Домашна работа 1, №45342, група 3, Информатика

Иво Стратев

7 април 2017 г.

Задача 1.

$$\left|\begin{array}{ll} 35x + 24 \equiv 0 \pmod{17} \\ 23x + 47 \equiv 0 \pmod{38} \end{array}\right.$$

$35x + 24 \equiv 0 \pmod{17} \iff 35x + 24 = 17k,\ k \in \mathbb{Z}$

$x = \frac{17k-24}{35} = m,\ m \in \mathbb{Z}$

$k = \frac{35m+24}{17} = 2m + 1 + \frac{m+7}{17}$

$\frac{m+7}{17} = t,\ t \in \mathbb{Z}$

$m = 17t - 7$

$x = m = 17t - 7 \implies x \equiv -7 \pmod{17}$

$23x + 47 \equiv 0 \pmod{38} \iff 23x + 47 = 38h,\ h \in \mathbb{Z}$

$x = \frac{38h-47}{23} = h - 2 + \frac{15h-1}{23}$

$\frac{15h-1}{23} = t,\ t \in \mathbb{Z}$

$h = \frac{23t+1}{15} = t + \frac{8t+1}{15}$

$\frac{8t+1}{15} = u,\ u \in \mathbb{Z}$

$t = \frac{15u-1}{8} = u + \frac{7u-1}{8}$

$\frac{7u-1}{8} = r,\ r \in \mathbb{Z}$

$u = \frac{8r+1}{7} = r + \frac{r+1}{7}$

$\frac{r+1}{7} = z,\ z \in \mathbb{Z}$

$r = 7z - 1$

$u = 7z - 1 + z = 8z - 1$

$t = 8z - 1 + 7z - 1 = 15z - 2$

$h = 15z - 2 + 8z - 1 = 23z - 3$

$x = 23z - 3 - 2 + 15z - 2 = 38z - 7 \implies x \equiv -7 \pmod{38}$

Тв. 1.

$a, b \in \mathbb{Z},\ n, m \in \mathbb{N}\ a \equiv b \pmod{n}, a \equiv b \pmod{m} \implies a \equiv b \pmod{[m, n]}$

Док-во.

$m|[m, n], n|[m, n],\ \forall k \in \mathbb{Z};\ m|k,\ n|k \implies [m, n]|k$

$a \equiv b \pmod{n} \implies n|(a - b)$

$a \equiv b \pmod{m} \implies m|(a - b)$

$\implies [m, n]|(a - b) \implies a \equiv b \pmod{[m, n]} \quad \square$

$$\left| \begin{array}{ll} x \equiv -7 & \pmod{17} \\ x \equiv -7 & \pmod{38} \end{array} \right. \implies x \equiv -7 \pmod{[17, 38]}$$

$38 = 2.17 + 4$

$17 = 4.4 + 1$

$4 = 1.4 + 0 \implies (38, 17) = 1 \implies$

$[38, 17] = \frac{38.17}{1} = 646 \implies x \equiv -7 \pmod{646}$

Отговор: $x \equiv -7 \pmod{646}$

Задача 2.

$437^{101} + 403^{201} \equiv\ ? \pmod{1000}$

$1000 = 125.8 = 2^3.5^3$

$437 = 3.125 + 62$

$125 = 2.62 + 1$

$62 = 1.62 + 0 \implies (437, 125) = (437, 5^3) = 1$

$437 = 54.8 + 5$

$8 = 1.5 + 3$

$5 = 1.3 + 2$

$3 = 1.2 + 1$

$2 = 1.1 + 0 \implies (437, 8) = (437, 2^3) = 1$

Тв. 2.

$n, k \in \mathbb{N}\ \varphi(n^k) = n^k - n^{k-1}$

Док-во.

$D = [0, \dots, n^k - 1] \subset \mathbb{N} \implies |D| = n^k$

$D = \{mn + r \mid m, r \in \mathbb{N} \cup \{0\},\ 0 \leq r < n,\ 0 \leq mn + r < n^k\}$

$M = \{mn \mid m \in \mathbb{N} \cup \{0\},\ 0 \leq mn < n^k\} \implies |M| = \frac{|D|}{n} = \frac{n^k}{n} = n^{k-1}$

$P = \{mn + r \mid m, r \in \mathbb{N} \cup \{0\},\ 1 \leq r < n,\ 0 \leq mn + r < n^k\} \implies$

$P = D \backslash M \implies |P| = |D \backslash M| \implies = |D| - |M| = n^k - n^{k-1}$

$\varphi(n^k) = |P| = n^k - n^{k-1} \quad \square$

$\implies$ От Th на Ойлер-Ферма

$437^{\varphi(2^3)} \equiv 1 \pmod 8 \implies 437^4 \equiv 1 \pmod 8$

$437^{\varphi(5^3)} \equiv 1 \pmod{125} \implies 437^{100} \equiv 1 \pmod{125}$

Тв. 3.

$a, b \in \mathbb{Z},\ m, n \in \mathbb{N}\ a \equiv b \pmod m \implies a^n \equiv b^n \pmod m$

Док-во.

$a \equiv b \pmod m \implies m|(a - b) \iff \left| \begin{array}{l} a = a_1.m + r \\ b = b_1.m + r \end{array} \right. \quad a_1, b_1, r \in \mathbb{Z};\ 0 \leq r < |m|$

$\implies a - b = a_1.m + r - (b_1.m + r) = (a_1 - b_1)m + (r - r) = (a_1 - b_1)m$

$$a^n = (r + a_1.m)^n = \sum_{k=0}^{n} \binom{n}{k} r^{n-k} (a_1.m)^k$$

$$b^n = (r + b_1.m)^n = \sum_{k=0}^{n} \binom{n}{k} r^{n-k} (b_1.m)^k$$

$$a^n - b^n = \sum_{k=0}^{n} \binom{n}{k} r^{n-k}.m^k.(a_1^k - b_1^k) =$$

$$= \binom{n}{0} r^n.m^0.(a_1^0 - b_1^0) + \sum_{k=1}^{n} \binom{n}{k} r^{n-k}.m^k.(a_1^k - b_1^k) =$$

$$= r^k - r^k + \sum_{k=1}^{n} \binom{n}{k} r^{n-k}.m^k.(a_1^k - b_1^k) =$$

$$= \sum_{k=1}^{n} \binom{n}{k} r^{n-k}.m^k.(a_1^k - b_1^k) \implies$$

$m|(a^n - b^n) \implies a^n \equiv b^n \pmod{m} \quad \square$

$\implies (437^4)^{25} \equiv 1^{25} \pmod{8} \implies 437^{100} \equiv 1 \pmod{8}$

$\implies 437^{100} \equiv 1 \pmod{[8, 125]} \implies 437^{100} \equiv 1 \pmod{1000}$

Тв. 4.

$a, b, z \in \mathbb{Z},\ m \in \mathbb{N};\ a \equiv b \pmod{m} \implies za \equiv zb \pmod{m}$

Док-во.

$a \equiv b \pmod{m} \implies m|(a - b) \implies$

$m|z(a - b) \implies m|(za - zb) \implies za \equiv zb \pmod{m} \quad \square$

$\implies 437.437^{100} \equiv 437.1 \pmod{1000} \implies 437^{101} \equiv 437 \pmod{1000}$

$403 = 3.125 + 28$

$125 = 4.28 + 13$

$28 = 2.13 + 2$

$13 = 6.2 + 1$

$2 = 1.2 + 0 \implies (403, 125) = (403, 5^3) = 1$

$403 = 50.8 + 3$

$8 = 2.3 + 2$

$3 = 1.2 + 1$

$2 = 1.1 + 0 \implies (437, 8) = (437, 2^3) = 1$

$403^{\varphi(2^3)} \equiv 1 \pmod 8 \implies 403^4 \equiv 1 \pmod 8$

$403^{\varphi(5^3)} \equiv 1 \pmod{125} \implies 403^{100} \equiv 1 \pmod{125}$

$(403^4)^{50} \equiv 1^{50} \pmod 8 \implies 403^{200} \equiv 1 \pmod 8$

$(403^{100})^2 \equiv 1^2 \pmod{125} \implies 403^{200} \equiv 1 \pmod{125}$

$403^{200} \equiv 1 \pmod{[8, 125]} \implies 437^{200} \equiv 1 \pmod{1000}$

$403.403^{200} \equiv 403.1 \pmod{1000} \implies 403^{201} \equiv 403 \pmod{1000}$

Тв. 5.

$a, b, c, d \in \mathbb{Z},\ m \in \mathbb{N} \left| \begin{array}{l} a \equiv b \pmod m \\ c \equiv d \pmod m \end{array} \right. \implies (a + c) \equiv (b + d) \pmod m$

Док-во.

$a \equiv b \pmod m \implies m|(a - b) \implies a - b = km,\ k \in \mathbb{Z}$

$c \equiv d \pmod m \implies m|(c - d) \implies c - d = nm,\ n \in \mathbb{Z}$

$(a + c) - (b + d) = (a - b) + (c - d) = km - nm = (k - n)m \implies$

$m|[(a + c) - (b + d)] \implies (a + c) \equiv (b + d) \pmod m \quad \square$

$\implies 437^{101} + 403^{201} \equiv 437 + 403 \pmod{1000} \implies$

$437^{101} + 403^{201} \equiv 840 \pmod{1000}$

Отговор: 840

Задача 3.

$(J, \circ_J),\ (C, \circ_C)$

$J \times C = \{(j, c) \mid j \in J,\ c \in C\}$

$(j_1, c_1) \circ (j_2, c_2) = (j_1 \circ_J j_2, c_1 \circ_C c_2)$

$\forall (j_1, j_2), (c_1, c_2) \in J \times C\ (j_1, c_1) \circ (j_2, c_2) = (j_1 \circ_J j_2, c_1 \circ_C c_2)$

$j_1 \circ_J j_2 \in J\ (\quad j_1, j_2 \in J,\ (J, \circ_J) \quad)$

$c_1 \circ_C c_2 \in C\ (\quad c_1, c_2 \in C,\ (C, \circ_C) \quad)$

$$\Longrightarrow \ \forall (j_1, c_1), (j_2, c_2) \in J \times C \implies (j_1, c_1) \circ (j_2, c_2) \in J \times C$$

а)

$\forall (j_1, c_1), (j_2, c_2), (j_3, c_3) \in J \times C$
$((j_1, c_1) \circ (j_2, c_2)) \circ (j_3, c_3) = (j_1 \circ_J j_2, c_1 \circ_C c_2) \circ (j_3, c_3) =$

$= ((j_1 \circ_J j_2) \circ_J j_3, (c_1 \circ_C c_2) \circ_C c_3) = (j_1 \circ_J (j_2 \circ_J j_3), c_1 \circ_C (c_2 \circ_C c_3)) =$

$= (j_1, c_1) \circ (j_2 \circ_J j_3, c_2 \circ_C c_3) = (j_1, c_1) \circ ((j_2, c_2) \circ (j_3, c_3))$

$\forall (j, c) \in J \times C \ (e_G, e_C) \circ (j, c) = (e_J \circ_J j, e_C \circ_C c) = (j, c) =$

$= (j \circ_J e_J, c \circ_C e_C) = (e_J, e_C) \circ (j, c) \implies e = (e_G, e_C)$

$\forall (j, c) \ (j, c) \circ (j^{-1}, c^{-1}) = (j \circ_J j^{-1}, c \circ_C c^{-1}) = (e_J, e_C) =$

$= (j^{-1} \circ_J j, c^{-1} \circ_C c) = (j^{-1}, c^{-1}) \circ (j, c) \implies$

$\forall (j, c) \in J \times C \ (j, c)^{-1} = (j^{-1}, c^{-1})$

$\Longrightarrow \ (J \times C, \circ)$

$|J| < \infty, \ |C| < \infty \implies |J \times C| = |J||C|$

б)

Тв. 6.

$|J| < \infty, \ |C| < \infty, \ J, C -$ циклични $\implies J \times C$ е циклична $\iff (|J|, |C|) = 1$

Док-во.

$|J| < \infty, \ |J| = n \in \mathbb{N}, \ J -$ циклична $\implies$

$\exists j \in J; \ |j| = n, \ J = \langle j \rangle = \{j^k \mid k \in \mathbb{Z}\}$

$|C| < \infty, \ |C| = m \in \mathbb{N}, \ C -$ циклична $\implies$

$\exists c \in C; \ |c| = m, \ C = \langle c \rangle = \{c^k \mid k \in \mathbb{Z}\}$

$a, b \in \mathbb{Z} \ (j^a, c^b) \in J \times C, k \in \mathbb{N} \quad (j^a, c^b)^k = \underbrace{(j^a, c^b) \circ (j^a, c^b) \circ \cdots \circ (j^a, c^b)}_{k} =$

$= (\underbrace{j^a \circ_J j^a \circ_J \cdots \circ_J j^a}_{k}, \underbrace{c^b \circ_C c^b \circ_C \cdots \circ_C c^b}_{k}) = ((j^a)^k, (c^b)^k) = (j^{ak}, c^{bk})$

$(j^a, c^b)^{-k} = \underbrace{(j^a, c^b)^{-1} \circ (j^a, c^b)^{-1} \circ \cdots \circ (j^a, c^b)^{-1}}_{k} =$

$= \underbrace{(j^{-a}, c^{-b}) \circ (j^{-a}, c^{-b}) \circ \cdots \circ (j^{-a}, c^{-b})}_{k} =$

$= (\underbrace{j^{-a} \circ_J j^{-a} \circ_J \cdots \circ_J j^{-a}}_{k}, \underbrace{c^{-b} \circ_C c^{-b} \circ_C \cdots \circ_C c^{-b}}_{k}) =$

$= ((j^{-a})^k, (c^{-b})^k) = (j^{-ak}, c^{-bk})$

$\Longrightarrow \ \forall r, t \in Z \ ((j^a, c^b)^r)^t = ((j^{ar}), (c^{ar}))^t = ((j^{ar})^t, (c^{ar})^t) = (j^{art}, c^{brt}) =$

$= ((j^{at})^r, (c^{bt})^r) = ((j^{at}), (c^{bt}))^r = ((j^a, c^b)^t)^r = ((j^{rt})^a, (c^{rt})^b)$

$\Longrightarrow \ \forall r, t \in Z \ (j^a, c^b)^r \circ (j^a, c^b)^t = (j^a, c^b)^{r+t}$

$(\Rightarrow)$

$J \times C$ е циклична $\Longrightarrow \ \exists y, w \in \mathbb{Z}; \ (j^y, c^w) \in J \times C;$

$|(j^y, c^w)| = |J \times C| = |J||C|, \ J \times C = \langle (j^y, c^w) \rangle$

$$d = (n, m) \Longrightarrow \left| \begin{array}{l} d|n \Longrightarrow 1 \le d \le n \\ d|m \Longrightarrow 1 \le d \le m \end{array} \right. \Longrightarrow$$

$$1 \le d \le min\{m, n\} \Longrightarrow \left| \begin{array}{l} n = n_1 d, \ n_1 \in \mathbb{N} \\ m = m_1 d, \ n_2 \in \mathbb{N} \end{array} \right.$$

Доп. $1 < d \le min\{m, n\} \Longrightarrow$

$[m, n] = \frac{mn}{d} = \frac{m_1 d n_1 d}{d} = m_1 d n_1 \Longrightarrow [m, n] < (m, n)$

$u, v \in \mathbb{Z}, \ (j^u, c^v)^{[m,n]} = ((j^u)^{[m,n]}, (c^v)^{[m,n]}) = (j^{u[m,n]}, c^{v[m,n]}) = (j^{u m_1 d n_1}, c^{v m_1 d n_1})$

$= (j^{n u m_1}, c^{m v n_1}) = ((j^n)^{u m_1}, (c^m)^{v n_1}) = (e_J^{u m_1}, e_C^{v n_1}) = (e_J, e_C) = e \Longrightarrow$

$\forall s, z \in \mathbb{Z} \ |(j^s, c^z)| \le [m, n] < (m, n) \Longrightarrow \lightning \Longrightarrow$

$d = (m, n) = (|J|, |C|) = 1$

$(\Leftarrow)$

$(m, n) = 1 \Longrightarrow [m, n] = \frac{mn}{(m,n)} = \frac{mn}{1} = mn$

$(j, c)^n = (j^n, c^n) = (e_J, c^n), \ (m, n) = 1 \Longrightarrow n = q_1 m + 1, \ q_1 \in \mathbb{Z} \Longrightarrow$

$c^n = c^{q_1 m + 1} = c^{q_1 m} c = (c^n) q_1 c = e_C^{q_1} c = e_C c = c \Longrightarrow$

$(e_J, c^n) = (e_J, c),\ (e_J, c)^m = (e_J^m, c^m) = (e_J, e_C) = e$

$(m, n) = 1 \implies mn = min\{q \in \mathbb{N} \mid (j, c)^q = e\} \implies$

$|(j, c)| = |J \times C|$

$h, l \in \mathbb{N}; 0 \leq h < l < mn$

Доп. $(j, c)^h = (j, c)^l \mid (j, c)^{-h} \implies e = (j, c)^{l-h} \implies$

$0 < l - h < mn \implies \lightning \implies (j, c)^h \neq (j, c)^l$

$x \in \mathbb{Z}\ x = q(mn) + x_0,\ q, x_0 \in \mathbb{Z},\ ; 0 \leq x_0 < mn \implies$

$(j, c)^x = (j, c)^{q(mn)+x_0} = (j, c)^{q(mn)}(j, c)^{x_0} =$

$= ((j, c)^{mn})^q (j, c)^{x_0} = e^q (j, c)^{x_0} = (j, c)^{x_0} = (j^{x_0}, c^{x_0})$

$$\left| \begin{array}{l} x_0 = q_j n + x_j,\ q_j, x_j \in \mathbb{Z};\ 0 \leq x_j < n \\ x_0 = q_c m + x_c,\ q_c, x_c \in \mathbb{Z};\ 0 \leq x_c < m \end{array} \right. \implies$$

$(j^{x_0}, c^{x_0}) = (j^{q_j n + x_j}, c^{q_c m + x_c}) = (j^{q_j n} j^{x_j}, c^{q_c m} j^{x_c}) =$

$= ((j^n)^{q_j} j^{x_j}, (j^m)^{q_c} c^{x_c}) = (e_J^{q_j} j^{x_j}, e_C^{q_c} c^{x_c}) = (e_J j^{x_j}, e_C c^{x_c}) =$

$$= (j^{x_j}, c^{x_c}) \in J \times C \implies \left| \begin{array}{ll} x \equiv x_j & \pmod{n} \\ x \equiv x_c & \pmod{m} \end{array} \right.$$

$\implies J \times C = \langle (j, c) \rangle = \{(j, c)^{k_g} \mid k_g \in \mathbb{Z}\}$

$\implies (J, \circ_J), (C, \circ_C);\ J = \langle j \rangle, C = \langle c \rangle \implies$

$(J \times C, \circ) = \langle (j, c) \rangle \iff (|J|, |C|) = 1 \quad \square$

Тв. 7.

$\mathbb{C}_m \times \mathbb{C}_n \cong \mathbb{C}_{mn} \iff (m, n) = 1$

Док-во.

$\mathbb{C}_m = \langle w_1 \rangle = \{1, w_1, w_1^2, \ldots, w_1^{m-1}\},\ |\mathbb{C}_m| = m$

$\mathbb{C}_n = \langle w_1 \rangle = \{1, w_1, w_1^2, \ldots, w_1^{n-1}\},\ |\mathbb{C}_n| = n$

$(m, n) = 1 \iff \mathbb{C}_m \times \mathbb{C}_n = \langle w_1, w_1 \rangle =$

$= \{(1, 1), (w_1, w_1), (w_1, w_1)^2, \ldots, (w_1, w_1)^{mn-1}\},\ |\mathbb{C}_m \times \mathbb{C}_n| = mn$

$\mathbb{C}_{mn} = \langle w_1 \rangle = \{1, w_1, w_1^2, \ldots, w_1^{mn-1}\},\ |\mathbb{C}_{mn}| = mn$

$$\begin{array}{rcl} \varphi: \ \mathbb{C}_{mn} & \to & \mathbb{C}_m \times \mathbb{C}_n \\ w_1^k & \mapsto & (w_1, w_1)^k \end{array} \qquad \begin{array}{rcl} \varphi^*: \ \mathbb{C}_m \times \mathbb{C}_n & \to & \mathbb{C}_{mn} \\ (w_1, w_1)^k & \mapsto & w_1^k \end{array}$$

$\varphi(w_1^k) = (w_1, w_1)^k,\ k = 0, 1, \ldots, mn-1$

$\varphi^*((w_1, w_1)^k) = w_1^k,\ k = 0, 1, \ldots, mn-1$

$(\varphi \circ \varphi^*)((w_1, w_1)^k) = \varphi(\varphi^*((w_1, w_1)^k) = \varphi(w_1^k) = (w_1, w_1)^k \implies \varphi \circ \varphi^* = id$

$(\varphi^* \circ \varphi)(w_1^k) = \varphi^*(\varphi(w_1^k)) = \varphi^*((w_1, w_1)^k) = w_1^k \implies \varphi^* \circ \varphi = id$

$\implies \varphi^* = \varphi^{-1} \implies \varphi$ е биекция

$i, j, r \in \mathbb{N};\ 0 \leq i, j, r < mn,\ i + j \equiv r \pmod{mn}$

$\varphi(w_1^i w_1^j) = \varphi(w_1^{i+j}) = \varphi(w_1^r) = (w_1, w_1)^r =$

$= (w_1, w_1)^{i+j} = (w_1, w_1)^i (w_1, w_1)^j = \varphi(w_1^i)\varphi(w_1^j)$

$\implies \mathbb{C}_m \times \mathbb{C}_n \cong \mathbb{C}_{mn} \iff (m, n) = 1 \quad \square$

в)

$35 = 3.9 + 8$

$9 = 1.8 + 1$
$8 = 8.1 + 0 \implies (35, 9) = 1,\ 35.9 = 315 \implies$

$\mathbb{C}_{35} \times \mathbb{C}_9 \cong \mathbb{C}_{315}$

г)

$63 = 12.5 + 3$

$5 = 1.3 + 2$

$3 = 1.2 + 1$

$2 = 2.1 = 0 \implies (5, 63) = 1,\ 5.63 = 315 \implies$

$\mathbb{C}_5 \times \mathbb{C}_{63} \cong \mathbb{C}_{315} \implies \exists \tau;$

$$\begin{array}{rcl} \tau: \ \mathbb{C}_{315} & \to & \mathbb{C}_5 \times \mathbb{C}_{63} \\ w_1^k & \mapsto & (w_1, w_1)^k \end{array} \qquad \begin{array}{rcl} \tau^{-1}: \ \mathbb{C}_5 \times \mathbb{C}_{63} & \to & \mathbb{C}_{315} \\ (w_1, w_1)^k & \mapsto & w_1^k \end{array}$$

$47 = 6.7 + 3$

$7 = 2.3 + 1$

$3 = 3.1 + 0 \implies (7, 45) = 1,\ 7.45 = 315 \implies$

$\mathbb{C}_7 \times \mathbb{C}_{45} \cong \mathbb{C}_{315} \implies \exists \psi$

$$\begin{array}{rccc} \psi: & \mathbb{C}_{315} & \to & \mathbb{C}_7 \times \mathbb{C}_{45} \\ & w_1^k & \mapsto & (w_1, w_1)^k \end{array} \qquad \begin{array}{rccc} \psi^{-1}: & \mathbb{C}_7 \times \mathbb{C}_{45} & \to & \mathbb{C}_{315} \\ & (w_1, w_1)^k & \mapsto & w_1^k \end{array} \implies$$

$\rho = \psi \circ \tau^{-1} : \mathbb{C}_5 \times \mathbb{C}_{63} \to \mathbb{C}_7 \times \mathbb{C}_{45}$

$\rho((w_1, w_1)^k_{5\times 63}) = (\psi \circ \tau^{-1})((w_1, w_1)^k_{5\times 63}) = \psi(\tau^{-1}((w_1, w_1)^k_{5\times 63})) =$

$= \psi(w_1^k) = (w_1, w_1)^k_{7\times 45} \in \mathbb{C}_7 \times \mathbb{C}_{45},\ k = 0, 1, \dots, mn - 1$

$\rho^{-1} = \tau \circ \psi^{-1} : \mathbb{C}_7 \times \mathbb{C}_{45} \to \mathbb{C}_5 \times \mathbb{C}_{63}$

$\rho((w_1, w_1)^k_{7\times 45}) = (\psi \circ \tau^{-1})((w_1, w_1)^k_{7\times 45}) = \psi(\tau^{-1}((w_1, w_1)^k_{7\times 45})) =$

$= \psi(w_1^k) = (w_1, w_1)^k_{5\times 63} \in \mathbb{C}_5 \times \mathbb{C}_{63},\ k = 0, 1, \dots, mn - 1$

$\rho \circ \rho^{-1} = (\tau \circ \psi^{-1}) \circ (\psi \circ \tau^{-1}) = \tau \circ ((\psi^{-1} \circ \psi) \circ \tau^{-1}) =$

$= \tau \circ (id \circ \tau^{-1}) = \tau \circ \tau^{-1} = id$

$\rho^{-1} \circ \rho = (\psi \circ \tau^{-1}) \circ (\tau \circ \psi^{-1}) = \psi \circ ((\tau^{-1} \circ \tau) \circ \psi^{-1}) =$

$= \psi \circ (id \circ \psi^{-1}) = \psi \circ \psi^{-1} = id \implies \rho$ е биекция

$i, j, r \in \mathbb{N};\ 0 \le i, j, r < mn,\ i + j \equiv r \pmod{mn}$

$\rho((w_1, w_1)^i_{5\times 63}(w_1, w_1)^j_{5\times 63}) = \rho((w_1, w_1)^{i+j}_{5\times 63}) = \rho((w_1, w_1)^r_{5\times 63}) = (w_1, w_1)^r_{7\times 45} =$

$= (w_1, w_1)^{i+j}_{7\times 45} = (w_1, w_1)^i_{7\times 45}(w_1, w_1)^j_{7\times 45} = \rho((w_1, w_1)^i_{5\times 63})\rho((w_1, w_1)^j_{5\times 63})$

$\implies \mathbb{C}_5 \times \mathbb{C}_{63} \cong \mathbb{C}_7 \times \mathbb{C}_{45}$

д)

$JC = \{jc \mid j \in J,\ c \in C\},\ J \triangleleft JC,\ C \triangleleft JC,\ J \cap C = \{1\}$

Тв. 8.

$H, G -$ групи $H \triangleleft G \implies \forall g \in G,\ \forall h \in H\ ghg^{-1} \in H$

Док-во.

$H \triangleleft G \implies \forall g \in G\ gH = Hg \implies$

$h \in H \implies gh \in gH = Hg \implies \exists h^* \in H;\ gh = h^*g \mid g^{-1} \implies$

$ghg^{-1} = h^* \in H \implies \forall g \in G,\ \forall h \in H\ ghg^{-1} \in H \quad \square$

$j \in J, c \in C,\ J \triangleleft JC,\ C \triangleleft JC \implies JC \ni j, c, j^{-1}, c^{-1} \implies$

$jcj^{-1} \in C,\ cj^{-1}c^{-1} \in J \implies jcj^{-1}c^{-1} \in J \cap C = \{1\} \implies$

$jcj^{-1}c^{-1} = jj^{-1}cc^{-1} = 1.1 = 1 \implies jc = cj \implies$

$\forall y \in J, x \in C\ yx = xy$

$$\begin{array}{rccc} \sigma: & J \times C & \to & JC \\ & (j,c) & \mapsto & jc \end{array} \qquad \begin{array}{rccc} \sigma^{-1}: & JC & \to & J \times C \\ & jc & \mapsto & (j,c) \end{array}$$

$(j_1, c_1), (j_2, c_2) \in J \times C \implies$

$\sigma((j_1, c_1) \circ (j_2, c_2)) = \sigma((j_1 j_2, c_1 c_2)) = j_1 j_2 c_1 c_2 =$

$= j_1(j_2 c_1)c_2 = j_1(c_1 j_2)c_2 = (j_1 c_1)(j_2 c_2) = \sigma((j_1, c_1))\sigma((j_2, c_2))$

$\sigma^{-1}(jc) = \{(u, v) \in J \times C \mid \sigma((u, v)) = jc\}$

$\sigma((u, v)) = jc \iff uv = jc \mid u^{-1} \implies$

$v = u^{-1}jc \mid c^{-1} \implies uv = jc \iff vc^{-1} = u^{-1}j = z$

$u, j \in J,\ v, c \in C \implies z \in J \cap C = \{1\} \implies \begin{cases} vc^{-1} = 1 \mid c \implies v = c \\ u^{-1}j = 1 \mid u \implies j = u \end{cases} \implies$

$|\sigma^{-1}(jc)| = |J \cap C| = 1 \implies \sigma$ е инекция и сюрекция $\implies \sigma$ е биекция

$\implies JC \cong J \times C$

Задача 4.

$(G, .), |G| = n \in \mathbb{N}, p$ - просто $\in N,\ p|n$

$M = \{(g_0, g_1, \dots, g_{p-1}) \in G^p \mid g_0.g_1.\dots.g_{p-1} = e_G\}$

a)

$k \in [0, p-1] \subset N,\ g_0, g_1, \dots g_{k-1}, g_{k+1}, \dots, g_{p-1} \in G$

$g_k = (g_0.g_1.\dots.g_{k-1})^{-1}(g_{k+1}.\dots.g_{p-1})^{-1} = (g_{k-1}^{-1}.\dots.g_1^{-1}.g_0^{-1})(g_{p-1}^{-1}.\dots.g_{k+1}^{-1})$

$g_0 {\cdot} g_1 {\cdot} \dots {\cdot} g_{k-1} {\cdot} g_k {\cdot} g_{k+1} {\cdot} \dots {\cdot} g_{p-1} =$

$= g_0 {\cdot} g_1 {\cdot} \dots {\cdot} g_{k-1} g_{k-1}^{-1} {\cdot} \dots {\cdot} g_1^{-1} {\cdot} g_0^{-1} g_{p-1}^{-1} {\cdot} \dots {\cdot} g_{k+1}^{-1} {\cdot} g_{k+1} {\cdot} \dots {\cdot} g_{p-1} =$

$$= \prod_{i=0}^{k-1} g_i \prod_{j=k-1}^{0} g_j^{-1} \prod_{l=p-1}^{k+1} g_l^{-1} \prod_{h=k+1}^{p-1} g_h = \prod_{t=0}^{p-1} g_t = e_G \implies$$

$\forall k \in [0, p-1] \subset N,\ \forall g_0, g_1, \dots g_{k-1}, g_{k+1}, \dots, g_{p-1} \in G \implies$

$$g_k = \prod_{j=k-1}^{0} g_j^{-1} \prod_{l=p-1}^{k+1} g_l^{-1} \implies \prod_{i=0}^{p-1} g_i = e_G \implies$$

$(g_0, g_1, \dots, g_{p-1}) \in M \implies |M| = |G|^{p-1} = n^{p-1}$

б)

$$\begin{array}{rccc} \sigma : & M & \to & G^p \\ & (g_0, g_1, \dots, g_{p-1}) & \mapsto & (g_{p-1}, g_0, g_1, \dots, g_{p-2}) \end{array}$$

$g \in M \implies g = (g_0, g_1, \dots, g_{p-1}),\ g_i \in G,\ i = 0, \dots, p-1$

$g \in M \implies g_0 {\cdot} g_1 {\cdot} \dots {\cdot} g_{p-1} = e_G \mid g_{p-1}^{-1} \implies$

$g_0 {\cdot} g_1 {\cdot} \dots {\cdot} g_{p-2} = g_{p-1}^{-1} \mid g_{p-1} \implies g_{p-1} {\cdot} g_0 {\cdot} g_1 {\cdot} \dots {\cdot} g_{p-2} = e_G \implies$

$(g_{p-1}, g_0, g_1, \dots, g_{p-2}) \in M$

$\sigma(g) = \sigma((g_0, g_1, \dots, g_{p-1})) = (g_{p-1}, g_0, g_1, \dots, g_{p-2}) \implies \sigma : M \to M$

$$\begin{array}{rccc} \upsilon : & M & \to & G^p \\ & (g_0, g_1, \dots, g_{p-1}) & \mapsto & (g_1, g_2, \dots, g_{p-1}, g_0) \end{array}$$

$g_0 {\cdot} g_1 {\cdot} \dots {\cdot} g_{p-1} = e_G \mid g_0^{-1} \implies$

$g_1 {\cdot} \dots {\cdot} g_{p-1} = g_0^{-1} \mid g_0 \implies g_1 {\cdot} g_2 {\cdot} \dots {\cdot} g_{p-1} {\cdot} g_0 = e_G \implies$

$(g_1, g_2, \dots, g_{p-1}, g_0) \in M$

$\upsilon(g) = \upsilon((g_0, g_1, \dots, g_{p-1})) = (g_1, g_2, \dots, g_{p-1}, g_0) \implies \upsilon : M \to M$

$(\sigma \circ \upsilon)(g) = \sigma(\upsilon(g)) = \sigma((g_1, g_2, \dots, g_{p-1}, g_0)) = (g_0, g_1, \dots, g_{p-1}) = g$

$(\upsilon \circ \sigma)(g) = \upsilon(\sigma(g)) = \upsilon(g_{p-1}, g_0, g_1, \dots, g_{p-2})) = (g_0, g_1, \dots, g_{p-1}) = g$

$\implies \upsilon = \sigma^{-1} \implies \sigma$ е биекция от M в M

в)

$H = \langle \sigma \rangle < S_M \implies |H| = |\sigma|$

$g \in M \implies g = (g_0, g_1, \ldots, g_{p-1}),\ g_i \in G,\ i = 0, \ldots, p-1$

$\sigma(g) = \sigma((g_0, g_1, \ldots, g_{p-1})) = (g_{p-1}, g_0, g_1, \ldots, g_{p-2})$

$(\sigma^2)(g) = \sigma(\sigma(g))) = \sigma((g_{p-1}, g_0, g_1, \ldots, g_{p-2})) = (g_{p-2}, g_{p-1}, g_0, g_1, \ldots, g_{p-3})$

$(\sigma^3)(g) = \sigma(\sigma(\sigma(g)))) = \sigma((g_{p-2}, g_{p-1}, g_0, g_1, \ldots, g_{p-3})) = (g_{p-3}, g_{p-2}, g_{p-1}, g_0, g_1, \ldots, g_{p-4})$

$\implies (\sigma^i)(g) = \sigma^i((g_0, g_1, \ldots, g_{p-1})) = (g_{(-i\ mod\ p)}, g_{(1-i\ mod\ p)}, \ldots, g_{(p-1-i\ mod\ p)}) \implies$

$\sigma^i = id \iff -i \equiv 0 \pmod p \implies i = p = min\{q \in \mathbb{N} \mid \sigma^q = id\} \implies$

$(\sigma^p)(g) = id(g) \implies |\sigma| = p \implies |H| = p$

г)

$$\begin{array}{rccc} \varphi: & H \times M & \to & M \\ & (\rho, m) & \mapsto & \rho(m) \end{array}$$

$\forall g \in M \quad \varphi(id, g) = id(g) = g$

$\forall g \in M,\ \forall \sigma^i, \sigma^j,\ i, j \in \mathbb{Z} \quad \varphi(\sigma^i, \varphi(\sigma^j, g)) =$

$= \varphi(\sigma^i, \sigma^j(g)) = \sigma^i(\sigma^j(g)) = (\sigma^i \sigma^j)(g) = \varphi(\sigma^i \sigma^j, g)$

д)

$St((g_0, g_1, \ldots, g_{p-1})) = \{h \in H \mid \varphi(h, (g_0, g_1, \ldots, g_{p-1})) = (g_0, g_1, \ldots, g_{p-1})\}$

$St((g_0, g_1, \ldots, g_{p-1})) = H \iff \forall \sigma^i \neq id \in H,\ i \in \mathbb{Z},\ 0 < i < p$

$\sigma^i((g_0, g_1, \ldots, g_{p-1})) = (g_{(-i\ mod\ p)}, g_{(1-i\ mod\ p)}, \ldots, g_{(p-1-i\ mod\ p)}) =$

$$= (g_0, g_1, \ldots, g_{p-1}) \iff \left| \begin{array}{l} g_0 = g_1 = \cdots = g_{p-1} = g_s \\ \\ g_s^p = e_G \end{array} \right. \iff g_s = e_G \vee |g_s| = p$$

е)

$\forall g \in M\ O(g) = \{\varphi(h, g) \mid h \in H\} \implies O(x) = O(y) \iff x \sim y$

$\forall a, b \in M \ \ a = (a_0, a_1, \ldots a_{p-1}),\ b = (b_0, b_1, \ldots b_{p-1}) \implies$

$a \sim b \iff \{a_0, a_1, \ldots a_{p-1}\} = \{b_0, b_1, \ldots b_{p-1}\}$

$St(g) = \{h \in H \mid \varphi(h, g) = g)\}$

$h_1, h_2 \in H \varphi(h_1, g) = \varphi(h_2, g) \iff h_1(g) = h_2(g) \iff$

$(h_2^{-1}h_1)(g) = g \iff h_2^{-1}h_1 \in St(g) \iff h_1St(g) = h_2St(g) \implies$

$|O(g)| = |H : St(g)| \implies |O(g)|||H|$

$|H| = p \implies |O(g)| = 1 \vee |O(g)| = p \implies$

$|M| = n^{p-1} = s.1 + o.p,\ s, o \in \mathbb{N},\ s \geq 1(\ (e_G, e_G, \ldots, e_G) \in M)\ )$

$p|n \implies p|s \implies$

$\exists S = \{v = (x, x, \ldots, x) \in M \mid |O(v)| = 1,\ x^p = e_G\};\ |S| \geq p \implies$

$\exists Y = \{y \in G \mid y^p = e_G\};\ |Y| \geq p \implies$

$\exists u \in G;\ u \neq e_G,\ u^p = e_G \implies\ |u| = p$