Families of Square Commutative 2x2 Matrices

Anatoly Shcherba[1], Emil Faure[1,2], Artem Skutskyi[1], and Oleksandr Kharin[1]

[1] *Cherkasy State Technological University, 460 Shevchenko blvd., Cherkasy, 18006, Ukraine*
[2] *State Scientific and Research Institute of Cybersecurity Technologies and Information Protection,*
3 M. Zaliznyak str., Kyiv, 03142, Ukraine

Abstract

The objective of this study is to define and investigate the families of square matrices of order 2 with a commutative multiplication operation to be used in cryptographic information transformation. The general linear group of order *n* over the prime field of integers modulo *p* has been investigated. Six families of matrices from the general linear group of order 2 for which the multiplication operation is commutative have been defined. The current study has found the cardinalities of these families. The study has also regarded the family of matrices from the general linear group of order 2 with a commutative multiplication operation, extended by an identity matrix. The research has revealed that this matrix family is a multiplicative abelian group. For this purpose, the authors have proved that the axioms of the group are fulfilled, confirmed that the multiplication is commutative, and demonstrated the order of the group. The results of this study create prerequisites for using the obtained multiplicative abelian groups of square matrices of order 2 while solving the tasks of constructing cryptographic key agreement protocols, asymmetric encryption algorithms, and three-pass cryptographic protocols.

Keywords

Matrix family, commutative transformation, commutative encryption, multiplicative abelian group, key agreement, cryptography.

1. Introduction

Commutative operations play an essential role in cryptographic information transformation algorithms widely used in modern information and communication systems, smart technologies, and the Internet of Things. In particular, key agreement procedures, asymmetric encryption, and three-pass cryptographic protocols apply commutative cryptographic transformations [1–5]. Some of the classic cryptographic schemes that deploy commutative exponentiation in modular arithmetic (modular exponentiation) are the Diffie-Hellman key agreement protocol [6], RSA [7], SRA [8], Massey-Omura cryptosystem [9].

The scientific search for commutative cryptographic transformations is still relevant today. Algorithms whose strength relies on the computational complexity of factorization and discrete logarithm procedures are not protected against attacks with quantum computers and can be broken over polynomial time [10].

Moldovyan et al. [11] refer to the literature [12] as one of the first attempts to solve the problem of building a post-quantum commutative cipher. The proposed approach is based on the hidden discrete logarithm problem, however, this approach does not achieve an increase in cryptographic strength [13]. Methods for applying forms of the hidden discrete logarithm problem have been developed in studies [14–16] and are based on operations in a multidimensional vector space. In the study [14], the authors propose a secure encryption method based on commutative transformations. The three basic components

CPITS-2023-II: Cybersecurity Providing in Information and Telecommunication Systems, October 26, 2023, Kyiv, Ukraine
EMAIL: a.shcherba@chdtu.edu.ua (A. Shcherba); e.faure@chdtu.edu.ua (E. Faure); a.b.skutskyi.asp21@chdtu.edu.ua (A. Skutskyi); o.kharin@chdtu.edu.ua (O. Kharin)
ORCID: 0000-0002-3049-3497 (A. Shcherba); 0000-0002-2046-481X (E. Faure); 0000-0002-8632-1176 (A. Skutskyi); 0000-0003-1791-6755 (O. Kharin)

of this method are the following cryptographic protocols: Diffie-Hellman key agreement protocol [6], Pohlig-Hellman commutative encryption algorithm [17], and Shamir three-pass protocol [8]. An exponentiation cipher is used to perform commutative encryption.

Kryvyi [18] has demonstrated a method for constructing a symmetric cryptosystem based on the properties of finite associative-commutative rings with unity and discusses conditions for using discrete logarithm functions in the rings.

The study [19] develops encryption using cryptography methods such as Diffie-Hellman, commutative supersingular isogeny, and group action inverse problems.

Examples of using commutative encryption to protect secret key exchange are offered in the studies [20–21]. Research undertaken by Sihare [22] further develops the schemes and offers a dynamic multi-party quantum key agreement protocol.

Studies [23–26] use permutations to represent data, and operations on permutations to construct key agreement protocol [27] and to improve three-pass cryptographic protocol, including for use in noisy channels [28–30].

A previous study [31] suggests using public-key cryptography based on commutative semirings of tropical circular matrices, where multiplication is the ordinary addition of numbers and there is no ordinary multiplication of numbers in the tropical semiring.

Shamir's three-pass random matrix ciphering mechanism [32] uses a three-pass protocol with encryption operators that are random commutative matrices.

The current study focuses on identifying and researching families of square matrices with commutative multiplication. The matrices will be limited by 2×2 dimension, and their elements will belong to the prime field of integers modulo *p*.

2. Families of Commutative 2×2 Matrices

We first introduce a definition.

Definition 1 [33–34]. A general linear group of order n over any field F or ring R is a group of invertible matrices $n \times n$ containing elements from F (or R) with ordinary matrix multiplication as the group multiplication operation.

$GL(n,F)$ will denote the general linear group of order n over the field F.

Note that the square matrix A is invertible if and only if its determinant $|A| \neq 0$ [35].

Here, we consider the group $\Gamma = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, a,b,c,d \in Z_p, |A| \neq 0 \right\}$, where Z_p is the prime field of integers modulo p. Then, $\Gamma = GL(2, Z_p)$.

Theorem 1. Multiplication is commutative for the following families of matrices Γ:

$$\Gamma_1 = \left\{ t \cdot \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}, t,a \in Z_p, t \neq 0, a \neq 0 \right\},$$

$$\Gamma_2 = \left\{ t \cdot \begin{pmatrix} 1 & 0 \\ a & ak+1 \end{pmatrix}, \begin{matrix} t,a,k \in Z_p, t \neq 0, \\ ak+1 \neq 0 \end{matrix} \right\},$$ k is fixed,

$$\Gamma_3 = \left\{ t \cdot \begin{pmatrix} 1 & a \\ 0 & ak+1 \end{pmatrix}, \begin{matrix} t,a,k \in Z_p, t \neq 0, \\ ak+1 \neq 0 \end{matrix} \right\},$$ k is fixed,

$$\Gamma_4 = \left\{ t \cdot \begin{pmatrix} a & 1 \\ b & 0 \end{pmatrix}, \begin{matrix} t,a,b \in Z_p, \\ t \neq 0, b \neq 0 \end{matrix} \right\},$$ a, b are fixed,

$$\Gamma_5 = \left\{ t \cdot \begin{pmatrix} 0 & 1 \\ b & a \end{pmatrix}, \begin{matrix} t,a,b \in Z_p, \\ t \neq 0, b \neq 0 \end{matrix} \right\},$$ a, b are fixed,

$$\Gamma_6 = \left\{ t \cdot \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}, \begin{matrix} t,a,b,k \in Z_p, t \neq 0, b \neq 0, \\ a(a+k) - b \neq 0 \end{matrix} \right\}$$

, b, k are fixed.

Proof.

Note that in the general case, Γ is non-abelian.

Consider the following cases:

$b = c = 0$, $ad \neq 0$

$b = 0$ or $c = 0$, $ad \neq 0$

$bc \neq 0$, $ad = 0$

$ad \neq 0$, $bc \neq 0$.

Case 1: $b = c = 0$, $ad \neq 0$.

In this case, $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} = a \begin{pmatrix} 1 & 0 \\ 0 & d/a \end{pmatrix}$. The set of such diagonal non-degenerate matrices is equivalent to the set $\Gamma_1 = \left\{ t \cdot \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}, t,a \in Z_p, t \neq 0, a \neq 0 \right\}$, which forms an abelian group [36]: for $\forall A,B\in\Gamma_1$, $AB=BA$ is true.

Case 2: $b=0$ or $c=0$, $ad\neq 0$.

Let $b=0$ and $ad\neq 0$. Then, matrix $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}=\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}=a\begin{pmatrix} 1 & 0 \\ c/a & d/a \end{pmatrix}$. The set of such matrices is a family of non-degenerate lower triangular matrices $\Upsilon=\left\{t\cdot\begin{pmatrix} 1 & 0 \\ a & b \end{pmatrix}, \begin{matrix} t,a,b\in Z_p, \\ t\neq 0, b\neq 0 \end{matrix}\right\}$. According to [36], Υ forms a group by multiplication.

Let $A,B\in\Upsilon$ and $A=\begin{pmatrix} 1 & 0 \\ a & b \end{pmatrix}$, $B=\begin{pmatrix} 1 & 0 \\ x & y \end{pmatrix}$. The product $A\cdot B=\begin{pmatrix} 1 & 0 \\ a+bx & by \end{pmatrix}$. The product $B\cdot A=\begin{pmatrix} 1 & 0 \\ x+ay & by \end{pmatrix}$.

Value $A\cdot B=B\cdot A$, if $a+bx=x+ay$ or $x(b-1)=a(y-1)$. If $a=x=0$, Υ degenerates into Γ_1, which is abelian. If $a,x\neq 0$, we assume that $\frac{b-1}{a}=\frac{y-1}{x}=k$, $k\in Z_p$. Then $\begin{cases} b=ak+1, \\ y=xk+1; \end{cases}$ and matrices $A=\begin{pmatrix} 1 & 0 \\ a & ak+1 \end{pmatrix}$, $B=\begin{pmatrix} 1 & 0 \\ x & xk+1 \end{pmatrix}$, where $a\neq 0$, $x\neq 0$, $ak+1\neq 0$, $xk+1\neq 0$, $\forall k\in Z_p$.

Then $\Gamma_2=\left\{t\cdot\begin{pmatrix} 1 & 0 \\ a & ak+1 \end{pmatrix}, \begin{matrix} t,a,k\in Z_p, t\neq 0, \\ ak+1\neq 0 \end{matrix}\right\}$ is an abelian group, where a and t values may be arbitrary, while k value is a fixed parameter of group Γ_2.

Adopting that $c=0$, $ad\neq 0$, and reasoning by analogy, we can prove that a group of non-degenerate upper triangular matrices of $A=\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ type is abelian if it forms the group $\Gamma_3=\left\{t\cdot\begin{pmatrix} 1 & a \\ 0 & ak+1 \end{pmatrix}, \begin{matrix} t,a,k\in Z_p, t\neq 0, \\ ak+1\neq 0 \end{matrix}\right\}$.

Case 3: $bc\neq 0$, $ad=0$.

Let $bc\neq 0$ and $d=0$. Then $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}=\begin{pmatrix} a & b \\ c & 0 \end{pmatrix}=a\begin{pmatrix} a/b & 1 \\ c/b & 0 \end{pmatrix}$. Such matrices define the set $\Xi=\left\{t\cdot\begin{pmatrix} a & 1 \\ b & 0 \end{pmatrix}, \begin{matrix} t,a,b\in Z_p, \\ t\neq 0, b\neq 0 \end{matrix}\right\}$.

Let $A,B\in\Xi$ and $A=t\begin{pmatrix} a & 1 \\ b & 0 \end{pmatrix}$, $B=s\begin{pmatrix} x & 1 \\ y & 0 \end{pmatrix}$. An equality $A\cdot B=B\cdot A$ means $\begin{pmatrix} ax+y & a \\ bx & b \end{pmatrix}=\begin{pmatrix} ax+b & x \\ ay & y \end{pmatrix}$ or $\begin{cases} x=a, \\ y=b. \end{cases}$ Therefore, if $bc\neq 0$ and $d=0$ the commutative family is the set $\Gamma_4=\left\{t\cdot\begin{pmatrix} a & 1 \\ b & 0 \end{pmatrix}, \begin{matrix} t,a,b\in Z_p, \\ t\neq 0, b\neq 0 \end{matrix}\right\}$, where a and b are fixed.

Taking $bc\neq 0$, $a=0$, it can be shown by analogy that the commutative family is the set $\Gamma_5=\left\{t\cdot\begin{pmatrix} 0 & 1 \\ b & a \end{pmatrix}, \begin{matrix} t,a,b\in Z_p, \\ t\neq 0, b\neq 0 \end{matrix}\right\}$, where a and b are fixed.

Note that the families Γ_4, Γ_5 are not closed under multiplication, so they do not form a group.

Case 4: $ad\neq 0$, $bc\neq 0$.

Since $b\neq 0$, $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}=b\begin{pmatrix} a/b & 1 \\ a/c & a/d \end{pmatrix}$. The set of such matrices forms the set of non-degenerate matrices $\Psi=\left\{t\cdot\begin{pmatrix} a & 1 \\ b & c \end{pmatrix}, \begin{matrix} t,a,b,c\in Z_p, t\neq 0, \\ b\neq 0, ac-b\neq 0 \end{matrix}\right\}$.

Let $A,B\in\Psi$ and $A=\begin{pmatrix} a & 1 \\ b & c \end{pmatrix}$, $B=\begin{pmatrix} x & 1 \\ y & z \end{pmatrix}$. The product $A\cdot B=\begin{pmatrix} ax+y & a+z \\ bx+cy & b+cz \end{pmatrix}$. The product $B\cdot A=\begin{pmatrix} ax+b & x+c \\ ay+bz & y+cz \end{pmatrix}$.

Equality $A\cdot B=B\cdot A$ is achieved if $\begin{cases} ax+y=ax+b; \\ a+z=x+c; \\ bx+cy=ay+bz; \\ b+cz=y+cz. \end{cases}$ It follows that $\begin{cases} y=b; \\ c-a=z-x. \end{cases}$

Let $c-a=z-x=k$, $k\in Z_p$. Then $A=\begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}$, $B=\begin{pmatrix} x & 1 \\ b & x+k \end{pmatrix}$, and $\Gamma_6=\left\{t\cdot\begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}, \begin{matrix} t,a,b,k\in Z_p, t\neq 0, b\neq 0, \\ a(a+k)-b\neq 0 \end{matrix}\right\}$ is a commutative family, wherein a and t values may be arbitrary, while b and k values are Γ_6 fixed parameters.

Now, we have got all $\Gamma_1 - \Gamma_6$ families of matrices from $\Gamma = GL(2, Z_p)$, which multiplication is commutative.

The theorem is proved.

The cardinality of each $\Gamma_1 - \Gamma_3$ family is equal to $(p-1)^2$, and the cardinality of each $\Gamma_4 - \Gamma_5$ family is equal to $p-1$, while the cardinality of Γ_6 family is $(p-1)(p-l)$, where $l = \{0;1;2\}$ is the number of integer roots of the equation $a^2 + ka - b = 0 (\mathrm{mod}\, p)$ concerning the variable a. The l value is defined by b and k parameters.

3. Commutative Family of 2×2 Matrices with Identity Matrix

Consider the matrix family Γ_6 supplemented by an identity matrix, as well as the case when $b = 0$, since it does not affect the commutativity of the matrices from Γ_6. We will denote this family by

$$CGL_{b,k}(2, \square_p) = \left\{ \begin{array}{l} t \cdot \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}, s \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \\ t, s, a, b, k \in Z_p, t, s \neq 0, \\ a(a+k) - b \neq 0 \end{array} \right\}.$$

Theorem 2. The matrix family $CGL_{b,k}(2, Z_p)$ is a commutative (abelian) group under multiplication.

Proof.

We will prove that the group axioms are fulfilled for $CGL_{b,k}(2, Z_p)$ and demonstrate that the multiplication operation in $CGL_{b,k}(2, Z_p)$ is commutative.

1. $CGL_{b,k}(2, Z_p)$ has a single identity element: $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

2. The operation of multiplying elements in $CGL_{b,k}(2, Z_p)$ is associative since this is a general property for matrices.

3. For each matrix $A \in CGL_{b,k}(2, Z_p)$, there is an inverse matrix $A^{-1} \in CGL_{b,k}(2, Z_p)$: $A \cdot A^{-1} = A^{-1} \cdot A = E$.

Thus, if $A = s \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, then $A^{-1} = \left[s \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right]^{-1} = s^{-1} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. In Z_p, for each $s \in Z_p$, there is an inverse element s^{-1}: $s \cdot s^{-1} = s^{-1} \cdot s = e = 1$, that is unique. Further, while proving this theorem, we will neglect multipliers s and t without limiting the generality of the foregoing.

Let $A = \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}$.

Then

$$A^{-1} = \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}^{-1} = \frac{1}{a(a+k) - b} \begin{pmatrix} a+k & -1 \\ -b & a \end{pmatrix}.$$

Let us assume that $t' = \frac{-1}{a(a+k) - b} \neq 0$, $a' = -a - k$. Then,

$$A^{-1} = t' \cdot \begin{pmatrix} a' & 1 \\ b & a' + k \end{pmatrix} \in CGL_{b,k}(2, Z_p).$$

Moreover, it follows therefrom that $\begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix} \begin{pmatrix} c & 1 \\ b & c+k \end{pmatrix}^{-1} = E$ if and only if $a = c$.

4. $CGL_{b,k}(2, Z_p)$ is closed under multiplication.

Let $A, B \in CGL_{b,k}(2, Z_p)$. If $A = E$ or $B = E$, this property is obvious.

Consider the situation when $A = \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}$ and $B = \begin{pmatrix} x & 1 \\ b & x+k \end{pmatrix}$ for arbitrary $a, x \in Z_p$.

Product $A \cdot B = \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix} \begin{pmatrix} x & 1 \\ b & x+k \end{pmatrix} =$

$$= \begin{pmatrix} ax + b & a + x + k \\ b(a + x + k) & b + (a+k)(x+k) \end{pmatrix}.$$

If $a + x + k = 0$, then

$$A \cdot B = \begin{pmatrix} ax + b & 0 \\ 0 & ax + b \end{pmatrix} = (ax + b) \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Since $|A| \neq 0$ and $|B| \neq 0$, then

$|A\cdot B| = |A|\cdot|B| \neq 0$ and $ax+b \neq 0$ correspondingly. From whence it follows that $A\cdot B \in CGL_{b,k}\left(2,Z_p\right)$.

If $a+x+k \neq 0$, then $A\cdot B = \dfrac{1}{a+x+k}\begin{pmatrix} \dfrac{ax+b}{a+x+k} & 1 \\ b & k+\dfrac{ax+b}{a+x+k} \end{pmatrix}$. Let $t = \dfrac{1}{a+x+k} \neq 0$ and $y = \dfrac{ax+b}{a+x+k}$. Then $A\cdot B = t\begin{pmatrix} y & 1 \\ b & y+k \end{pmatrix} \in CGL_{b,k}\left(2,Z_p\right)$.

5. $CGL_{b,k}\left(2,Z_p\right)$ is an abelian group.

If $A=E$, then $A\cdot B = E\cdot B = B = B\cdot E = B\cdot A$.

Let $A=\begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}$ and $B=\begin{pmatrix} x & 1 \\ b & x+k \end{pmatrix}$.

Then $A\cdot B = \begin{pmatrix} ax+b & a+x+k \\ b(a+x+k) & b+(a+k)(x+k) \end{pmatrix}$

and $B\cdot A = \begin{pmatrix} ax+b & a+x+k \\ b(a+x+k) & b+(x+k)(a+k) \end{pmatrix}$,

from where it follows that $A\cdot B = B\cdot A$.

The theorem is proved.

To exponentiate the square matrix $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, we will use the following expression from [37]:

$$A^n = \begin{pmatrix} u_{n+1}-du_n & bu_n \\ cu_n & u_{n+1}-au_n \end{pmatrix}, \qquad (1)$$

where

$u_{n+1} = (a+d)u_n - |A|u_{n-1} = tr(A)u_n - |A|u_{n-1}$,

$tr(A)$ is a trace of the matrix A [38];

$u_0 = 0$, $u_1 = 1$.

For a matrix group element $A=\begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix} \in CGL_{b,k}\left(2,Z_p\right)$, we obtain $tr(A) = 2a+k$, $|A| = a(a+k)-b \neq 0$. Then $u_{n+1} = (2a+k)u_n - \left(a(a+k)-b\right)u_{n-1}$ and $A^n = \begin{pmatrix} u_{n+1}-(a+k)u_n & u_n \\ bu_n & u_{n+1}-au_n \end{pmatrix}$.

Note that $\left|A^n\right| = |A|^n \neq 0$.

Since $CGL_{b,k}\left(2,Z_p\right)$ is a commutative group under multiplication, $A^n \in CGL_{b,k}\left(2,Z_p\right)$. According to (1):

If $u_n = 0$, then $A^n = \begin{pmatrix} u_{n+1} & 0 \\ 0 & u_{n+1} \end{pmatrix} = u_{n+1}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in CGL_{b,k}\left(2,Z_p\right)$.

If $u_n \neq 0$, then

$$A^n = u_n\begin{pmatrix} \dfrac{u_{n+1}}{u_n}-a-k & 1 \\ b & \dfrac{u_{n+1}}{u_n}-a \end{pmatrix} \in CGL_{b,k}\left(2,Z_p\right).$$

Theorem 3. The order of the matrix group $CGL_{b,k}\left(2,Z_p\right)$ for $D = k^2+4b \neq u^2 \in Z_p$ is p^2-1.

Proof.

It is appropriate at this point to recall that

$$CGL_{b,k}\left(2,\square_p\right) = \left\{\begin{matrix} t\cdot\begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}, s\cdot\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \\ t,s,a,b,k \in Z_p, t,s \neq 0, \\ a(a+k)-b \neq 0 \end{matrix}\right\}.$$

Values b and k are fixed for the group, then $t,a,s \in Z_p$, $t,s \neq 0$ are variable. Then, the number of different values that matrices $t\cdot\begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}$ may take on is equal to the number of different possible pairs $\{t,a\}$ with the given restraints. The value t may take on $p-1$ different values from $\square_p$ $(t \neq 0)$. Value a is restricted by the condition $a(a+k)-b \neq 0$. For $D = k^2+4b \neq u^2 \in Z_p$, this equation does not have integer roots concerning the variable a, therefore, it can take on p different values with Z_p.

The number of different values that matrices $s\cdot\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ may take on is equal to the number $p-1$ of different possible values $s \in Z_p$, $s \neq 0$.

Therefore, the order of the matrix group $CGL_{b,k}\left(2,Z_p\right)$ is $(p-1)p+p-1 = p^2-1$.

The theorem is proved.

Thus, for $D = k^2 + 4b \neq u^2 \in Z_p$. $CGL_{b,k}\left(2, Z_p\right)$ is a multiplicative abelian group of order $p^2 - 1$.

Remark 1 [39]**.** For prime $p \geq 3$, the number of nonzero values $D \in Z_p :\ D = u^2 \in Z_p$ and the number of $D \in Z_p :\ D \neq u^2 \in Z_p$ values coincide and are equal to $\frac{p-1}{2}$.

4. Conclusion

The paper defines six families of matrices from the general linear group $GL\left(2, Z_p\right)$ with order 2 over the prime field of integers modulo p with commutative multiplication operation. The set cardinality for the defined families has been determined.

The research results indicate that the matrix set $\left\{ \begin{matrix} t \cdot \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}, \\ t, a, b, k \in Z_p, t \neq 0, \\ a\left(a+k\right) - b \neq 0 \end{matrix} \right\}$ supplemented by the matrix set $\left\{ s \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, s \in Z_p, s \neq 0 \right\}$ forms an abelian group under multiplication. The order of this group is $p^2 - 1$.

Further studies of square matrix groups commutative under multiplication, may involve the selection of matrix parameters, as well as their application in cryptographic transformation operations.

5. Acknowledgments

This research was funded by the Ministry of Education and Science of Ukraine under grant 0123U100270.

References

[1] A. Bessalov, et al., CSIKE-ENC Combined Encryption Scheme with Optimized Degrees of Isogeny Distribution, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 36–45.

[2] A. Bessalov, et al., Modeling CSIKE Algorithm on Non-Cyclic Edwards Curves, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3288 (2022) 1–10.

[3] A. Bessalov, et al., Implementation of the CSIDH Algorithm Model on Supersingular Twisted and Quadratic Edwards Curves, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3187, no. 1 (2022) 302–309.

[4] A. Bessalov, et al., Implementation of the CSIDH Algorithm Model on Supersingular Twisted and Quadratic Edwards Curves, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3187, no. 1 (2022) 302–309.

[5] A. Bessalov, et al., Computing of Odd Degree Isogenies on Supersingular Twisted Edwards Curves, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 2923 (2021) 1–11.

[6] W. Diffie, M. Hellman, New Directions in Cryptography, IEEE Transactions on Information Theory 22(6) (1976) 644–654. doi: 10.1109/TIT.1976.1055638.

[7] R. Rivest, A. Shamir, L. Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM 21(2) (1978) 120–126. doi: 10.1145/359340.359342.

[8] A. Shamir, R. Rivest, L. Adleman, Mental Poker, The Mathematical Gardner (1981) 37–43. doi: 10.1007/978-1-4684-6686-7_5.

[9] J. Massey, J. Omura, Method and Apparatus for Maintaining the Privacy of Digital Messages Conveyed by Public Transmission (1986).

[10] P. Shor, Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, SIAM J. Comput. 26(5) (1997) 1484–1509. doi: 10.1137/S0097539795293172.

[11] A. Moldovyan, D. Moldovyan, N. Moldovyan, Post-Quantum Commutative Encryption Algorithm, Comput. Sci. J. Moldova 81(3) (2019) 299–317.

[12] D. Moldovyan, Non-Commutative Finite Groups as Primitive of Public-Key Cryptoschemes, Quasigroups Relat. Syst. 18(2) (2010) 165–176.

[13] A. Kuzmin, et al., Cryptographic Algorithms on Groups and Algebras, J. Math. Sci. 223(5) (2017) 629–641. doi: 10.1007/s10958-017-3371-y.

[14] N. Nguyen, et al., No-Key Protocol for Deniable Encryption, Inf. Syst. Des. Intel. Appl. 672 (2018) 96–104. doi: 10.1007/978-981-10-7512-4_10.

[15] D. Moldovyan, et al., Post-quantum Commutative Encryption Algorithm, Context-Aware Systems and Applications, and Nature of Computation and Communication (2019) 205–214. doi: 10.1007/978-3-030-34365-1_16.

[16] N. Moldovyan, A. Moldovyan, V. Shcherbacov, Post-Quantum No-Key Protocol, Buletinul Academiei de Stiinte a Republicii Moldova, Matematica 85(3) (2017) 115–119.

[17] M. Hellman, S. Pohlig, Exponentiation Cryptographic Apparatus and Method, (1984).

[18] S. Kryvyi, Application of Commutative Rings with Unity for Construction of Symmetric Encryption System, Cybern Syst. Anal. 58(3) (2022) 319–330. doi: 10.1007/s10559-022-00464-z.

[19] K. Dey, et al., A Post-Quantum Signcryption Scheme Using Isogeny Based Cryptography, J. Inf. Secur. Appl. 69 (2022). doi: 10.1016/j.jisa.2022.1032 80.

[20] Z. Sun, J. Huang, P. Wang, Efficient Multiparty Quantum Key Agreement Protocol Based on Commutative Encryption, Quantum Inf. Process 15(5) (2016) 2101–2111. doi: 10.1007/s11128-016-1253-8.

[21] R. Mohajer, Z. Eslami, Cryptanalysis of a Multiparty Quantum Key Agreement Protocol Based on Commutative Encryption, Quantum Inf. Process 16(8) (2017). doi: 10.1007/s11128-017-1647-2.

[22] S. Sihare, Dynamic Multi-Party Quantum Key Agreement Protocol Based on Commutative Encryption, Int. J. Theor. Physics 61(9) (2022). doi: 10.1007/s10773-022-05203-w.

[23] E. Faure, et al., Permutation-Based Block Code for Short Packet Communication Systems, Sensors 22(14) (2022). doi: 10.3390/s22145391.

[24] J. Al-Azzeh, et al. Permutation-Based Frame Synchronization Method for Data Transmission Systems with Short Packets, Egyptian Inform. J. 23(3) (2022) 529–545. doi: 10.1016/j.eij.2022.05.005.

[25] E. Faure, A. Shcherba, B. Stupka, Permutation-Based Frame Synchronisation Method for Short Packet Communication Systems, 11th IEEE Int. Conf. Intell. Data Acquisition Adv. Comput. Syst. Technol. Appl. (2021) 1073–1077. doi: 10.1109/IDAACS53288. 2021.9660996.

[26] J. Al-Aazzeh, et al., Telecommunication Systems with Multiple Access Based on Data Factorial Coding, Int. J. Commun. Antenna Propagation 10(2) (2020) 102–113. doi: 10.15866/irecap.v10i2.17216.

[27] E. Faure, et al., Cryptographic Key Exchange Method for Data Factorial Coding, in: International Workshop on Cyber Hygiene vol. 2654 (2020) 643–664.

[28] E. Faure, et al., Concept for Using Permutation-Based Three-Pass Cryptographic Protocol in Noisy Channels, Systems, Decision and Control in Energy V (2023) 99–113. doi: 10.1007/978-3-031-35088-7_7.

[29] E. Faure, et al., A Method for Reliable Permutation Transmission in Short-Packet Communication Systems, Information Technology for Education, Science, and Technics (2023) 177–195. doi: 10.1007/978-3-031-35467-0_12.

[30] A. Shcherba, E. Faure, O. Lavdanska, Three-Pass Cryptographic Protocol Based on Permutations, IEEE 2nd Int. Conf. Adv. Trends Inf. Theory (2020) 281–284. doi: 10.1109/ATIT50783. 2020.9349343.

[31] H. Huang, C. Li, L. Deng, Public-Key Cryptography Based on Tropical Circular Matrices, Appl. Sci. 12(15) (2022). doi: 10.3390/app12157401.

[32] F. Dupont, A New Shamir's Three Pass Random Matrix Ciphering Mechanism, J. Comput. Virology Hacking Techniques, (2023) 1–12. doi: 10.1007/s11416-023-00467-0.

[33] T. Springer, Linear Algebraic Groups, Modern Birkhäuser Classic, 2nd ed.,

Berlin (1998). doi: 10.1007/978-0-8176-4840-4.

[34] A. Baker, Matrix Groups. An Introduction to Lie Group Theory, Springer (2002). doi: 10.1007/978-1-4471-0183-3.

[35] S. Lipschutz, Schaum's Outline of Theory and Problems of Linear Algebra, 2nd ed., McGraw-Hill, NY (1991).

[36] F. Gantmacher, The Theory of Matrices, Reprinted, American Mathematical Society, Providence, RI (1959).

[37] J. Laughlin, Combinatorial Identities Deriving from the n-th Power of a 2x2 Matrix, Integers 4 (2004) 1–15. doi: 10.48550/ARXIV.1812.11168.

[38] V. Arnold, Fermat Dynamics, Matrix Arithmetics, Finite Circles, and Finite Lobachevsky Planes, Functional Analysis Its Appl. 38(1) (2004) 1–13. doi: 10.1023/B:FAIA.0000024863.06462.68.

[39] S. Wright, Quadratic Residues and Non-Residues, Lecture Notes in Mathematics 2171 (2016). doi: 10.1007/978-3-319-45955-4.