Výzkumný úkol: Počet prvků a akce grupy $SL(m, \mathbb{Z}_n)$

Petr Novotný

13. září 2002

Obsah

1 Úvod

Při hledání gradovaných kontrakcí Lieovy algebry $SL(3,\mathbb{C})$ zachovávajících Pauliovskou gradaci, je potřeba řešit systém 48 kontrakčních rovnic, jejichž proměnné jsou indexovány dvojicí dvojic nezáporných celých čísel 0,1,2. Grupou symetrie tohoto systému je právě grupa $SL(2,\mathbb{Z}_3)$. Chceme-li vědět, na které proměnné může působením grupy symetrie přecházet pevně zvolená proměnná, pak se dostáváme k úkolu nalézt orbity akce této grupy na okruhu $(\mathbb{Z}_n \times \mathbb{Z}_n) \times (\mathbb{Z}_n \times \mathbb{Z}_n)$. Touto problematikou se zabýval A.A. Kirillov v [4] , avšak pouze pro případ grupy $SL(2,\mathbb{Z}_p)$ kde $p \in \mathbb{P}$ je prvočíslo. Cílem této práce bude určit řád grupy $SL(m,\mathbb{Z}_n)$ a nalézt orbity akce grup $SL(m,\mathbb{Z}_n)$, $SL(2,\mathbb{Z}_n)$ na okruzích $(\mathbb{Z}_n)^m$ a $(\mathbb{Z}_n)^2 \times (\mathbb{Z}_n)^2$ pro libovolné $n \in \mathbb{N}$.

2 Řád grupy $SL(m, \mathbb{Z}_n)$

V této kapitole postupně definujeme strukturu $SL(m, \mathbb{Z}_n)$, ukážeme, že jde o grupu a určíme počet jejích prvků.

Značení 2.1. Pro $n \in \mathbb{N}$ označme $\mathbb{Z}_n := (\{0, 1, ..., n-1\}; +_{mod\, n}, \cdot_{mod\, n})$.

Poznámka 2.2.

1. V celé práci budeme užívat standardní značení pro množiny přirozených čísel a prvočísel $\mathbb{N} = \{1, 2, 3, \dots\}$, $\mathbb{P} = \{2, 3, 5, \dots\}$.

2. $\mathbb{Z}_n$ je asociativní komutativní okruh s jednotkou a s děliteli nuly pro $n \in \mathbb{N} \backslash \mathbb{P}$ resp. těleso pro $n \in \mathbb{P}$.

3. Operace $+_{mod\, n}, \cdot_{mod\, n}$ na okruhu $\mathbb{Z}_n$ budeme značit stejně jako součet a součin celých čísel tj. $+, \cdot$, ale vždy musíme dbát na to v jakém okruhu pracujeme.

Značení 2.3. Pro $m, n \in \mathbb{N}$, označme $\mathbb{Z}_n^m = \underbrace{\mathbb{Z}_n \times \mathbb{Z}_n \times \ldots \times \mathbb{Z}_n}_{m}$ kartézský součin okruhů.

Poznámka 2.4. Prvky množiny $\mathbb{Z}_n^m$ jsou m-tice čísel z $\mathbb{Z}_n$. Pokud na této množině definujeme operace součin a součet po složkách dostaneme asociativní komutativní okruh s jednotkou a s děliteli nuly. Jeho prvky budeme někdy nazývat řádkovými vektory nebo body.

Značení 2.5. Pro $m, n \in \mathbb{N}$, označme $\mathbb{Z}_n^{m,m}$ množinu všech čtvercových matic typu $m \times m$ s prvky z $\mathbb{Z}_n$. Buď $k \in \mathbb{N}$, $A \in \mathbb{Z}_n^{m,m}$ označme $(A)_{mod\, k}$ matici, která z původní matice vznikne provedením operace $mod\, k$ na jednotlivé její prvky. Dále na množině $\mathbb{Z}_n^{m,m}$ definujeme součin (matic) $\circ$ jako klasický součin matic plus provedení operace $mod\, n$ na výslednou matici.

Poznámka 2.6. Tento součin bude díky asociativitě operací součin matic a $mod\, n$ asociativní. Tedy množina $\mathbb{Z}_n^{m,m}$ spolu s operací $\circ$ je asociativní grupoid.
Jsou-li $A, B \in \mathbb{Z}_n^{m,m}$ takové, že $det(A)_{mod\, n} = det(B)_{mod\, n} = 1$ pak i $det(A \circ B)_{mod\, n} = 1$ a tedy omezíme-li se pouze na matice s determinantem jedna dostaneme opět asociativní grupoid, nebo prázdnou množinu (v případě n=1).

Definice 2.7. Pro $m, n \in \mathbb{N}$, $n \geq 2$ definujme grupoid

$$SL(m, \mathbb{Z}_n) := (\{A \in \mathbb{Z}_n^{m,m} \mid det(A)_{mod\, n} = 1\}; \circ) \ .$$

Lemma 2.8. *Pro $m, n \in \mathbb{N}$, $n \geq 2$ je $SL(m, \mathbb{Z}_n)$ grupa.*

Důkaz. Již víme, že je to asociativní grupoid (tj. pologrupa). Je zřejmé, že jednotkou bude jednotková matice příslušného rozměru. Zbývá ukázat existenci inverzního prvku k matici $A \in SL(m, \mathbb{Z}_n)$. Víme, že pro libovolné matice (a tedy i pro matice s celočíselnými prvky) platí rovnost $AA^{adj} = det(A)I$, kde A^{adj} je matice adjungovaná k matici A s elementy $A^{adj}_{i,j} = (-1)^{i+j} detA(j, i)$ kde detA(j,i) značí determinant matice vzniklé z matice A vynecháním j-tého řádku a i-tého sloupce. Tato rovnost bude jistě platit i po provedení operace *modulo n* na obě strany rovnice a neboť $det(A)_{mod\, n} = 1$ bude $A^{adj}_{mod\, n}$ pravý inverzní prvek k prvku A. Odtud již plyne, že jde o grupu. □

Než přistoupíme k počítání prvků grupy $SL(m, \mathbb{Z}_n)$ definujeme akci této grupy na množině $\mathbb{Z}_n^m$.

Definice 2.9. Buď G grupa a $X \neq \emptyset$ množina. Zobrazení $\psi : G \times X \mapsto X$ nazveme levou resp. pravou akcí grupy G na množině X pokud

1. $\forall g, h \in G \;\; \forall x \in X \quad \psi(gh, x) = \psi(g, \psi(h, x))$ resp. $\psi(gh, x) = \psi(h, \psi(g, x))$
2. $\forall x \in X \;\; \psi(e, x) = x$.

Definice 2.10. Je-li ψ akce grupy G na množině X pak relace $a \sim b \Leftrightarrow \exists g \in G \;\; \psi(g, a) = b$ je ekvivalence na množině X a třída rozkladu množiny X podle této ekvivalence příslušná prvku $a \in X$ tj. množina $\{b \in X \mid \exists g \in G \;\; b = \psi(g, a)\}$ se nazývá orbita (dráha, trajektorie) prvku $a \in X$ vzhledem k akci ψ grupy G.

Definice 2.11. Je-li ψ akce grupy G na množině X pak podgrupou stability bodu $a \in X$ nazýváme množinu $\{g \in G | \; \psi(g, a) = a\}$.

Definice 2.12. Pro $m, n \in \mathbb{N}$, $n \geq 2$ definujeme pravou akci grupy $SL(m, \mathbb{Z}_n)$ na množině $\mathbb{Z}_n^m$ jako násobení řádkového vektoru z $\mathbb{Z}_n^m$ maticí z $SL(m, \mathbb{Z}_n)$ zprava plus příslušné *modulo* n.

Poznámka 2.13. Veškeré operace na daném okruhu, nebude-li řečeno jinak, budou prováděny *modulo* n. V dalším budeme užívat zjednodušeného zápisu, kde budeme příslušné modulo u operací vynechávat. Pokud to bude nutné, pak naznačíme dané modulo na konci celého výrazu. Stejně tak budeme o operacích s *modulo* n mluvit jako o operacích běžných.

2.1 Řád grupy $SL(m, \mathbb{Z}_n)$ pro $n \in \mathbb{P}$ prvočíslo

Nechť je $n = p \in \mathbb{P}, \;\; m \geq 2$. Případ $m = 1$ je triviální $SL(1, \mathbb{Z}_n) = \{(1)\}$, a my se jím proto nadále nebudeme zabývat. Vezměme prvek $(0, \ldots, 0, 1) \in \mathbb{Z}_p^m$ a zkusme nalézt orbitu tohoto prvku. Hledáme matici, která převede tento prvek na libovolný prvek z $\mathbb{Z}_p^m$. Libovolný prvek $a \in \mathbb{Z}_p^m$ je tvaru $(a_1, a_2, \ldots, a_m)$ kde $a_i \in \mathbb{Z}_p, \;\; i \in \widehat{m} = \{1, 2, \ldots, m\}$. Tedy požadavek na matici $A \in SL(m, \mathbb{Z}_p)$ je následující:

$$(0, \ldots, 0, 1) \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1,m} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m-1,1} & a_{m-1,2} & \ldots & a_{m-1,m} \\ a_{m,1} & a_{m,2} & \ldots & a_{m,m} \end{pmatrix} = (a_1, a_2, \ldots, a_m)$$

odtud vidíme, že matice A musí být tvaru:

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1,m} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m-1,1} & a_{m-1,2} & \ldots & a_{m-1,m} \\ a_1 & a_2 & \ldots & a_m \end{pmatrix} .$$

Matice A však musí mít determinant roven jedné, což okamžitě vylučuje prvek $(0,\dots,0)$. Tento prvek lze převést akcí grupy $SL(m,\mathbb{Z}_p)$ pouze sám na sebe, tedy tvoří jednobodovou orbitu a jeho podgrupou stability je celá tato grupa. Ostatní (nenulové) prvky lze získat násobením maticí z prvku $(0,\dots,0,1)$. Nechť $a=(a_1,a_2,\dots,a_m)\in\mathbb{Z}_n^m$ je nenulový tj. $\exists j\in\widehat{m}$ tak, že $a_j\neq 0$ pak je zřejmé, že u matice která má poslední řádek tvaru $(a_1,a_2,\dots,a_m)$ lze volbou ostatních prvků docílit toho, aby byl její determinant roven jedné. Například vynulováním prvních m-1 míst j-tého řádku a nastavením prvků matice A tak, aby po vynechání m-tého řádku a j-tého sloupce měla tvar $diag(1,1,\dots,(-1)^{j+m}(a_j)^{-1})$ tj. tak, aby determinant matice A(m,j) byl roven $(-1)^{j+m}(a_j)^{-1}$. Tedy v tomto případě $(n=p)$ dostáváme dvě orbity:

1. jednobodová orbita reprezentovaná prvkem $(0,\dots,0)$
2. p^m-1 bodová orbita $\mathbb{Z}_p^m\backslash(0,\dots,0)$ reprezentovaná prvkem $(0,\dots,0,1)$.

Podgrupu stability bodu $(0,\dots,0,1)$ označíme $S_{(0,\dots,0,1)}$ a určíme její řád. $S_{(0,\dots,0,1)}$ je tvořena maticemi:

$$A=\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1,m} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m-1,1} & a_{m-1,2} & \dots & a_{m-1,m} \\ 0 & 0 & \dots & 1 \end{pmatrix}\ ,\quad detA=1\ .$$

Rozvojem determinantu podle posledního řádu dostaneme:

$$detA=(-1)^{m+m}detA(m,m)=det\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1,m-1} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m-1,1} & a_{m-1,2} & \dots & a_{m-1,m-1} \end{pmatrix}=1 \quad \backslash mod_p\ .$$

Poslední rovnost splňují právě všechny matice z $SL(m-1,\mathbb{Z}_p)$ a neboť prvky $a_{1,m},\dots,a_{m-1,m}$ jsou libovolné, bude řád podgrupy stability bodu $(0,\dots,0,1)$ roven:

$$|S_{(0,\dots,0,1)}|=p^{m-1}|SL(m-1,\mathbb{Z}_p)|\ .$$

Z Lagrageovy věty víme, že součin řádu a indexu libovolné podgrupy dané konečné grupy je roven řádu této grupy. Řád naší podgrupy stability už známe, zbývá určit její index. Definujeme-li na grupě $SL(m,\mathbb{Z}_p)$ levou ekvivalenci indukovanou podgrupou stability bodu $(0,\dots,0,1)$ tj.

$$A,B\in SL(m,\mathbb{Z}_p)\qquad A\equiv_{S_{(0,\dots,0,1)}}B\ \Leftrightarrow\ AB^{-1}\in S_{(0,\dots,0,1)}$$

dostaneme třídy rozkladu grupy $SL(m,\mathbb{Z}_p)$ podle podgrupy $S_{(0,\dots,0,1)}$ ve tvaru $S_{(0,\dots,0,1)}B$, $B\in SL(m,\mathbb{Z}_p)$. Je zřejmé, že si třídy rozkladu vzájemně jednoznačně odpovídají s body p^m-1 bodové orbity. A tedy index rozkladu grupy $SL(m,\mathbb{Z}_p)$ podle podgrupy stability bodu $(0,\dots,0,1)$ je p^m-1. Odtud dostáváme rekurentní vzorec pro řád grupy $SL(m,\mathbb{Z}_p)$:

$$|SL(m,\mathbb{Z}_p)|=p^{m-1}|SL(m-1,\mathbb{Z}_p)|(p^m-1)$$

platný pro $m \geq 2$. Grupa $SL(1, \mathbb{Z}_p)$ je jednoprvková a tedy matematickou indukcí jsme získali vzorec pro počet prvků grupy $SL(m, \mathbb{Z}_p)$:

$$|SL(m, \mathbb{Z}_p)| = \prod_{i=1}^{m-1} (p^i(p^{i+1} - 1)) = p^{m^2-1} \prod_{j=2}^{m} (1 - \frac{1}{p^j}). \tag{2.1}$$

Poznámka 2.14. V této práci budeme užívat následující konvenci

$$\prod_{i=a}^{b} x_i = 1 \; pro \; a > b \; .$$

2.2 Řád grupy $SL(m, \mathbb{Z}_n)$ pro $n = p^k, \; p \in \mathbb{P}, \; k \in \mathbb{N}, \; k \geq 2$

Řád grupy $SL(m, \mathbb{Z}_{p^k})$ chceme získat indukcí podle k. Za tímto účelem definujeme zobrazení, které nám umožní zjistit, kolik prvků má grupa $SL(m, \mathbb{Z}_{p^k})$ vzhledem ke grupě $SL(m, \mathbb{Z}_{p^{k-1}})$.

Definice 2.15. Pro $n = p^k, \; p \in \mathbb{P}, \; k \in \mathbb{N}, \; p, k \geq 2$. definujeme zobrazení

$$h : SL(m, \mathbb{Z}_{p^k}) \to SL(m, \mathbb{Z}_{p^{k-1}})$$

předpisem

$$h(A) = (A)_{mod p^{k-1}} , \quad \forall A \in SL(m, \mathbb{Z}_{p^k}) \; .$$

Nejprve ukážeme některé jeho vlastnosti:

1. Zobrazení h je dobře definované tj. $h(A) \in SL(m, \mathbb{Z}_{p^{k-1}}) \; \forall A \in SL(m, \mathbb{Z}_{p^k})$.

   Důkaz. $\forall A \in SL(m, \mathbb{Z}_{p^k}) : \quad detA = 1 \; \backslash mod \, p^k \Leftrightarrow detA - 1 = 0 \; \backslash mod \, p^k \Rightarrow$
   $\Rightarrow detA - 1 = 0 \; \backslash mod \, p^{k-1} \Leftrightarrow detA = 1 \; \backslash mod \, p^{k-1} \Leftrightarrow det(A)_{mod \, p^{k-1}} = 1 \Leftrightarrow$
   $\Leftrightarrow deth(A) = 1 \backslash mod \, p^{k-1}$ □

2. Zobrazení h je homomorfismus grup tj. $h(AB) = h(A)h(B) \;\; \forall A, B \in SL(m, \mathbb{Z}_{p^k})$.

   Důkaz. $\forall A, B \in SL(m, \mathbb{Z}_{p^k}) : \qquad h(AB) = ((AB)_{mod \, p^k})_{mod \, p^{k-1}} = (AB)_{mod \, p^{k-1}} =$
   $= ((A)_{mod \, p^{k-1}} (B)_{mod \, p^{k-1}})_{mod \, p^{k-1}} = h(A)h(B)$ □

3. Zobrazení h je epimorfismus grup tj. $\forall A \in SL(m, \mathbb{Z}_{p^{k-1}}) \; \exists B \in SL(m, \mathbb{Z}_{p^k}) \quad h(A) = B$.

   Důkaz. Stačí dokázat, že zobrazení h je surjektivní (na), zbytek plyne z bodu 2. Budeme hledat vzory matice $A \in SL(m, \mathbb{Z}_{p^{k-1}})$. Množina všech vzorů matice A je:

   $$h^{-1}(A) = \{A^v \in SL(m, \mathbb{Z}_{p^k}) |\; h(A^v) = A\} = \{A^v = A + p^{k-1}B |\; B \in \mathbb{Z}_p^{m,m}, \; detA^v = 1\}.$$

   Označíme prvky matic A, B příslušnými malými písmeny s indexy tj.

   $$a_{i,j} = (A)_{i,j} \in \mathbb{Z}_{p^{k-1}} \qquad b_{i,j} = (B)_{i,j} \in \mathbb{Z}_p$$

a upravíme podmínku pro vzor:

$$detA^v = det(A + p^{k-1}B) = \sum_{\pi \in S_m} sgn\pi \prod_{i=1}^{m} (p^{k-1}b_{i,\pi(i)} + a_{i,\pi(i)}) =$$

$$= \sum_{\pi \in S_m} sgn\pi (\prod_{i=1}^{m} a_{i,\pi(i)} + p^{k-1} \sum_{i=1}^{m} b_{i,\pi(i)} \prod_{j=1, j\neq i}^{m} a_{j,\pi(j)} + (p^{k-1})^2 .OST) =$$

$$= \underbrace{\sum_{\pi \in S_m} sgn\pi \prod_{i=1}^{m} a_{i,\pi(i)}}_{=detA} + p^{k-1} \sum_{i=1}^{m} \underbrace{\sum_{\pi \in S_m} sgn\pi \, a_{i,\pi(i)} \prod_{j=1, j\neq i}^{m} a_{j,\pi(j)}}_{=detA(i,B)} + (p^{k-1}) \underbrace{\sum_{\pi \in S_m} sgn\pi \, .OST}_{=OS} =$$

$$= detA + p^{k-1} \sum_{i=1}^{m} detA(i,B) + (p^{k-1})^2 .OS = 1 \quad \backslash mod\, p^k \ .$$

Symbolem $detA(i,B)$ značíme determinant matice, která vznikne z matice A záměnou jejího i-tého řádku s i-tým řádkem matice B a symbolem OST značíme ostatní členy vzniklé při roznásobení dvojčlenů. Pokud rozvineme determinanty ve druhém členu podle jejich i-tých řádků dostaneme následující rovnost:

$$detA + p^{k-1} \sum_{i=1}^{m} \sum_{j=1}^{m} (-1)^{i+j} \, b_{i,j} \, detA(i,j) + (p^{k-1})^2 .OS = 1 \quad \backslash mod\, p^k \ .$$

Neboť $A \in SL(m, \mathbb{Z}_{p^{k-1}})$ platí $detA - 1 = 0 \ \backslash mod p^{k-1}$ a tedy $\exists u \in \mathbb{Z}$ tak, že $detA - 1 = up^{k-1}$. Dosadíme tedy za $detA - 1$ a dostaneme:

$$up^{k-1} + p^{k-1} \sum_{i,j=1}^{m} (-1)^{i+j} \, b_{i,j} \, detA(i,j) + (p^{k-1})^2 .OS = 0 \ \backslash mod\, p^k$$

Obě strany této rovnosti jsou dělitelné číslem p^{k-1}, tedy vydělíme a dostaneme:

$$u + \sum_{i,j=1}^{m} (-1)^{i+j} \, b_{i,j} \, detA(i,j) + \underbrace{p^{k-1}.OS}_{=0 \ mod\, p} = 0 \ \backslash mod\, p \ .$$

Poslední člen na levé straně je dělitelný číslem p, tedy je roven nule. Čísla $u, detA(i,j)$, $i,j \in \widehat{m}$ jsou pevně dána maticí A a vzhledem k tomu, že celá rovnost je $mod\, p$ lze i tato čísla redukovat na zbytky po dělení číslem p. Označme

$$u_0 = (u)_{mod\, p} \qquad u_{i,j} = (detA(i,j))_{mod\, p}$$

potom dostaneme:

$$u_0 + \sum_{i,j=1}^{m} (-1)^{i+j} \, u_{i,j} \, b_{i,j} = 0 \quad \backslash mod\, p \ .$$

To je rovnice pro neznámé $b_{i,j},\ i,j \in \mathbb{Z}_p$ a teď vyvstává otázka její řešitelnosti. Pokud by všechny koeficienty $u_{i,j},\ i,j \in \mathbb{Z}_p$ byly nulové a člen $u_0 \neq 0$, pak by tato rovnice neměla žádné řešení. Sporem ukážeme, že tento případ nemůže nastat. Nechť

$$\forall i,j \in \mathbb{Z}_p \quad u_{i,j} = 0 \quad tj. \quad (detA(i,j))_{mod\, p} = 0$$

pak

$$\forall i,j \in \mathbb{Z}_p\ \exists v_{i,j} \in \mathbb{Z}_{p^{k-2}} \qquad detA(i,j) = p.v_{i,j}\ \backslash mod\, p^{k-1}$$

ale současně je

$$detA = \sum_{j=1}^{m} (-1)^{i+j}\, a_{i,j}\, detA(i,j) = p(\sum_{j=1}^{m} (-1)^{i+j}\, a_{i,j}\, v_{i,j}) = \ \backslash mod\, p^{k-1}$$

což je spor, neboť na levé straně stojí násobek dělitele nuly tj. dělitel nuly (nebo nula) a na pravé straně jednotka, která dělitelem nuly není. Tedy

$$\exists i_0, j_0 \in \widehat{m} \qquad u_{i_0,j_0} \neq 0$$

a neboť rovnici řešíme v tělese, což zaručuje existenci inverzního prvku, dostaneme:

$$b_{i_0,j_0} = u^{-1}_{i_0,j_0}(u_0) - \sum_{i,j=1,\ (i,j)\neq(i_0,j_0)}^{m} (-1)^{i+j}\, u_{i,j}\, b_{i,j} \quad \backslash mod\, p\ .$$

Odtud již vidíme, že tato rovnice má p^{m^2-1} řešení a tedy, že každá matice $A \in SL(m, \mathbb{Z}_{p^{k-1}})$ má p^{m^2-1} vzorů. □

Z věty o homomorfismu pro grupy víme:

$$SL(m, \mathbb{Z}_{p^{k-1}}) = h(SL(m, \mathbb{Z}_{p^k})) \cong SL(m, \mathbb{Z}_{p^k})/_{Ker\, h}\ .$$

Jádro zobrazení h tvoří normální podgrupu grupy $SL(m, \mathbb{Z}_{p^k})$ a podle Lagrangeovy věty je součin jeho řádu a indexu roven řádu grupy $SL(m, \mathbb{Z}_{p^k})$. Index jádra $Ker\, h$ je podle předchozí rovnosti roven řádu grupy $SL(m, \mathbb{Z}_{p^{k-1}})$ a řád jádra známe ze třetí vlastnosti zobrazení h:

$$|Ker\, h| = p^{m^2-1}\ .$$

Tedy dostáváme opět rekurentní vztah pro řád grupy $SL(m, \mathbb{Z}_{p^k})$:

$$|SL(m, \mathbb{Z}_{p^k})| = p^{m^2-1}.|SL(m, \mathbb{Z}_{p^{k-1}})|\ .$$

Upravíme

$$|SL(m, \mathbb{Z}_{p^k})| = (p^{m^2-1})^{k-1} |SL(m, \mathbb{Z}_p)|$$

a dosadíme z 2.1 za řád $SL(m, \mathbb{Z}_p)$:

$$|SL(m, \mathbb{Z}_{p^k})| = (p^{m^2-1})^{k-1}\, p^{m^2-1} \prod_{j=2}^{m} (1 - \frac{1}{p^j}) =$$

$$= (p^k)^{m^2-1} \prod_{j=2}^{m} (1 - \frac{1}{p^j}) \ .$$

Neboť v tomto případě je $n = p^k$ dostáváme vztah pro řád grupy $SL(m, \mathbb{Z}_{p^k})$:

$$|SL(m, \mathbb{Z}_{p^k})| = (n)^{m^2-1} \prod_{j=2}^{m} (1 - \frac{1}{p^j}) \ . \tag{2.2}$$

2.3 Řád grupy $SL(m, \mathbb{Z}_n)$ pro $n = pq,\ \delta(p,q) = 1,\ p,q \in \mathbb{N},\ p,q \geq 2$

Obdobně jako v předcházející části i zde se budeme snažit dopracovat k řádu grupy skrze srovnávání s jinou grupou, u které řád známe. Touto grupou bude kartézský součin grup $SL(m, \mathbb{Z}_p) \times SL(m, \mathbb{Z}_q)$, kde operace součin je prováděna po složkách.

Značení 2.16. Buďte $p, q \geq 2$ přirozená čísla. Největší společný dělitel čísel p, q budeme značit $\delta(p, q)$.

Definice 2.17. Nechť $n = pq$ a $\delta(p, q) = 1$ tj. čísla p, q jsou nesoudělná. Pak definujeme zobrazení

$$g : SL(m, \mathbb{Z}_{pq}) \to SL(m, \mathbb{Z}_p) \times SL(m, \mathbb{Z}_q)$$

předpisem

$$g(A) = ((A)_{mod\, p}, (A)_{mod\, q}) \, , \qquad \forall A \in SL(m, \mathbb{Z}_{pq}) \ .$$

Ukážeme některé vlastnosti zobrazení g:

1. Zobrazení g je dobře definované tj. $\forall A \in SL(m, \mathbb{Z}_{pq}) \quad g(A) \in SL(m, \mathbb{Z}_p) \times SL(m, \mathbb{Z}_q)$.

   Důkaz. Stačí ověřit, zda determinant obou složek obrazu je roven jedné (samozřejmě počítáno příslušné modulo). $\forall A \in SL(m, \mathbb{Z}_{pq}) \quad detA = 1 \ \backslash mod\, pq \Leftrightarrow detA - 1 = 0 \ \backslash mod\, pq$ tedy číslo $detA - 1$ je dělitelné součinem pq a tedy je současně dělitelné číslem p i číslem q tj. $detA - 1 = 0 \ \backslash mod\, p \ \wedge \ detA - 1 = 0 \ \backslash mod\, q \ \Leftrightarrow \ detA = 1 \ \backslash mod\, p \ \wedge \ detA = 1 \ \backslash mod\, q$. □

2. Zobrazení g je homomorfismus grup tj. $\forall A, B \in SL(m, \mathbb{Z}_{pq}) \quad g(AB) = g(A)g(B)$.

   Důkaz. $\forall A, B \in SL(m, \mathbb{Z}_{pq}) \quad g(AB) = (((AB)_{mod\, pq})_{mod\, p}, ((AB)_{mod\, pq})_{mod\, q}) =$

   $$((AB)_{mod\, p}, (AB)_{mod\, q}) = ((A)_{mod\, p}, (A)_{mod\, q}).((B)_{mod\, p}, (B)_{mod\, q}) = g(A)g(B)$$

   □

3. Zobrazení g je izomorfismus grup.

Důkaz. Neboť již víme, že g je homomorfismus stačí ukázat, že je to současně i bijekce tj. že

$$\forall A^p, A^q \in SL(m,\mathbb{Z}_p) \times SL(m,\mathbb{Z}_q) \quad \exists_1 A \in SL(m,\mathbb{Z}_{pq}) \qquad g(A) = (A^p, A^q) \ .$$

Pro složky vzoru dostáváme podmínky:

$$(A_{i,j})_{mod\, p} = A^p_{i,j} \in \mathbb{Z}_p \quad \wedge \quad (A_{i,j})_{mod\, q} = A^q_{i,j} \in \mathbb{Z}_q \qquad \forall i,j \in \widehat{m}$$

odtud:

$$\exists m \in \mathbb{Z}_q \ \exists n \in \mathbb{Z}_p \quad A_{i,j} = mp + A^p_{i,j} \ \wedge \ A_{i,j} = nq + A^q_{i,j} \quad \forall i,j \in \widehat{m}$$

a dále

$$mp + A^p_{i,j} = nq + A^q_{i,j} \quad \forall i,j \in \widehat{m}$$

Tato rovnost musí platit i pro zbytky po dělení čísly p a q tj.

$$A^p_{i,j} = nq + A^q_{i,j} \ \backslash mod\, p \ \wedge \ mp + A^p_{i,j} = A^q_{i,j} \ \backslash mod\, q \quad \forall i,j \in \widehat{m}$$

Neboť jsou čísla p, q nesoudělná existuje v okruhu $\mathbb{Z}_p$ právě jeden inverzní prvek k prvku $(q)_{mod\, p}$ (označme ho q^{-1}) a naopak v okruhu $\mathbb{Z}_q$ existuje právě jeden inverzní prvek k prvku $(p)_{mod\, q}$ (ozn. p^{-1}) a tedy dostáváme:

$$n = q^{-1}(A^p_{i,j} - A^q_{i,j}) \ \backslash mod\, p \ \wedge \ m = p^{-1}(A^q_{i,j} - A^p_{i,j}) \ \backslash mod\, q \quad \forall i,j \in \widehat{m}$$

Odtud vidíme, že čísla m, n jsou určeny jednoznačně a tedy ke každému prvku z grupy $SL(m,\mathbb{Z}_p) \times SL(m,\mathbb{Z}_q)$ existuje právě jeden vzor při zobrazení i. □

Zkonstruované zobrazení je podle 3. vlastnosti izomorfismem grup a tedy obě grupy $SL(m,\mathbb{Z}_{pq})$ a $SL(m,\mathbb{Z}_p) \times SL(m,\mathbb{Z}_q)$ mají stejný počet prvků. A neboť řád kartézského součinu grup je roven součin řádů těchto grup dostáváme vzorec:

$$|SL(m,\mathbb{Z}_{pq})| = |SL(m,\mathbb{Z}_p)|.|SL(m,\mathbb{Z}_q)| \ . \tag{2.3}$$

2.4 Řád grupy $SL(m,\mathbb{Z}_n)$ pro $n \in \mathbb{N}, \ n \geq 2$

Nechť $n \in \mathbb{N}, \ n \geq 2$, pak n lze rozložit na součin mocnin prvočísel tj.

$$\exists r \in \mathbb{N} \ \forall i \in \widehat{r} \ \exists p_i \in \mathbb{P} \ \exists k_i \in \mathbb{N} \quad n = \prod_{i=1}^{r} p_i^{k_i} \ .$$

Vzorec 2.2 udává počet prvků grupy $SL(m,\mathbb{Z}_n)$ pro n mocninu prvočísla a neboť mocniny různých prvočísel jsou nesoudělné, lze užít vzorec 2.3, a dostaneme tak vzorec pro případ n rovno součinu mocnin prvočísel. V této kapitole jsme tedy postupně dokázali následující tvrzení.

Tvrzení 2.18. *Buďte $m, n \in \mathbb{N}, \ n \geq 2$ a nechť $n = \prod_{i=1}^{r} p_i^{k_i}, \ p_i \in \mathbb{P}, \ k_i \in \mathbb{N}, \ \forall i \in \widehat{r}$ je rozklad čísla n na součin mocnin prvočísel. Potom řád grupy $SL(m,\mathbb{Z}_n)$ je:*

$$|SL(m,\mathbb{Z}_n)| = n^{m^2-1} \prod_{i=1}^{r} \prod_{j=2}^{m} (1 - \frac{1}{p_i^j}) \ . \tag{2.4}$$

3 Orbity akce grupy $SL(m, \mathbb{Z}_n)$ na $\mathbb{Z}_n^m$

Akci grupy $SL(m, \mathbb{Z}_n)$ na okruhu $\mathbb{Z}_n^m$ jsme zavedli již v definici 2.12 jako násobení řádkového vektoru z okruhu zprava maticí z této grupy. Dále zavedeme ekvivalenci indukovanou touto akcí na okruhu $\mathbb{Z}_n^m$. Prvky

$$a = (a_1, \ldots, a_m), b = (b_1, \ldots, b_m) \in \mathbb{Z}_n^m$$

jsou ekvivalentní

$$a \sim b \Leftrightarrow \exists A \in SL(m, \mathbb{Z}_n) \quad aA = b \quad tj. \forall i \in \widehat{m} \sum_{j=1}^{m} a_j (A)_{i,j} = b_i \ .$$

Největší společný dělitel prvku $a = (a_1, \ldots, a_m) \in \mathbb{Z}_n^m$ a čísla n budeme značit $\delta(a, n) = \delta(a_1, \ldots, a_m, n)$.

Lemma 3.1. *Největší společný dělitel prvku $a \in \mathbb{Z}_n^m$ a čísla n se při akci grupy $SL(m, \mathbb{Z}_n)$ (při násobení prvku a maticemi z této grupy) nemění tj.*

$$\forall a \in \mathbb{Z}_n^m \ \forall A \in SL(m, \mathbb{Z}_n) \quad \delta(aA, n) = \delta(a, n) \ .$$

Důkaz. Neboť $aA = (\sum_{i=1}^{m} a_i A_{i,1}, \ldots, \sum_{i=1}^{m} a_i A_{i,m})$ a $\forall i \in \widehat{m} \quad \delta(a_i, n) \geq \delta(a, n)$ je zřejmé, že $\delta(aA, n) \geq \delta(a, n)$. Tedy po vynásobení maticí se největší společný dělitel prvku a a čísla n může pouze zvětšit nebo zůstat stejný. Pokud nyní vezmeme prvek aA a vynásobíme ho maticí A^{-1} dostaneme pro největší společné dělitele vztah $\delta(a, n) \geq \delta(aA, n)$, což dohromady s první nerovností dává vztah $\delta(aA, n) = \delta(a, n)$. □

V následujících podkapitolách uvedeme dva způsoby jak nalézt hledané orbity.

3.1 První způsob

Zde budeme postupovat obdobně jako při hledání řádu grupy $SL(m, \mathbb{Z}_n)$ tj. rozdělíme si úlohu na tři případy podle tvaru čísla n a definujeme si vhodná zobrazení.

3.1.1 Případ $n = p \in \mathbb{P}$

Byl již vyřešen v oddíle 2.1 zde pouze uvedeme, že v tomto případě se celý okruh $\mathbb{Z}_n^m$ rozpadá na dvě orbity:

1. Jednobodová orbita $(0, \ldots, 0)$
2. $n^m - 1$ bodová orbita $\mathbb{Z}_n^m \backslash (0, \ldots, 0)$ charakterizovaná prvkem $(0, \ldots, 1)$.

3.1.2 Případ $n = p^k, p \in \mathbb{P},\ k \in \mathbb{N},\ k \geq 2$

Zde budeme postupovat indukcí podle k, případ k=1 je vyřešen výše. Definujeme zobrazení

$$H : \mathbb{Z}_{p^k}^m \to \mathbb{Z}_{p^{k-1}}^m$$

předpisem

$$H(a) = (a)_{mod\, p^{k-1}} = ((a_1)_{mod\, p^{k-1}}, \ldots, (a_m)_{mod\, p^{k-1}}), \quad a \in \mathbb{Z}_{p^k}^m\ .$$

Snadno se přesvědčíme o tom, že takto definované zobrazení je homomorfismus okruhů a neboť:

$$a \in \mathbb{Z}_{p^{k-1}} \subset \mathbb{Z}_{p^k}^m \qquad H(a) = (a)_{mod\, p^{k-1}} = a$$

je zobrazení H současně i surjektivní. Jedná se tedy o epimrofismus okruhů.

Podíváme se jak působí zobrazení H na prvek $aA,\ a \in \mathbb{Z}_{p^k}^m,\ A \in SL(m, \mathbb{Z}_{p^k})$:

$$H(aA) = (aA)_{mod\, p^{k-1}} = (a)_{mod\, p^{k-1}}(A)_{mod\, p^{k-1}} = H(a)h(A)$$

kde h je zobrazení definované v 2.15. Dále ukážeme, že zobrazení H zachovává ekvivalenci indukovanou akcí příslušné grupy tj. jsou-li dva prvky $a, b \in \mathbb{Z}_{p^k}^m$ ekvivalentní, pak jsou ekvivalentní i jejich obrazy:

$$a \sim b \Leftrightarrow \exists A \in SL(m, \mathbb{Z}_{p^k}) \quad aA = b \Rightarrow H(aA) = H(a)h(A) = H(b) \Rightarrow H(a) \sim H(b)$$

Tato vlastnost zaručuje, že obraz celé orbity z $\mathbb{Z}_{p^k}^m$ při zobrazení H bude ležet v jedné z orbit v $\mathbb{Z}_{p^{k-1}}^m$ a současně, že vzor orbity z $\mathbb{Z}_{p^{k-1}}^m$ bude složen z celých orbit z $\mathbb{Z}_{p^k}^m$. Zobrazení H je epimorfismus a proto přenáší ekvivalenci jen jedním směrem. My bychom ale chtěli zkonstruovat prosté zobrazení, které bude ekvivalenci přenášet oběma směry. Proto nejprve prozkoumáme jádro zobrazení H:

$$KerH = H^{(-1)}(0) = \{p^{k-1} | a \in \mathbb{Z}_p^m\}\ .$$

Již v případě prvočíselného n tvořila nula (nulový prvek $0 = (0, \ldots, 0)$) jednobodovou orbitu, a tak tomu bude i ve všech ostatních případech, neboť nulu nelze pomocí násobení matic převést na nic jiného než opět na nulu. Tedy jádro $KerH$ je vzorem orbity a proto bude složeno z celých orbit v $\mathbb{Z}_{p^k}^m$, a lze ho tedy vyšetřovat odděleně od zbytku okruhu. Definujeme zobrazení

$$F : KerH \to \mathbb{Z}_p^m$$

předpisem:

$$F(p^{k-1}a) = (p^{k-1}a)_{div\, p^{k-1}} = a \qquad \forall a \in \mathbb{Z}_p\ .$$

Je zřejmé, že toto zobrazení je bijektivní. Dále si definujeme zobrazení

$$\widehat{h} : SL(m, \mathbb{Z}_{p^k}) \to SL(m, \mathbb{Z}_p)$$

předpisem:

$$\widehat{h}(A) = (A)_{mod\, p} \qquad \forall A \in SL(m, \mathbb{Z}_{p^k}) \ .$$

Snadno se přesvědčíme, že takto definované zobrazení je epimorfismus grup, neboť ho lze získat složením epimorfismů h. Nyní se podíváme jak zobrazení F působí na prvek $aA,\ a \in KerH,\ a = p^{k-1}a',\ a' \in \mathbb{Z}_p,\ A \in SL(m, \mathbb{Z}_{p^k})$:

$$F(aA) = ((p^{k-1}a'A)_{mod\, p^k})_{div\, p^{k-1}} = ((p^{k-1}a'A)_{div\, p^{k-1}})_{mod\, p}) = (a')_{mod\, p}(A)_{mod\, p} = F(a)\widehat{h}(A) \ .$$

Dále se podíváme jak je to s přenosem ekvivalence. Pro $a, b \in KerH$ platí

$$a \sim b \ \Leftrightarrow\ \exists A \in SL(m, \mathbb{Z}_{p^k}) \quad aA = b \ \Rightarrow\ F(b) = F(aA) = F(a)\widehat{h}(A) \ \Rightarrow\ F(a) \sim F(b)$$

naopak:

$$\forall a', b' \in \mathbb{Z}_p^m\ \exists_1 a, b \in KerH \qquad F(a) = a',\ F(b) = b'$$

$$\forall A' \in SL(m, \mathbb{Z}_p)\ \exists A \in SL(m, \mathbb{Z}_{p^k}) \qquad \widehat{h}(A) = A'$$

a tedy

$$a' \sim b' \ \Leftrightarrow\ \exists A' \in SL(m, \mathbb{Z}_p) \quad b' = a'A' \ \Leftrightarrow\ F(b) = F(a)A' = F(a)\widehat{h}(A) = F(aA)$$

a neboť F je bijekce platí

$$F(b) = F(aA) \ \Leftrightarrow\ b = aA \ \Rightarrow b \sim a \ .$$

Zobrazení F tedy přenáší ekvivalenci oběma směry tj. obrazy dvou prvků jsou ekvivalentní právě tehdy, když jsou ekvivalentní tyto prvky. Odtud plyne, že jádro se rozpadá na dvě orbity jež jsou vzory orbit v $\mathbb{Z}_p^m$:

1. Jednobodová orbita $(0, \ldots, 0)$
2. $p^m - 1$ bodová orbita $KerH \backslash (0, \ldots, 0)$ charakterizovaná prvkem $(0, \ldots, p^{k-1})$

Poznámka 3.2. Prvek $(0, \ldots, p^{k-1})$ skutečně charakterizuje orbitu, neboť do této orbity patří všechny prvky okruhu, jejichž největší společný dělitel s číslem n je p^{k-1}, tedy číslo, které jsme zapsali jako poslední složku reprezentačního prvku. V dalším budeme často orbity reprezentovat obdobně zvolenými prvky.

Dále chceme vyšetřit zbytek okruhu. Jádro $KerH$ je ideál okruhu $\mathbb{Z}_{p^k}^m$, a tudíž indukuje na tomto okruhu kongruenci:

$$a, b \in \mathbb{Z}_{p^k}^m \quad a \equiv_H b \ \Leftrightarrow\ a - b \in KerH \ .$$

Faktor okruh okruhu $\mathbb{Z}_{p^k}^m$ podle jádra $KerH$ (resp. podle indukované kongruence) je množina:

$$\mathbb{Z}_{p^k}^m /_{KerH} = \{[a] \mid a \in \mathbb{Z}_{p^k}^m\}$$

kde $[a] = a + KerH$ je třída prvků kongruentních s prvkem a a operace součet a součin jsou definovány následovně:

$$\forall [a], [b] \in \mathbb{Z}_{p^k}^m / _{KerH} \qquad [a] + [b] = [a + b], \quad [a].[b] = [ab] \ .$$

Dále chceme na tomto faktorokruhu definovat ekvivalenci indukovanou akcí grupy $SL(m, \mathbb{Z}_{p^k})$ například takto:

$$[a], [b] \in \mathbb{Z}_{p^k}^m / _{KerH} \qquad [a] \approx [b] \ \Leftrightarrow \ \exists A \in SL(m, \mathbb{Z}_{p^k}) \quad [a]A = [b] \ .$$

K tomu, aby měla tato relace smysl je potřeba dokázat dvě věci:

1. $\forall [a] \in \mathbb{Z}_{p^k}^m / _{KerH} \ \forall A \in SL(m, \mathbb{Z}_{p^k}) \qquad [a]A = [aA]$

   Důkaz. Nejprve ukážeme, že $(KerH)A = KerH \quad \forall A \in SL(m, \mathbb{Z}_{p^k})$. Protože platí $\forall x \in KerH \quad H(xA) = H(x)h(A) = 0.h(A) = 0$ máme inkluzi $(KerH)A \subseteq KerH$. Opačná inkluze plyne z následujícího:

   $$\forall x \in KerH \ \forall A \in SL(m, \mathbb{Z}_{p^k}) \ \exists y = xA^{-1} \in KerH \qquad yA = x \ .$$

   Potom

   $$[a]A = (a + KerH)A = aA + (KerH)A = aA + KerH = [aA] \ .$$

   □

2. Prvky třídy $[a] \neq KerH, \ a \in \mathbb{Z}_{p^k}^m$ jsou navzájem $\sim$ ekvivalentní tj.

   $$a, b \in \mathbb{Z}_{p^k}^m \backslash KerH \quad a \equiv_H b \ \Rightarrow \ a \sim b \ .$$

   Důkaz. Ukážeme, že pro libovolný prvek $a \in \mathbb{Z}_{p^k}^m \backslash KerH$ platí $a \sim a + e \quad \forall e \in KerH$. Tedy, že $\forall e \in KerH \ \exists A \in SL(m, \mathbb{Z}_{p^k}) \quad aA = a + e$. Neboť $H(aA) = H(a)h(A) \ \wedge \ H(aA) = H(a) + H(e) = H(a)$ stačí se omezit při hledání matice A na vzory matic z podgrupy stability bodu $H(a)$. Nechť $\delta(a, p^k) = p^s, \ s \in \mathbb{Z}_{k-2}$ pak $\exists a' \in \mathbb{Z}_{p^{k-s}}, \ \delta(a', p^k) = 1, \quad a = p^s a'$ a my se pokusíme hledat matici A ve tvaru

   $$A = E + p^{k-1-s} A', \ A' \in \mathbb{Z}_{p^{s+1}}^{m,m} \ .$$

   Dosadíme do rovnosti $aA = a + e$ za matici A a dostaneme:

   $$aA = a(E + p^{k-s-1}A') = aE + ap^{k-s-1}A' = a + ap^{k-1-s}A' = a + e \ \backslash mod \, p^k$$

   $$ap^{k-s-1}A' = e \ \backslash mod \, p^k \ .$$

   Dále dosadíme za prvek z jádra $e = p^{k-1}e', \ e' \in \mathbb{Z}_p^m$ a za $a = p^s a'$:

   $$p^s a' p^{k-s-1} A' = p^{k-1} a' A' = p^{k-1} e' \ \backslash mod \, p^k$$

vydělíme p^{k-1} a dostaneme soustavu m rovnic v tělese $\mathbb{Z}_p$:

$$a'A' = e' \ \backslash mod\, p \quad tj. \ \sum_{i=1}^{m} a'_i A'_{i,j} = e'_j \ \backslash mod\, p \quad \forall j \in \widehat{m} \ .$$

Dále musí být $det(E + p^{k-s-1}A') = 1 \ \backslash mod\, p^k$. Obdobným postupem jako v části 2.2 u důkazu 3. vlastnosti zobrazení odtud dostaneme podmínku:

$$\sum_{i=1}^{m} A'_{i,i} = 0 \ \backslash mod\, p^{s+1} \ .$$

Máme tedy řešit soustavu $m+1$ rovnic pro m^2 neznámých $A'_{i,j}$:

$$\sum_{i=1}^{m} A'_{i,i} = 0 \ \backslash mod\, p^{s+1}, \qquad \sum_{i=1}^{m} a'_i A'_{i,j} = e'_j \ \backslash mod\, p \quad \forall j \in \widehat{m}$$

Neboť $\delta(a', p^k) = 1 \ \Rightarrow \ \exists l \in \widehat{m} \ (a'_l)_{mod\, p} \neq 0$, existuje v tělese $\mathbb{Z}_p$ inverzní prvek k prvku $(a'_l)_{mod\, p}$ označme ho $a_l'^{-1}$ a systém rovnic lze převést na:

$$\sum_{i=1}^{m} A'_{i,i} = 0 \ \backslash mod\, p^{s+1}, \qquad A'_{l,j} = a_l'^{-1}(e'_j - \sum_{i=1, i\neq j}^{m} a'_i A'_{i,j}) \ \backslash mod\, p \quad \forall j \in \widehat{m}$$

Řešit tuto soustavu lze například tak, že spočteme prvek $A'_{l,l}$ z libovolně zvoleného zbytku l-tého slupce matice A' a z první rovnice dopočteme diagonální prvky matice A'. Pak podle zbývajících rovnic volbou dalších prvků dopočteme celý l-tý řádek. Tedy soustava má alespoň jedno řešení a $\sim$ ekvivalence prvků nenulové třídě kongruence je tím dokázána. □

Nyní definujeme zobrazení

$$\tilde{H} : \mathbb{Z}^m_{p^k}/_{kerH} \to \mathbb{Z}^m_{p^{k-1}}$$

předpisem:

$$\tilde{H}([a]) = H(a) = (a)_{mod\, p^{k-1}} \quad \forall [a] \in \mathbb{Z}^m_{p^k}/_{KerH} \ .$$

Toto zobrazení je zřejmě izomorfismus okruhů. Dále ukážeme, že zobrazení $\tilde{H}$ zachovává ekvivalenci:

$$[a], [b] \in \mathbb{Z}^m_{p^k}/_{KerH}, \quad [a] \approx [b] \ \Leftrightarrow \ \exists A \in SL(m, \mathbb{Z}_{p^k}) \quad [a]A = [b] \ \Leftrightarrow$$

$$\tilde{H}([a]A) = H(aA) = H(a)h(A) = \tilde{H}([a])h(A) = \tilde{H}([b]) = H(b)$$
$$\Leftrightarrow \ \exists A' = h(A) \in SL(m, \mathbb{Z}_{p^{k-1}}) \quad aA' = b \ \Leftrightarrow \ a \sim b \ .$$

Zobrazení $\tilde{H}$ je izomorfismus přenášející ekvivalenci oběma směry a tedy orbity v $\mathbb{Z}_{p^k}/_{KerH}$ a v $\mathbb{Z}_{p^{k-1}}$ si budou jedno jednoznačně odpovídat. Jak vypadají orbity v okruhu $\mathbb{Z}_{p^k}$ zjistíme

snadno. Díky tomu, že prvky ve třídách kongruence ve faktorokruhu $\mathbb{Z}_{p^k}/_{KerH}$ jsou navzájem $\sim$ ekvivalentní (vyjma třídy $[0] = KerH$, která se rozpadá na dvě orbity) budou orbity $\mathbb{Z}_{p^k}/_{KerH}$ (vyjma jádra $KerH$) v současně i orbitami v $\mathbb{Z}_{p^k}$, avšak ty budou mít $|KerH|$ krát více prvků. Neboť se jádro $KerH$ jako jediné rozpadá na dvě orbity, dostaneme pro počet $P(p^k)$ orbit v okruhu $\mathbb{Z}_{p^k}$ rekurentní vztah:

$$P(p^k) = P(p^{k-1}) + 1$$

a ze znalosti případu pro n prvočíselné, kde $P(p^1) = 2$ dostaneme:

$$P(p^k) = k + 1 \ . \tag{3.1}$$

Dále chceme zjistit jaký je tvar orbit a kolik mají prvků. Při každém indukčním kroku od $k-1$ ke k vzniká jedna nová orbita charakterizovaná největším společným dělitelem (nsd.) libovolného prvku a čísla n rovným p^{k-1}. V případě $k = 1$ máme pouze dvě orbity charakterizované pomocí nsd.:

1. $(0, \ldots, 0)$ $\qquad nsd. = p$
2. $(0, \ldots, 1)$ $\qquad nsd. = 1$

Předpokládejme tedy, že i v případě $k-1$ jsou všechny orbity charakterizovány pomocí nsd. svých prvků a čísla $n = p^{k-1}$. Vzor prvku $a \neq 0 \in \mathbb{Z}^m_{p^{k-1}}$ při zobrazení H je množina

$$H^{-1}(a) = a + KerH \subset \mathbb{Z}_{p^k}$$

a je-li

$$\delta(a, p^{k-1}) = p^j, \ \ j \in \mathbb{Z}_{k-1}$$

pak

$$\forall e \in KerH \qquad \delta(a + e, p^k) = p^j$$

a tedy všechny vzory tohoto prvku mají stejný nsd. s číslem $n = p^k$ jako tento prvek s číslem p^{k-1}. Vzor nulového prvku je jádro $KerH$ a v něm jsou obě orbity charakterizované pomocí nsd. s číslem $n = p^k$. Odtud plyne, že všechny orbity v okruhu $\mathbb{Z}_{p^k}$ jsou charakterizovány pomocí nsd. svých prvků s číslem $n = p^k$. Protože orbit v okruhu $\mathbb{Z}_{p^k}$ je $k+1$, stejně jako dělitelů čísla p^k, charakterizuje každé z čísel $1, p, p^2, p^3, \ldots, p^k$ právě jednu orbitu.

Počet prvků v orbitě charakterizované dělitelem $p^j, \ j \in \mathbb{Z}, \ 0 \leq j \leq k$ v okruhu $\mathbb{Z}_{p^k}$ označíme $Q(p^k, p^j)$. Počty prvků v orbitách, které vznikly rozpadem jádra $KerH$ již známe:

$$Q(p^k, p^k) = 1 \qquad Q(p^k, p^{k-1}) = p^m - 1 \ .$$

Ostatní orbity vznikají jako vzory nenulových orbit z okruhu $\mathbb{Z}_{p^{k-1}}$ při zobrazení H a počet jejich prvků bude proto $KerH = p^m$ krát větší než u jejich obrazů:

$$Q(p^k, p^j) = p^m Q(p^{k-1}, p^j) \qquad 0 \leq j \leq k-2 \ .$$

Z indukce pro ně dostaneme vzorec:

$$Q(p^k, p^j) = p^{(k-j-1)m} Q(p^{j+1}, p^j) = p^{(k-j-1)m}(p^m - 1) \qquad 0 \leq j \leq k-2 \ .$$

Celkem pro počet prvků v orbitě charakterizované pomocí nsd. $p^j,\ 0 \leq j \leq k$ v okruhu $\mathbb{Z}_{p^k}^m$ máme vzorec:

$$Q(p^k, p^j) = p^{(k-j)m}(1 - p^{-m})^{sgn(k-j)} \ . \tag{3.2}$$

Poznámka 3.3. $sgn(k-j)$ může nabývat pouze hodnot 0 *pro* $k = j$ a 1 *pro* $k > j$ a ve vzorci se vyskytuje kvůli případu $k = j$, kdy $O(k, j) = 1$.

3.1.3 Případ $n = pq,\ \delta(p, q) = 1,\ p, q \in \mathbb{N},\ p, q \geq 2$

V tomto případě definujeme zobrazení

$$G : \mathbb{Z}_{pq}^m \to \mathbb{Z}_p^m \times \mathbb{Z}_q^m$$

předpisem:

$$G(a) = ((a)_{mod\, p}, (a)_{mod\, q}) \qquad a \in \mathbb{Z}_{pq}^m$$

a ukážeme, že jde o izomorfismus okruhů.

Důkaz. Z definice je zřejmé, že jde o homomorfismus a zbývá tedy dokázat, že se jedná o bijekci tj. že

$$\forall (a^p, a^q) \in \mathbb{Z}_p^m \times \mathbb{Z}_q^m \ \exists_1 a \in \mathbb{Z}_{pq}^m \qquad G(a) = (a^p, a^q) \ .$$

Tedy

$$(a)_{mod\, p} = a^p \Rightarrow \ \exists m \in \mathbb{Z}_q \quad a = a^p + pm$$

$$(a)_{mod\, q} = a^q \Rightarrow \ \exists n \in \mathbb{Z}_p \quad a = a^q + qn$$

$$a^p + pm = a^q + qn \ \backslash mod\, pq$$

$$a^p + pm = a^q + qn \ \backslash mod\, p \quad \wedge \quad a^p + pm = a^q + qn \ \backslash mod\, q$$

$$a^p = a^q + qn \ \backslash mod\, p \quad \wedge \quad a^p + pm = a^q \ \backslash mod\, q \ .$$

Neboť p a q jsou nesoudělná čísla existuje v okruhu $\mathbb{Z}_p^m$ ($\mathbb{Z}_q^m$) inverzní prvek k prvku $(q)_{mod\, p}$ ($(p)_{mod\, q}$) označme ho p^{-1} (q^{-1}):

$$n = q^{-1}(a^p - a^q) \ \backslash mod\, p \quad \wedge \quad m = p^{-1}(a^q - a^q) \ \backslash mod\, q \ .$$

Čísla m, n a tedy i vzor jsou určeny jednoznačně a tedy zobrazení je bijektivní. □

Dále musíme určit jak vypadají orbity na kartézském součinu okruhů $\mathbb{Z}_p^m \times \mathbb{Z}_q^m$. Definujeme zde tedy akci grupy $SL(m, \mathbb{Z}_p) \times SL(m, \mathbb{Z}_q)$ jako násobení zprava po složkách :

$$a = (a^1, a^2) \in \mathbb{Z}_p^m \times \mathbb{Z}_q^m,\ A = (A^1, A^2) \in SL(m, \mathbb{Z}_p) \times SL(m, \mathbb{Z}_q)$$

$$aA = (a^1, a^2)(A^1, A^2) = (a^1 A^1, a^2 A^2) \ .$$

Dále zde definujeme ekvivalenci indukovanou touto akcí:

$$a = (a^1, a^2), b = (b^1, b^2) \in \mathbb{Z}_p^m \times \mathbb{Z}_q^m \quad a \sim b \ \Leftrightarrow \ \exists A = (A^1, A^2) \in SL(m, \mathbb{Z}_p) \times SL(m, \mathbb{Z}_q)$$

$$aA = b \ \Leftrightarrow \ a^1 \sim b^1 \ \wedge \ a^2 \sim b^2 \ .$$

Přímo z definice vidíme, že orbity na kartézském součinu okruhů $\mathbb{Z}_p^m \times \mathbb{Z}_q^m$ jsou kartézským součinem orbit na jednotlivých okruzích.

Podíváme se ještě jak působí zobrazení G na prvek $aA,\ a \in \mathbb{Z}_p^m \times \mathbb{Z}_q^m,\ A \in SL(m, \mathbb{Z}_p) \times SL(m, \mathbb{Z}_q)$:

$$G(aA) = ((aA)_{mod\, p}, (aA)_{mod\, q}) = ((a)_{mod\, p}, (a)_{mod\, q})((A)_{mod\, p}, (A)_{mod\, q}) = G(a)g(A)$$

kde g je izomorfismus grup definovaný v 2.17. Dokážeme, že toto zobrazení přenáší ekvivalenci oběma směry tj. $a, b \in \mathbb{Z}_p^m \times \mathbb{Z}_q^m \quad a \sim b \ \Leftrightarrow \ G(a) \sim G(b)$.

Důkaz. Neboť G i g jsou bijekce platí:

$$a \sim b \ \Leftrightarrow \ \exists A \in SL(m, \mathbb{Z}_{pq}) \qquad aA = b \ \Leftrightarrow \ G(a)g(A) = G(b) \ \Leftrightarrow$$

$$\exists A' = g(A) \in SL(m, \mathbb{Z}_p) \times SL(m, \mathbb{Z}_q) \qquad G(a)A' = G(b) \ \Leftrightarrow \ \ G(a) \sim G(b) \ .$$

□

Protože je zobrazení G izomorfismus a přenáší ekvivalenci oběma směry budou orbity v okruhu $\mathbb{Z}_{pq}^m$ jedno jednoznačně odpovídat orbitám v kartézském součinu okruhů $\mathbb{Z}_p^m \times \mathbb{Z}_q^m$. Předpokládejme, že v okruhu $\mathbb{Z}_p^m$ resp. $\mathbb{Z}_q^m$ jsou orbity charakterizovány největším společným dělitelem prvků a čísla p resp. q, pak díky nesoudělnosti čísel p a q budou i odpovídající orbity na okruhu $\mathbb{Z}_{pq}^m$ charakterizovány největšími společnými děliteli prvků s číslem $n = pq$. Neboť číslo p resp. q lze zapsat jako součin mocnin prvočísel a u mocnin prvočísel tento předpoklad platí bude platit i pro p a q. Počet orbit bude:

$$P(pq) = P(p)P(q) \ . \tag{3.3}$$

Počet prvků v orbitě bude:

$$Q(pq, p_1 q_1) = Q(p, p_1)Q(q, q_1) \tag{3.4}$$

kde p_1/p a q_1/q tedy p_1 dělí p resp. q_1 dělí q.

3.1.4 Případ $n \in \mathbb{N},\ n \geq 2$

Spojením výsledků předešlých tří kapitol dostáváme následující tvrzení.

Tvrzení 3.4. *Buď $m, n \in \mathbb{N},\ m, n \geq 2$ a nechť $n = \prod_{i=1}^{r} p_i^{k_i},\ p_i \in \mathbb{P},\ k_i \in \mathbb{N},\ \forall i \in \widehat{r}$ je rozklad čísla n na součin mocnin prvočísel, pak počet orbit akce grupy $SL(m, \mathbb{Z}_n)$ na okruhu $\mathbb{Z}_n^m$ je roven počtu dělitelů čísla n tj.*

$$P(n) = \prod_{i=1}^{r} (k_i + 1) \ . \tag{3.5}$$

Orbity jsou jednoznačně určeny největším společným dělitelem svých prvků s číslem n a počet prvků v orbitě určené nsd. $d = \prod_{i=1}^{r} p_i^{l_i},\ 0 \leq l_i \leq k_i$ je

$$Q(n, d) = \prod_{i=1}^{r} p_i^{(k_i - l_i)m} (1 - p_i^{-m})^{sgn(k_1 - l_i)} \ . \tag{3.6}$$

3.2 Druhý způsob

V celé této části budeme uvažovat $n \in \mathbb{N},\ n \geq 2$, jehož rozklad na součin mocnin prvočísel je:

$$n = \prod_{i=1}^{r} p_i^{k_i}, \qquad p_i \in \mathbb{P},\ k_i \in \mathbb{N},\ i \in \hat{r} \ .$$

Víme, že při násobení prvku $a \in \mathbb{Z}_n^m$ maticí $A \in SL(m, \mathbb{Z}_n)$ se zachovává největší společný dělitel tohoto prvku s číslem n tj.

$$\delta(aA, n) = \delta(a, n) \ .$$

Vezmeme prvek $(0, \ldots, 1)$ a pokusíme se najít orbitu ve které leží. Obecně platí, že počet prvků v orbitě je dán podílem řádu grupy $SL(m, \mathbb{Z}_n)$ a řádu podgrupy stability libovolného prvku z této orbity. Podgrupu stability prvku $(0, \ldots, 1)$ již známe:

$$S_{(0,\ldots,1)} = \{A = \begin{pmatrix} & & & a_{1,m} \\ & A' & & a_{2,m} \\ & & & \vdots \\ 0 & 0 & \ldots & 1 \end{pmatrix} \in SL(m, \mathbb{Z}_n) |\ A' \in SL(m-1, \mathbb{Z}_n),\ a_{i,m} \in \mathbb{Z}_n,\ \forall i \in \widehat{m}\}$$

její řád je:

$$|S_{(0,\ldots,1)}| = n^{m^2 - m - 1} \prod_{i=1}^{r} \prod_{j=2}^{m-1} (1 - p_i^{-j}) \ .$$

Tedy počet prvků v orbitě obsahující prvek $(0, \ldots, 1)$ bude:

$$P((0, \ldots, 1)) = n^m \prod_{i=1}^{r} (1 - p_i^m) \ . \tag{3.7}$$

Dále určíme počet všech prvků z okruhu $\mathbb{Z}_n^m$ nesoudělných s číslem n. Za tímto účelem definujeme Jordanovu funkci a uvedeme bez důkazu některé její vlastnosti (viz [3]).

Definice 3.5. Pro $m \in \mathbb{N}$ je zobrazení $\varphi_m : \mathbb{N} \to \mathbb{N}$ definované předpisem:

$$\varphi_m(n) = |\{(a_1, a_2, \dots, a_m) \in \{1, \dots, n\}^m | \delta(a_1, a_2, \dots, a_m, n) = 1\}|$$

Jordanova funkce řádu m.

Tvrzení 3.6. *Pro každou Jordanovu funkci φ_m, $m \in \mathbb{N}$ a $n \in \mathbb{N}$ platí:*

1.

$$\varphi_m(n) = n^m \prod_{p/n,\ p \in \mathbb{P}} (1 - p^{-m}) \ . \tag{3.8}$$

2.

$$\sum_{d/n,\ d \in \mathbb{N}} \varphi_m(d) = n^m \tag{3.9}$$

3.

$$\begin{aligned} \varphi_m(\frac{n}{d}) &= |\{(a_1, a_2, \dots, a_m) \in \{1, \dots, \frac{n}{d}\}^m \mid \delta(a_1, a_2, \dots, a_m, \frac{n}{d}) = 1\}| \\ &= |\{(a_1, a_2, \dots, a_m) \in \{1, \dots, n\}^m \mid \delta(a_1, a_2, \dots, a_m, n) = d\}| \end{aligned} \tag{3.10}$$

Jordanova funkce $\varphi_m(n)$ udává počet prvků okruhu $\mathbb{Z}_n^m$ nesoudělných s číslem n. Tento počet je roven počtu prvků hledané orbity 3.7 a odtud plyne, že hledaná orbita je složená právě z prvků nesoudělných s číslem n. Tedy máme orbitu

$$O(n, 1) = \{a \in \mathbb{Z}_n^m | \ \delta(a, n) = 1\} \ .$$

Definice 3.7. Pro $d \in \hat{n},\ d/n$ definujeme zobrazení

$$F^d : \mathbb{Z}_n^m \to \mathbb{Z}_n^m$$

předpisem:

$$F^d(a) = (d.a)_{mod\, n} \qquad \forall a \in \mathbb{Z}_n^m \ .$$

Lemma 3.8. *Nechť $d \in \hat{n},\ d/n$, pak pro $a, b \in \mathbb{Z}_n^m$ platí:*

$$a \sim b \Rightarrow F^d(a) \sim F^d(b) \ .$$

Důkaz.

$$a, b \in \mathbb{Z}_n^m \quad a \sim b \ \Leftrightarrow \ \exists A \in SL(m, \mathbb{Z}_n) \quad aA = b \ \Rightarrow \ F^d(aA) = F^d(b)$$

$$F^d(aA) = (daA)_{mod\, n} = (da)_{mod\, n}(A)_{mod\, n} = F^d(a)A = F^d(b) \ \Rightarrow \ F^d(a) \sim F^d(b)$$

□

Obrazem naší orbity $O(n,1)$ při zobrazení F^d je množina všech prvků, jejichž nsd. s číslem n je d. A neboť v orbitě jsou všechny prvky navzájem ekvivalentní jsou i prvky v této množině navzájem ekvivalentní a jde tedy o orbitu. Jednotlivé orbity jsou tedy charakterizovány největším společným dělitelem svých prvků a čísla n Orbit v okruhu $\mathbb{Z}_n^m$ je stejně jako dělitelů čísla n. Počty prvků v orbitách lze získat buď spočtením prvků s daným nsd. nebo pomocí řádu podgrupy stability reprezentantů. Prvním způsobem dostaneme pro počet prvků v orbitě určené dělitelem d vzorec:

$$Q(n,d) = \varphi_m(\frac{n}{d}) = (\frac{n}{d})^m \prod_{p/\frac{n}{d},\ p\in\mathbb{P}} (1 - p^{-m}) \ . \tag{3.11}$$

4 Orbity ace grupy $SL(2,\mathbb{Z}_n)$ na okruhu $(\mathbb{Z}_n^2)^2$

Nejprve zavedeme následující označení:

$$\begin{aligned} G &= SL(4,\mathbb{Z}_n) \\ G_1 &= \{A_1 \oplus A_2 = diag(A_1,A_2) \mid A_1, A_2 \in SL(2,\mathbb{Z}_n)\} \\ G_2 &= \{A \oplus A = diag(A,A) \mid A \in SL(2,\mathbb{Z}_n)\}. \end{aligned}$$

Množiny G,G_1 a G_2 spolu s operací násobení matic a příslušné modulo n jsou zřejmě grupy. Z následujícího lemma plyne, že jsou to dokonce podgrupy

$$G_2 \subset\subset G_1 \subset\subset G \ .$$

Lemma 4.1. *Buďte $A \in \mathbb{Z}_n^r,\ B \in \mathbb{Z}_n^s$, pak $det(A \oplus B) = detA.detB$.*

Důkaz.

$$det(A \oplus B) = \sum_{\pi \in S_{r+s}} sgn(\pi) \prod_{i=1}^{r} A_{i,\pi(i)} \prod_{j=r+1}^{r+s} B_{j,\pi(j)} =$$

$$= \sum_{\rho \in S_r,\ \sigma \in S_s} sgn(\rho)sgn(\sigma) \prod_{i=1}^{r} A_{i,\rho(i)} \prod_{j=1}^{s} B_{j,\sigma(j)} =$$

$$= \sum_{\rho \in S_r} sgn(\rho) \prod_{i=1}^{r} A_{i,\rho(i)} \sum_{\sigma \in S_s} sgn(\sigma) \prod_{j=1}^{m} B_{j,\sigma(j)} = detA.detB$$

□

Prvky okruhu $(\mathbb{Z}_n^2)^2 = \mathbb{Z}_n^2 \times \mathbb{Z}_n^2$ budeme chápat jako dvojice dvousložkových vektorů tj. $a \in (\mathbb{Z}_n^2)^2,\ a = (a^1,a^2) = ((a_1^1,a_2^1),(a_1^2,a_2^2)) \quad a_j^i \in \mathbb{Z}_n,\ i,j = 1,2$ a akci grupy $SL(2,\mathbb{Z}_n)$ na tomto okruhu jako násobení vektorů maticí $A \in SL(2,\mathbb{Z})$ tj.

$$aA = (a^1A, a^2A) \ .$$

Ve skutečnosti je okruh $(\mathbb{Z}_n^2)^2$ shodný s okruhem $\mathbb{Z}_n^4$ 4-složkových vektorů a výše definovaná akce s akcí grupy G_2 definovanou jako násobení řádkového vektoru maticí $A \in G_2$ zprava. Na okruhu $\mathbb{Z}_n^2 \times \mathbb{Z}_n^2$ tak můžeme definovat i akce grup G a G_1 jako násobení maticemi zprava. Vzhledem k tomu, že G_2 je podgrupa grupy G_1 a to je podgrupa grupy G, bude pro ekvivalence indukované jednotlivými akcemi platit vztah:

$$a,b \in \mathbb{Z}_n^2 \times \mathbb{Z}_n^2 \qquad a \sim_{G_2} b \ \Rightarrow\ a \sim_{G_1} b \ \Rightarrow\ a \sim_G b \ .$$

Orbity akce grupy G (nadále G orbity) se tedy budou skládat z orbit akce grupy G_1 (nadále G_1 orbity) a ty se budou skládat z orbit akce grupy G_2 (nadále jen orbit). Odtud plyne, že lze vyšetřovat jednotlivé G_1 orbity odděleně. G orbity známe z minulé kapitoly a G_1 orbity jsou zřejmě kartézské součiny orbit akce grupy $SL(2,\mathbb{Z}_n)$ na $\mathbb{Z}_n^2$.

Poznámka 4.2. Budeme-li nadále mluvit o G, G_1 a G_2 grupách, orbitách resp. ekvivalenci, budeme tím mínit tyto struktury definované pro příslušné n. Dále budeme o G_2 orbitách resp. ekvivalenci mluvit jako o $SL(2,\mathbb{Z}_n)$ orbitách resp. ekvivalenci.

Již víme, že při akci grupy $Sl(2,\mathbb{Z}_n)$ se bude zachovávat největší společný dělitel jednotlivých částí prvku a čísla n tj. $a=(a^1,a^2)\in\mathbb{Z}_p^2\times\mathbb{Z}_p^2,\ A\in SL(2\mathbb{Z}_n)$:

$$\delta(a^i,n)=\delta(a^iA,n)\,,\qquad i=1,2\,.$$

Dále ukážeme, že se bude zachovávat i determinant matice sestavené ze složek našeho prvku:

$$det\begin{pmatrix} a_1^1 & a_2^1\\ a_1^2 & a_2^2\end{pmatrix}=a_1^1a_2^2-a_2^1a_1^2$$

$$det\begin{pmatrix} a_1^1A_{1,1}+a_2^1A_{2,1} & a_1^1A_{1,2}+a_2^1A_{2,2}\\ a_1^2A_{1,1}+a_2^2A_{2,1} & a_1^2A_{1,2}+a_2^2A_{2,2}\end{pmatrix}=det(\begin{pmatrix} a_1^1 & a_2^1\\ a_1^2 & a_2^2\end{pmatrix}A)=$$
$$=det\begin{pmatrix} a_1^1 & a_2^1\\ a_1^2 & a_2^2\end{pmatrix}detA=det\begin{pmatrix} a_1^1 & a_2^1\\ a_1^2 & a_2^2\end{pmatrix}$$

4.1 Orbity na $\mathbb{Z}_n^2\times\mathbb{Z}_n^2$ pro $n=p\in\mathbb{P}$ prvočíslo

Nechť $n=p\in\mathbb{P}$. Následující diagram zachycuje rozklad okruhu postupně na G a G_1 orbity. Orbity znázorňujeme pomocí jejich reprezentantů uzavřených v hranatých závorkách a podle příslušné grupy:

G	*orbita*	$[(0,0,0,1)]$
G_1	*orbita*	$[(0,0)\times(0,1)]=[(0,0)]\times[(0,1)]$
G_2	*orbita*	$[((0,0),(0,1))]\,.$

$$\begin{array}{rcll}
\mathbb{Z}_p^2\times\mathbb{Z}_p^2\longrightarrow\overbrace{[(0,0,0,0)]}^{G} & \longrightarrow & \overbrace{[(0,0)\times(0,0)]}^{G_1}\longrightarrow\overbrace{[((0,0),(0,0))]}^{G_2}\\
\longrightarrow[(0,0,0,1)] & \longrightarrow & [(0,0)\times(0,1)]\longrightarrow[((0,0),(0,1))]\\
 & \longrightarrow & [(0,1)\times(0,0)]\longrightarrow[((0,1),(0,0))]\\
 & \longrightarrow & [(0,1)\times(0,1)]\longrightarrow\ ?
\end{array}$$

První řádek diagramu symbolizuje jednobodovou orbitu obsahující pouze nulový prvek. Orbity na druhém a třetím řádku jsou až na pořadí nulového a nenulového vektoru stejné, jsou totiž vytvořeny jako kartézský součin orbit $[(0,1)]$ a $[(0,0)]$ v $\mathbb{Z}_p^2$. Tyto orbity zřejmě rovnou G_2 orbitami. Zbývá tedy určit rozklad G_1 orbity $[(0,1)^2]=[(0,1)\times(0,1)]$ na G_2 orbity. K tomu dospějeme následující úvahou. Bod $(0,1)$ je $SL(2,\mathbb{Z}_p)$ ekvivalentní se všemi body v orbitě $[(0,1)]=\mathbb{Z}_p^2\backslash(0,0)$ kterou reprezentuje a proto v každé G_2 orbitě v $[(0,1)^2]$ musí ležet bod jehož první část tvoří vektor $(0,1)$ tj. bod tvaru $((0,1),(\dots))$. Zjistíme-li počet navzájem G_2 neekvivalentních bodů tohoto typu dostaneme počet G_2 orbit v $[(0,1)^2]$, neboť

každý z těchto bodů je reprezentantem nějaké orbity. Chceme-li zkoumat ekvivalenci bodů typu $((0,1),(\dots))$ musíme uvažovat pouze takové matice, které při akci nemění první část těchto bodů tj. matice z podgrupy stability bodu $(0,1)$. Protože se první část bodů nemění lze zkoumat druhou část samostatně. Uděláme tedy rozklad orbity $[(0,1)]$ podle podgrupy stability bodu $(0,1)$. Podgrupa stability bodu $(0,1)$ je:

$$S_{(0,1)} = \{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \ | b \in \mathbb{Z}_p\}$$

Vezmeme prvek $(a_1, a_2) \in [(0,1)]$ vynásobíme ho maticí z $S_{(0,1)}$:

$$(a_1, a_2)\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = (a_1, a_1 b + a_2)$$

a budeme hledat prvky, na které lze převést v závislosti na jeho tvaru. První složka se při násobení maticí nemění, a tedy prvky s různou první složkou leží v různých orbitách. Podíváme se co se děje s druhou složkou:

1. $a_1 = 0 \Rightarrow a_2 \neq 0 \quad (0, a_2) \to (0, a_2)$
2. $a_1 \neq 0 \Rightarrow (a_1, a_2) \to (a_1, x)$, $kde\ x = a_1 b + a_2$ a neboť pracujeme v tělese může x nabývat libovolné hodnoty, což lze zařídit volbou $b = a_1^{-1}(x - a_2)$.

Odtud dostaneme orbity akce grupy $S_{(0,1)}$ na $[(0,1)]$:

- $[(0, a_2)] \quad kde\ a_2 \in \mathbb{Z}_p \backslash 0 \ \dots\ p-1$ orbit jednobodových
- $[(a_1, 0)] \quad kde\ a_1 \in \mathbb{Z}_p \backslash 0 \ \dots\ p-1$ orbit p-bodových.

Body z různých orbit jsou $S_{(0,1)}$ neekvivalentní a tedy odpovídají G_2 neekvivalentním bodům typu $((0,1),(\dots))$ a počet těchto bodů odpovídá počtu G_2 orbit na $[(0,1)^2]$. Počty bodů v orbitách získáme pomocí řádu podgrup stability jejich reprezentantů.

1. Podgrupa stability bodu $((0,1),(0,a_2)) \quad a_2 \in \mathbb{Z}_p \backslash 0$ je přímo $S_{(0,1)}$ a tedy má řád $|S_{(0,1)}| = p$. Uděláme-li levý rozklad grupy $SL(2, \mathbb{Z}_p)$ na třídy ekvivalence podle její podgrupy $S_{(0,1)}$ dostaneme

   $$\frac{|SL(2,\mathbb{Z}_p)|}{|S_{(0,1)}|} = \frac{p^2(p-1)}{p} = p(p-1)$$

   tříd ekvivalence. Každá třída vyrobí akcí z našeho reprezentanta právě jeden prvek. Počet prvků v orbitě $[((0,1),(0,a_2))]$ tedy je : $p(p-1)$.

2. Podgrupa stability bodu $((0,1),(a_1,0)) \quad a_1 \in \mathbb{Z}_p \backslash 0$ je tvořena maticí $diag(1,1)$ a tedy počet prvků v orbitě $[((0,1),(a_1,0))]$ je: $p^2(p-1)$.

Počet prvků v dané orbitě lze získat i jinak, a to z úvahy, že bod $(0,1)$ jde převést na p^2-1 bodů a počet bodů v orbitě tedy bude roven součinu tohoto čísla s počtem bodů v odpovídající $S_{(0,1)}$ orbitě. Tedy můžeme zakreslit jak se rozloží orbita $[(0,1)^2]$:

$$\begin{array}{rcll} [(0,1)\times(0,1)] & \longrightarrow & [((0,1),(0,a_2))]\ kde\ a_2 \in \mathbb{Z}_p\backslash 0 \ldots p-1\ orbit & p^2-1\ bodových \\ & \longrightarrow & [((0,1),(a_1,0))]\ kde\ a_1 \in \mathbb{Z}_p\backslash 0 \ldots p-1\ orbit & p(p^2-1)\ bodových. \end{array}$$

V první skupině orbit tj. $[((0,1),(0,a_2))]$ je determinant $det\begin{pmatrix} 0 & 1 \\ 0 & a_2 \end{pmatrix} = 0$ nulový a proto zde body mají úměrnou první a druhou složku. Orbity v této skupině se navzájem liší koeficientem úměrnosti, jímž je právě číslo a_2. Ve druhé skupině jsou orbity charakterizovány determinantem bodů $-det\begin{pmatrix} 0 & 1 \\ a_1 & 0 \end{pmatrix} = a_1$.

Celkem jsme získali v okruhu $\mathbb{Z}_p^2 \times \mathbb{Z}_p^2$

$$P_2(p) = 2p+1 \tag{4.1}$$

orbit:

- $[((0,0),(0,0))]$ ... jednobodová orbita
- $[((0,0),(0,1))]$ ... p^2-1 bodová orbita
- $[((0,1),(0,0))]$ ... p^2-1 bodová orbita
- $[((0,1),(0,a_2))]$ $kde\ a_2 \in \mathbb{Z}_p\backslash 0$ ... $p-1$ orbit p^2-1 bodových
- $[((0,1),(a_1,0))]$ $kde\ a_1 \in \mathbb{Z}_p\backslash 0$ ... $p-1$ orbit $p(p^2-1)$ bodových.

Nakonec se podíváme jak najít orbitu, do které patří obecný bod $((a_1^1,a_2^1),(a_1^2,a_2^2)) \in \mathbb{Z}_p^2 \times \mathbb{Z}_p^2$. Postup je následující:

1. Určíme největšího společného dělitele první a druhé složky bodu s číslem p tj. $\delta(a^1,p)$, $\delta(a^2,p)$. Pokud $\delta(a^1,p)\delta(a^1,p)=0$ pak bod patří do orbity $[((0,\delta(a^1,p)),(0,\delta(a^2,p))]$. V opačném případě pokračujeme.

2. Spočteme determinant $-det\begin{pmatrix} a_1^1 & a_2^1 \\ a_1^2 & a_2^2 \end{pmatrix} = D\ \backslash mod\, p$. Pokud $D \neq 0$ pak bod patří do orbity $[((0,1),(D,0))]$. Pokud $D=0$ pak pokračujeme.

3. Nechť např. pro $i=1$ platí $\delta(a_i^1,p)=1$ pak řešíme rovnici: $a_i^1 x = a_i^2\ \backslash mod\, p$, což v tělese $\mathbb{Z}_p$ dává $x=(a_i^1)^{-1}a_i^2\ \backslash mod\, p$ a bod patří do orbity: $[((0,1),(0,x))]$.

4.2 Orbity na $\mathbb{Z}_n^2 \times \mathbb{Z}_n^2$ pro $n = p^k,\ p \in \mathbb{P},\ k \in \mathbb{N},\ k \geq 2$

Nechť $n = p^k,\ p \in \mathbb{P},\ k \in \mathbb{N},\ k \geq 2$. Začneme opět znázorněním již známých G a G_1 orbit na okruhu $\mathbb{Z}_{p^k}^2 \times \mathbb{Z}_{p^k}^2$.

$$
\begin{array}{lll}
\mathbb{Z}_{p^k}^2 \times \mathbb{Z}_{p^k}^2 & \overbrace{\longrightarrow [(0,0,0,0)]}^{G} & \left.\begin{array}{l} \\ \\ \\ \\ \end{array}\right\} \quad (a) \\
& \longrightarrow [(0,0,0,p^{k-1}] & \\
& \longrightarrow [(0,0,0,p^{k-2}] & \\
& \vdots & \\
& \longrightarrow [(0,0,0,p)] & \\
\longrightarrow [(0,0,0,1)] & \overbrace{\longrightarrow [(0,1)\times(0,1)]}^{G_1} & \} \quad (b) \\
& \longrightarrow [(0,p)\times(0,1)] & \left.\begin{array}{l} \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{array}\right\} \quad (c) \\
& \longrightarrow [(0,p^2)\times(0,1)] & \\
& \vdots & \\
& \longrightarrow [(0,p^{k-1})\times(0,1)] & \\
& \longrightarrow [(0,0)\times(0,1)] & \\
& \longrightarrow [(0,1)\times(0,p)] & \\
& \longrightarrow [(0,1)\times(0,p^2)] & \\
& \vdots & \\
& \longrightarrow [(0,1)\times(0,p^{k-1})] & \\
& \longrightarrow [(0,1)\times(0,0)] &
\end{array}
$$

Budeme postupovat indukcí podle k. G_2 orbity v případě $k = 1$ již známe. Předpokládejme, že také známe G_2 orbity v případě $k - 1$.

4.2.1 Orbity (a)

Definujeme zobrazení

$$F : \mathbb{Z}_{p^k}^2 \times \mathbb{Z}_{p^k}^2 \backslash [(0,0,0,1)] \to \mathbb{Z}_{p^{k-1}}^2 \times \mathbb{Z}_{p^{k-1}}^2$$

předpisem:

$$F(a) = (a)_{div\, p} \qquad a \in \mathbb{Z}_{p^k}^2 \times \mathbb{Z}_{p^k}^2 \backslash [(0,0,0,1)]\ .$$

Toto zobrazení je zřejmě bijekce, neboť prvky $\mathbb{Z}_{p^k}^2 \times \mathbb{Z}_{p^k}^2 \backslash [(0,0,0,1)]$ jsou právě p násobky prvků z $\mathbb{Z}_{p^{k-1}}^2 \times \mathbb{Z}_{p^{k-1}}^2$. Dále se podíváme jak působí zobrazení F na prvek $aA,\ a \in \mathbb{Z}_{p^k}^2 \times \mathbb{Z}_{p^k}^2 \backslash [(0,0,0,1)],\ A \in SL(2, \mathbb{Z}_{p^k})$

$$F(aA) = ((aA)_{mod\, p^k})_{div\, p} = (a)_{div\, p}(A)_{mod\, p^{k-1}} = F(a)h(A)$$

kde h je epimorfismus grup definovaný v 2.15. Díky výše uvedeným vlastnostem zobrazení F platí:

$$a, b \in \mathbb{Z}_{p^k}^2 \times \mathbb{Z}_{p^k}^2 \backslash [(0,0,0,1)] \qquad a \sim_{G_2} b \ \Leftrightarrow\ \exists A \in SL(2, \mathbb{Z}_{p^k}) \quad aA = b \ \Leftrightarrow$$

$$\Leftrightarrow\ F(aA) = F(b)\ \Leftrightarrow\ \exists A' = h(A) \in SL(2, \mathbb{Z}_{p^{k-1}}) \quad F(a)A' = F(b)\ \Leftrightarrow F(a) \sim_{G_2} F(b)$$

a tedy obrazy dvou prvků jsou G_2 ekvivalentní právě tehdy jsou-li G_2 ekvivalentní tyto prvky. Zobrazení F je tedy bijekce a zachovává G_2 ekvivalenci. Odtud je již zřejmé, že G_2 orbity v $\mathbb{Z}_{p^k}^2 \times \mathbb{Z}_{p^k}^2 \backslash [(0,0,0,1)]$ a G_2 jsou p násobky orbit v $\mathbb{Z}_{p^{k-1}}^2 \times \mathbb{Z}_{p^{k-1}}^2$. Tedy počet orbit (a) bude:

$$P_2^{(a)}(p^k) = P_2(p^{k-1})\ .$$

4.2.2 Orbity (b)

V této části rozložíme G_1 orbitu $[(0,1) \times (0,1)]$ na G_2 orbity. Budeme postupovat obdobně jako u prvočísel v předchozí kapitole. V každé G_2 orbitě bude ležet alespoň jeden prvek typu $((0,1),(\dots))$. Najdeme-li všechny takové G_2 neekvivalentní prvky budeme znát i všechny orbity, neboť každý z těchto prvků bude reprezentovat nějakou orbitu. Uděláme tedy rozklad orbity $[(0,1)]$ podle podgrupy stability bodu $(0,1)$:

$$S_{(0,1)} = \{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \ | b \in \mathbb{Z}_{p^k} \}\ .$$

Vynásobíme obecný prvek $a = (a_1, a_2) \in \mathbb{Z}_{p^k}^2$ maticí $A \in S_{(0,1)}$ budeme zkoumat jaké prvky můžeme získat:

$$(a_1, a_2) \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = (a_1, a_1 b + a_2)\ .$$

Vidíme, že první složka se při násobení nemění a tedy body s různou první složkou budou ležet v různých $S_{(0,1)}$ orbitách. Druhou složku budeme vyšetřovat v závislosti na tvaru první složky. Víme, že vždy musí být alespoň jedna složka nesoudělná s číslem p^k.

1. $\delta(a_1, p^k) = 1$ označme $a_1 = a_1^N$ a hledáme čemu se může rovnat $a_1^N b + a_2 = x$. Zvolme $x \in \mathbb{Z}_{p^k}$ libovolně a zkusme najít b. Neboť je $\delta(a_1^N, p^k)$ existuje k a_1^N v okruhu $\mathbb{Z}_{p^k}$ inverzní prvek a platí
$$b = (a_1^N)^{-1}(a_2 - x) \quad \backslash mod\, p^k\ .$$
Tedy x může nabývat libovolné hodnoty. Odtud dostáváme p^k bodové orbity $[(a_1^N, 0)]$ určené svojí první složkou. počet těchto orbit je roven počtu čísel v okruhu $\mathbb{Z}_{p^k}$ nesoudělných s číslem p^k
$$p^k - p^{k-1}\ .$$

2. $\delta(a_1, p^k) = p^j,\ 1 \le j \le k$ pak $\exists a_1^N \in \mathbb{Z}_{p^{k-j}},\ \delta(a_1^N, p^k) = 1\ (pro\ j < k)\ resp.\ a_1^N = 0\ (pro\ j = k),\ a_1 = p^j a_1^N$. Druhá složka musí být nesoudělná s číslem p^k tj. $a_2 = a_2^N \in \mathbb{Z}_{p^k}$. Vezměme a_2^N pevně a zkusme, kolik bodů dostaneme: $a_1 b + a_2^N = a_1^N p^j b + a_2^N = x$.
$$a_1^N p^j b = 0\ \Leftrightarrow\ b = p^{k-j} c,\ c \in \mathbb{Z}_{p^j}$$
Pokud budeme postupně zvyšovat b, pak pro $b \in \mathbb{Z}_{p^{k-j}}$ dostaneme různé body, až pro $b = p^{k-j}$ dostaneme bod (a_1, a_2^N), který již máme (pro $b = 0$) a dále již žádné

nové body nezískáme. Odtud plyne, že počet bodů v orbitě bude p^{k-j}. Z rovnosti $(a_1^N p^j b + a_2^N)_{mod\, p^j} = (a_2^N)_{mod\, p^j}$ plyne, že v celé orbitě platí: $(a_2^N)_{mod\, p^j} = konst.$ Naopak ukážeme, že body $(a_1^N p^j, a_2^N), (a_1^N p^j, c_2^N)$ pro něž platí $(a_2^N)_{mod\, p^j} = (c_2^N)_{mod\, p^j}$ leží v jedné orbitě. Najdeme matici, která převede první z těchto bodů na druhý. První složky se nemění a pro druhé musí platit:

$$a_1^N p^j b + a_2^N = a_1^N p^j + c_2^N \quad \backslash mod\, p^k$$

$$a_1^N p^j b = a_1^N p^j + (c_2^N - a_2^N) \quad \backslash mod\, p^k$$

ale $(c_2^N - a_2^N)_{mod\, p^j} = 0$ a tedy $(c_2^N - a_2^N) = up^j,\ u \in \mathbb{Z}_{p^{k-j}}$

$$a_1^N b = a_1^N + u \quad \backslash mod\, p^{k-j}$$

K a_1^N existuje v okruhu $\mathbb{Z}_{p^{k-j}}$ inverzní prvek a tedy:

$$b = 1 + (a_1^N)^{-1} u \quad \backslash mod\, p^{k-j}\ .$$

Odtud vidíme, že orbita je kromě první složky určena i druhou složkou $a_2^N \in \mathbb{Z}_{p^j}$, $\delta(a_2^N, p) = 1$ a tedy počet orbit s danou první složkou $a_1^N p^j,\ 1 \le j \le k$ bude:

$$p^j - p^{j-1}\ .$$

Celkem jsme získali následující $S_{(0,1)}$ orbity:

$$[(p^j a_1^N, a_2^N)] \qquad 0 \le j \le k, \qquad a_1^N \in \mathbb{Z}_{p^{k-j}}, \qquad a_2^N \in \mathbb{Z}_{p^j}$$

kde index N značí nesoudělnost s číslem p^k tedy:

$$\delta(a_1^N, p^k) = 1 \quad pro\ j < k \quad resp. \quad a_1^N = 0 \quad pro \quad j = k$$

$$\delta(a_2^N, p^k) = 1 \quad pro\ 0 < j \quad resp. \quad a_2^N = 0 \quad pro\ j = 0$$

Počet bodů v orbitě je p^{k-j} a počet orbit pro dané j je:

$$p^k (1 - p^{-1})^{sgn(k-j)} (1 - p^{-1})^{sgn(j)}\ .$$

Podgrupa stability uvedených reprezentantů má řád:

$$|\{ \begin{pmatrix} 1 & cp^{k-j} \\ 0 & 1 \end{pmatrix} \mid c \in \mathbb{Z}_{p^j} \}| = p^j\ .$$

G_2 orbity v $[(0,1) \times (0,1)]$ tedy budou tvaru:

$$[(0,1), (a_1^N p^j, a_2^N)]$$

kde:

$$0 \le j \le k, \quad a_1^N \in \mathbb{Z}_{p^{k-j}}, \quad a_2^N \in \mathbb{Z}_{p^j}\ .$$

Počet bodů v orbitě bude:

$$\frac{|SL(2,\mathbb{Z}_{p^k})|}{p^j} = \frac{p^{k(2^2-1}(1-p^{-2})}{p^j} = p^{3k-j}(1-p^{-2}) \ .$$

Počet orbit pro dané j je:

$$p^k(1-p^{-1})^{sgn(k-j)}(1-p^{-1})^{sgn(j)} \ .$$

Celkový počet G_2 orbit v $[(0,1)\times(0,1)]$ je:

$$P_2^{(b)}(p^k) = \sum_{j=0}^{k} p^k(1-p^{-1})^{sgn(k-j)}(1-p^{-1})^{sgn(j)} = 2p^k(1-p^{-1}) + (k-1)p^k(1-p^{-1})^2 =$$

$$= p^k(1-p^{-1})(2+(k-1)(1-p^{-1})) \ .$$

Podíváme se ještě na charakteristiku orbit. Složka $p^j a_1^N$ je zřejmě opět minus determinant utvořený ze složek bodu. Pokud vezmeme reprezentanta $((0,1),(p^j a_1^N, a_2^N))$ a vynásobíme ho vhodnou maticí $A \in SL(2,\mathbb{Z}_{p^k})$ dostaneme libovolný prvek z $[((0,1),(p^j a_1^N, a_2^N))]$:

$$((0,1),(p^j a_1^N, a_2^N)) \begin{pmatrix} A_{1,1} & A_{1,2} \\ A_{2,1} & A_{2,2} \end{pmatrix} = ((A_{2,1},A_{2,2}),(A_{1,1}p^j a_1^N + A_{2,1}a_2^N, A_{1,2}p^j a_1^N + A_{2,2}a_2^N))$$

Odtud vidíme, že složka a_2^N nebude přímo koeficientem úměrnosti mezi prvním a druhým dvojvektorem, jako tomu bylo u prvočísel, ale stane se jím pokud na celý bod aplikujeme operaci $mod\, p^j$, a bude tedy dána řešením rovnice pro x: $A_{2,i}x = A_{2,i}a_2^N \ \backslash mod\, p^j$.

4.2.3 Orbity (c)

Zbývá prozkoumat dva typy orbit $[(0,1)\times(0,p^j)]$, $[(0,p^j)\times(0,1)]$, $0 < j \leq k$. Je zřejmé, že stačí vyšetřovat jen jeden z těchto typů, neboť druhý bude až na pořadí vektorů stejný. Budeme vyšetřovat typ $[(0,1)\times(0,p^j)]$. Z části 3.1.2 již víme, že zobrazení $H : \mathbb{Z}^2_{p^k} \to \mathbb{Z}^2_{p^{k-1}}$ definované předpisem: $H(a) = (a)_{mod\, p^{k-1}}$ je epimorfismus okruhů a že zachovává $\sim$ ekvivalenci (tj. ekvivalenci indukovanou grupou $SL(2,\mathbb{Z}_n)$). Také víme, že zobrazení $\tilde{H} : \mathbb{Z}^2_{p^k}/_{KerH} \to \mathbb{Z}^2_{p^{k-1}}$ definované předpisem: $\tilde{H}([a]) = H(a)$ je izomorfismus okruhů a zachovává $\sim$ ekvivalenci a tedy zobrazuje orbitu $[(0,1)]_{p^k} \subset \mathbb{Z}^2_{p^k}$ na orbitu $[(0,1)]_{p^{k-1}} \subset \mathbb{Z}_{p^{k-1}}$. Dále definujeme zobrazení $F : \mathbb{Z}^2_{p^k}\backslash[(0,1)] \to \mathbb{Z}^2_{p^{k-1}}$ předpisem: $F(a) = (a)_{div\, p}$. Zobrazení F je zřejmě bijekce a zachovává $\sim$ ekvivalenci, což lze snadno dokázat obdobným způsobem jako v případě (a). Důležité je, že zobrazení F zobrazuje bijektivně orbitu $[(0,p^j)]_{p^k}$ na orbitu $[(0,p^{j-1})]_{p^{k-1}}$.

Poznámka 4.3. Občas budeme pro přehlednost vyznačovat dolním indexem u orbit z jakého okruhu pochází.

Nyní zavedeme označení $[(0,1)]_{p^k}/_{KerH} = \{[a] = a + KerH \ | a \in [(0,1)] \subset \mathbb{Z}_{p^k}\}$ čímž míníme orbitu $[(0,1)] \in \mathbb{Z}_{p^k}$ faktorizovanou podle jádra $KerH$. Toto označení má smysl, jelikož jak již víme z 3.1.2 platí $a \in [(0,1)] \ \Rightarrow \ [a] \in [(0,1)]$. Dále definujeme zobrazení

$$L^j : [(0,1)]_{p^k}/_{KerH} \times [(0,p^j)]_{p^k} \to [(0,1)]_{p^{k-1}} \times [(0,p^{j-1})]_{p^{k-1}}$$

předpisem: $\forall([a^1],a^2) \in [(0,1)]_{p^k}/_{KerH} \times [(0,p^j)]_{p^{k-1}}$

$$L^j([a^1],a^2) = (H(a^1),F(a^2)) = ((a^1)_{mod\, p^{k-1}},(a^2)_{div\, p}) \ .$$

Takto definované zobrazení je zřejmě bijekce. Zkoumáme množinu $[(0,1)]_{p^k}/_{KerH} \times [(0,p^j)]_{p^k}$ s prvky tvaru $([a^1],a^2) = (a^1 + KerH, a^2) = \{(a^1 + e, a^2) | e \in KerH\}$. Vzniká otázka zda jsou prvky množin $([a^1],a^2)$ navzájem G_2 ekvivalentní:

$$(a^1,a^2) \sim_{G_2} (a^1 + e, a^2) \quad e \in KerH \ \Leftrightarrow \ \exists A \in SL(2,\mathbb{Z}_{p^k}) \quad (a^1A, a^2A) = (a^1 + e, a^2) \ .$$

Matici A budeme hledat ve tvaru

$$A = E + A'p^{k-1}, \ A' \in \mathbb{Z}_p^{2,2} \ .$$

Dostáváme podmínky:

$$a^1E + a^1A'p^{k-1} = a^1 + e \quad \backslash mod\, p^k$$
$$a^2E + a^2A'p^{k-1} = a^2 \quad \backslash mod\, p^k \ .$$

Neboť $\delta(a^2,p^k) = p^j, \ 0 < j \leq k$ je druhá z rovností splněna. Do první rovnosti dosadíme za $e = p^{k-1}e', \ e' \in \mathbb{Z}_p$ a dostaneme:

$$a^1A'p^{k-1} = e'p^{k-1} \quad \backslash mod\, p^k$$

$$a^1A' = e' \quad \backslash mod\, p \ .$$

Připojíme podmínku

$$1 = detA = det \begin{pmatrix} 1 + A'_{1,1}p^{k-1} & A'_{1,2}p^{k-1} \\ A'_{2,1}p^{k-1} & 1 + A'_{2,2}p^{k-1} \end{pmatrix} = 1 + A'_{1,1}p^{k-1} + A'_{2,2}p^{k-1} + (p^{k-1})^2 detA'$$

$$A'_{1,1} + A'_{2,2} = 0 \quad \backslash mod\, p^k$$

a dostaneme tak soustavu tří rovnic pro čtyři neznámé. Její řešitelností jsme se zabývali již v 3.1.2 (případ $s = 0$) a tedy víme, že řešení existuje. Prvky množin $([a^1],a^2)$ jsou navzájem G_2 ekvivalentní a zavedeme G_2 ekvivalenci i na množině $[(0,1)]_{p^k}/_{KerH} \times [(0,p^j)]_{p^k}$:

$$([a^1],a^2) \sim_{G_2} ([b^1],b^2) \ \Leftrightarrow \ \exists A \in SL(2,\mathbb{Z}_{p^k} \quad ([a^1]A, a^2A) = ([b^1],b^2) \ .$$

Podíváme se jak působí zobrazení L^j na bod $([a^1]A, a^2A)$:

$$L^j([a^1]A,a^2A) = (H(a^1A),F(a^2A)) = (H(a^1)h(A),F(a^2)h(A)) = L^j([a^1],a^2)h(A) \ .$$

Nakonec ukážeme, že zobrazení L^j zachovává G_2 ekvivalenci. Protože L^j je bijekce a h je surjektivní platí:

$$([a^1],a^2) \sim_{G_2} ([b^1],b^2) \;\Leftrightarrow\; \exists A \in SL(2,\mathbb{Z}_{p^k}) \quad ([a^1]A, a^2A) = ([b^1],b^2) \;\Leftrightarrow$$

$$\Leftrightarrow\; L^j([a^1]A, a^2A) = L^j([a^1],a^2)h(A) = L^j([b^1],b^2) \;\Leftrightarrow$$

$$\Leftrightarrow\; \exists A' = h(A) \in SL(2,\mathbb{Z}_{p^{k-1}}) \quad L^j([a^1],a^2)A' = L^j([b^1],b^2) \;\Leftrightarrow\; L^j([a^1],a^2) \sim_{G_2} L^j([b^1],b^2)\ .$$

G_2 orbity v $[(0,1)]_{p^k}/_{KerH} \times [(0,p^j)]_{p^k}$ a tedy i orbity v $[(0,1)]_{p^k} \times [(0,p^j)]_{p^k}$ jedno jednoznačně odpovídají G_2 orbitám v $[(0,1)]_{p^{k-1}} \times [(0,p^{j-1})]_{p^{k-1}}$. Počet prvků v orbitě z $[(0,1)]_{p^k} \times [(0,p^j)]_{p^k}$ bude $|KerH| = p^2$ krát větší, než počet prvků v odpovídající orbitě v $[(0,1)]_{p^{k-1}} \times [(0,p^{j-1})]_{p^{k-1}}$. Z indukce potom plyne, že pro $j < k$ bude počet G_2 orbit v $[(0,1)]_{p^k} \times [(0,p^j)]_{p^k}$ roven počtu G_2 orbit v $[(0,1)]_{p^{k-j}} \times [(0,1)]_{p^{k-j}}$ (pro $j = k$ bude jen jedna orbita) a počet prvků v těchto orbitách bude p^{2j} krát větší, než počet v odpovídajících G_2 orbitách v $[(0,1)]_{p^{k-j}} \times [(0,1)]_{p^{k-j}}$.

Jednotlivé G_2 orbity vzniklé z orbit prvního typu tj. $[(0,1) \times (0,p^{j_2})]_{p^k}$ budou tvaru:

$$[(0,1), p^{j_2}(p^{j_1}a_1^N, a_2^N)] \quad 0 < j_2 \le k, \quad 0 \le j_1 \le k - j_2, \quad a_1^N \in \mathbb{Z}_{p^{k-j_1-j_2}}, \quad a_2^N \in \mathbb{Z}_{p^{j_1}}$$

s počtem prvků:

$$p^{2j_2}p^{3(k-j_2)-j_1}(1-p^{-2}) = p^{3k-j_1-j_2}(1-p^{-2})\ .$$

Počet orbit pro dané j_1, j_2 je:

$$p^{k-j_2}(1-p^{-1})^{sgn(k-j_2-j_1)}(1-p^{-1})^{sgn(j_1)}\ .$$

Počet G_2 orbit vzniklých z G_1 orbity $[(0,1) \times (0,p^j)]_{p^k}$ je:

$$2p^{k-j}(1-p^{-1}) + (k-j-1)p^{k-j}(1-p^{-1})^2 \quad pro\ k > j$$

$$1 \quad pro\ k = j\ .$$

Počet G_2 orbit vzniklých z druhého typu G_1 orbit tj. z $[(0,p^{j_2}) \times (0,1)]_{p^k}$ bude stejný jako počet G_2 orbit prvního typu. Tyto orbity budou mít stejný počet prvků jako odpovídající orbity prvního typu a budou charakterizovány reprezentanty s prohozeným pořadím dvojvektorů. Nám se však bude hodit jiná charakteristika, kterou by jsme získali při jejich postupném odvození obdobném jako u orbit prvního typu:

$$[p^{j_2}(0,1), (p^{j_1}a_1^N, (a_2^N)^{sgn(k-j_2)})] \quad 0 < j_2 \le k, \quad 0 \le j_1 \le k - j_2, \quad a_1^N \in \mathbb{Z}_{p^{k-j_1-j_2}}, \quad a_2^N \in \mathbb{Z}_{p^{j_1}}$$

kde

$$(a_2^N)^{sgn(k-j_2)} = \begin{cases} a_2^N & pro\ k > j_2 \\ 1 & pro\ k = j_2\ . \end{cases}$$

Signum je zde uvedeno kvůli případu $j_2 = k$ ve kterém je jediná orbita $[((0,0),(0,1))]$. Celkový počet orbit v případě (c) bude:

$$P_2^{(c)}(p^k) = 2 + 2\sum_{j=1}^{k-1} 2p^{k-j}(1-p^{-1}) + (k-j-1)p^{k-j}(1-p^{-1})^2.$$

Nebo rekurentně:

$$P_2^{(c)}(p^k) = P_2^{(c)}(p^{k-1}) + P_2^{(b)}(p^{k-1}) = P_2(p^{k-1}) - P_2(p^{k-2}) + P_2^{(b)}(p^{k-1}) \ .$$

Vyřešili jsme postupně všechny tři případy orbit (a),(b),(c). Dáme-li tyto výsledky dohromady dostaneme G_2 orbity na okruhu $\mathbb{Z}_{p^k}^2 \times \mathbb{Z}_{p^k}^2$:

$$[p^{j_1}(0,1), p^{j_2}(p^{j_3}a_1^N, (a_2^N)^{sgn(k-j_1)})], \qquad 0 \le j_1, j_2 \le k, \quad 0 \le j_3 \le k - max(j_1, j_2) \tag{4.2}$$

$$a_1^N \in \mathbb{Z}_{p^{k-max(j_1,j_2)-j_3}}, \quad a_2^N \in \mathbb{Z}_{p^{j_3}} \ .$$

O tvaru ve kterém zde uvádíme reprezentanty budeme někdy mluvit jako o normalizovaném. Počet orbit pro dané j_1, j_2, j_3 je: Počet bodů v dané orbitě je:

$$Q(p^k; p^{j_1}, p^{j_2}, p^{j_3}) = p^{3k-2min(j_1,j_2)-max(j_1,j_2)-j_3}(1-p^{-2})^{sgn(2k-j_1-j_2)} \ . \tag{4.3}$$

$$P(p^k; p^{j_1}, p^{j_2}, p^{j_3}) = p^{k-max(j_1,j_2)}(1-p^{-1})^{sgn(k-max(j_1,j_2)-j_3)}(1-p^{-1})^{sgn(j_3)} \ . \tag{4.4}$$

Celkový počet G_2 orbit v tomto případě je dán řešením rekurentního vztahu:

$$P_2(p^k) = P_2^{(a)}(p^k) + P_2^{(b)}(p^k) + P_2^{(c)}(p^k) = P_2(p^{k-1}) + P_2^{(b)}(p^k) + P_2(p^{k-1}) - P_2(p^{k-2}) + P_2^{(b)}(p^{k-1})$$

$$= 2P_2(p^{k-1}) - P_2(p^{k-2}) + P_2^{(b)}(p^k) + P_2^{(b)}(p^{k-1})$$

kde $P_2^{(b)}(p^k) = p^k(1-p^{-1})(2+(k-1)(1-p^{-1}))$, $P_2(p^1) = 2p+1$ a $P_2(p^2) = 3p^2+2p$. Tedy

$$P_2(p^k) = (k+1)p^k + kp^{k-1} \ . \tag{4.5}$$

Nakonec opět uvedeme návod jak určit ve které orbitě leží obecný bod $a \in \mathbb{Z}_{p^k}^2 \times \mathbb{Z}_{p^k}^2$, $a = ((a_1^1, a_2^1,), (a_1^2, a_2^2))$.

1. Určíme $\delta(a^1, p^k) = p^{j_1}$, $\delta(a^2, p^k) = p^{j_2}$, $min(j_1, j_2) = m$, $max(j_1, j_2) = M$. Pokud $M = k$ pak bod náleží do orbity $[((0, p^{j_1}), (0, p^{j_2}))]$, v opačném případě $M < k$ pokračujeme.

2. Přejdeme k bodu $b \in \mathbb{Z}_{p^{k-M}} \times \mathbb{Z}_{p^{k-M}}$.
   Pro $j_1 = j_2 \ \Rightarrow \ b = (a)_{div\, p^{j_1}}$
   $j_1 > j_2 \ \Rightarrow \ b = ((a^1)_{div\, p^{j_1}}, ((a^2)_{div\, p^{j_2}})_{mod\, p^{k-j_1}})$
   $j_1 < j_2 \ \Rightarrow \ b = (((a^1)_{div\, p^{j_1}})_{mod\, p^{k-j_2}}, (a^2)_{div\, p^{j_2}})$

3. Spočteme determinant $D = -\begin{pmatrix} b_1^1 & b_2^1 \\ b_1^2 & b_2^2 \end{pmatrix} \ \backslash mod\, p^{k-M}$ a určíme $\delta(D, p^{k-M}) = p^{j_3}$.

4. Nyní nechť např. pro $i = 1$ je $\delta(b_i^1, p^{k-M}) = 1$ řešíme rovnici $b_i^1 x = b_i^2 \ \backslash mod\, p^{j_3}$ tj. $x = (b_i^1)^{-1} b_i^2 \ \backslash mod\, p^{j_3}$. Bod tedy patří do orbity:

$$[((0, p^{j_1}), p^{j_2}(D, x))] \ .$$

4.3 Orbity na $\mathbb{Z}_n^2 \times \mathbb{Z}_n^2$ pro $n = pq,\ p,q \in \mathbb{P},\ \delta(p,q) = 1,\ p,q \geq 2$

Definujeme zobrazení $G : \mathbb{Z}_{pq}^2 \times \mathbb{Z}_{pq}^2 \to (\mathbb{Z}_p^2 \times \mathbb{Z}_p^2) \times (\mathbb{Z}_q^2 \times \mathbb{Z}_q^2)$ předpisem:

$$G(a^1, a^2) = ((a^1)_{mod p}, (a^2)_{mod p}, (a^1)_{mod q}, (a^1)_{mod q}) \qquad (a^1, a^2) \in \mathbb{Z}_{pq}^2 \times \mathbb{Z}_{pq}^2 \ .$$

Obdobným způsobem jako v 3.1.3 lze dokázat, že toto zobrazení je izomorfismus okruhů. Definujeme-li na kartézském součinu okruhů $(\mathbb{Z}_p^2 \times \mathbb{Z}_p^2) \times (\mathbb{Z}_q^2 \times \mathbb{Z}_q^2)$ akci grupy $SL(2, \mathbb{Z}_p) \times SL(2, \mathbb{Z}_q)$ jako násobení zprava:

$$a = (a^p, a^q) \in (\mathbb{Z}_p^2 \times \mathbb{Z}_p^2) \times (\mathbb{Z}_q^2 \times \mathbb{Z}_q^2),\ A = (A^p, A^q) \in SL(2, \mathbb{Z}_p) \times SL(2, \mathbb{Z}_q)$$

$$aA = (a^p, a^q)(A^p, A^q) = (a^p A^p, a^q A^q)$$

pak tato akce odpovídá akcím typu G_2, a o ekvivalenci indukované touto akcí budeme proto mluvit jako o G_2 ekvivalenci. G_2 orbity na tomto kartézském součinu okruhů budou přímo kartézské součiny G_2 orbit na jednotlivých okruzích $\mathbb{Z}_p^2 \times \mathbb{Z}_p^2$ a $\mathbb{Z}_q^2 \times \mathbb{Z}_q^2$. Prakticky stejným způsobem jako v 3.1.3 lze dokázat, že zobrazení G zachovává G_2 ekvivalenci. Odtud již plyne, že orbity v $\mathbb{Z}_{pq}^2 \times \mathbb{Z}_{pq}^2$ budou jedno jednoznačně odpovídat orbitám v $(\mathbb{Z}_p^2 \times \mathbb{Z}_p^2) \times (\mathbb{Z}_q^2 \times \mathbb{Z}_q^2)$ a tedy, že pro počet orbit bude platit:

$$P_2(pq) = P_2(p)P_2(q) \ .$$

Počty bodů v odpovídajících si orbitách budou stejné. Z nesoudělnosti čísel p, q plyne, že orbity budou opět rozděleny do skupin podle dělitelů čísla pq. Počty prvků v orbitách závisí pouze na skupině do které orbita patří a tedy bude platit:

$$Q(pq; p_1q_1, p_2q_2, p_3q_3) = Q(p; p_1, p_2, p_3)Q(q; q_1, q_2, q_3)$$

kde $p_l/p,\ q_l/q, \quad l = 1, 2, 3.$

Podíváme se ještě na tvary orbit v $\mathbb{Z}_{pq}^2 \times \mathbb{Z}_{pq}^2$ a to v případě, že p, q budou mocniny prvočísel. Nechť tedy $p = p_0^u,\ q = q_0^v,\ p_0, q_0 \in \mathbb{P},\ u, v \in \mathbb{N}$. Orbity v okruhu $\mathbb{Z}_p^2 \times \mathbb{Z}_p^2$ jsou tvaru:

$$[(p_0^{i_1}(0,1), p_0^{i_2}(p_0^{i_3}a_1^N, (a_2^N)^{sgn(u-i_1)}))], \quad 0 \leq i_1, i_2 \leq u,\ 0 \leq i_3 \leq u - max(i_1, i_2)$$

$$a_1^N \in \mathbb{Z}_{p_0^{u-max(i_1,i_2)-i_3}}, \quad a_2^N \in \mathbb{Z}_{p_0^{i_3}}$$

a orbity v okruhu $\mathbb{Z}_q^2 \times \mathbb{Z}_q^2$ jsou:

$$[(q_0^{j_1}(0,1), q_0^{j_2}(q_0^{j_3}b_1^N, (b_2^N)^{sgn(v-j_1)}))], \quad 0 \leq j_1, j_2 \leq v,\ 0 \leq j_3 \leq v - max(j_1, j_2)$$

$$b_1^N \in \mathbb{Z}_{q_0^{v-max(j_1,j_2)-j_3}}, \quad b_2^N \in \mathbb{Z}_{q_0^{j_3}} \ .$$

Ukážeme, že orbity na okruhu $\mathbb{Z}_{pq}^2 \times \mathbb{Z}_{pq}^2$ budou tvaru:

$$[(p_0^{i_1}q_0^{j_1}(0,1), p_0^{i_2}q_0^{j_2}(p_0^{i_3}q_0^{j_3}x_1^N, (x_2^N)^{sgn(pq-p_0^{i_1}q_0^{j_1})}))] \tag{4.6}$$

$$x_1^N \in \mathbb{Z}_{p_0^{u-max(i_1,i_2)-i_3} q_0^{v-max(j_1,j_2)-j_3}}, \quad x_2^N \in \mathbb{Z}_{p_0^{i_3} q_0^{j_3}} \ .$$

Z nesoudělnosti čísel p, q plyne, že skupina orbit určená děliteli $p_0^{i_l} q_0^{j_l}, \quad l = 1,2,3$ se zobrazí (při zobrazení G) na kartézské součiny orbit z výše uvedených skupin v okruzích $\mathbb{Z}_p^2 \times \mathbb{Z}_p^2$ a $\mathbb{Z}_q^2 \times \mathbb{Z}_q^2$ určených děliteli $p_0^{i_l},\ l = 1,2,3$ a $q_0^{j_l},\ l = 1,2,3$. Počet orbit v této skupině se tedy musí rovnat součin počtu orbit v odpovídajících skupinách v $\mathbb{Z}_p^2 \times \mathbb{Z}_p^2$ a $\mathbb{Z}_q^2 \times \mathbb{Z}_q^2$. Tedy číslu:

$$P(p_0^k; p_0^{i_1}, p_0^{i_2}, p_0^{i_3}) P(q_0^k; q_0^{j_1}, q_0^{j_2}, q_0^{j_3}) = p_0^{u-max(i_1,i_2)} q_0^{v-max(j_1,j_2)} (1-p_0^{-1})^{sgn(u-max(i_1,i_2)-i_3)}$$

$$(1-q_0^{-1})^{sgn(v-max(j_1,j_2)-j_3)} (1-p_0^{-1})^{sgn(i_3)} (1-q_0^{-1})^{sgn(j_3)} \ .$$

Počet orbit v naší skupině určíme z toho jak lze volit čísla x_1^N a x_2^N Počet prvků v množině $\mathbb{Z}_{p_0^{i_3} q_0^{j_3}}$ nesoudělných s číslem $p_0^{i_3} q_0^{j_3}$ udává Jordanova funkce (viz def. 3.5):

$$\varphi_1(p_0^{i_3} q_0^{j_3}) = p_0^{i_3} q_0^{j_3} (1-p_0^{-1})(1-q_0^{-1}) \ .$$

Vzorec jsme napsali pro případ $i_3, j_3 > 0$, v ostatních případech bude platit až po ošetření pomocí funkce sgn. Tedy počet možností jak volit $x_2^N \in \mathbb{Z}_{p_0^{i_3} q_0^{j_3}}$ je:

$$V(x_2^N) = p_0^{i_3} q_0^{j_3} (1-p_0^{-1})^{sgn(i_3)} (1-q_0^{-1})^{sgn(j_3)} \ .$$

Obdobně získáme počet možností jak volit $x_1^N \in \mathbb{Z}_{p_0^{u-max(i_1,i_2)-i_3} q_0^{v-max(j_1,j_2)-j_3}}$

$$V(x_1^N) = p_0^{u-max(i_1,i_2)-i_3} q_0^{v-max(j_1,j_2)-j_3} (1-p_0^{-1})^{sgn(u-max(i_1,i_2)-i_3)} (1-q_0^{-1})^{sgn(v-max(j_1,j_2)-j_3)} \ .$$

Součin těchto dvou čísel dává počet orbit v této skupině:

$$V(x_1^N) V(x_2^N) = p_0^{u-max(i_1,i_2)} q_0^{v-max(j_1,j_2)} (1-p_0^{-1})^{sgn(u-max(i_1,i_2)-i_3)}$$

$$(1-q_0^{-1})^{sgn(v-max(j_1,j_2)-j_3)} (1-p_0^{-1})^{sgn(i_3)} (1-q_0^{-1})^{sgn(j_3)} \ .$$

Počet orbit ve skupině 4.6 je tedy v pořádku. Zbývá ukázat, že uvedené orbity jsou navzájem různé. Zvolme tedy dva různé reprezentanty libovolných orbit ze skupiny 4.6:

$$x = (p_0^{i_1} q_0^{j_1}(0,1), p_0^{i_2} q_0^{j_2} (p_0^{i_3} q_0^{j_3} x_1^N, x_2^N)) \qquad y = (p_0^{i_1} q_0^{j_1}(0,1), p_0^{i_2} q_0^{j_2} (p_0^{i_3} q_0^{j_3} y_1^N, y_2^N))$$

$$x_1^N, y_1^N \in \mathbb{Z}_{p_0^{u-max(i_1,i_2)-i_3} q_0^{v-max(j_1,j_2)-j_3}}, \quad x_2^N, y_2^N \in \mathbb{Z}_{p_0^{i_3} q_0^{j_3}}$$

$$max(i_1,i_2) < u \ \vee \ max(j_1,j_2) < v \ .$$

a ukažme, že jsou neekvivalentní. V případech kdy $max(i_1,i_2) = u \wedge max(j_1,j_2) = v$ není co dokazovat, neboť je ve skupině jen jedna orbita. Využijeme toho, že zobrazení G zachovává ekvivalenci. Zobrazíme oba body do okruhu $(\mathbb{Z}_p^2 \times \mathbb{Z}_p^2) \times (\mathbb{Z}_q^2 \times \mathbb{Z}_q^2)$ a určíme orbity do kterých padnou. Tyto orbity pak rozložíme na dvojice orbit z $(\mathbb{Z}_p^2 \times \mathbb{Z}_p^2)$ resp. $(\mathbb{Z}_q^2 \times \mathbb{Z}_q^2)$, které dále je vyjádříme pomocí reprezentantů v normalizovaném tvaru podle nějž snadno určíme, zda jsou či nejsou ekvivalentní. Body x, y se zobrazí na dvojice bodů:

$$x^p = (x)_{mod\, p_0^u}, \quad x^q = (x)_{mod\, q_0^v}$$

$$y^p = (y)_{mod\, p_0^u}, \quad y^q = (y)_{mod\, q_0^v} \ .$$

Bod x^p upravíme postupem uvedeným na konci části 4.2. Pokud $max(i_1, i_2) = u$ pak $x_1^N, y_1^N \in \mathbb{Z}_{q_0^{v-max(j_1,j_2)-j_3}}$ a body $x_2^N, y_2^N \in \mathbb{Z}_{q_0^{j_3}}$ a o ekvivalenci reprezentantů se bude rozhodovat z úpravy bodů x^q, y^q Nechť např. $i_1 \leq i_2 < u$ pak bod x^p převedeme na bod:

$$((0, (q_0^{j_1})_{mod\, p_0^{u-i_2}}), (p_0^{j_3} q_0^{i_2} q_0^{j_3} x_1^N, q_0^{j_2} x_2^N)_{mod\, p_0^{u-i_2}}) \ .$$

Určíme determinant

$$D = -det \begin{pmatrix} 0 & q_0^{j_1} \\ p_0^{j_3} q_0^{i_2} q_0^{j_3} x_1^N & q_0^{j_2} x_2^N \end{pmatrix}_{mod\, p_0^{u-i_2}} = p_0^{j_3} q_0^{j_1} q_0^{i_2} q_0^{j_3} x_1^N \ \backslash mod\, p_0^{u-i_2}$$

a $\delta(D, p_0^{u-i_2}) = p_0^{j_3}$. Bod x^p tedy leží v orbitě:

$$x^p \in [(p_0^{i_1}(0,1), p_0^{i_2}((p_0^{j_3} q_0^{j_1} q_0^{i_2} q_0^{j_3} x_1^N)_{mod\, p_0^{u-i_2}}, ((q_0^{j_1})^{-1} q_0^{j_2} x_2^N)_{mod\, p_0^{i_3}})]$$

a obdobně bod y^p dostaneme:

$$x^p \in [(p_0^{i_1}(0,1), p_0^{i_2}((p_0^{j_3} q_0^{j_1} q_0^{i_2} q_0^{j_3} y_1^N)_{mod\, p_0^{u-i_2}}, ((q_0^{j_1})^{-1} q_0^{j_2} y_2^N)_{mod\, p_0^{i_3}})] \ .$$

Pokud by tyto dva body byly ekvivalentní pak zřejmě musí platit:

$$p_0^{j_3} q_0^{j_1} q_0^{i_2} q_0^{j_3} x_1^N = p_0^{j_3} q_0^{j_1} q_0^{i_2} q_0^{j_3} y_1^N \quad \backslash mod\, p_0^{u-i_2}$$
$$(q_0^{j_1})^{-1} q_0^{j_2} x_2^N = (q_0^{j_1})^{-1} q_0^{j_2} y_2^N \quad \backslash mod\, p_0^{i_3} \ .$$

Odtud úpravami, s využitím existence inverzních prvků k prvkům $q_0^{j_l}, \quad l = 1, 2, 3$ dostaneme podmínky:

$$x_1^N = y_1^N \quad \backslash mod\, p_0^{u-i_2-i_3} \tag{4.7}$$
$$x_2^N = y_2^N \quad \backslash mod\, p_0^{i_3} \ . \tag{4.8}$$

V případě $max(j_1, j_2) = v$ jsou

$$x_1^N, y_1^N \in \mathbb{Z}_{p_0^{u-max(i_1,i_2)-i_3}}, \qquad x_2^N, y_2^N \in \mathbb{Z}_{p_0^{i_3}}$$

a tedy z rovnic 4.7 plyne, že body $x, y \in \mathbb{Z}_{pq}^2 \times \mathbb{Z}_{pq}^2$ ekvivalentní nejsou (pokud by ekvivalentní byly, pak by se musely rovnat a to je spor s volbou různých reprezentantů). V případě $max(j_1, j_2) < v$ dostaneme podobně jako výše podmínky:

$$x_1^N = y_1^N \quad \backslash mod\, q^{u-i_2-i_3} \tag{4.9}$$
$$x_2^N = y_2^N \quad \backslash mod\, p^{i_3} \ , \tag{4.10}$$

které v případě $max(i_1, i_2) = u$ přímo dokazují neekvivalenci bodů $x \neq y$. V případě $max(i_1, i_2) < u$ společně se vztahy 4.9 ukazují, že body x, y jsou ekvivalentní pouze pokud jsou si rovné. Tím je různost orbit ve skupině 4.6 dokázána. Pokud by čísla p, q nebyly mocniny prvočísel, pak by k důkazu tvaru orbit bylo potřeba definovat zobrazení, které by vyšetřovaný okruh zobrazilo do kartézského součinu okruhů, odpovídajících mocninám jednotlivých prvočísel z nichž je složeno číslo n a dokázat že toto zobrazení je bijekce zachovávající ekvivalenci. Důkaz tvaru orbit by pak byl obdobný jako výše uvedený, pouze méně přehledný a složitější.

4.4 Orbity na $\mathbb{Z}_n^2 \times \mathbb{Z}_n^2$ pro $n \in \mathbb{N},\ n \geq 2$

V této části již pouze shrneme dříve dokázané výsledky. Buď $n \in \mathbb{N},\ n \geq 2$ a nechť

$$n = \prod_{i=1}^{r} p_i^{k_i}, \quad p_i \in \mathbb{P},\ k_i \in \mathbb{N}$$

je rozklad čísla n na součin mocnin navzájem různých prvočísel. Orbity akce grupy $SL(2, \mathbb{Z}_n)$ na okruhu $\mathbb{Z}_n^2 \times \mathbb{Z}_n^2$ jsou:

$$[(d_1(0,1), d_2(d_3 a_1^N, (a_2^N)^{sgn(n-d_1)}))] \qquad kde\ d_j/n, \quad j = 1,2,3 \tag{4.11}$$

$$d_j = \prod_{i=1}^{r} p_i^{l_i^{(j)}}, \qquad 0 \leq l_i^{(1)}, l_i^{(2)} \leq k_i, \quad 0 \leq l_i^{(3)} \leq k_i - max(l_i^{(1)}, l_i^{(2)}), \qquad i \in \hat{r}$$

$$a_1^N \in \mathbb{Z}_{\frac{n}{D_{1,2}d_3}} \qquad a_2^N \in \mathbb{Z}_{d_3}$$

kde $D_{1,2} = \prod_{i=1}^{r} p_i^{max(l_i^{(1)}, l_i^{(2)})}$ a index N opět značí nesoudělnost tj.:

$$\delta(a_1^N, \frac{n}{D_{1,2}d_3}) = 1\ pro\ \frac{n}{D_{1,2}d_3} > 1 \quad resp. \quad a_1^N = 0\ pro\ \frac{n}{D_{1,2}d_3} = 1$$

$$\delta(a_2^N, d_3) = 1\ pro\ d_3 > 1 \quad resp. \quad a_2^N = 0\ pro\ d_3 = 1\ .$$

Počet prvků v orbitě je:

$$Q(n, d_1, d_2, d_3) = \prod_{i=1}^{r} p_i^{3k_i - 2min(l_i^{(1)}, l_i^{(2)}) - max(l_i^{(1)}, l_i^{(2)}) - l_i^{(3)}} (1 - p_i^{-2})^{sgn(2k_i - l_i^{(1)} - l_i^{(2)})}$$

$$= \frac{n^3}{d_{1,2}^2 D_{1,2} d_3} \prod_{i=1}^{r} (1 - p_i^{-2})^{sgn(2k_i - l_i^{(1)} - l_i^{(2)})} \tag{4.12}$$

kde $d_{1,2} = \prod_{i=1}^{r} p_i^{min(l_i^{(1)}, l_i^{(2)})}$.

Počet orbit pro dané d_1, d_2, d_3 je:

$$P_2(n, d_1, d_2, d_3) = \prod_{i=1}^{r} p_i^{k_i - max(l_i^{(1)}, l_i^{(2)})} (1 - p_i^{-1})^{sgn(k_i - max(l_i^{(1)}, l_i^{(2)}) - l_i^{(3)})} (1 - p_i^{-1})^{sgn(l_i^3)}$$

$$= \frac{n}{D_{1,2}} \prod_{i=1}^{r} (1 - p_i^{-1})^{sgn(k_i - max(l_i^{(1)}, l_i^{(2)}) - l_i^{(3)})} (1 - p_i^{-1})^{sgn(l_i^3)}\ . \tag{4.13}$$

Celkový počet orbit akce grupy $SL(2, \mathbb{Z}_n)$ na okruhu $\mathbb{Z}_n^2 \times \mathbb{Z}_n^2$ je:

$$P_2(n) = \prod_{i=1}^{r} ((k_i + 1)p_i^{k_i} + k_i p_i^{k_i - 1})\ . \tag{4.14}$$

Reference

[1] M. Havlíček, J. Patera, E. Pelantová, J. Tolar: Automorphisms of the fine grading of $SL(n, \mathbb{C})$ associated with the generalized Pauli matrices, J. Math. Phys., Vol. 43, No. 2 (2002), pp. 1083-1094.

[2] You Hong, Gao You: Computation of the orders of classical groups over finite commutative rings, Chinese Science Bulletin, Vol. 39, No. 14 (1994), pp. 1150-1154.

[3] Jörg Schulte: U̇ber die Jordanisch Verallgemeinerung der Eulerschen Funktion, Resultate der Mathematik, Vol. 36 (1999), No. 3/4, pp. 354-364.

[4] A.A. Kirillov: Elementy teorii predstavlenij, Nauka, Moskva 1978

[5] L.E. Dickson: Linear Groups with an exposition of the Galois field theory, Leipzig 1901.

[6] B.L. van der Waerden: Gruppen von linearen Transformationen, Springer-Verlag, Berlin 1935.