Домашняя работа №4 Прохоренко И.О. РВ-35

③ а) $x^2 \equiv 10 \bmod 21 \Rightarrow \begin{cases} x^2 \equiv 10 \bmod 3 \\ x^2 \equiv 10 \bmod 7 \end{cases} \Rightarrow \begin{cases} x^2 \equiv 1 \bmod 3 \\ x^2 \equiv 3 \bmod 7 \end{cases} \Rightarrow \varnothing$

$\left(\frac{3}{7}\right) = (-1)^{\frac{3-1}{2}\cdot\frac{7-1}{2}}\left(\frac{7}{3}\right) = -1\cdot\left(\frac{1}{3}\right) = -1 \quad x \in \varnothing$

б) $x^2 \equiv 93 \bmod 371 \Rightarrow \begin{cases} x^2 \equiv 93 \bmod 7 \\ x^2 \equiv 93 \bmod 53 \end{cases} = \begin{cases} x^2 \equiv 2 \bmod 7 \ ① \\ x^2 \equiv 40 \bmod 53 \ ② \end{cases}$

① $x^2 \equiv \overset{a}{2} \bmod \overset{p}{7}$

$p = 7 = 2\cdot 4 + 3, \ k = 1$

$\left(\frac{2}{7}\right) = (-1)^{\frac{7^2-1}{8}} = (-1)^6 = 1$

$a^{\frac{p-1}{2}} \equiv 1 \bmod p$

$2^3 \equiv 1 \bmod 7 \mid \times a = 2$

$2^4 \equiv 2 \bmod 7$

$x^2 \equiv 2^4 \bmod 7 \Rightarrow x = \pm 4 \bmod 7 = \pm 4$

② $x^2 \equiv 40 \bmod 53$

$p = 53 = 8\cdot 6 + 5, \ k = 6$

$\left(\frac{40}{53}\right) = \left(\frac{2\cdot 2^2}{53}\right)\left(\frac{5}{53}\right) = (-1)^{\frac{53^2-1}{8}}\cdot(-1)^{2\cdot 26}\left(\frac{53}{5}\right) =$

$= (-1)^{351}\cdot\left(\frac{3}{5}\right) = -(-1)^{1\cdot 2} = 1$

$40^{26} \equiv 1 \bmod 53$

$40^{13} \bmod 53 = (40^2)^6 \cdot 40 \bmod 53 =$

$= 10^6 \cdot 40 \bmod 53 = 52 \bmod 53 = -1$

$40^{13} \equiv -1 \bmod 53 \mid \times 2^{\frac{p-1}{2}}, \times 40$

$40^{14}\cdot 2^{26} \equiv 40 \bmod 53$

$x^2 \equiv 40^{14}\cdot 2^{26} \bmod 53$

$x = \pm 40^7 \cdot 2^{13} \bmod 53 = \pm 40\cdot(40^2)^3\cdot 2\cdot(2^6)^2 \bmod 53 =$

$= \pm 40\cdot 10^3\cdot 2\cdot 11^2 \bmod 53 = \pm 27$

---

③ $\begin{cases} x = \pm 4 \bmod 7 \\ x = \pm 27 \bmod 53 \end{cases} \quad \begin{cases} x = 4 \bmod 7 \\ x = 27 \bmod 53 \end{cases}$

$M = 371$

$M_1 = 53 \mid N_1 = 53^{-1} \bmod 7 = 4^{-1} \bmod 7 = 2$

$M_2 = 7 \mid N_2 = 7^{-1} \bmod 53 = 38$

$x_1 = (4\cdot 53\cdot 2 + 27\cdot 7\cdot 38) \bmod 371 = (424 + 7182) \bmod 371 = 7606 \bmod 371 = 186$

$x_2 = (424 - 7182) \bmod 371 = -6758 \bmod 371 = 251$

$x_1 = \pm 186$
$x_2 = \pm 251$

$(186^2 - 93) : 371 = 93 \in \mathbb{Z}$ ✓

$(281^2 - 93) : 371 = 226 \in \mathbb{Z}$ ✓

		-7	-1	-1
0	1	-7	8	(-15)

$-15 \bmod 53 = 38 \bmod 53$

6) $x^2 \equiv 102 \bmod 1159 \Rightarrow \begin{cases} x^2 \equiv 102 \bmod 11 = 3 \bmod 11 & ① \\ x^2 \equiv 102 \bmod 109 & ② \end{cases}$

① $x^2 \equiv 3 \bmod 11$

$p = 11 = 4 \cdot 2 + 3,\ k = 2$

$\left(\frac{3}{11}\right) = (-1)^{\frac{11-1}{2}\cdot\frac{3-1}{2}} \left(\frac{11}{3}\right) = -\left(\frac{2}{3}\right) = -(-1)^{\frac{9-1}{8}} = 1$

$3^5 \equiv 1 \bmod 11 \quad | \cdot 3$

$3^6 \equiv 3 \bmod 11$

$x^2 \equiv 3^6 \bmod 11 \Rightarrow x = \pm 3^3 \bmod 11 \equiv \pm 5 \bmod 11$

② $x^2 \equiv 102 \bmod 109$

$p = 109 = 8 \cdot 13 + 5,\ k = 13.$

$\left(\frac{102}{109}\right) = \left(\frac{2}{109}\right)\left(\frac{3}{109}\right)\left(\frac{17}{109}\right) = (-1)^{\frac{109^2-1}{8}} \cdot (-1)^{1\cdot 54}\left(\frac{109}{3}\right) \cdot (-1)^{8\cdot 54}\left(\frac{109}{17}\right) =$ (1485)

$= -\left(\frac{109}{3}\right)\left(\frac{109}{17}\right) = -\left(\frac{1}{3}\right)\cdot\left(\frac{7}{17}\right) =$

$= -\left(\frac{7}{17}\right) = (-1)^{3\cdot 8}\left(\frac{17}{7}\right) = -\left(\frac{3}{7}\right) = -(-1)^{1\cdot 3}\left(\frac{7}{3}\right) =$

$= -\left(-\left(\frac{1}{3}\right)\right) = 1.$

$102^{54} \equiv 1 \bmod 109$

$102^{27} \bmod 109 = \cancel{49^{13} \bmod 109 = 3^7 \bmod 109 =}$

$\cancel{= 2187 \bmod 109 =} = 49^{13} \cdot 102 \bmod 109 =$

$= 3^6 \cdot 49 \cdot 102 \bmod 109 = 102 \cdot 75 \cdot 49 \bmod 109 =$

$= -1 \bmod 109 = -1$

$102^{27} \equiv -1 \bmod 109 \quad \begin{vmatrix} \cdot 2^{54} \\ \cdot 102 \end{vmatrix}$

$102^{28} \cdot 2^{54} \equiv 102 \bmod 109$

$X^2 = 102^{28} \cdot 2^{54} \bmod 109 \Rightarrow X = \pm 102^{14} \cdot 2^{27} \bmod 109 =$

$= \cancel{\pm 49^7 \cdot 14^4 \bmod 109 = \pm 3^3 \cdot 43 \cdot 87^2 \bmod 109 = 81 \cdot 43 \cdot 48 \bmod 109 =}$

$= \pm 49^7 \cdot 76^3 \bmod 109 = \pm 87 \cdot 89 \cdot 33 \bmod 109 =$

$= \pm 59 \bmod 109.$

③ $\begin{cases} x = \pm 5 \bmod 11 \\ x = \pm 59 \bmod 109 \end{cases} \quad \begin{cases} x = 5 \bmod 11 \\ x = 59 \bmod 109 \end{cases}$

$M = 1199$

$M_1 = 109 \quad N_1 = 109^{-1} \bmod 11 = 10^{-1} \bmod 11 = 10 \bmod 11$

$M_2 = 11 \quad N_2 = 11^{-1} \bmod 109 = 10 \bmod 109$

$x_1 = (5 \cdot 109 \cdot 10 + 59 \cdot 11 \cdot 10) \bmod 1199 =$

$= (5450 + 6490) \bmod 1199 = 11940 \bmod 1199 =$

$= (1149)$

$x_2 = (5450 - 6490) \bmod 1199 = -1040 \bmod 1199 =$

$= (159)$

$x_1 = \pm 1149 \quad (1149^2 - 102) : 1199 = 1101 \in \mathbb{Z}$ ✓

$x_2 = \pm 159 \quad (159^2 - 102) : 1199 = 21 \in \mathbb{Z}$ ✓

② а) $\langle \mathbb{Z}, * \rangle$, $a*b = a^2b$

асоціативність: $(a*b)*c = (a^2b)*c = a^4b^2c$ # - не є асоціативною.
$a*(b*c) = a*(b^2c) = a^2b^2c$

Не утворює

б) $\langle \mathbb{N}, * \rangle$, $a*b = 2ab$

асоціативність: $(a*b)*c = (2ab)*c = 4abc$
$a*(b*c) = a*(2bc) = 4abc$ // - є асоціативною

нейтральний елемент: $a*e = 2ae$ - не існує

не утворює моноїд, утворює напівгрупу

в) $\langle \mathbb{Q}, * \rangle$, $a*b = \frac{a+b}{2}$

асоціативність: $(a*b)*c = \left(\frac{a+b}{2}\right)*c = \frac{\frac{a+b}{2}+c}{2} = \frac{a+b+2c}{4}$
$a*(b*c) = a*\left(\frac{b+c}{2}\right) = \frac{a+\frac{b+c}{2}}{2} = \frac{2a+b+c}{4}$ # - не є асоціативною

не утворює.

г) $\langle \mathbb{N}_0, * \rangle$, $a*b = |a-b|$

асоціативність: $(a*b)*c = (|a-b|)*c = |\,|a-b|-c\,|$ # - не є асоціативною
$a*(b*c) = a*(|b-c|) = |a-|b-c||$

не утворює

③ а) $\langle 2\mathbb{Z}, + \rangle$

$(a+b)+c = a+b+c$ // - асоціативна
$a+(b+c) = a+b+c$

$\exists e \in 2\mathbb{Z}, \forall a \in 2\mathbb{Z}: e+a = a+e = a$, при $e=0$ виконується

$\forall g \in 2\mathbb{Z}, \exists g^{-1} \in 2\mathbb{Z}: g+g^{-1} = g^{-1}+g = e$ - виконується (наприклад: $2+(-2) = -2+2 = 0$.)
$g^{-1} = -g$

$a, b \in 2\mathbb{Z}: a+b = b+a$ - виконується.

Дана алгебраїчна система утворює абелеву групу.

б) $\langle \mathbb{Q}, * \rangle$, $a*b = 2ab$

$(a*b)*c = (2ab)*c = 4abc$ - асоціативність виконується
$a*(b*c) = a*(2bc) = 4abc$

$\exists e \in \mathbb{Q}, \forall a \in \mathbb{Q}: a*e = e*a = a$, при $e = \frac{1}{2}$ виконується

$\forall g \in \mathbb{Q}, \exists g^{-1} \in \mathbb{Q}: g*g^{-1} = g^{-1}*g = e$, при $g^{-1} = \frac{1}{4g}$ - виконується.

$a, b \in \mathbb{Q}: a*b = b*a$
$2ab = 2ba$

Утворює абелеву групу

в) $\langle \{1\}, \cdot \rangle$

$(1\cdot 1)\cdot 1 = 1\cdot(1\cdot 1)$ – выполняется

$1\cdot 1 = 1\cdot 1 = 1$ – выполняется $e=1$

$1\cdot 1 = 1\cdot 1 = 1$ – выполняется

a^{-1} a^{-1} e

$1\cdot 1 = 1\cdot 1$ – выполняется

утворює абелеву групу

г) $\langle \{z \in \mathbb{C} \mid |z| > 1\}, \cdot \rangle$

$(a\cdot b)c = ((a_x+a_y i)(b_x+b_y i))\cdot(c_x+c_y i) = (a_x+a_y i)(b_x+b_y i)(c_x+c_y i)$ // – асоціативна

$a\cdot(b\cdot c) = (a_x+a_y i)\cdot((b_x+b_y i)(c_x+c_y i)) = (a_x+a_y i)(b_x+b_y i)(c_x+c_y i)$

$\exists e \in \{z\in\mathbb{C} \mid |z|>1\}$: $\forall a : a\cdot e = e\cdot a = a$, при $e = 1+0i$ – не виконується, оскільки $|e|=1$

утворює напівгрупу

д) Нехай M – матриці вигляду $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$, $a,b,c \in \mathbb{R}$

$\langle M, \cdot \rangle$

$\forall A,B,C \in M$

$(AB)C = A(BC)$ – виконується

$\exists E \in M$, $\forall A \in M$: $A\cdot E = E\cdot A = A$, при $E = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, E – нейтральна відносно операції множення.

$\forall A \in M$ $\exists A^{-1} \in M$: $A\cdot A^{-1} = A^{-1}\cdot A = E$

$A = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$, $A^{-1} = \frac{1}{|A|}\begin{bmatrix} A_{11} & A_{21} \\ A_{12} & A_{22} \end{bmatrix} = \frac{1}{ac}\begin{bmatrix} c & -b \\ 0 & a \end{bmatrix} = \begin{bmatrix} \frac{1}{a} & \frac{-b}{ac} \\ 0 & \frac{1}{c} \end{bmatrix}$

$A\cdot A^{-1} = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\cdot\begin{pmatrix} \frac{1}{a} & \frac{-b}{ac} \\ 0 & \frac{1}{c} \end{pmatrix} = \begin{pmatrix} \frac{a}{a}+b\cdot 0 & -\frac{ab}{ac}+\frac{b}{c} \\ 0\cdot\frac{1}{a}+0 & -\frac{bc}{ac}+\frac{c}{c} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$\forall A,B \in M$ $A\cdot B = B\cdot A$

$A = \begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix}$, $B = \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix}$

$A\cdot B = \begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} = \begin{pmatrix} a_1a_2+b_1\cdot 0 & a_1b_2+b_1c_2 \\ 0a_2+c_1\cdot 0 & 0b_2+c_1c_2 \end{pmatrix}$

$B\cdot A = \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix}\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix} = \begin{pmatrix} a_2a_1+b_2\cdot 0 & a_2b_1+b_2c_1 \\ 0a_1+c_2\cdot 0 & 0b_1+c_2c_1 \end{pmatrix}$

// не є комутативною

утворює групу

$a * b = ab \bmod m$

④ $\mathbb{Z}_9 \setminus \{0\} = \{1,2,3,4,5,6,7,8\}$

a)

*	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	4	6	8	1	3	5	7
3	3	6	0	3	6	0	3	6
4	4	8	3	7	2	6	1	5
5	5	1	6	2	7	3	8	4
6	6	3	0	6	3	0	6	3
7	7	5	3	1	8	6	4	2
8	8	7	6	5	4	3	2	1

$3 \cdot 3 \bmod 9 = 0$
$3 \cdot 6 \bmod 9 = 0$
$6 \cdot 3 \bmod 9 = 0$
$6 \cdot 6 \bmod 9 = 0$
$\Rightarrow$ nie je grupa

b) $\mathbb{Z}_{11} \setminus \{0\} = \{1,2,3,4,5,6,7,8,9,10\}$

*	1	2	3	4	5	6	7	8	9	10	a^{-1}	ord a
1	1	2	3	4	5	6	7	8	9	10	1	1
2	2	4	6	8	10	1	3	5	7	9	6	10
3	3	6	9	1	4	7	10	2	5	8	4	5
4	4	8	1	5	9	2	6	10	3	7	3	5
5	5	10	4	9	3	8	2	7	1	6	9	5
6	6	1	7	2	8	3	9	4	10	5	2	10
7	7	3	10	6	2	9	5	1	8	4	8	10
8	8	5	2	10	7	4	1	9	6	3	7	10
9	9	7	5	3	1	10	8	6	4	2	5	5
10	10	9	8	7	6	5	4	3	2	1	10	2

$1^1 = 1 \bmod 11$
$2^{10} = 1024 = 1 \bmod 11$
$3^5 = 243 = 1 \bmod 11$
$4^5 = 2^{10} = 1 \bmod 11$
$5^5 = 3125 = 1 \bmod 11$
$6^{10} = 1 \bmod 11$
$7^{10} = 1 \bmod 11$
$8^{10} = 1 \bmod 11$
$9^5 = 1 \bmod 11$
$10^2 = 100 = 1 \bmod 11$

m. Lagrange vyhovuje

$(a \cdot b) \cdot c = abc$
$a \cdot (b \cdot c) = abc$ – ✓

$\exists e \in \mathbb{Z}_{11} \setminus \{0\} : a \cdot e = e \cdot a = a$, napr. $e = 1$. – ✓

$\exists a^{-1} \in \mathbb{Z}_{11} \setminus \{0\} \; \forall a \in \mathbb{Z}_{11} \setminus \{0\} : a \cdot a^{-1} = a^{-1} \cdot a = e$ – ✓

$2 \cdot 6 \bmod 11 = 1$

$\forall a, b \in \mathbb{Z}_{11} \setminus \{0\} : a \cdot b = b \cdot a$ – ✓

$2 \cdot 3 \bmod 11 = 6$
$3 \cdot 2 \bmod 11 = 6$

vytvorí abelovskú grupu – ✓

c) $\mathbb{Z}_{13} \setminus \{0\} = \{1,2,3,4,5,6,7,8,9,10,11,12\}$

*	1	2	3	4	5	6	7	8	9	10	11	12	a^{-1}	ord a
1	1	2	3	4	5	6	7	8	9	10	11	12	1	1
2	2	4	6	8	10	12	1	3	5	7	9	11	7	12
3	3	6	9	12	2	5	8	11	1	4	7	10	9	3
4	4	8	12	3	7	11	2	6	10	1	5	9	10	6
5	5	10	2	7	12	4	9	1	6	11	3	8	8	4
6	6	12	5	11	4	10	3	9	2	8	1	7	11	12
7	7	1	8	2	9	3	10	4	11	5	12	6	2	12
8	8	3	11	6	1	9	4	12	7	2	10	5	5	4
9	9	5	1	10	6	2	11	7	3	12	8	4	3	3
10	10	7	4	1	11	8	5	2	12	9	6	3	4	6
11	11	9	7	5	3	1	12	10	8	6	4	2	6	12
12	12	11	10	9	8	7	6	5	4	3	2	1	12	2

$1^1 = 1 \bmod 13$
$2^{12} = 1036 = 1 \bmod 13$
$3^3 = 27 = 1 \bmod 13$
$4^6 = 2^{12} = 1 \bmod 13$
$5^4 = 1 \bmod 13$
$6^{12} = 2^{12} 3^{12} = 1 \bmod 13$
$7^{12} = 1 \bmod 13$
$8^4 = 2^{12} = 1 \bmod 13$
$9^3 = 729 = 1 \bmod 13$
$10^6 = 1 \bmod 13$
$11^{12} = 1 \bmod 13$
$12^2 = 144 = 1 \bmod 13$

m. Lagrange vyhovuje.
asoc. vyhovuje
$e = 1$
$a * a^{-1} = 1 \bmod 13$
komut. vyhovuje.
$\Rightarrow$ vytvorí abelovskú grupu

г) $Z_{14} \setminus \{0\} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13\}$

$2 \cdot 7 \bmod 14 = 0 \quad - \quad 0 \notin Z_{14} \setminus \{0\}$

не утворює групу

(5.) $X = \{a, b\}$ $B = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$

$\langle X, \cup \rangle$

$\cup$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a, b\}$
$\emptyset$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a, b\}$
$\{a\}$	$\{a\}$	$\{a\}$	$\{a, b\}$	$\{a, b\}$
$\{b\}$	$\{b\}$	$\{a, b\}$	$\{b\}$	$\{a, b\}$
$\{a, b\}$	$\{a, b\}$	$\{a, b\}$	$\{a, b\}$	$\{a, b\}$