Ladislav Bican
O jistých grupách matic

Časopis pro pěstování matematiky, Vol. 94 (1969), No. 3, 305--313

Persistent URL: http://dml.cz/dmlcz/108600

Časopis pro pěstování matematiky, roč. 94 (1969), Praha

O JISTÝCH GRUPÁCH MATIC

LADISLAV BICAN, Praha

(Došlo 18. ledna 1968)

Práce se zabývá studiem grup matic s jednotkovým determinantem s prvky z okruhu zbytkových tříd modulo n. Je odvozen vzorec pro počet prvků takové grupy a popsána její struktura. Odtud je vidět, že vlastnosti grup matic nad konečným okruhem a nad konečným tělesem jsou zcela odlišné. Zatímco grupy matic nad tělesem jsou „skoro" jednoduché (přesněji: jednoduchá je faktor-grupa podle centra, které je tvořeno skalárními maticemi), jsou grupy matic nad okruhem „skoro" řešitelné (viz věta 5). První polovina práce má pomocný charakter, nezbytně nutný pro stanovení řádů studovaných grup, což spolu s jejich strukturou je popsáno v druhé polovině.

Označení. (k, l) bude v dalším značit největšího společného dělitele čísel k, l. Symbolem $\varphi_n(k)$ označme počet čísel z posloupnosti $1, 2, \ldots, k$ nesoudělných s (n, k), kde n a k jsou přirozená čísla.

Lemma 1. *Pro všechna přirozená n a k platí:*

a) *Je-li* $d = (n, k)$, *je*

$$\varphi_n(k) = \frac{k}{d}\varphi(d)\,, \tag{1}$$

kde φ *je Eulerova funkce.*

b) $\varphi_n(k)$ je *multiplikativní*[1]) *funkce proměnné k.*

c) *Pro k pevné,* $(n_1, n_2) = 1$ *je*

$$\varphi_{n_1}(k)\,\varphi_{n_2}(k) = k\,\varphi_{n_1 n_2}(k)\,. \tag{2}$$

Důkaz. a) Zřejmě jest $(a + rd, d) = (a, d)$. Avšak počet přirozených čísel nesoudělných s d a menších než d je $\varphi(d)$, odkud plyne (1). b) a c) jsou jednoduchými důsledky (1) a vlastností funkce φ.

[1]) Funkce f se nazývá multiplikativní, jestliže $(k_1, k_2) = 1 \Rightarrow f(k_1, k_2) = f(k_1)\,.\,f(k_2)$.

Důsledek. *Pro n, α, k přirozená, p prvočíslo platí*

$$p \mid n \Rightarrow \varphi_n(p^\alpha) = p^\alpha - p^{\alpha-1}, \tag{3}$$

$$p \nmid n \Rightarrow \varphi_n(p^\alpha) = p^\alpha, \tag{4}$$

$$p \mid k \Rightarrow \varphi_{p^\alpha}(k) = k(1 - 1/p), \tag{5}$$

$$p \nmid k \Rightarrow \varphi_{p^\alpha}(k) = k. \tag{6}$$

Lemma 2. *Nechť $n_1 \mid k_1$, $n_2 \mid k_2$, $(k_1, k_2) = 1$. Pak*

$$\varphi_{n_1}(k_1)\,\varphi_{n_2}(k_2) = \varphi_{n_1 n_2}(k_1 k_2). \tag{7}$$

Důkaz. Zřejmě $(n_1, n_2) = 1$ a $(n_1 n_2, k_1 k_2) = n_1 n_2$, takže

$$\varphi_{n_1 n_2}(k_1 k_2) = \frac{k_1 k_2}{n_1 n_2}\varphi(n_1 n_2) = \frac{k_1}{n_1}\varphi(n_1)\frac{k_2}{n_2}\varphi(n_2) = \varphi n_1(k_1)\,\varphi_{n_2}(k_2).$$

Definice 1. Pro k a n přirozená definujme funkce $\psi_k(n)$ takto:

$$\psi_1(n) = \varphi(n), \quad \psi_k(n) = \sum_{d \mid n} \varphi_d(n)\,\psi_{k-1}\left(\frac{n}{d}\right) \quad k = 2, 3, \ldots. \tag{8}$$

Lemma 3. *Pro každé přirozené k je $\psi_k(n)$ multiplikativní funkce.*

Důkaz. Indukcí podle k: pro $k = 1$ zřejmé.
Nechť ψ_{k-1} je multiplikativní. Pak pro $(n_1, n_2) = 1$ platí

$$\psi_k(n_1)\,\psi_k(n_2) = \sum_{d_1 \mid n_1} \varphi_{d_1}(n_1)\,\psi_{k-1}\left(\frac{n_1}{d_1}\right) \cdot \sum_{d_2 \mid n_2} \varphi_{d_2}(n_2)\,\psi_{k-1}\left(\frac{n_2}{d_2}\right) =$$

$$= \sum_{d_1 d_2 \mid n_1 n_2} \varphi_{d_1}(n_1)\,\varphi_{d_2}(n_2)\,\psi_{k-1}\left(\frac{n_1}{d_1}\right)\psi_{k-1}\left(\frac{n_2}{d_2}\right) = \psi_k(n_1 n_2)$$

podle lemmatu 1 a indukčního předpokladu.

Úmluva. Slovy „k-tice čísel $\{a_1, a_2, \ldots, a_k\}$ má s n největšího společného dělitele d" budeme rozumět, že $(a_1, a_2, \ldots, a_k, n) = d$.

Podobně slovy „k-tice čísel $\{a_1, a_2, \ldots, a_k\}$ je nesoudělná" budeme vždy rozumět, že $(a_1, a_2, \ldots, a_k) = 1$.

Lemma 4. *$\psi_k(n)$ značí počet uspořádaných k-tic přirozených čísel nejvýš rovných n nesoudělných s n.*

Důkaz. Indukcí podle k: pro $k = 1$ zřejmé.
Nechť tedy $\psi_{k-1}(n)$ značí počet uspořádaných $(k-1)$-tic přirozených čísel nejvýš

čísel nejvýš rovných n nesoudělných s n. Nechť $d \mid n$, pak $\psi_{k-1}(n/d)$ značí počet uspořádaných $(k-1)$-tic přirozených čísel nejvýš rovných n/d nesoudělných s n/d a tedy také počet uspořádaných $(k-1)$-tic přirozených čísel nejvýš rovných n, majících s n největšího společného dělitele d. Ke každé takové $(k-1)$-tici můžeme vzít za k-tý prvek takové číslo nejvýš rovné n, které je nesoudělné s $d = (d, n)$. Těch je ale právě $\varphi_d(n)$.

Lemma 5. *Pro libovolná α, k přirozená, p prvočíslo platí*

$$\psi_k(p^\alpha) = p^{\alpha k} - p^{(\alpha-1)} = (p^k)^{\alpha-1}(p^k - 1). \tag{9}$$

Důkaz. Všech k-tic z p^α prvků je $(p^\alpha)^k$. Prvků soudělných s p^α je $p^{\alpha-1}$. Všech k-tic z těchto prvků utvořených je $(p^{\alpha-1})^k$.

Definice 2. Označme $G(m, n)$ multiplikativní grupu matic typu (m, m) s jednotkovým determinantem nad okruhem C_n zbytkových tříd modulo n, $g(m, n)$ buď řád této grupy.

Úmluva. Pokud nebude řečeno jinak, budeme pod prvky matice z $G(m, n)$, tj. prvky z C_n rozumět vždy nejmenší nezáporné zbytky modulo n.

Definice 3. $A_{kl} = (a_{ij})$ bude značit matici z $G(m, n)$ definovanou takto:

$$a_{ii} = 1\,, \quad a_{kl} = 1\,, \quad a_{ij} = 0 \quad \text{jinak.} \tag{10}$$

Definujme operátory L_{kl} a P_{kl} takto:

$$(\forall A \in G(m, n))\; L_{kl}(A) = A_{kl}A\,; \quad P_{kl}(A) = AA_{kl}\,. \tag{11}$$

Je-li L libovolný L_{kl} a P libovolný P_{kl} definujeme skládání operátorů

$$(P \circ L)(A) = P(L(A)) \quad \text{a analogicky} \quad L \circ L,\; P \circ P,\; L \circ P\,, \tag{12}$$

načež položme

$$L^s_{kl} = L_{kl} \circ L^{s-1}_{kl} \quad \text{a} \quad P^s_{kl} = P_{kl} \circ P^{s-1}_{kl}\,. \tag{13}$$

Lemma 6. *Provést operátor $L^s_{kl}(P^s_{kl})$ na matici A znamená přičíst s-násobek l-tého řádku ke k-tému (k-tého sloupce k l-tému).*

Důkaz zřejmý.

Lemma 7. *Matice $A^s_{kl} = (a^{(s)}_{ij})$ má prvky*

$$a^{(s)}_{ii} = 1\,; \quad a^{(s)}_{kl} = s\,; \quad a^{(s)}_{ij} = 0 \quad \textit{jinak.} \tag{14}$$

Důkaz. $A_{kl} = L_{kl}(E) \Rightarrow A^s_{kl} = L^s_{kl}(E)$ takže tvrzení plyne z lemmatu 6.

Věta 1. *Matice A_{kl} generují grupu $G(m, n)$.*

Důkaz. Provedeme indukcí podle m. Pro $m = 1$ je věta zřejmá. Nechť tedy věta platí pro grupu $G(m-1, n)$ a buď $A = (a_{ij})$ libovolná matice z grupy $G(m, n)$. Označme pro jednoduchost $a_{11} = a$; $a_{12} = b$ a na a, b, která na chvíli uvažujme jako přirozená čísla, užijme Eukleidův algoritmus:

$$
\begin{aligned}
a &= bq_1 + r_1, && 0 \leqq r_1 < b,\\
b &= r_1q_2 + r_2, && 0 \leqq r_2 < r_1,\\
r_1 &= r_2q_3 + r_3, && 0 \leqq r_3 < r_2,\\
&\vdots \quad\; \vdots \quad\; \vdots && \vdots\\
r_{t-2} &= r_{t-1}q_t + r_t, && 0 \leqq r_t < r_{t-1},\\
r_{t-1} &= r_tq_{t+1}. &&
\end{aligned} \tag{15}
$$

Postupným užitím operátorů $P_{21}^{-q_1}$ [2]), $P_{12}^{-q_2}, \ldots$ zřejmě po $t+1$ krocích dospějeme k matici tvaru

$$
A_1' = \begin{pmatrix} 0, & r_t, & \ldots \\ \vdots & & \end{pmatrix} \quad \text{nebo} \quad A_1 = \begin{pmatrix} r_t, & 0, & \ldots \\ \vdots & & \end{pmatrix}. \tag{16}
$$

Avšak matici tvaru A_1' převedeme na tvar A_1 užitím operátoru $P_{12}^{-1} \circ P_{21}$. Analogickým postupem anulujeme ostatní prvky 1. řádku. Máme tedy nyní matici tvaru

$$
A_2 = \begin{pmatrix} a_{11}^{(2)}, & 0, & \ldots, & 0 \\ a_{21}^{(2)}, & a_{22}^{(2)}, & \ldots, & a_{2m}^{(2)} \\ \vdots & \vdots & & \vdots \\ a_{m1}^{(2)}, & a_{m2}^{(2)}, & \ldots, & a_{mm}^{(2)} \end{pmatrix}. \tag{17}
$$

Ježto $\det A_2 = a_{11}A_{11}$ kde A_{11} je algebraický doplněk prvku a_{11}, má prvek a_{11} inversní v C_n, označme ho a_{11}^{-1}. Zřejmě užitím operátoru $P_{12}^{-1} \circ P_{21}^{-a_{11}+1} \circ P_{12}^{a_{11}-1}$ obdržíme matici tvaru

$$
A_3 = \begin{pmatrix} 1, & 0, & \ldots, & 0 \\ a_{21}^{(3)}, & a_{22}^{(3)}, & \ldots, & a_{2m}^{(3)} \\ \vdots & \vdots & & \vdots \\ a_{m1}^{(3)}, & a_{m2}^{(3)}, & \ldots, & a_{mm}^{(3)} \end{pmatrix}. \tag{18}
$$

Postupným užitím operátorů $L_{21}^{-a_{21}}, L_{31}^{-a_{31}} \ldots, L_{m_1}^{-a_{m1}}$ konečně dostaneme matici

$$
A_4 = \begin{pmatrix} 1, & 0, & \ldots, & 0 \\ 0, & a_{22}^{(4)}, & \ldots, & a_{2m}^{(4)} \\ \vdots & \ldots & & \vdots \\ 0, & a_{m_2}^{(4)}, & \ldots, & a_{mm}^{(4)} \end{pmatrix}. \tag{19}
$$

[2]) $-q_1$ značí ovšem opačný prvek ke q_1 v additivní grupě okruhu C_n.

Nyní vzhledem k tomu, že libovolnou operaci na dílčí matici vzniklou vyškrtnutím 1. řádku i sloupce lze provést i na matici A_4 aniž se změní 1. řádek nebo sloupec, stačí užít indukčního předpokladu.

Věta 2. *Buď* $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}$. *Pak platí*

$$G(m, n) \cong G(m, p_1^{\alpha_1}) \dot{\times} G(m, p_2^{\alpha_2}) \dot{\times} \ldots \dot{\times} G(m, p_s^{\alpha_s}) . \tag{20}$$

Důkaz. Každému $a \in C_n$ přiřaďme s-člennou posloupnost $\{a^{(1)}, a^{(2)}, \ldots, a^{(s)}\}$ tak, že

$$a^{(i)} \equiv a \pmod{p_{pi}^{\alpha_i}}, \quad a^{(i)} \text{ je nejmenší nezáporný zbytek.} \tag{21}$$

Definujme nyní sčítání těchto posloupností po složkách, při čemž i-tou sloužku součtu redukujme mod $p_i^{\alpha_i}$. Zřejmě nejmenší přirozený násobek prvku $\{1, 1, \ldots, 1\}$ rovný $\{0, 0, \ldots, 0\}$ je $n \times \{1, 1, \ldots, 1\}$. Odtud plyne, že uvedené přiřazení je vzájemně jednoznačné přiřazení mezi prvky z C_n a posloupnostmi $\{a^{(1)}, a^{(2)}, \ldots, a^{(s)}\}$ s podmínkou (21).

Nyní pravá strana (20) je množina všech konečných posloupností $\{A_1, A_2, \ldots, A_s\}$, $A_i \in G(m, p_p^{\alpha_i})$ s operací

$$\{A_1, A_2, \ldots, A_s\} \cdot \{B_1, B_2, \ldots, B_s\} = \{A_1B_1, A_2B_2, \ldots, A_sB_s\} .$$

Zřejmě zobrazení φ: $(\{A_1, A_2, \ldots, A_s\})\,\varphi = A$ definované takto: prvek a_{kl} matice A je prvek přiřazený posloupnosti $\{a_{kl}^{(1)}, a_{kl}^{(2)}, \ldots, a_{kl}^{(s)}\}$, je vzájemně jednoznačné zobrazení $G(m, p_1^{\alpha_1}) \dot{\times} G(m, p_2^{\alpha_2}) \dot{\times} \ldots \dot{\times} G(m, p_s^{\alpha_s})$ na $G(m, n)$, takže k dokončení důkazu stačí ukázat, že φ je homomorfní.

Jest

$$A_l = (a_{ij}^{(l)}), \quad B_l = (b_{ij}^{(l)}), \quad l = 1, 2, \ldots, s ,$$

a označme

$$A_lB_l = (c_{ij}^{(l)}) .$$

Podle (21) je

$$a_{ij}^{(l)} \equiv a_{ij} \pmod{p_l^{\alpha_l}}, \quad b_{ij}^{(l)} \equiv b_{ij} \pmod{p_l^{\alpha_l}} ,$$

takže i

$$c_{ij}^{(l)} = \sum_{k=1}^{m} a_{ik}^{(l)} b_{kj}^{(l)} \equiv \sum_{k=1}^{m} a_{ik} b_{kj} = c_{ij} \pmod{p_l^{\alpha_l}}$$

čímž je věta dokázána.

Lemma 8. *Pro všechna* m, α *přirozená*, p *prvočíslo platí*

$$g(m, p^{\alpha}) = (p^{\alpha})^{m-1} \psi_m(p^{\alpha})\, g(m - 1, p^{\alpha}) . \tag{22}$$

Důkaz. Buď $A = (a_{ij}) \in G(m, p^{\alpha})$, $D = \det A$, D_{ij} algebraický doplněk prvku a_{ij}.

Jest

$$D = \sum_{i=1}^{m} a_{i1} D_{i1} \quad (v\, C_{p^\alpha}). \tag{23}$$

m-tice prvků $(a_{11}, a_{21}, \ldots, a_{m1})$ musí být nesoudělná s p^α. Takových m-tic však existuje právě $\psi_m(p^\alpha)$.

Rovnice (23) pro neznámé D_{i1} má pro každou nesoudělnou m-tici $(a_{11}, a_{21}, \ldots, a_{m1})$ právě $(p^\alpha)^{m-1}$ řešení (viz např. [3] úloha 1,d ke kap. IV str. 62). Všechna D_{i1} nemohou být současně dělitelna p (jako přirozená čísla ovšem), buď tedy např. D_{11} s p nesoudělné. Jelikož matice s determinantem nesoudělným s p tvoří grupu, v níž je podgrupa všech matic s determinantem 1 normální, existuje právě $g(m-1, p^\alpha)$ matic s determinantem D_{11}. K dokončení důkazu stačí ukázat, že čísla $a_{12}, \ldots, a_{1m}$ jsou již jednoznačně určena. To však plyne snadno z toho, že pro těchto $m-1$ čísel dostaneme rozvojem D_{i1} podle prvního řádku $m-1$ lineárních rovnic, při čemž vhodnou lineární kombinací řádků lze dosáhnout toho, že nalevo zůstane $D_{11}a_{1k}$ pro každé $k = 2, 3, \ldots, m$ a napravo prvek z C_{p^α}. D_{11} má však v C_{p^α} inversní prvek.

Věta 3. *Pro všechna přirozená $m, n > 1$ platí*

$$g(m, n) = n^{m-1}\psi_m(n)\, g(m-1, n). \tag{24}$$

Důkaz. Plyne z lemmatu 8, věty 2 a lemmatu 3.

Důsledek. *Je-li $(a_1, a_2, \ldots, a_m)$ libovolná s n nesoudělná m-tice prvků z C_n, pak existuje právě $n^{m-1}g(m-1, n)$ matic v $G(m, n)$ takových, že daná m-tice je jejich i-tým sloupcem (resp. řádkem).*

Věta 4. *Pro všechna přirozená $m, n > 1$, $n = p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_s^{\alpha_s}$ platí*

$$g(m, n) = n^{m^2} \prod_{i=1}^{s} \frac{\prod_{k=2}^{m}(p_i^k - 1)}{p_i^{m(m+1)/2} \cdot p_i^{\alpha_i - 1}}. \tag{25}$$

Důkaz. Postupným užitím (24) máme

$$g(m, n) = n^{m-1}\psi_m(n)\, g(m-1, n) = n^{m-1}\psi_m(n)\, n^{m-2}\psi_{m-1}(n)\, g(m-2, n) =$$
$$= n^{m-1}n^{m-2}\ldots n\psi_m(n)\,\psi_{m-1}(n)\ldots\psi_2(n)\, g(1, n).$$

Užijeme nyní lemmat 3 a 5 a uvědomíme si, že $g(1, n) = 1$. Máme

$$g(m, n) = n^{m(m-1)/2} \prod_{i=1}^{s} \psi_m(p_i^{\alpha_i})\,\psi_{m-1}(p_i^{\alpha_i})\ldots\psi_2(p_i^{\alpha_i}) =$$

$$= n^{m(m-1)/2} \prod_{i=1}^{s} (p_i^m)^{\alpha_i - 1}(p_i^m - 1)(p_i^{m-1})^{\alpha_i - 1}(p_{i-1}^{m-1} - 1)\ldots(p_i^2)^{\alpha_i - 1}(p_i^2 - 1) =$$

$$= n^{m(m-1)/2} \prod_{i=1}^{s} \frac{(p_i^{m(m+1)/2})^{\alpha_i - 1}}{p_i^{\alpha_i - 1}} \prod_{k=2}^{m} (p_i^k - 1),$$

odkud (25) snadno plyne.

Důsledek. *Speciálně platí*

$$g(m, p^\alpha) = (p^\alpha)^{m^2} \frac{\prod_{k=2}^{m} (p^k - 1)}{p^{m(m+1)/2} \cdot p^{\alpha - 1}} \tag{26}$$

a pro $\alpha = 1$

$$g(m, p) = p^{m(m-1)/2} \prod_{k=2}^{m} (p^k - 1) = o(SL(m, p)), \tag{27}$$

což je ve shodě teorií lineárních grup (viz [1] post. 97 až 109), přičemž $o(G)$ značí řád grupy G.

Poznámka. Jestliže místo ψ_k vezmeme funkci $\overline{\psi}_k$ definovanou pro mocniny prvočísel vztahem

$$\overline{\psi}_k(p^\alpha) = p^{k\alpha} - 1 \tag{28}$$

a odvodíme ze vzorce (24) analogickým způsobem vzorec (26) dostaneme řád speciální lineární grupy $SL(m, p^\alpha)$.

Věta 5. *$G(m, p^\alpha)$ je rozšířením p-grupy pomocí grupy $SL(m, p)$. Řády komposičních faktorů grupy $G(m, p^\alpha)$ jsou $(o(LF(m, p)), q_1, q_2, \ldots, q_l, \underbrace{p, p, \ldots, p}_{(\alpha - 1)(n^2 - 1) \text{ krát}})$, kde $q_1 q_2 \ldots q_l = (m, p - 1)$.*

Důkaz. Zobrazení $\varphi : G(m, p^\alpha) \to G(m, p)$, které každé matici A přiřazuje matici definovanou tak, že každý prvek matice A redukujeme modulo p jest zřejmě homomorfismus.

Podle věty o izomorfismu je

$$G(m, p^\alpha)/\mathrm{Ker}\ \varphi \cong G(m, p). \tag{29}$$

Pro řády těchto grup platí podle (26) a (27)

$$o(\mathrm{Ker}\ \varphi) = \frac{(p^\alpha)^{m^2} \frac{\prod_{k=2}^{m} (p^k - 1)}{p^{m(m+1)/2} p^{\alpha - 1}}}{p^{m(m-1)/2} \prod_{k=2}^{m} (p^k - 1)} = p^{(\alpha - 1)(m^2 - 1)}. \tag{30}$$

Odtud plyne první část tvrzení. Druhá plyne z vět z [1] odst. 97 až 109, zejména 103 a 108.

Důsledek. *Mezi všemi grupami* $G(m, n)$ *jsou řešitelné právě grupy* $G(2, 2^\alpha \cdot 3^\beta)$ $\alpha, \beta = 0, 1$.

Důkaz. $G(2, 6) = G(2, 2) \times G(2, 3)$ podle věty 2, zbytek plyne z tvrzení odst. 103 z [1].

Věta 6. *Pro počet s matic typu* (m, m) *nad* C_n, *k nimž neexistuje inversní platí*

$$s = n^{m^2}\left(1 - \prod_{i=1}^{s} \frac{\prod_{k=1}^{m}(p_i^k - 1)}{p_i^{m(m+1)/2}}\right). \tag{31}$$

Důkaz. Všechny matice s determinantem nesoudělným s n zřejmě tvoří grupu $\bar{G}$, v níž je $G(m, n)$ normální podgrupa. Odtud plyne

$$o(\bar{G}) = \varphi(n)\, g(m, n)\,. \tag{32}$$

Ježto všech matic typu (m, m) nad C_n je n^{m^2} máme podle (25)

$$\begin{aligned} s &= n^{m^2} - \varphi(n)\, g(m, n) = \\ &= n^{m^2}\left(1 - \prod_{i=1}^{s} \frac{\prod_{k=2}^{m}(p_i^k - 1)}{p_i^{m(m+1)/2}\, p_i^{\alpha_i - 1}}\, \varphi(p_i^{\alpha_i})\right), \end{aligned} \tag{33}$$

odkud (31) ihned plyne.

Literatura

[1] *L. Dickson:* Linear groups. Leipzig 1901.
[2] *А. Г. Курош*: Теория групп. Москва 1953.
[3] *I. M. Vinogradov:* Základy teorie čísel. Praha 1953.

Adresa autora: Praha 8, Sokolovská 83 (Matematicko-fyzikální fakulta UK).

Summary

ON SOME GROUPS OF MATRICES

LADISLAV BICAN, Praha

This note studies the groups of matrices with unit determinant over the ring of integers modulo n. The number of elements and the structure of such a group are given.

Definition 2. Let us denote $G(m, n)$ the multiplicative group of matrices of order m with unit determinant over the ring of integers modulo n and $g(m, n)$ be the order of this group.

The main results are contained in the following theorems:

Theorem 2. *Let* $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}$ *be a canonical decomposition of* n. *Then*

$$G(m, n) \cong G(m, p_1^{\alpha_1}) \dot{\times} G(m, p_2^{\alpha_2}) \dot{\times} \ldots \dot{\times} G(m, p_s^{\alpha_s}) .$$

Theorem 4. *For all natural integers* $m, n > 1$, $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}$ *it holds*

$$g(m, n) = n^{m^2} \prod_{i=1}^{s} \frac{\prod_{k=2}^{m} (p_i^k - 1)}{p_i^{m(m+1)/2} \cdot p_i^{\alpha_i - 1}} .$$

Theorem 5. $G(m, p^\alpha)$ *is an extension of a p-group by* $SL(m, p)$. *The orders of composition of* $G(m, p^\alpha)$ *are* $(o(LF(m, p)), q_1, q_2, \ldots, q_l, \underbrace{p, p, \ldots, p}_{(\alpha - 1)(m^2 - 1)\text{-times}})$ *where* $q_1 \cdot q_2 \cdot \ldots \cdot q_l = (m, p - 1)$.

Theorem 6. *For the number* s *of non-invertible matrices of order* m *over the ring of integers modulo* n *it holds*:

$$s = n^{m^2} \left(1 - \prod_{i=1}^{s} \frac{\prod_{k=1}^{m} (p_i^k - 1)}{p_i^{m(m+1)/2}} \right) .$$