New York Journal of Mathematics

New York J. Math. **32** (2026) 1089–1104.

The conjugacy class structure of the Qd(p) groups

Colin M. Lawson and Jane H. Long

ABSTRACT. In this paper, we provide a classification of the conjugacy classes in the special affine group $\mathrm{Qd}(p) = (\mathbb{Z}_p \times \mathbb{Z}_p) \rtimes \mathrm{SL}(2, p)$ for odd primes. We use the known conjugacy class structure in $\mathrm{SL}(2, p)$ to lift elements to their conjugacy class in $\mathrm{Qd}(p)$. More specifically, for an element in $\mathrm{Qd}(p)$, its conjugacy class depends on whether the matrix component of the element is the identity, has eigenvalue 1, which is split into two classes in $\mathrm{SL}(2, p)$, or whether it lies in some other conjugacy class in $\mathrm{SL}(2, p)$. In addition, we provide formulas, in terms of p, for both the number and sizes of conjugacy classes in $\mathrm{Qd}(p)$.

CONTENTS

1. Background 1091
2. Conjugacy classes in SL(2, p) 1092
3. Linear transformations 1093
4. Conjugacy classes in Qd(p) 1095
5. Summary of conjugacy class data 1098
References 1103

Understanding the conjugacy classes of finite groups is a fundamental problem in group theory and can often serve as a first step in understanding the structure of other algebraic objects (e.g., group cohomology and the study of Hochschild cohomology rings; see [5], [12], [13]). The special affine group $\mathrm{Qd}(p) = (\mathbb{Z}_p \times \mathbb{Z}_p) \rtimes \mathrm{SL}(2, p)$ is of particular interest as these groups arise naturally in many contexts, such as a well-known conjecture by Benson and Carlson (see [2]) concerning group actions on products of spheres. For $p > 3$, the $\mathrm{Qd}(p)$ groups fail to possess a particular cohomology class, i.e., an *effective Euler class* (see [4]), which is necessary for a construction technique described in [1]. Although some results on the cohomology of the $\mathrm{Qd}(p)$ groups are known (see, for

Received July 30, 2025.

2010 *Mathematics Subject Classification.* Primary: 20E45, Secondary: 20G40.

Key words and phrases. Finite groups, semi-direct products, conjugacy classes, special affine group.

The authors are sincerely grateful for the Simons Foundation Scheme for the Provision of Magma at US Educational and Scientific Research Organizations, which provided access to the Magma Computer Algebra system.

ISSN 1076-9803/2026

example, [7], [8], [9], [10]), a description of conjugacy classes in $\mathrm{Qd}(p)$ seems to be unavailable in the literature.

In this paper, we prove the following complete classification of the conjugacy classes in $\mathrm{Qd}(p)$. In particular, we exploit the known characterization of conjugacy classes in $\mathrm{SL}(2,p)$ to obtain explicit splittings of certain conjugacy classes in $\mathrm{Qd}(p)$ that are governed by a distinguished set vectors, which we call *shifted vectors*. For an element (v, A) in $\mathrm{Qd}(p)$, its conjugacy class, $\mathrm{Class}_{\mathrm{Qd}(p)}(v, A)$, is determined by the conjugacy class of the matrix component A in $\mathrm{SL}(2,p)$. In particular, we distinguish the cases where $A = I$ (the identity matrix), where A is conjugate to a unipotent (upper-triangular) matrix with eigenvalue 1, or where A belongs to one of the remaining $\mathrm{SL}(2,p)$-conjugacy classes. The classes $\mathcal{C}$ and $\mathcal{D}$ denote the matrices in $\mathrm{SL}(2,p)$ with eigenvalue 1. Thus, the conjugacy class of (v, A) depends on the structure of the matrix A.

Theorem 0.1. *Let $p > 2$ be prime and $(v, A) \in \mathrm{Qd}(p)$ for $A \in \mathrm{SL}(2,p)$ and $v \in \mathbb{F}_p^2$. Then*

$$\mathrm{Class}_{\mathrm{Qd}(p)}(v,A) = \begin{cases} \{(0,I)\} & \text{if } A = I \text{ and } v = 0 \\ \{(w,I) \mid w \in \mathbb{F}_p^2 \setminus \{0\}\} & \text{if } A = I \text{ and } v \neq 0 \\ \displaystyle\bigcup_{\substack{B \in \mathcal{C}\cup\mathcal{D} \\ B \sim A}} \{(\pm w_{v,B} + z,\ B) \,\big|\, z \in \mathrm{Fix}(B)\} & \text{if } A \in \mathcal{C}\cup\mathcal{D}, \text{ where } w_{v,B} \text{ is the s.v. for } B \text{ determined by } v \\ \{(w,B) \mid B \sim A,\ w \in \mathbb{F}_p^2\} & \text{otherwise,} \end{cases}$$

where s.v. is an abbreviation for "shifted vector," defined in definition 4.5.

We establish the main result in propositions 4.2, 4.7 and 4.8, and to our knowledge, this is the first explicit description of the conjugacy classes for these groups. Our result provides a first step for future work in understanding the Hochschild cohomology ring, $\mathrm{HH}^*(\mathbb{F}_p[\mathrm{Qd}(p)])$, as techniques described in [13] rely on the ability to make explicit choices of conjugacy class representatives in $\mathrm{Qd}(p)$.

Outline of paper. We provide the necessary group theoretic definitions, notation, and background in section 1. We recall in section 2 the structure of the conjugacy classes in $\mathrm{SL}(2,p)$, categorizing the classes in terms of their eigenvalues and quadratic (non)residues modulo p. Section 3 contains the lemmas needed to prove the main result in section 4, where we provide an explicit description of the conjugacy classes in $\mathrm{Qd}(p)$ in terms of the lifted categories of conjugacy classes from $\mathrm{SL}(2,p)$. Lastly, in section 5, we provide formulas for the sizes of each conjugacy class in $\mathrm{Qd}(p)$ in terms of the prime p. Tables summarizing conjugacy class data for $\mathrm{SL}(2,p)$ and $\mathrm{Qd}(p)$ appear in Sections 2 and 5, respectively.

1. Background

We recall here the structure of the group Qd(p), as well as some definitions and notation that we will use throughout the remainder of this paper.

The special affine group. We assume throughout that p is an odd prime. By definition, Qd(p) is a semi-direct product group $(\mathbb{Z}_p \times \mathbb{Z}_p) \rtimes \mathrm{SL}(2, p)$, where the special linear group $\mathrm{SL}(2, p)$ acts on the group $\mathbb{Z}_p \times \mathbb{Z}_p$ by left matrix multiplication. We identify the abelian group $\mathbb{Z}_p \times \mathbb{Z}_p$ with the two-dimensional $\mathbb{F}_p$-vector space $\mathbb{F}_p \times \mathbb{F}_p = \mathbb{F}_p^2$, where $\mathbb{F}_p$ denotes a field with p elements. The group Qd(p) is sometimes referred to as the *special affine group over* $\mathbb{F}_p^2$.

The group operation. A generic element of Qd(p) is written as an ordered pair (v, A), where v is an element of $\mathbb{F}_p^2$ and A is an element of $\mathrm{SL}(2, p)$. For elements $g = (v, A)$ and $h = (z, P)$ of Qd(p), the multiplication is given by $gh = (v, A) \cdot (z, P) = (v + Az, AP)$, where Az is the action of A on z and AP is multiplication in $\mathrm{SL}(2, p)$. The identity element of Qd(p) is $(0, I)$. The inverse in Qd(p) of the element $h = (z, P)$ is $h^{-1} = \left(-P^{-1}z,\ P^{-1}\right)$, and so conjugating g by h in Qd(p) yields

$$hgh^{-1} = \left((I - PAP^{-1})z + Pv,\ PAP^{-1}\right). \tag{1}$$

Note that eq. (1) implies that conjugation in Qd(p) involves conjugation of A in $\mathrm{SL}(2, p)$ in the matrix component and a change in v within $\mathbb{F}_p^2$ in the vector component. Consequently, if A and B are not $\mathrm{SL}(2, p)$-conjugate, then in Qd(p), the elements (v, A) and (w, B) are not conjugate for any choice of vectors v and w. Even when A and B are $\mathrm{SL}(2, p)$-conjugate, the elements (v, A) and (w, B) in Qd(p) may fail to be conjugate, where the obstruction to conjugacy can be expressed in terms of a distinguished "shifted vector" defined in definition 4.5. We also note that it is possible to realize Qd(p) as a subgroup of $\mathrm{SL}(3, p)$ by embedding each element (v, A) with $v = (x, y)^T$ into $\mathrm{SL}(3, p)$ using the following identification:

$$(v, A) \mapsto \begin{pmatrix} & & x \\ & A & y \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{SL}(3, p).$$

Notation and conventions. We use the standard notation of $\mathbb{F}_p^\times$ for the multiplicative group of nonzero elements of $\mathbb{F}_p$. For arbitrary elements of the field, we generally use the lowercase letters a, b, c, d, x, or y, while for elements of $\mathbb{F}_p^2$, we generally use the letters u, v, w, or z, and we use 0 for the zero vector. Matrices in $\mathrm{SL}(2, p)$ are usually denoted by A, B, P, Q, S, and Z, and the script letters $\mathcal{C}$, $\mathcal{D}$, $\mathcal{E}$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ are reserved to denote conjugacy classes in $\mathrm{SL}(2, p)$. For $A, B \in \mathrm{SL}(2, p)$, we write $A \sim B$ to mean A and B are conjugate in $\mathrm{SL}(2, p)$. For a set X, we write $|X|$ for the cardinality of X, and for a matrix A in $\mathrm{SL}(2, p)$, we write $|A|$ for its order in $\mathrm{SL}(2, p)$. For (v, A) in Qd(p), we denote by $\mathrm{Class}_{\mathrm{Qd}(p)}(v, A)$ the conjugacy class of (v, A) in Qd(p), and for an element A in $\mathrm{SL}(2, p)$, we denote the conjugacy class in $\mathrm{SL}(2, p)$ by $\mathrm{Class}_{\mathrm{SL}(2,p)}(A)$. For

a matrix A in $\mathrm{SL}(2,p)$, we denote by $\mathrm{Fix}(A)$ the set of elements of $\mathbb{F}_p^2$ that are fixed by the action of A. For a set $X \subseteq \mathbb{F}_p^2$, we write $\mathrm{Span}\{X\}$ for the $\mathbb{F}_p$-span of X.

2. Conjugacy classes in SL(2, p)

Here, we recall the conjugacy classes in $\mathrm{SL}(2,p)$; refer to [6] and see table 1 for a summary of the class data. These conjugacy classes can be categorized by their eigenvalues or by *quadratic (non)residues*, which we recall in the following definition.

TABLE 1. Conjugacy class data in $\mathrm{SL}(2,p)$.
(See Appendix C.4 in [6] and [3].)

Label	Size	Number	Rep. Element	Element Order	Nature	Eigenvalues Eigenvectors	Characteristic Polynomial
I	1	1	$\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$	1	Scalar	$1,1$	$(x-1)^2$
$-I$	1	1	$\left(\begin{smallmatrix}-1&0\\0&-1\end{smallmatrix}\right)$	2	Scalar	$-1,-1$	$(x+1)^2$
$\mathcal{C}$	$\frac{p^2-1}{2}$	1	$\left(\begin{smallmatrix}1&c\\0&1\end{smallmatrix}\right)$	p	Nondiag. c residue	$1,\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$	$(x-1)^2$
$\mathcal{D}$	$\frac{p^2-1}{2}$	1	$\left(\begin{smallmatrix}1&d\\0&1\end{smallmatrix}\right)$	p	Nondiag. d nonresidue	$1,\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$	$(x-1)^2$
$\mathcal{E}$	$\frac{p^2-1}{2}$	1	$\left(\begin{smallmatrix}-1&c\\0&-1\end{smallmatrix}\right)$	$2p$	Nondiag. c residue	$-1,\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$	$(x+1)^2$
$\mathcal{F}$	$\frac{p^2-1}{2}$	1	$\left(\begin{smallmatrix}-1&d\\0&-1\end{smallmatrix}\right)$	$2p$	Nondiag. d nonresidue	$-1,\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$	$(x+1)^2$
$\mathcal{G}_i$	$p(p-1)$	$\frac{p-1}{2}$	$\left(\begin{smallmatrix}0&-1\\1&1\end{smallmatrix}\right)$	Divisor of p^2-1	Diag. over $\mathbb{F}_{p^2}$ Nondiag. over $\mathbb{F}_p$	None in $\mathbb{F}_p$	x^2-ax+1 Irreducible
$\mathcal{H}_j$	$p(p+1)$	$\frac{p-3}{2}$	$\left(\begin{smallmatrix}j&0\\0&\frac{1}{j}\end{smallmatrix}\right)$	Order of $j \in \mathbb{F}_p^\times$ Divisor of $p-1$	Diag. over $\mathbb{F}_p$	$j,\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$ $\frac{1}{j},\left(\begin{smallmatrix}0\\1\end{smallmatrix}\right)$	$(x-j)(x-\frac{1}{j})$

Definition 2.1. [11, section 11.1]. For a prime p, a nonzero integer b is a *quadratic residue* of p if the congruence $x^2 \equiv b \mod p$ has a solution. If no solution exists in $\mathbb{F}_p$, then b is a *quadratic nonresidue* of p.

Class of the identity matrix. The identity matrix forms its own conjugacy class of size one.

Classes of types $\mathcal{C}$ and $\mathcal{D}$. The matrices in these two conjugacy classes have repeated eigenvalue 1, and their corresponding eigenspaces are one-dimensional. In $\mathrm{GL}(2,p)$, such matrices form a single conjugacy class, but in $\mathrm{SL}(2,p)$, they split into two distinct classes, where each class is represented by an upper-triangular matrix with 1's along the diagonal. The following lemma uses the notion of quadratic (non)residues modulo p to characterize this splitting, and

a full characterization of classes $\mathcal{C}$ and $\mathcal{D}$ is given following the proof of the lemma.

Lemma 2.2. *Let p be an odd prime. Then the matrices $\left(\begin{smallmatrix}1 & x\\ 0 & 1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}1 & y\\ 0 & 1\end{smallmatrix}\right)$ are conjugate in* SL(2, p) *if and only if x and y are both quadratic residues modulo p or both quadratic nonresidues modulo p; an analogous result holds for matrices of the form $\left(\begin{smallmatrix}-1 & x\\ 0 & -1\end{smallmatrix}\right)$.*

Proof. Let $P = \left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)$ be a matrix in SL(2, p) and fix an element $x \in \mathbb{F}_p^\times$. By a straightforward calculation, we observe that $\left(\begin{smallmatrix}1 & x\\ 0 & 1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}1 & y\\ 0 & 1\end{smallmatrix}\right)$ are conjugate in SL(2, p) if and only if $y = a^2x$ for some $a \in \mathbb{F}_p$. We claim that $y = a^2x$ is a quadratic residue modulo p if and only if x is. If x is a quadratic residue, there exists some $w \in \mathbb{F}_p^\times$ such that $x \equiv w^2 \mod p$. Writing

$$y = a^2x \equiv a^2w^2 \mod p \equiv (aw)^2 \mod p,$$

we see that y is also a quadratic residue; the proof of the converse direction proceeds similarly. Furthermore, since 1 is a quadratic residue modulo p, we conclude that $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}1 & a^2\\ 0 & 1\end{smallmatrix}\right)$ are conjugate for every $a \in \mathbb{F}_p^\times$. By theorem 11.1 in [11], there are exactly $\frac{p-1}{2}$ distinct quadratic residues and $\frac{p-1}{2}$ distinct quadratic nonresidues in $\mathbb{F}_p^\times$. Fixing a nonresidue c that is not equal to 1, we observe that there are $\frac{p-1}{2}$ matrices of the form $\left(\begin{smallmatrix}1 & a^2c\\ 0 & 1\end{smallmatrix}\right)$, all of which are conjugate to each other in SL(2, p). The argument for matrices of the form $\left(\begin{smallmatrix}-1 & x\\ 0 & -1\end{smallmatrix}\right)$ is completely analogous. □

We give the label $\mathcal{C}$ to the conjugacy class containing the upper-triangular matrices of the form $\left(\begin{smallmatrix}1 & x\\ 0 & 1\end{smallmatrix}\right)$, where x is a quadratic residue; in general, $\mathcal{C}$ also contains matrices which do not have this form. It is often convenient to select $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ as the class representative. Similarly, we give the label $\mathcal{D}$ to the conjugacy class containing the upper-triangular matrices of the form $\left(\begin{smallmatrix}1 & b\\ 0 & 1\end{smallmatrix}\right)$, where b is a quadratic nonresidue; in general, $\mathcal{D}$ also contains matrices which do not have this form.

Remaining class types. The labels $\mathcal{E}$ and $\mathcal{F}$ are given to classes containing elements of the form $\left(\begin{smallmatrix}-1 & b\\ 0 & -1\end{smallmatrix}\right)$, where b is a quadratic residue or nonresidue modulo p, respectively, and each of these classes is larger than the set of matrices of the indicated upper-triangular form. The matrices in the remaining conjugacy classes in SL(2, p) also have eigenvalues not equal to 1, and so they fix no vectors. These classes are labeled as $-I$ (for negative of the identity), $\mathcal{G}_i$, and $\mathcal{H}_j$.

3. Linear transformations

In this section, we record the results that we will need to prove the results of the Qd(p)-conjugacy class. The statements here are in terms of the conjugacy class types described in section 2.

Lemma 3.1. *If $A \in \mathcal{C} \cup \mathcal{D} \subset \mathrm{SL}(2,p)$, then there exists a basis $\{v_1, v_2\}$ for $\mathbb{F}_p^2$ such that $Av_1 = v_1$ and $Av_2 = bv_1 + v_2$ for some $b \in \mathbb{F}_p^\times$.*

Proof. Since $A \in \mathcal{C} \cup \mathcal{D}$, then by lemma 2.2 and the discussion following its proof, A is $\mathrm{SL}(2,p)$-conjugate to some upper-triangular matrix Z with 1 along the diagonal and some $b \in \mathbb{F}_p^\times$ in the upper right entry. Let $P \in \mathrm{SL}(2,p)$ be such that $A = PZP^{-1}$ and set $v_1 = Pe_1$ and $v_2 = Pe_2$ for standard basis vectors e_1 and e_2 of $\mathbb{F}_p^2$. Then $\{v_1, v_2\}$ is a basis for $\mathbb{F}_p^2$ (as P invertible) and since $Ze_1 = e_1$ and $Ze_2 = be_1 + e_2$, we have that $Av_1 = PZP^{-1}Pe_1 = Pe_1 = v_1$ and $Av_2 = PZP^{-1}Pe_2 = bPe_1 + Pe_2 = bv_1 + v_2$. □

Lemma 3.2. *Let A be a matrix in $\mathrm{SL}(2,p)$. Then $A \in \mathrm{SL}(2,p)\backslash(\mathcal{C} \cup \mathcal{D} \cup \{I\})$ if and only if the map $(I - A) : \mathbb{F}_p^2 \longrightarrow \mathbb{F}_p^2$ is a bijection, and if $A \in \mathcal{C} \cup \mathcal{D}$, then $(I - A) : \mathbb{F}_p^2 \longrightarrow \mathrm{Fix}(A)$ is surjective.*

Proof. We begin by proving the first claim. Let $A \in \mathrm{SL}(2,p)\backslash(\mathcal{C} \cup \mathcal{D} \cup \{I\})$. Then the claim is true if and only if $I - A$ is an invertible matrix. Suppose, for the sake of contradiction, that $I - A$ is not invertible. Then its nullspace contains a nonzero vector, say v. Thus,

$$(I - A)v = 0 \qquad \text{which implies that} \qquad Av = v\,.$$

Therefore v is fixed by A, so v is an eigenvector of A with eigenvalue 1. But since $A \in \mathrm{SL}(2,p)\backslash(\mathcal{C} \cup \mathcal{D} \cup \{I\})$, its eigenvalues are not equal to 1. Contradiction. Therefore $I - A$ is a bijection.

Conversely, assume that $I - A$ is a bijection (note that $A \neq I$). Then $Av = v$ if and only if $(I - A)v = 0$ if and only if $v = 0$. So $\mathrm{Fix}(A) = \{0\}$. Thus, 1 cannot be an eigenvalue of A. Hence, A is not in $\mathcal{C} \cup \mathcal{D} \cup \{I\}$.

Now we prove the second statement. Assume that $A \in \mathcal{C} \cup \mathcal{D}$. We first argue that $I - A : \mathbb{F}_p^2 \longrightarrow \mathrm{Fix}(A)$ is well-defined, i.e., that $(I - A)v$ is fixed by A for every $v \in \mathbb{F}_p^2$. Since $A \in \mathcal{C} \cup \mathcal{D}$, lemma 3.1 implies that there exists a basis $\{v_1, v_2\}$ for $\mathbb{F}_p^2$ such that $Av_1 = v_1$ and $Av_2 = bv_1 + v_2$ for some $b \in \mathbb{F}_p^\times$. Thus, $(I-A)v_1 = 0$ and $(I-A)v_2 = v_2 - (bv_1 + v_2) = -bv_1$, which lies in $\mathrm{Fix}(A)$, and so for any $v \in \mathbb{F}_p^2$, the vector $(I - A)v$ lies in $\mathrm{Fix}(A)$. Therefore the map is well-defined. Lastly, we argue that the map $(I - A) : \mathbb{F}_p^2 \to \mathrm{Fix}(A)$ is surjective. Fix $w \in \mathrm{Fix}(A) = \mathrm{Span}\{v_1\}$ and write $w = a\,v_1$ for some $a \in \mathbb{F}_p$. Then for $z = -ab^{-1}v_2$,

$$(I - A)z = (I - A)(-ab^{-1}v_2) = (-ab^{-1})v_2 - (-ab^{-1})(bv_1 + v_2) = av_1 = w\,,$$

and so the map is surjective. This completes the proof of the lemma. □

Lemma 3.3. *Let $A \in \mathrm{SL}(2,p)$ with $|A| = n > 1$ and define $T_A : \mathbb{F}_p^2 \to \mathbb{F}_p^2$ by $T_A = \sum_{i=0}^{n-1} A^i$. Then $T_A = 0$.*

Proof. Observe that $\mathrm{Im}(T_A) \subseteq \mathrm{Fix}(A)$ since $(I-A)T_A = T_A - T_AA = T_A - T_A = 0$. So, if $A \in \mathrm{SL}(2,p)\backslash(\mathcal{C}\cup\mathcal{D}\cup\{I\})$, then lemma 3.2 implies that the matrix $I-A$ is invertible, and hence $\mathrm{Im}(T_A) \subseteq \mathrm{Fix}(A) = \{0\}$. Now assume that $A \in \mathcal{C} \cup \mathcal{D}$

and let $v \in \mathbb{F}_p^2$. Then $|A| = n = p$ and by lemma 3.1, there is a basis $\{v_1, v_2\}$ for $\mathbb{F}_p^2$ so that $Av_1 = v_1$ and $Av_2 = bv_1 + v_2$ for some $b \in \mathbb{F}_p^\times$. So,

$$T_A(v_1) = \sum_{i=1}^{p-1} A^i v_1 = pv_1 = 0 \quad \text{and} \quad T_A(v_2) = \sum_{i=1}^{p-1} A^i v_2 = pbv_1 + \frac{p(p-1)}{2} v_2 = 0\,.$$

Writing v with respect to $\{v_1, v_2\}$, we have $T_A(v) = 0$, and so $T_A = 0$. □

4. Conjugacy classes in Qd(p)

Now we turn our attention to describing the conjugacy classes in Qd(p). We characterize the Qd(p)-conjugates in terms of the conjugacy class types in SL(2, p) as described in section 2. We saw in eq. (1) that conjugation in Qd(p) yields an ordered pair where conjugation in SL(2, p) occurs in both components. So, for an arbitrary element (v, A) in Qd(p),

$$\text{Class}_{\text{Qd}(p)}(v, A) = \{((I - PAP^{-1})z + Pv,\ PAP^{-1}) \mid P \in \text{SL}(2,p),\ z \in \mathbb{F}_p^2\}\,. \quad (2)$$

We describe the conjugacy classes corresponding to the identity, followed by the elements corresponding to matrices of type $\mathcal{C}$ and $\mathcal{D}$, and lastly, the elements corresponding to matrices from $\text{SL}(2,p)\backslash(\mathcal{C} \cup \mathcal{D} \cup \{I\})$.

Classes corresponding to the identity matrix. Fix (v, I) for some v in $\mathbb{F}_p^2$, where I is the identity matrix in SL(2, p). As I is SL(2, p)-conjugate only to itself, eq. (2) implies that

$$\text{Class}_{\text{Qd}(p)}(v, I) = \{(Pv,\ I) \mid P \in \text{SL}(2,p)\}\,. \quad (3)$$

To describe the conjugacy class $\text{Class}_{\text{Qd}(p)}(v, I)$, we need the following well-known lemma.

Lemma 4.1. *The group* SL(2, p) *acts transitively on* $\mathbb{F}_p^2 \setminus \{0\}$.

Proof. Let $e_1 = (1,0)^T$ be a standard basis vector for $\mathbb{F}_p^2$ and let $w = (w_1, w_2)^T \in \mathbb{F}_p^2$ with $w \neq 0$ so that at least one of w_1, w_2 is nonzero. We first argue that there exists a matrix $P \in \text{SL}(2,p)$ such that $Pe_1 = v$. If $P = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, then $Pe_1 = w$ implies that the first column of P must be w as

$$Pe_1 = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right) = \left(\begin{smallmatrix} w_1 \\ w_2 \end{smallmatrix}\right)\,.$$

Thus, $a = w_1$ and $c = w_2$, and since $\det(P) = 1$, we must have $w_1 d - bw_2 = 1$, which implies that we can set $b = 1$ and $d = (1 + w_2)w_1^{-1}$ if $w_1 \neq 0$ or $d = 1$ and $b = -w_2^{-1}$ if $w_1 = 0$. Now, if v, w are two nonzero vectors in $\mathbb{F}_p^2$, then by the above, there exists matrices P_1 and P_2 such that $P_1 e_1 = v$ and $P_2 e_1 = w$. Therefore, $P_2 P_1^{-1} v = w$, and so SL(2, p) acts transitively on the nonzero vectors of $\mathbb{F}_p^2$, as claimed. □

Now we describe the Qd(p)-conjugacy classes corresponding to the identity matrix.

Proposition 4.2. *For (v, I) in $\mathrm{Qd}(p)$, where I is the identity matrix and $v \in \mathbb{F}_p^2$,*

$$\mathrm{Class}_{\mathrm{Qd}(p)}(v, I) = \begin{cases} \{(0, I)\} & \text{if } v = 0 \\ \{(w, I) \mid w \in \mathbb{F}_p^2 \backslash \{0\}\} & \text{if } v \neq 0 \end{cases}.$$

Proof. If $v = 0$, then eq. (3) implies that (w, B) is conjugate to (v, I) if an only if $(w, B) = (Pv, I)$ for some $P \in \mathrm{SL}(2, p)$. Thus, $B = I$ and $Pv = 0$ for all $P \in \mathrm{SL}(2, p)$, as $v = 0$. The result follows for this case.

Now, if $v \neq 0$, then eq. (3) implies that $(w, B) \in \mathrm{Qd}(p)$ is conjugate to (v, I) if and only if $(w, B) = (Pv, I)$ for some $P \in \mathrm{SL}(2, p)$. By lemma 4.1, $\mathrm{SL}(2, p)$ acts transitively on $\mathbb{F}_p^2 \setminus \{0\}$, and so there exists $P \in \mathrm{SL}(2, p)$ with $Pv = w$. So, conjugating (v, I) by, for example, $(0, P)$, yields (w, I). □

Classes corresponding to matrices of types $\mathcal{C}$ or $\mathcal{D}$. The matrices in conjugacy classes $\mathcal{C}$ and $\mathcal{D}$ in $\mathrm{SL}(2, p)$ all have 1 as an eigenvalue, meaning that they fix nonzero vectors. It follows from lemma 3.2 that the following linear transformation has nontrivial kernel:

$$(I - A) : \mathbb{F}_p^2 \longrightarrow \mathbb{F}_p^2, \quad \text{where} \quad A \in \mathcal{C} \cup \mathcal{D}.$$

The kernel must have dimension 1 since A cannot be the identity. In the following lemma, we let e_1 and e_2 denote the standard basis vectors for $\mathbb{F}_p^2$. We observe that there can be distinct matrices P and Q that conjugate A to the same result.

Lemma 4.3. *Let $J = \left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{SL}(2, p)$ with $x \in \mathbb{F}_p^\times$, let $A = SJS^{-1}$ for some $S \in \mathrm{SL}(2, p)$, and fix $v \in \mathbb{F}_p^2$. Define $v_1 = PSe_1$ and $v_2 = PSe_2$ for some $P \in \mathrm{SL}(2, p)$. Suppose that $PAP^{-1} = QAQ^{-1}$ for some $Q \in \mathrm{SL}(2, p)$. Then the coefficients of v_2 in the expression of Pv and Qv with respect to the basis $\{v_1, v_2\}$ are either equal or are negatives of each other.*

Proof. For J, A, S, P, and Q as given in the statement, we have that $PSJS^{-1}P^{-1} = QSJS^{-1}Q^{-1}$, and so $S^{-1}P^{-1}QS$ commutes with J, which implies that

$$S^{-1}P^{-1}QS = \left(\begin{smallmatrix} \pm 1 & c \\ 0 & \pm 1 \end{smallmatrix}\right) \text{ i.e., } R := P^{-1}Q = S\left(\begin{smallmatrix} \pm 1 & c \\ 0 & \pm 1 \end{smallmatrix}\right)S^{-1} \text{ for some } c \in \mathbb{F}_p.$$

Set $e_1' = Se_1$ and $e_2' = Se_2$, so that $Re_1' = \pm e_1'$ and $Re_2' = ce_1' \pm e_2'$, and thus

$$R(ae_1' + be_2') = \pm(ae_1' + be_2') + bce_1'.$$

That is, $Rw = \pm w + bce_1'$ for any $w = ae_1' + be_2'$.

Now define $v_1 = Pe_1'$, $v_2 = Pe_2'$ (a basis for $\mathbb{F}_p^2$) and write $Pv = \alpha v_1 + \beta v_2$ for some $\alpha, \beta \in \mathbb{F}_p$. Then

$$Qv = PRv = P(\pm v + bce_1') = \pm Pv + bc \cdot Pe_1' = (\pm\alpha + bc)v_1 \pm \beta v_2.$$

Hence, the coefficients of v_2 in Pv and Qv differ by at most a sign. □

Lemma 4.4. *Fix $(v, A) \in \mathrm{Qd}(p)$ with $A \in \mathcal{C} \cup \mathcal{D}$ and let B be $\mathrm{SL}(2, p)$-conjugate to A. Then there exists a distinguished vector $w_{v,B}$ in $\mathbb{F}_p^2$ such that for every $P \in \mathrm{SL}(2, p)$ with $PAP^{-1} = B$,*

$$Pv = \pm w_{v,B} + z \qquad \text{for some } z \in \mathrm{Fix}(B).$$

In particular, if $Av = v$, then $w_{v,B} = 0$.

Proof. Since $A \in \mathcal{C} \cup \mathcal{D}$, we know A is SL(2, p)-conjugate to $J = \left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right)$ for some $x \in \mathbb{F}_p^\times$. Let $S, P \in \mathrm{SL}(2,p)$ be such that $A = SJS^{-1}$, and $B = PAP^{-1}$ and set $v_1 = PSe_1$ and $v_2 = PSe_2$. Then $\{v_1, v_2\}$ is a basis for $\mathbb{F}_p^2$ and we may write $Pv = \alpha v_1 + \beta v_2$ for some $\alpha, \beta \in \mathbb{F}_p$. Then by lemma 4.3, we may take the distinguished vector to be $w_{v,B} = \beta v_2$ to see that if $Q \in \mathrm{SL}(2,p)$ is any matrix such that $QAQ^{-1} = B$, then $Qv = \pm w_{v,B} + z$ for some z in Fix(B). Note that if $Av = v$, then Pv is fixed by B, so $Pv = \alpha v_1$, and thus $w_{v,B} = 0$. □

Definition 4.5. Let $A \in \mathcal{C} \cup \mathcal{D}$ and let $B \sim A$. By lemma 4.4, there exists a vector $w_{v,B} \in \mathbb{F}_p^2$ such that for every $P \in \mathrm{SL}(2,p)$ satisfying $PAP^{-1} = B$, the matrix P sends v to a vector of the form

$$Pv = \pm w_{v,B} + z \qquad \text{for some } z \in \mathrm{Fix}(B)\,.$$

We call any such choice of $w_{v,B}$ the *shifted vector* for B determined by v (*s.v. of* B, for short).

Remark 4.6. *By lemma 4.3, different choices of basis or conjugating matrix alter $w_{v,B}$ by only a sign. Consequently, the set*

$$\big(w_{v,B} + \mathrm{Fix}(B)\big) \cup \big(-w_{v,B} + \mathrm{Fix}(B)\big)$$

is independent of the choice of shifted vector.

In the proposition below, recall $A \sim B$ means A is SL(2, p)-conjugate to B.

Proposition 4.7. *Let $(v,\ A) \in \mathrm{Qd}(p)$ with $A \in \mathcal{C} \cup \mathcal{D}$. Then the conjugacy class* $\mathrm{Class}_{\mathrm{Qd}(p)}(v,\ A)$ *is given by the following set:*

$$\bigcup_{\substack{B \in \mathcal{C} \cup \mathcal{D} \\ B \sim A}} \Big\{ (\pm w_{v,B} + z,\ B) \,\Big|\, z \in \mathrm{Fix}(B) \text{ and } w_{v,B} \text{ is the s.v. for } B \text{ determined by } v \Big\}.$$

Proof. Let (x, B) be in the union. Then $(x,\ B) = (\pm w_{v,B} + z,\ B)$, where $A \sim B$, $z \in \mathrm{Fix}(B)$, and $w_{v,B}$ is a shifted vector of B. We show $(x,\ B)$ is Qd(p)-conjugate to $(v,\ A)$. As $A \sim B$, there exists $P \in \mathrm{SL}(2,p)$ such that $B = PAP^{-1}$, and so by lemma 4.4, $Pv = \pm w_{v,B} + z'$ for some $z' \in \mathrm{Fix}(B)$. As $I - B$ is surjective onto Fix(B), there is $w \in \mathbb{F}_p^2$ with $(I - B)w = z - z'$. So, by conjugating $(v,\ A)$ by $(w,\ P)$,

$$\begin{aligned} &((I - PAP^{-1})w + Pv,\ PAP^{-1}) \\ &\qquad = ((I - B)w + Pv,\ B) = (z - z' \pm w_{v,B} + z',\ B) = (\pm w_{v,B} + z,\ B)\,. \end{aligned}$$

Therefore $(x,\ B)$ lies in $\mathrm{Class}_{\mathrm{Qd}(p)}(v,\ A)$.

Now suppose $(x,\ B)$ is Qd(p)-conjugate to $(v,\ A)$. Then there exists $(w,\ P)$ in Qd(p) such that

$$(x, B) = ((I - PAP^{-1})w + Pv,\ PAP^{-1})\,.$$

Thus, we immediately see that $B = PAP^{-1}$ and so $A \sim B$. By lemma 4.4, there exists a shifted vector $w_{v,B}$ in $\mathbb{F}_p^2$ such that $Pv = \pm w_{v,B} + z'$ for some $z' \in \mathrm{Fix}(B)$.

Since $(I-PAP^{-1})w = (I-B)w := z''$ lies in $\mathrm{Fix}(B)$, then $z := z'+z'' \in \mathrm{Fix}(B)$ (as $z' \in \mathrm{Fix}(B)$). Thus, $x = \pm w_{v,B} + z$ for $w_{v,B}$ a shifted vector for B and $z \in \mathrm{Fix}(B)$. Thus, (x, B) lies in the union. □

As a consequence of proposition 4.7, each conjugacy class in $\mathrm{Qd}(p)$ is completely determined by the corresponding shifted vector up to sign.

Classes corresponding to the remaining class types. Here, we characterize the conjugacy class of an element $g = (v, A)$, where $A \neq I$ is not conjugate to any matrix of type $\mathcal{C}$ or $\mathcal{D}$.

Proposition 4.8. *Let $(v, A) \in \mathrm{Qd}(p)$ with $A \in \mathrm{SL}(2,p)\backslash(\mathcal{C} \cup \mathcal{D} \cup \{I\})$ and $v \in \mathbb{F}_p^2$. Then*

$$\mathrm{Class}_{\mathrm{Qd}(p)}(v, A) = \left\{(w, B) \mid B \sim A \text{ and } w \in \mathbb{F}_p^2\right\}.$$

In other words, the conjugacy class is as large as possible.

Proof. Let A be in $\mathrm{SL}(2,p)\backslash(\mathcal{C} \cup \mathcal{D} \cup \{I\})$ and v in $\mathbb{F}_p^2$. We claim that (v, A) is $\mathrm{Qd}(p)$-conjugate to (w, B) if and only if $B = PAP^{-1}$ for some P in $\mathrm{SL}(2,p)$. Suppose that (v, A) is conjugate to (w, B) in $\mathrm{Qd}(p)$ for some element (w, B) of $\mathrm{Qd}(p)$. Then there exists an element (z, P) in $\mathrm{Qd}(p)$ such that conjugating (v, A) by this element results in (w, B). eq. (2) implies

$$((I - PAP^{-1})z + Pv,\ PAP^{-1}) = (w, B),$$

which implies that $B = PAP^{-1}$, as claimed.

Conversely, fix $(w, B) \in \mathrm{Qd}(p)$ and suppose $B = PAP^{-1}$ for some P in $\mathrm{SL}(2,p)$. We argue that (v, A) is $\mathrm{Qd}(p)$-conjugate to (w, B). Since $A \notin \mathcal{C} \cup \mathcal{D} \cup \{I\}$, lemma 3.2 implies that, as a linear transformation, $I - B$ is a bijection, and so is invertible. Set $z := (I - B)^{-1}(w - Pv)$ and conjugate (v, A) by (z, P) to get

$$((I - B)z + Pv,\ B) = ((I - B)(I - B)^{-1}(w - Pv) + Pv,\ B) = (w, B).$$

Thus, (v, A) and (w, B) are $\mathrm{Qd}(p)$-conjugate, completing the proof. □

Combine propositions 4.2, 4.7 and 4.8 to yield our main result, theorem 0.1.

5. Summary of conjugacy class data

In this section, we justify the conjugacy class data for $\mathrm{Qd}(p)$ provided in table 2. We provide, in terms of the prime p, the sizes of the conjugacy classes and the number of such conjugacy classes of each type, and we also include the order of each element in $\mathrm{Qd}(p)$.

TABLE 2. Conjugacy class data in Qd(p)

Label	Size	Number	Elements	Element Order
I	1	1	$\{(0, I)\}$	1
$-I$	p^2	1	$\mathbb{F}_p^2 \times \{-I\}$	2
I^c	$p^2 - 1$	1	$\left(\mathbb{F}_p^2 \backslash \{0\}\right) \times \{I\}$	p
$\widehat{\mathcal{C}_0}$	$\frac{p(p^2-1)}{2}$	1	$\{(v, A) \mid Av = v,\ A \in \mathcal{C}\}$	p
$\widehat{\mathcal{C}_k}$	$p(p^2 - 1)$	$\frac{p-1}{2}$	See proposition 4.7	p
$\widehat{\mathcal{D}_0}$	$\frac{p(p^2-1)}{2}$	1	$\{(w, B) \mid Bw = w, B \in \mathcal{D}\}$	p
$\widehat{\mathcal{D}_k}$	$p(p^2 - 1)$	$\frac{p-1}{2}$	See proposition 4.7	p
$\widehat{\mathcal{E}}$	$\frac{p^2(p^2-1)}{2}$	1	$\mathbb{F}_p^2 \times \mathcal{E}$	$2p$
$\widehat{\mathcal{F}}$	$\frac{p^2(p^2-1)}{2}$	1	$\mathbb{F}_p^2 \times \mathcal{F}$	$2p$
$\widehat{\mathcal{G}_i}$	$p^3(p - 1)$	$\frac{p-1}{2}$	$\mathbb{F}_p^2 \times \mathcal{G}_i$	order of i in $\mathbb{F}_{p^2}^\times$ divisor of $p^2 - 1$ (proposition 5.7)
$\widehat{\mathcal{H}_j}$	$p^3(p + 1)$	$\frac{p-3}{2}$	$\mathbb{F}_p^2 \times \mathcal{H}_j$	order of j in $\mathbb{F}_p^\times$ divisor of $p - 1$ (proposition 5.7)

Sizes of conjugacy classes. We consider sizes of each of the cases in theorem 0.1 in reverse order. We first consider the conjugacy class corresponding to matrices in $\mathrm{SL}(2,p)\backslash(\mathcal{C}\cup\mathcal{D}\cup\{I\})$.

Proposition 5.1. *Let $(v,A)\in \mathrm{Qd}(p)$. If $A\in \mathrm{SL}(2,p)\backslash(\mathcal{C}\cup\mathcal{D}\cup\{I\})$ and $v\in\mathbb{F}_p^2$, then*

$$|\mathrm{Class}_{\mathrm{Qd}(p)}(v,A)| = p^2\cdot|\mathrm{Class}_{\mathrm{SL}(2,p)}(A)|\,,$$

where $|\mathrm{Class}_{\mathrm{SL}(2,p)}(A)|$ depends on A and is given in table 1.

Proof. By proposition 4.8, $\mathrm{Class}_{\mathrm{Qd}(p)}(v,A)=\{(w,B)\,|\,B\sim A \text{ and } w\in\mathbb{F}_p^2\}$. So, since there are $|\mathbb{F}_p^2|=p^2$ choices for w and since the are $|\mathrm{Class}_{\mathrm{SL}(2,p)}(A)|$ choices for a matrix B with $B\sim A$, the given formula for $|\mathrm{Class}_{\mathrm{Qd}(p)}(v,A)|$ follows immediately. □

In the following proposition, we see that the size of the conjugacy class of $(v,A)\in\mathrm{Qd}(p)$, where A is of type $\mathcal{C}$ or $\mathcal{D}$, depends on whether or not v is fixed by A.

Proposition 5.2. *Let $(v,A)\in\mathrm{Qd}(p)$. If $A\in\mathcal{C}\cup\mathcal{D}\subset\mathrm{SL}(2,p)$ and $v\in\mathbb{F}_p^2$, then*

$$\left|\mathrm{Class}_{\mathrm{Qd}(p)}(v,A)\right| = \begin{cases}\dfrac{p(p^2-1)}{2} & \text{if } Av=v\\[2ex] p(p^2-1) & \text{if } Av\neq v\,.\end{cases}$$

Proof. Let A be a matrix in $\mathcal{C}\cup\mathcal{D}\subset\mathrm{SL}(2,p)$ and v is a vector in $\mathbb{F}_p^2$ such that $Av\neq v$. By lemma 4.4, we see that each matrix B that is conjugate to A is paired with vectors of the form $\pm w_{v,B}+z$, where B is $\mathrm{SL}(2,p)$-conjugate to A and $z\in\mathrm{Fix}(B)$. By lemma 4.3, the (nonzero) vector $w_{v,B}$ is uniquely determined up to sign. Since $\mathrm{Fix}(B)$ is a one-dimensional vector space, we can express each $z\in\mathrm{Fix}(B)$ as a scalar multiple of some nonzero vector that spans $\mathrm{Fix}(B)$. In summary, there are $|\mathcal{C}|=|\mathcal{D}|$ choices for B such that B is $\mathrm{SL}(2,p)$-conjugate to A, and once B is chosen, there is one shifted vector $w_{v,B}$ for B with 2 choices for its sign, and p choices for the vector $z\in\mathrm{Fix}(B)$. This yields a total of $2p\cdot|\mathcal{C}|=2p\cdot|\mathcal{D}|$ elements in $\mathrm{Qd}(p)$ that are conjugate to (v,A). In the case $Av=v$, the shifted vector $w_{v,B}=0$ by lemma 4.4, so the order of $\mathrm{Class}_{\mathrm{Qd}(p)}(v,A)$ is $p\cdot|\mathcal{C}|$. □

We note that it is also possible to determine the size of the conjugacy class (v,A) by applying the Orbit-Stabilizer Theorem as follows: in the case $Av\neq v$, proposition 5.2 implies that

$$|\mathrm{Centralizer}_{\mathrm{Qd}(p)}(v,A)| = \frac{|\mathrm{Qd}(p)|}{|\mathrm{Class}_{\mathrm{Qd}(p)}(v,A)|} = \frac{p^3(p^2-1)}{p(p^2-1)} = p^2\,.$$

Lastly, we analyze the classes that correspond to the identity matrix. The conjugacy class size of (v,I) depends on whether or not v is the zero vector.

Proposition 5.3. *Let* $(v, A) \in \mathrm{Qd}(p)$. *If* $A = I$ *and* $v \in \mathbb{F}_p^2$, *then*

$$|\mathrm{Class}_{\mathrm{Qd}(p)}(v, A)| = \begin{cases} 1 & \text{if } v = 0 \\ p-1 & \text{if } v \neq 0\,. \end{cases}$$

Proof. First assume that $v = 0$. Then $\mathrm{Class}_{\mathrm{Qd}(p)}(v, A) = \{(0, I)\}$ by proposition 4.2, which clearly has cardinality one, as claimed. Now assume that $v \neq 0$. Then again by proposition 4.2, we have that $\mathrm{Class}_{\mathrm{Qd}(p)}(v, A) = \{(w, I) \ : \ w \in \mathbb{F}_p^2 \backslash \{0\}\}$, which has cardinality $p - 1$. □

Number of conjugacy classes. Here, we provide the number of conjugacy class in Qd(p) of each type. Again, we consider the conjugacy classes listed in theorem 0.1 in reverse order.

Proposition 5.4. *For each of the conjugacy classes* $-I$, $\mathcal{E}$, $\mathcal{F}$, $\mathcal{G}_i$ *and* $\mathcal{H}_j$ *in* SL(2, p), *there exists exactly one corresponding conjugacy class in* Qd(p).

Proof. By proposition 4.8, each of these conjugacy classes takes the form of a direct product of the SL(2, p)-conjugacy class with $\mathbb{F}_p^2$, and so the class is as large as possible. □

The classes in Qd(p) corresponding to the matrices in of types $\mathcal{C}$ and $\mathcal{D}$ split into multiple classes depending on whether the shifted vector involved (see definition 4.5) is zero or nonzero.

Proposition 5.5. *In* Qd(p), *there are* $\frac{p+1}{2}$ *distinct conjugacy classes corresponding to the conjugacy class* $\mathcal{C}$ *in* SL(2, p): *one class of cardinality* $\frac{p(p^2-1)}{2}$ *and* $\frac{p-1}{2}$ *classes of cardinality* $p(p^2 - 1)$. *A completely analogous result holds for the conjugacy class* $\mathcal{D}$.

Proof. By eq. (1), a conjugate of $(v, A) \in \mathrm{Qd}(p)$ must be contained in the set $\mathbb{F}_p^2 \times \mathcal{C}$, which has cardinality $\frac{p^2(p^2-1)}{2}$. First, we claim that if (v, A) and (v', A') are two elements of Qd(p) such that $A, A' \in \mathcal{C}$ and $Av = v$ and $A'v' = v'$, then (v, A) and (v', A') lie in the same conjugacy class. Since $Av = v$ and $Av' = v'$, lemma 4.4 implies the corresponding shifted vectors for a conjugate of A and A' are always equal to zero. Thus, as $A \sim A'$,

$$\mathrm{Class}_{\mathrm{Qd}(p)}(v, A) = \left\{(z, B) \mid B \sim A, \text{ and } Bz = z\right\} = \mathrm{Class}_{\mathrm{Qd}(p)}(v', A')\,.$$

Therefore, the set of all elements $(v, A) \in \mathrm{Qd}(p)$ such that $A \in \mathcal{C}$ and $Av = v$ are contained in a single conjugacy class in Qd(p), of which there are

$$|\mathrm{Fix}(A)| \cdot |\mathcal{C}| = \frac{p(p^2 - 1)}{2}$$

such elements. So, since proposition 5.2 implies that

$$|\mathrm{Class}_{\mathrm{Qd}(p)}(v, A)| = \frac{p(p^2 - 1)}{2}$$

when $A \in \mathcal{C}$, the set of all $(v, A) \in \mathrm{Qd}(p)$ with $A \in \mathcal{C}$ and $Av = v$ comprises the entire conjugacy class.

Now, there are

$$|\mathbb{F}_p^2 \times \mathcal{C}| - p \cdot |\mathcal{C}| = \frac{p^2(p^2-1)}{2} - \frac{p(p^2-1)}{2} = \frac{p(p-1)^2(p+1)}{2}$$

elements of the form (v, A) for which $Av \neq v$. By proposition 5.2, the size of every conjugacy class $\mathrm{Class}_{\mathrm{Qd}(p)}(v, A)$ in the case $Av \neq v$ is

$$2p \cdot |\mathcal{C}| = 2p \cdot \frac{p^2-1}{2} = p(p^2-1),$$

and so, as conjugacy classes are disjoint, we have

$$\frac{|\mathbb{F}_p^2 \times \mathcal{C}| - p \cdot |\mathcal{C}|}{2p \cdot |\mathcal{C}|} = \frac{\left(\frac{p(p-1)^2(p+1)}{2}\right)}{p(p^2-1)} = \frac{p-1}{2}.$$

Thus, there are $\frac{p-1}{2}$ such classes. A similar argument shows the result for classes corresponding to $\mathcal{D}$. □

Proposition 5.6. *There are two conjugacy classes in* $\mathrm{Qd}(p)$ *corresponding to the identity matrix in* $\mathrm{SL}(2, p)$*: one class of cardinality* 1 *and one class of cardinality* $p - 1$.

Proof. By proposition 4.2, the class corresponding to I splits into two classes: the singleton class containing $(0, I)$, and the set of nonzero vectors paired with the identity, $I^c = \{(v, I) \mid v \in \mathbb{F}_p^2, v \neq 0\}$. □

Sum of conjugacy class sizes. Since conjugacy classes partition the group, we can confirm that the size and number of conjugacy classes comprise

$$|\mathrm{Qd}(p)| = p^2|\mathrm{SL}(2, p)| = p^3(p^2-1)$$

elements:

$$\begin{aligned}
&|I| + |-I| + |I^c| + |\widehat{\mathcal{C}_0}| + |\widehat{\mathcal{D}_0}| + \tfrac{p-1}{2}|\widehat{\mathcal{C}_k}| + \tfrac{p-1}{2}|\widehat{\mathcal{D}_k}| + |\widehat{\mathcal{E}}| + |\widehat{\mathcal{F}}| + \tfrac{p-1}{2}|\widehat{\mathcal{G}_i}| + \tfrac{p-3}{2}|\widehat{\mathcal{H}_j}| \\
&\quad = 1 + p^2 + (p^2-1) + \tfrac{p(p^2-1)}{2} + \tfrac{p(p^2-1)}{2} + \tfrac{p-1}{2} \cdot p(p^2-1) + \tfrac{p-1}{2} \cdot p(p^2-1) \\
&\qquad\qquad + \tfrac{p^2(p^2-1)}{2} + \tfrac{p^2(p^2-1)}{2} + \tfrac{p-1}{2} \cdot p^3(p-1) + \tfrac{p-3}{2} \cdot p^3(p+1) \\
&\quad = p^3(p^2-1) = |\mathrm{Qd}(p)|, \text{ as expected.}
\end{aligned}$$

Element order. The order of an element is given in terms of the order of its matrix component.

Proposition 5.7. *Let* $v \in \mathbb{F}_p^2$*. If* $A \neq I$*, then the order of* (v, A) *in* $\mathrm{Qd}(p)$ *is equal to the order of* A *in* $\mathrm{SL}(2, p)$*. If* $v \neq 0$*, the order of* (v, I) *is* p.

Proof. Let $v \in \mathbb{F}_p^2$ and $A \in \mathrm{SL}(2,p)$. By the multiplication in $\mathrm{Qd}(p)$, for any nonnegative integer m,

$$(v,\, A)^m = (v + Av + \cdots + A^{m-1}v,\, A^m). \tag{4}$$

First, assume that $A \neq I$. If $A = -I$, then $A^2 = I$ and $(v,-I)^2 = (v - v, I) = (0, I)$. If the order of A is $n > 2$, then eq. (4) implies that $(v,\, A)^n$ yields the identity I in the second component. It remains to show that $v + Av + \cdots + A^{n-1}v = 0$, but this follows immediately from lemma 3.3. Now assume that $A = I$. In the case $(v,\, I)$ with $v = 0$, the order is one. If $v \neq 0$, observe that the additive order of v is equal to p, and so again by eq. (4), $(v,\, I)^p = (pv,\, I) = (0,\, I)$. □

Concluding remarks. Classifying the conjugacy classes in $\mathrm{Qd}(p)$ serves as a first step toward understanding the Hochschild cohomology $\mathrm{HH}^*(\mathbb{F}_p[\mathrm{Qd}(p)])$ of the group algebra $\mathbb{F}_p[\mathrm{Qd}(p)]$. In particular, the techniques developed by Siegel and Witherspoon in [13] require explicit conjugacy class representatives of the underlying group to understand the algebraic structure of the corresponding Hochschild cohomology ring. By giving a complete and explicit description of the conjugacy classes, our results make it possible to apply these techniques to investigate the ring structure of $\mathrm{HH}^*(\mathbb{F}_p[\mathrm{Qd}(p)])$.

References

[1] Adem, A.; Smith, J. H. Periodic complexes and group actions. *Ann. of Math.* **154** (2001), no. 2, 407–435. MR1865976, Zbl 0992.55011, doi: 10.2307/3062102. 1089

[2] Benson, J.; Carlson, J. F. Complexity and multiple complexes. *Math. Z.* **195** (1987), no. 2, 221–238. MR892053, Zbl 0593.20062, doi: 10.1007/BF01166459. 1089

[3] Groupprops: groupprops.subwiki.org: Element structure of special linear group of degree two over a finite field. https://groupprops.subwiki.org/wiki/Element_structure_of_special_linear_group_of_degree_two_over_a_finite_field [Accessed 06-08-2026] 1092

[4] Jackson, M. A. Qd(p)-free rank two finite groups act freely on a homotopy product of two spheres. *J. Pure Appl. Algebra* **208** (2007), no. 3, 821–831. MR2283428, Zbl 1109.57021, doi: 10.1016/j.jpaa.2006.03.018. 1089

[5] James, G.; Liebeck, M. Representations and characters of groups. Second edition. *Cambridge University Press, New York* (2001), viii+458 pp. ISBN: 0-521-00392-X. MR1864147, Zbl 0981.20004, doi: 10.1017/CBO9780511814532. 1089

[6] Kowalski, E. The large sieve and its applications. Arithmetic geometry, random walks and discrete groups. Cambridge Tracts in Mathematics, **175**. *Cambridge University Press, Cambridge*, (2008). xxii+293 pp. ISBN: 978-0-521-88851-6. MR2426239, Zbl 1177.11080, doi: 10.1017/CBO9780511542947. 1092

[7] Long, J. H. The cohomology rings of the special affine group of $\mathbb{F}_p^2$ and of PSL(3, $\mathbb{F}_p$. *ProQuest Dissertations and Theses*, 93 pp. MR2712167, 1090

[8] Long, J. H. Cohomology classes of the Qd(p) groups. *Matematica* **3** (2024), no. 1, 1–24. MR4723208, Zbl 1535.20274, doi: 10.1007/s44007-023-00073-y. 1090

[9] Long, J. H. Cohomology classes of Qd(3). *Matematica* **3** (2024), no. 1, 25–44. MR4723209, Zbl 1535.20275, doi: 10.1007/s44007-023-00074-x. 1090

[10] Long, J. H. A note on invariants of the cohomology of $\mathbb{Z}/p \times \mathbb{Z}/p$. *Missouri J. Math. Sci.* **36** (2024), no. 2, 170–175. MR4832267, Zbl 1560.20144, doi: 10.35834/2024/3602170. 1090

[11] ROSEN, K. Elementary number theory and its applications. Fifth edition. *Pearson Addison Wesley* (2005). xx+721 pp. ISBN: 0-321-23707-2. 1092, 1093

[12] THOMAS, C. B. Characteristic classes and the cohomology of finite groups. Cambridge Studies in Advanced Mathematics. **9** *Cambridge University Press, Cambridge,* 1986. xii+129 pp. ISBN: 0-521-25661-5. MR878978, Zbl 1156.20041, doi: 10.1017/CBO9780511897344. 1089

[13] SIEGEL, S. F.; WITHERSPOON, S. J. The Hochschild cohomology ring of a group algebra. *Proc. London Math. Soc. (3)* **9** (1999), no. 1, 131–157. MR1687539, Zbl 1044.16005, doi: 10.1112/S0024611599011958. 1089, 1090, 1103

(Colin M. Lawson) DEPARTMENT OF MATHEMATICS AND STATISTICS, STEPHEN F. AUSTIN STATE UNIVERSITY, NACOGDOCHES, TEXAS 75962, USA
Colin.Lawson@sfasu.edu

(Jane H. Long) DEPARTMENT OF MATHEMATICS AND STATISTICS, STEPHEN F. AUSTIN STATE UNIVERSITY, NACOGDOCHES, TEXAS 75962, USA
longjh@sfasu.edu

This paper is available via http://nyjm.albany.edu/j/2026/32-43.html.