетов коэффициентов $\Rightarrow$ φ – эпиморфизм колец.

$Ker\varphi = \{ f(x) \in \mathbf{Z}[x] \mid a_i \in n\mathbf{Z} \} = < n >$.

По 2-ой теореме о гомоморфизмах колец $\mathbf{Z}[x]/ < n > \cong \mathbf{Z}/n\mathbf{Z}[x]$.