6-1-2016

Commuting Pairs in Groups and Associated Probabilities

Tyler McAfee
Western Oregon University

Commuting Pairs in Groups and Associated Probabilities

By

Tyler McAfee

An Honors Thesis Submitted in Partial Fulfillment
of the Requirements for Graduation from the
Western Oregon University Honors Program

Dr. Michael Ward,
Thesis Advisor

Dr. Gavin Keulks,
Honors Program Director

Western Oregon University

June 2016

1. Acknowledgements

To my thesis advisor, Dr. Michael Ward, thank you for the motivation, thoughtful insight, and time that you have dedicated to the completion of this project. You were an inspiration both inside and outside of the classroom.

To Dr. Gavin Keulks, thank you for your guidance and support you have provided throughout my collegiate career.

To my parents, thank you for your encouragement and continual support throughout the years. You have instilled in me a sense of determination, which not only helped in the completion of this project, but will be something that I can utilize in the years to come.

2. Abstract

My area of research focuses on a field in mathematics called group theory. More specifically I will look at commutativity of pairs of elements in particular groups and the probabilities associated with them. My thesis will have both general and specific sections. This will allow me to generalize commutativity and more importantly, the probability associated with commuting pairs, before applying those generalizations to specific groups. Two groups will be focused on primarily, namely the dihedral groups and the matrix group $GL(2,\ \mathbb{Z}_p)$. My hope is that my work will be presented in a manner that allows mathematicians to obtain a better understanding of the theory involved. I will represent the theory with mathematical proof, both adapted from other papers and original ones as well. I enjoyed studying group theory previously and am looking forward to diving deeper into its application.

3. Introduction

The topic of studying the probability that two group elements commute is fairly new, beginning with Paul Erdos' and Paul Turan's work in 1968 [3]. Since then, mathematicians have been building upon the foundation that Erdos and Turan provided us with. For example, see [1, 5, 6, 7, 9]. This thesis will especially shine light on [2]. Furthermore, as will be seen throughout this thesis, many generalizations can be made about the probabilities associated with commutativity in specific groups. These generalizations include looking into the foundations of these probabilities as well as different ways to compute the probabilities. Several methods will be looked at in depth. We will begin with looking into the relationship that conjuacy has with commutativity, which will lead into looking at the $\frac{5}{8}$ bound that holds for the probability that two group elements commute. Next, we will look at dihedral groups and how to calculate some different probabilities associated with them. Using information about dihedral groups, we will prove a theorem that states for any positive integer m, there exists a group with the probability of two elements commuting equal to $\frac{1}{m}$. We will then turn our attention to looking at matrices, specifically the matrix group $GL(2, \mathbb{Z}_p)$. There will be an in depth analysis of the conjugacy classes associated with $GL(2, \mathbb{Z}_p)$ matrices, which will lead to calculating the probability that these group elements commute. To conclude, we will draw connections with both the dihedral groups and $GL(2, \mathbb{Z}_p)$ matrices.

4. Sufficient Background Information

The following definitions and theorems are needed to help guide our understanding of the concepts to come.

Definition 4.1 (Centralizer of a in G)**.** *Let a be a fixed element of a group G. The centralizer of a in G, $C(a)$, is that set of all elements in G that commute with a. In symbols,*

$$C(a) = \{g \in G \mid ga = ag\}.$$

[4, p. 68]

Definition 4.2 (Center of a group)**.** *The center, $Z(G)$, of a group G is the subset of elements in G that commute with every element of G. In symbols,*

$$Z(G) = \{a \in G \mid ax = xa \text{ for all } x \text{ in } G\}.$$

[4, p. 66]

Theorem 4.3 (Shoes and Socks Theorem)**.** *For group elements a and b, $(ab)^{-1} = b^{-1}a^{-1}$.* [4, p. 52]

Theorem 4.4. *Let G be a group and let $Z(G)$ be the center of G. If $G \Big/ Z(G)$ is cyclic, then G is abelian.* [4, p. 194]

Theorem 4.5 (Lagrange's Theorem)**.** *If G is a finite group and H is a subgroup of G, then H divides G. Moreover, the number of distinct left (or right) cosets of H in G is $\frac{|G|}{|H|}$, denoted $|G : H|$.* [4, p. 147]

Corollary 4.6 (Corollary 2 to Lagrange)**.** *In a finite group, the order of each element of the group divides the order of the group.* [4, p. 148]

Corollary 4.7 (Corollary 3 to Lagrange)**.** *A group of prime order is cyclic.* [4, p. 148]

Theorem 4.8 (Group Rules of Exponents (GRE))**.** *For every a in a group G and $i, j \in \mathbb{Z}$,*

1. $(a^i)^j = a^{ij}$.
2. $a^i a^j = a^{i+j}$.

Theorem 4.9 (Left Coset Equality Test)**.** *Let H be a subgroup of a group G, and let a and b belong to G. Then $aH = bH$ if and only if $a^{-1}b \in H$.* [4, p. 145]

Theorem 4.10. *Let a be an element of order n in a group and let k be a positive integer. Then $< a^k >=< a^{gcd(n,k)} >$ and $|a^k| = \frac{n}{gcd(n,k)}$.* [4, p. 80]

Theorem 4.11 (GCD Is a Linear Combination)**.** *For any nonzero integers a and b, there exists integers s and t such that $gcd(a, b) = as + bt$. Moreover, $gcd(a, b)$ is the smallest positive integer of the form $as + bt$.*

Corollary 4.12 ($|a| = | < a > |$)**.** *For any group element a, $|a| = | < a > |$.* [4, p. 79]

Theorem 4.13 (Fundamental Theorem of Cyclic Groups)**.** *Every Subgroup of a cyclic group is cyclic. Moreover, if $| < a > | = n$, then the order of any subgroup of $< a >$ is a divisor of n; and, for each positive divisor k of n, the group $< a >$ has exactly one subgroup of order k-namely, $a^{n/k}$.* [4, p. 82]

Lemma 4.14. *Suppose K is a field and F is a subfield of K. Further assume $w \in K \backslash F$. For every $x, y, c, d \in F$, $x + yw = c + dw$ if and only if $x = c$ and $y = d$.*

Lemma 4.15. *Suppose K is a field and F is a subfield of K. Further assume $w \in K \backslash F$. For every $x, y \in F$, $x + yw = 0$ if and only if $x = 0$ and $y = 0$.*

5. Conjugacy Classes

Before we begin looking into how commutative groups are, as mentioned above, we must first look into conjugacy. Conjugacy is an important concept to understand when looking into the abelianess of a group.

Definition 5.1. *Let a and b be elements of a group G. We say that a and b are conjugate in G (and call b a conjugate of a) if $xax^{-1} = b$ for some x in G. The conjugacy class of a is the set $cl(a) = \{xax^{-1} \mid x \in G\}$.*

You may recall from Abstract Algebra that one way to prove Lagrange's Theorem is to show that cosets of a subgroup partition the group. Another use for partitioning the elements of a group is to partition the group into disjoint conjugacy classes. This important concept leads to our first lemma.

Lemma 5.2. *Conjugacy is an equivalence relation on a group, G, and the conjugacy class of a is the equivalence class of a under conjugacy.*

Proof: Let G be a group. For $a, b \in G$, define $a \sim b$ to mean there is an $x \in G$ such that $xax^{-1} = b$. Let $a \in G$. Since G is a group, it follows that $eae^{-1} = a$ where e is the identity. Therefore $a \sim a$ and $\sim$ is reflexive.

Next let $b, c \in G$. Assume $b \sim c$, then $xbx^{-1} = c$ for some $x \in G$. By group algebra we have $b = x^{-1}cx = (x^{-1})c(x^{-1})^{-1}$ where $x^{-1} \in G$. Thus $c \sim b$ by definition and $\sim$ is symmetric.

Lastly, let $q, r, s \in G$. Assume $q \sim r$ and $r \sim s$, then $yqy^{-1} = r$ for some $y \in G$ and $zrz^{-1} = s$ for some $z \in G$. It follows that $z(yqy^{-1})z^{-1} = s = (zy)q(zy)^{-1}$ by group algebra and Theorem 4.3, where $zy \in G$. Hence, $q \sim s$ and $\sim$ is transitive. Therefore, conjugacy is an equivalence relation on G.

Now, let $m \in \{xax^{-1} : x \in G\}$. By definition, $m = xax^{-1}$ for some $x \in G$. Since $m \in G$, $m \in \{b \in G : b \sim a\}$. Next let $n \in \{b \in G : b \sim a\}$. Then $n \in G$ and $xax^{-1} = n$ for some $x \in G$. Thus $n \in \{xax^{-1} : x \in G\}$ by definition. Therefore, the conjugacy class of a is the equivalence relation of a under conjugacy and the lemma follows.

❏

Now that we know that conjugacy is an equivalence relation on G, let's look into the relationship between the size of $cl(a)$ and the number of left cosets of $C(a)$ in G.

Theorem 5.3. *Let G be a finite group and let a be an element of G. Then, $\mid cl(a) \mid = \mid G : C(a) \mid$.*

Proof: Define,

- $A := \{yC(a) : y \in G\}$ (The left cosets of $C(a)$ in G).
- $B := cl(a) = \{xax^{-1} : x \in G\}$ (The conjugacy class of a).

To show these sets are equal, we will show there exists a bijection from A to B.

Define $T : A \to B$ by $T(yC(a)) = yay^{-1}$. By definition of $cl(a)$ and $yay^{-1} \in cl(a)$. Thus T is defined and its outputs are in B. Let $t, z \in A$. Then by definition of A, $t = t_1C(a)$ and $z = z_1C(a)$ where $t_1, z_1 \in G$. Now, assuming $t = z$ gives us $t_1C(a) = z_1C(a)$. By Theorem 4.9 $t_1^{-1}z_1 \in C(a)$. Thus $at_1^{-1}z_1 = t_1^{-1}z_1a$ by definition of $C(a)$. Using group algebra, we obtain $t_1at_1^{-1} = z_1az_1^{-1}$. Next apply the function T, to both t and z to obtain $T(t) = t_1at_1^{-1} = z_1az_1^{-1} = T(z)$. Thus $T(t) = T(z)$, giving us that T is well-defined. Hence T is a function.

To show T is a one-to-one function, assume $T(yC(a)) = T(zC(a))$, then $yay^{-1} = zaz^{-1}$ by definition of T. By group algebra, $a(y^{-1}z) = y^{-1}(yay^{-1})z = (y^{-1}z)a$. By definition, $y^{-1}z \in C(a)$. Therefore, applying Theorem 4.9 again gives us $yC(a) = zC(a)$. Hence T is injective.

To show T is onto, let $xax^{-1} \in cl(a)$. By definition of $cl(a)$, $x \in G$. Since $C(a)$ is a subgroup of G, the coset $xC(a)$ exists. Applying T to this coset yields $T(xC(a)) = xax^{-1}$ by definition. Thus T is surjective.

Therefore, there exists a bijection from A to B, so $|cl(a)| = |B| = |A| = |G : C(a)|$.

❏

Lemma 5.4. *Suppose that a and a' are conjugate in a group G, then $|C(a)| = |C(a')|$.*

Proof: We will give an outline of the proof and leave the details for the reader.

Let a and a' be conjugate in a group G. Then $a = da'd^{-1}$ for some $d \in G$. The function $F : C(a) \to C(a')$ defined by $F(z) = dzd^{-1}$ is a bijection.

❏

Lemma 5.5. *Let G be a group and let $a, b \in G$. If $cl(a) = cl(b)$, then a is conjugate to b.*

Proof: Let G be a group and let $a, b \in G$. Assume $cl(a) = cl(b)$. Note that $a \in cl(a)$, because every element is in its own conjugacy class. It follows that $a \in cl(b)$, by hypotheses. Therefore a is conjugate to b, by definition of conjugacy class.

❏

We will now look at the relationship that conjugacy has with the center of a group.

Lemma 5.6. *If G is group and $a \in G$, then $|cl(a)| = 1$ if and only if $a \in Z(G)$.*

Proof: First assume $|cl(a)| = 1$. Let $x \in G$. By reflexivity and the definition of $cl(a)$, $a, xax^{-1} \in cl(a)$. Since there is only one element in $cl(a)$, it follows that $a = xax^{-1}$. Hence, $ax = xa$. So, by definition $a \in Z(G)$.

Next, assume $a \in Z(G)$. By definition, $a \in G$ such that $ax = xa$ for all $x \in G$. Using group algebra once more yields $a = xax^{-1}$. Since this holds for all $x \in G, cl(a) = \{a\}$. Thus $|cl(a)| = 1$.

❏

Note that "similar" in linear algebra is the same as "conjugate" in abstract algebra [10, p. 355]. This leads to a useful theorem from Strang which is the following.

Theorem 5.7 (No Change in λ's)**.** *Similar matrices A and $M^{-1}AM$ have the same eigenvalues.* [10, p. 355]

Theorem 5.8. *Suppose the 2×2 matrix A with entries in any field has two distinct eigenvalues λ_1, λ_2. Let S be the matrix with corresponding eigenvectors as its columns. Then S is invertible and $S^{-1}AS = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$. In other words A is conjugate to that diagonal matrix.* [10, pp. 300 and 298]

6. Commuting Pairs of a Group

The following two definitions are the foundation for our paper.

Definition 6.1. *For any group G, let $CP(G) \coloneqq \{(x, y) \in G \oplus G : xy = yx\}$ and $comm(G) = |CP(G)|$.*

Definition 6.2. *If G is finite group, then define $Pr(G) = \frac{comm(G)}{|G|^2}$*

Note that the denominator of $Pr(G)$, is the total number of possible pairs in G, and $comm(G)$ represents our favorable outcomes. So $Pr(G)$ is the probability that two randomly selected elements from a group commute. We will now express $Pr(G)$ in terms of how many conjugacy classes there are in a group.

Lemma 6.3. *If G is a finite group, then $Pr(G) = \frac{number\ of\ conjugacy\ classes}{|G|}$.*

Proof: Let G be a generic group and let m be the number of conjugacy classes in G. Choose one representative from each conjugacy class of G, ie. $a_1, a_2, ..., , a_m$. Since for each $a \in G$ we have $(a, b) \in CP(G)$ if and only if $b \in C(a)$, then

$$|CP(G)| = \sum_{a \in G} |C(a)|,$$

by the First Counting Principle, counting pairs by their first coordinate. Suppose that a and a' are conjugate, then $|C(a)| = |C(a')|$ by Lemma 5.4. We know that $|cl(a)| = |G : C(a)| = \frac{|G|}{|C(a)|}$ from Lemma 5.3 and Corollary 4.5. Now, we will count, using the First Counting Principle, the number of pairs with the first coordinate in the same conjugacy class. Doing this we obtain

$$\begin{aligned} |CP(G)| &= \sum_{i=1}^{m} |cl(a_i)||C(a_i)| \\ &= \sum_{i=1}^{m} \frac{|G|}{|C(a_i)|}|C(a_i) \\ &= \sum_{i=1}^{m} |G| \\ &= m|G|. \end{aligned}$$

Hence, from Definition 6.2 and above we get

$$\begin{aligned} Pr(G) &= \frac{|CP(G)|}{|G|^2} \\ &= \frac{m|G|}{|G|^2} \\ &= \frac{m}{|G|}. \end{aligned}$$

Since m is the number conjugacy classes in G, we have,

$$Pr(G) = \frac{\text{number of conjugacy classes}}{|G|}.$$

❏

The next result looks at the bound on how many cosets are associated with the subgroups of centers in a group.

Lemma 6.4. *If G is a finite, nonabelian group, then $|G : Z(G)| \geq 4$.*

Proof: Suppose that G is a finite, nonabelian group. In order to prove $|G : Z(G)| \geq 4$, we will suppose to the contrary that $|G : Z(G)| < 4$. Hence, $|G : Z(G)| = 1$,2, or 3. Assume that $|G : Z(G)| = 1$. Since $Z(G)$ is a subgroup of G, then $|G : Z(G)| = \frac{|G|}{|Z(G)|}$ by Theorem 4.5. Since the order of these groups is equal, they are the same sets and ultimately these sets contain the same elements. Thus every element of G is also in $Z(G)$. Therefore G is abelian and we have reached a contradiction, because G is a nonabelian group. Now, assume $|G : Z(G)| = 2$ or 3. Then we have $|G : Z(G)| = \frac{|G|}{|Z(G)|} = |{}^{G}\big/_{Z(G)}|$ by Theorem 4.5 and the definition of factor groups. Since 2 and 3 are prime, 4.7 states that ${}^{G}\big/_{Z(G)}$ is cyclic. Hence, by Theorem 4.4 G is abelian and again we have reached a contradiction since G is nonabelian by our original hypotheses. Thus, $|G : Z(G)| \geq 4$.

❏

Theorem 6.5. *If G is a finite, nonabelian group, then $Pr(G) \leq \frac{5}{8}$.*

Proof: First, choose one representative from each conjugacy class of G, ie. $a_1, a_2, ..., a_m$. Organize the elements so that $a_1, a_2, ..., a_i \in Z(G)$ and $a_{i+1}, a_{i+2}, ..., a_m \notin Z(G)$. We can express the number of conjugacy classes of G as $m = i + (m - i) = |Z(G)| + (m - i)$ by Lemma 5.6. Note that for $a_j \notin Z(G), |cl(a_j)| > 1$, by Lemma 5.6. Thus, there are a minimum of two elements per conjugacy class. Therefore $\frac{G \backslash Z(G)|}{2} \geq m - i$, which is the number of conjugacy classes for $a_j \notin Z(G)$, and

$$\begin{aligned} m &\leq |Z(G)| + \frac{|G \backslash Z(G)|}{2} \\ &= |Z(G)| + \frac{|G| - |Z(G)|}{2} \\ &= |Z(G)| + \frac{|G|}{2} - \frac{|Z(G)|}{2} \\ &= \frac{|Z(G)|}{2} + \frac{|G|}{2}. \end{aligned}$$

From Lemma 6.4, we have $|Z(G)| \leq \frac{|G|}{4}$. Therefore,

$$\begin{aligned} \frac{|Z(G)|}{2} + \frac{|G|}{2} &\leq \frac{\frac{|G|}{4}}{2} + \frac{|G|}{2} \\ &= \frac{5}{8}|G|. \end{aligned}$$

So we have $m \leq \frac{5}{8}|G|$. Hence $Pr(G) \leq \frac{\frac{5}{8}|G|}{|G|} = \frac{5}{8}$ by Lemma 6.3.

❏

Note, this result only holds for when G is finite and nonabelian. Clearly, if G is abelian, then $Pr(G) = 1$. Furthermore, if G is infinite, then we can only estimate the probability over a specified interval. This is beyond the scope of this research, so we will restrict ourselves to only looking at finite, nonabelian groups. We can now look at how the direct sum of groups relates to those specific probabilities. This result will be used a lot once we start looking at direct sums of dihedral groups.

Lemma 6.6. *If G and H are finite groups, then $Pr(G \oplus H) = Pr(G)Pr(H)$.*

Proof: Claim: For any finite groups G and H,

$$|CP(G \oplus H)| = |CP(G) \times CP(H)|.$$

Define $f : CP(G \oplus H) \to CP(G) \times CP(H)$ by $f((x_1, y_1), (x_2, y_2)) = ((x_1, x_2), (y_1, y_2))$. Let $a = ((x_1, y_1), (x_2, y_2)) \in CP(G \oplus H)$. By definition $(x_1, y_1), (x_2, y_2) \in G \oplus H$ and $(x_1, y_1)(x_2, y_2) = (x_2, y_2)(x_1, y_1)$. Furthermore, $(x_1x_2, y_1y_2) = (x_2x_1, y_2y_1)$ as well as $x_1x_2 = x_2x_1$ and $y_1y_2 = y_2y_1$ because equal pairs have equal coordinates. Since $x_1, x_2 \in G$ and $y_1, y_2 \in H$, $(x_1, x_2) \in CP(G)$ and $(y_1, y_2) \in CP(H)$ by definition. Thus $((x_1, x_2), (y_1, y_2)) \in CP(G) \times CP(H)$, so f is defined and $f(a)$ is in $CP(G) \times CP(H)$.

Now, let $((s_1, t_1), (s_2, t_2)) \in CP(G \oplus H)$ as well. Assume $((s_1, t_1), (s_2, t_2)) = ((x_1, y_1), (x_2, y_2))$. By definition of equal pairs $(s_1, t_1) = (x_1, y_1)$ and $(s_2, t_2) = (x_2, y_2)$. Furthermore, $s_1 = x_1,\ t_1 = y_1,\ s_2 = x_2,\ t_2 = y_2$. Applying f to the left-hand side of the equality above yields $f((s_1, t_1), (s_2, t_2)) = ((s_1, s_2), (t_1, t_2)) = ((x_1, x_2), (y_1, y_2))$. Applying f to the right-hand side yields $f((x_1, y_1), (x_2, y_2)) = ((x_1, x_2), (y_1, y_2))$. Thus by transitivity of equality, $f((s_1, t_1), (s_2, t_2)) = f((x_1, y_1), (x_2, y_2))$ and we conclude that f is a function.

Next, assume $f((s_1, t_1), (s_2, t_2)) = f((x_1, y_1), (x_2, y_2))$. By definition of f we have $((s_1, s_2), (t_1, t_2)) = ((x_1, x_2), (y_1, y_2))$. Similar to above, by definition of equal pairs we have $s_1 = x_1,\ t_1 = y_1,\ s_2 = x_2,\ t_2 = y_2$. Thus $(s_1, t_1) = (x_1, y_1)$ and $(s_2, t_2) = (x_2, y_2)$. Furthermore, $((s_1, t_1), (s_2, t_2)) = ((x_1, y_1), (x_2, y_2))$. Therefore f is injective.

Finally, let $((x_1, x_2), (y_1, y_2)) \in CP(G) \times CP(H)$. It follows that $(x_1, x_2) \in CP(G)$ and $(y_1, y_2) \in CP(H)$ by definition of $\times$. Consider $((x_1, y_1), (x_2, y_2))$. Since $(x_1, y_1),\ (x_2, y_2) \in G \oplus H$ and $(x_1x_2, y_1y_2) = (x_2x_1, y_2y_1),\ ((x_1, y_1), (x_2, y_2)) \in CP(G \oplus H)$. By definition of f, $f((x_1, y_1), (x_2, y_2)) = ((x_1, x_2), (y_1, y_2))$. Hence f is onto.

Therefore $f : CP(G \oplus H) \to CP(G) \times CP(H)$ is a bijection which shows our claim that $|CP(G \oplus H)| = |CP(G) \times CP(H)|$.

Hence, $comm(G \oplus H) = |CP(G \oplus H)| = |CP(G) \times CP(H)| = |CP(G)||CP(H)| = comm(G)comm(H)$, where the third equality follows from the Second Counting Principle. Therefore, $Pr(G \oplus H) = \frac{comm(G \oplus H)}{|G \oplus H|^2} = \frac{comm(G)comm(H)}{(|G||H|)^2} = \frac{comm(G)}{|G|^2}\frac{comm(H)}{|H|^2} = Pr(G)Pr(H)$ by definition. Hence, for any finite groups G and H, $Pr(G \oplus H) = Pr(G)Pr(H)$.

❏

7. Dihedral Groups

Recall that the dihedral group of order $2n$, denoted as D_n, can defined as the group of symmetries of a regular $n - gon$ where $n \geq 3$. There are two kinds of symmetries associated with regular $n - gons$: rotations and reflections. Denote a counterclockwise rotation with $\rho = R_{\frac{360}{n}}$. Then the elements of D_n are the rotations, $\rho^0 = R_0, \rho^1, \rho^2, ..., \rho^{n-1}$ plus n reflections. Let ϕ be any reflection. Recall that the operation in D_n is composition, however that will be dropped. Note that,

$$\rho^n = \phi^2 = R_0.$$

Lemma 7.1. *For any reflection ϕ in D_n with $n \geq 3$,*

$$\phi\rho^i = \rho^{-i}\phi$$

for every $i \geq 0$

Proof: Proceed by induction.

1.) We will consider two base cases: $i = 0$ and $i = 1$.

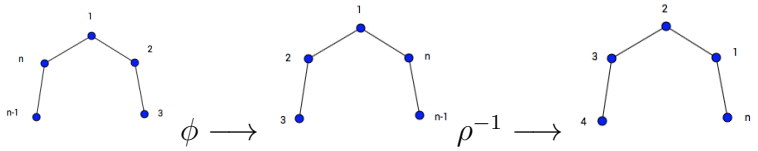
Case 1: $i = 0$.

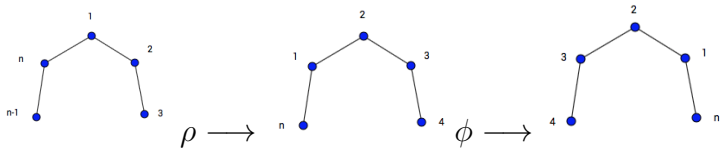
We have $\phi\rho^0 = \phi = \rho^{-0}\phi$ since $\rho^0 = R_0$. Therefore, $\phi\rho^0 = \rho^{-0}\phi$.

Case 2: $i = 1$.

Subcase: $n > 1$ is odd.

Then D_n has reflectional symmetries across axes from each vertex through midpoint of opposite side. The numbers will represent each vertex around our $n-gon$, and with both compositions, the line of reflection will be from vertex 1, to the midpoint of the opposite side. This is because n is odd.

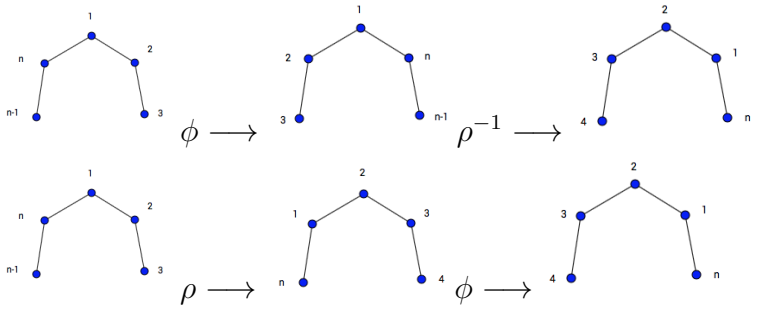




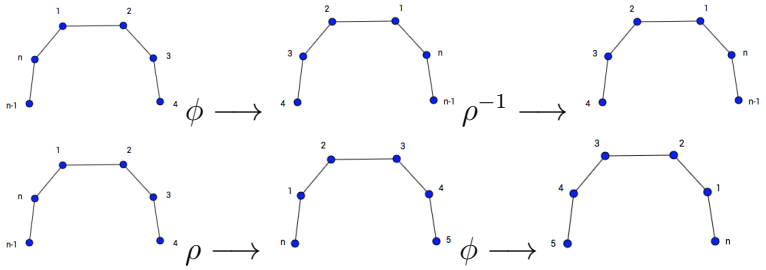
Since we obtained identical orientations for both compositions, we can conclude that $\phi\rho = \rho^{-1}\phi$ when $n > 1$ is odd.

Subcase: $n > 1$ is even.

Then D_n has two reflectional symmetries; across axes through opposite vertices, and through midpoints of opposite sides. Looking at when the reflection line is through vertex and opposite side, we have the same as with the odd case:



Looking at when the reflection line is through the midpoint of the side from vertex 1 to vertex 2, to the midpoint of opposite side, since this can occur when n is even, we obtain:



In both cases we obtain identical orientations for both $\rho\phi$ and $\phi\rho^{-1}$. Thus $\phi\rho = \rho^{-1}\phi$ when $n > 1$ is even.

Therefore, $\phi\rho = \rho^{-1}\phi$.

2.) Inductive Hypothesis: Let x be a nonnegative integer and suppose $\phi\rho^x = \rho^{-x}\phi$.

3.) Inductive Step: To show $\phi\rho^{x+1} = \rho^{-(x+1)}\phi$ note that $\phi\rho^{x+1} = \phi\rho^x\rho$. Applying our Inductive Hypothesis yields $\phi\rho^x\rho = \rho^{-x}\phi\rho$. Now, using our base case for $i = 1$ we get, $\rho^{-x}\phi\rho = \rho^{-x}\rho^{-1}\phi = \rho^{-(x+1)}\phi$. Thus $\phi\rho^{x+1} = \rho^{-(x+1)}\phi$.

Therefore, by the principle of induction, $\phi\rho^i = \rho^{-i}\phi$ for all $i \geq 0$.

❏

Lemma 7.2. *$< \rho >$ and $\phi < \rho >$ are the two left cosets of $< \rho >$ in D_n. Hence, $D_n =< \rho > \cup \phi < \rho >= \{R_0, \rho, \rho^2, ..., \rho^{n-1}, \phi, \phi\rho, \phi\rho^2, ..., \phi\rho^{n-1}\}$. Hence, the n reflections in D_n are $\phi, \phi\rho, \phi\rho^2, ..., \phi\rho^{n-1}$*

Proof: We know $< \rho >$ is a subgroup of D_n. Since $\rho^n = R_0$, and $\rho^i \neq R_0$ for any $0 < i < n$, $| < \rho > | = n$. Note, $|D_n| = 2n$. Thus by Theorem 4.5, the number of left cosets of $< \rho >$ in D_n is $\frac{|D_n|}{|<\rho>|} = \frac{2n}{n} = 2$. We can see that ${R_0}^{-1}\phi = \phi$ and by construction $\phi \notin < \rho >$. Therefore, by Theorem 4.9 $R_0 < \rho > \neq \phi < \rho >$. So $< \rho >$ and $\phi < \rho >$ are the two left cosets of $< \rho >$ in D_n. Therefore, $D_n =< \rho > \cup \phi < \rho >= \{R_0, \rho, \rho^2, ..., \rho^{n-1}, \phi, \phi\rho, \phi\rho^2, ..., \phi\rho^{n-1}\}$.

❏

Lemma 7.3. *If n is an integer and $n \geq 3$, then*

$$Z(D_n) = \begin{cases} \{R_0\} \text{ if } n \text{ is odd} \\ \{R_0, \rho^{n/2}\} \text{ if } n \text{ is even} \end{cases}$$

Proof: Assume $n \geq 3$.

($\subseteq$) Let $z \in Z(D_n)$ and ϕ be any reflection. By Lemma 7.2, suppose to the contrary that $z = \phi\rho^m$ for some m, $0 \leq m \leq n-1$. Thus $\rho(\phi\rho^m) = (\phi\rho^m)\rho$ by definition. By Lemma 7.1 we have $\rho\phi\rho^m = \rho\rho^{-m}\phi$ and $\phi\rho^m\rho = \rho^{-m}\rho^{-1}\phi$. Hence, $\rho^{-m+1}\phi = \rho^{-m-1}\phi$. Applying some group algebra yields $\rho^2 = R_0$, thus $|\rho| = 2$ because $\rho \neq R_0$. Since $|\rho| = n \geq 3$ by hypothesis, a contradiction has been reached.

Therefore, by Lemma 7.2 $z = \rho^m$ for some m, $0 \leq m \leq n-1$. This tells us that $\phi\rho^m = \rho^m\phi$ and by Lemma 7.1, $\rho^{-m}\phi = \rho^m\phi$. Applying the cancellation law we get $\rho^{-m} = \rho^m$, which implies that $(\rho^m)^2 = R_0$. Hence, $|\rho^m| = 1$ or 2.

Case 1: Assume n is odd.

First, note that $< \rho^m >$ is a subgroup of $< \rho >$. By Corollary 4.12 and Theorem 4.5, $|\rho^m| = | < \rho^m > |$ is a factor of $| < \rho > | = |\rho| = n$. It follows from n being odd that $|\rho^m| = 1$. Hence, $z = \rho^m = R_0 \in \{R_0\}$. Thus we can conclude that $Z(D_n) \subseteq \{R_0\}$ when n is odd.

Case 2: Assume n is even.

Subcase i: $|\rho^m| = 1$. Then $\rho^m = R_0 \in \{R_0, \rho^{n/2}\}$.

Subcase ii: $|\rho^m| = 2$. Remember $m \neq 0$, because $\rho^m \neq R_0$. By Theorem 4.10, $|\rho^m| = \frac{n}{GCD(n,m)}$. Since $|\rho^m| = 2$, $GCD(n, m) = \frac{n}{2}$. By definition of GCD, m is a multiple of $\frac{n}{2}$. Furthermore, $\frac{n}{2} = m$ because $\frac{n}{2}$ is the only multiple of $\frac{n}{2}$ that is less than

n. Therefore, $\rho^m = \rho^{n/2} \in \{R_0, \rho^{n/2}\}$. Thus we can conclude that $Z(D_n) \subseteq \{R_0, \rho^{n/2}\}$ when n is even.

($\supseteq$) Let $x \in D_n$. Then $xR_0 = x$ and $R_0x = x$. Hence, $xR_0 = R_0x$, so $R_0 \in Z(D_n)$ and $\{R_0\} \subseteq Z(D_n)$.

Case 1: Assume n is odd.

There is nothing to show.

Case 2: Assume n is even.

From above, $R_0 \in Z(D_n)$ for any $x \in D_n$. It remains to show that $\rho^{n/2} \in ZD_n$. Let $\phi \in D_n$, be a generic reflection. Using Lemma 7.1 and the fact that $\rho^n = R_0$, $\rho^{n/2}\phi = \phi\rho^{-n/2} = \phi\rho^{-n/2}\rho^n = \phi\rho^{n/2}$. It follows that $\rho^{n/2}\phi = \phi\rho^{n/2}$ for all $\phi \in D_n$. Now, let $\rho^i \in D_n$, $0 \leq i < n$ be generic. Then, $\rho^{n/2}\rho^i = \rho^{n/2+i} = \rho^{i+n/2} = \rho^i\rho^{n/2}$ by commutativity of $\mathbb{Z}$. Thus $\rho^{n/2}\rho^i = \rho^i\rho^{n/2}$ for any $\rho^i \in D_n$. Therefore, $\rho^{n/2} \in Z(D_n)$ when n is even, by definition. Furthermore, $\{\rho^{n/2}, R_0\} \subseteq Z(D_n)$ if n is even.

By showing these sets are subsets of each other we conclude,

$$Z(D_n) = \begin{cases} \{R_0\} \text{ if } n \text{ is odd} \\ \{R_0, \rho^{n/2}\} \text{ if } n \text{ is even} \end{cases}$$

❏

Lemma 7.4. *For every $l \in \mathbb{Z}$ $(\rho^l)^2 = R_0$ if and only if $\rho^l \in Z(D_n)$.*

Proof: Let $l \in \mathbb{Z}$. First, assume $(\rho^l)^2 = R_0$. By group algebra we obtain $\rho^l = \rho^{-l}$.

Suppose that σ is any reflection in D_n. Then $\sigma\rho^l = \sigma\rho^{-l} = \rho^l\sigma$ by Lemma 7.1.

Next suppose that ρ^m is any rotation in D_n. $\rho^l\rho^m = \rho^{l+m} = \rho^{m+l} = \rho^m\rho^l$ by GRE and commutativity of $\mathbb{Z}$. Thus by definition of $Z(D_n)$, $\rho^l \in Z(D_n)$ for every $l \in \mathbb{Z}$.

Next, assume $\rho^l \in Z(D_n)$. Then $x\rho^l = \rho^l x$ for every $x \in D_n$. Let σ be any reflection in D_n. Since $\rho^l \in Z(D_n)$, $\sigma\rho^l = \rho^l\sigma$. Applying group algebra yields $\rho^{-1}\sigma\rho^l = \sigma$. By Lemma 7.1 we have $\sigma\rho^l\rho^l = \sigma$ because σ is a reflection in D_n. Furthermore, by group algebra, $(\rho^l)^2 = R_0$.

Thus $(\rho^l)^2 = R_0$ if and only if $\rho^l \in Z(D_n)$.

❏

The next three lemmas look at the cases where commutativty holds with two elements from D_n. Looking at our pairs of elements, Lemma 7.5 deals with two rotations. Lemma 7.6 deals with a rotation and a reflection. Finally, Lemma 7.7 deals with commuting two reflections. These lemmas will lead to the proof of Theorem 7.9.

Lemma 7.5. *For every $0 \leq i, j < n$, ρ^i and ρ^j commute.*

Proof: Let $0 \leq i, j < n$. We can see that $\rho^i\rho^j = \rho^{i+j} = \rho^{j+i} = \rho^j\rho^i$ by Theorem 4.8 and commutativity of $\mathbb{Z}$. Thus $\rho^i\rho^j = \rho^j\rho^i$ for every $0 \leq i, j < n$.

❏

Lemma 7.6. *For every $0 \leq i, j < n$, ρ^j and $\phi\rho^i$ commute if and only if $\rho^j \in Z(D_n)$.*

Proof: Let $0 \leq i, j < n$. First, assume $\rho^j(\phi\rho^i) = (\phi\rho^i)\rho^j$. By associativity and Lemma 7.5, $\rho^j(\phi\rho^i) = \phi\rho^j\rho^i$. Applying Lemma 7.1 to the right hand side yields $\rho^j(\phi\rho^i) = \rho^{-j}\phi\rho^i$. By group algebra, $R_0 = \rho^{-2j}$. Since $\rho^{-2j} = R_0$ and $(\rho^j)^2 = R_0$, by Lemma 7.4 $\rho^j \in Z(D_n)$.

Now, assume $\rho^j \in Z(D_n)$. Therefore, ρ^j commutes with every element in D_n. Since $\phi\rho^i \in D_n$ by closure, ρ^j and $\phi\rho^i$ commute.

Hence, ρ^j and $\phi\rho^i$ commute if and only if $\rho^j \in Z(D_n)$, for every $0 \leq i, j < n$.

❏

Lemma 7.7. *For every $0 \leq i, j < n$, $\phi\rho^j$ and $\phi\rho^i$ commute, if and only if $\phi\rho^j = \phi\rho^i z$ for some $z \in Z(D_n)$.*

Proof: Let $0 \leq i, j < n$. First, assume that $\phi\rho^j$ and $\phi\rho^i$ commute. Then we have $\phi\rho^j\phi\rho^i = \phi\rho^i\phi\rho^j$. Applying Lemma 7.1 to both sides of the equality yields $\phi\phi\rho^{-j}\rho^i = \rho^{-j}\rho^i$ and $\phi\phi\rho^{-i}\rho^j = \rho^{-i}\rho^j$ because $\phi^2 = R_0$. Thus by group algebra, $\rho^{-j+i} = \rho^{-i+j} = (\rho^{-j+i})^{-1}$. By transitivity and group algebra we obtain $(\rho^{-j+i})^2 = R_0$. Therefore, by Lemma 7.4, $\rho^{-j+i} \in Z(D_n)$. Since $\phi\rho^j = \phi\rho^i\rho^{-i}\rho^j = \phi\rho^i(\rho^{-i+j})$ by group algebra, and because $\rho^{-j+i} \in Z(D_n)$, $\phi\rho^j = \phi\rho^i z$ for some $z \in Z(D_n)$.

Now, assume that $\phi\rho^j = \phi\rho^i z$ for some $z \in Z(D_n)$. Then, it follows that $(\phi\rho^j)(\phi\rho^i) = (\phi\rho^i z)(\phi\rho^i) = \phi\rho^i(\phi\rho^i z) = (\phi\rho^i)(\phi\rho^j)$.

Thus $\phi\rho^j$ and $\phi\rho^i$ commute if and only if $\phi\rho^j = \phi\rho^i z$ for some $z \in Z(D_n)$ and for every $0 \leq i, j < n$.

❏

Since we now have an idea of which elements commute from D_n, we can capture this with a lemma that involves counting how many commuting pairs we have.

Lemma 7.8. *For $n \geq 3$,*

$$CP(D_n) = \begin{cases} \{(\rho^i, \rho^j) : 0 \leq i, j \leq n-1\} \cup \{(R_0, \phi\rho^i) : 0 \leq i \leq n-1\} \\ \cup\{(\phi\rho^i, R_0) : 0 \leq i \leq n-1\} \cup \{(\phi\rho^j, \phi\rho^j) : 0 \leq j \leq n-1\} \text{ if } n \text{ is odd;} \\ \\ \{(\rho^i, \rho^j) : 0 \leq i, j \leq n-1\} \cup \{(R_0, \phi\rho^i) : 0 \leq i \leq n-1\} \\ \cup\{(\phi\rho^i, R_0) : 0 \leq i \leq n-1\} \cup \{(\phi\rho^j, \phi\rho^j) : 0 \leq j \leq n-1\} \\ \cup\{(\rho^{n/2}, \phi\rho^i) : 0 \leq i \leq n-1\} \cup \{(\phi\rho^i, \rho^{n/2}) : 0 \leq i \leq n-1\} \\ \cup\{(\phi\rho^i\rho^{n/2}, \phi\rho^i) : 0 \leq i \leq n-1\} \text{ if } n \text{ is even.} \end{cases}$$

and

$$Comm(D_n) = |CP(D_n)| = \begin{cases} n^2 + 3n \text{ if } n \text{ is odd;} \\ n^2 + 6n \text{ if } n \text{ is even.} \end{cases}$$

Proof: Let $n \geq 3$.

Case 1: Assume n is odd.

From Lemma 7.5, we get the commuting pairs in the first set in the union. From Lemma 7.6 and the fact that $Z(D-n) = \{R_0\}$, we get the second and third sets in the union. Finally, from Lemma 7.7 and the fact that $Z(D-n) = \{R_0\}$, we get the fourth set in the union.

We can see that all of these sets are disjoint because the first set in the union contains pairs of rotations, the second and third sets in the union contains pairs of a rotation and a reflection, and the fourth set in the union contains pairs of reflections.

Case 2: Assume n is even.

From Lemma 7.5, we get the commuting pairs in the first set in the union. From Lemma 7.6 and the fact that $Z(D-n) = \{R_0, \rho^{n/2}\}$, we get the second, third, fourth and fifth sets in the union. Finally, from Lemma 7.7 and the fact that $Z(D_n) = \{R_0, \rho^{n/2}\}$, we get the sets $\{(\phi\rho^i\rho^{n/2}, \phi\rho^i) : 0 \leq i \leq n-1\}$ (the last set in the union) and $\{(\phi\rho^i, \phi\rho^i\rho^{n/2}) : 0 \leq i \leq n-1\}$. However, we will show that these two sets are equal.

To do so, let $M \coloneqq \{(\phi\rho^i\rho^{n/2}, \phi\rho^i) : 0 \leq i \leq n-1\}$ and $T \coloneqq \{(\phi\rho^i, \phi\rho^i\rho^{n/2}) : 0 \leq i \leq n-1\}$. Suppose that $(\phi\rho^k, \phi\rho^k\rho^{n/2}) \in T$ where $0 \leq k \leq n-1$.

Case 1: Assume $0 \leq k < \frac{n}{2}$.

Then, $\frac{n}{2} \leq k + \frac{n}{2} < n$ and $(\phi\rho^k, \phi\rho^{k+n/2}) = (\phi\rho^n\rho^k, \phi\rho^{k+n/2}) = (\phi\rho^{n+k}, \phi\rho^{k+n/2}) = (\phi\rho^{(n/2+k)+n/2}, \phi\rho^{k+n/2}) \in M$, because $k + \frac{n}{2} < n$. Hence $(\phi\rho^k, \phi\rho^k\rho^{n/2}) \in M$.

Case 2: Assume $\frac{n}{2} \leq k < n$.

Then, $0 \leq k - \frac{n}{2} < \frac{n}{2}$ and $(\phi\rho^k, \phi\rho^{k+n/2}) = (\phi\rho^k, \phi\rho^{n+(k-n/2)}) = (\phi\rho^{k-n/2+n/2}, \phi\rho^n\rho^{k-n/2}) = (\phi\rho^{(k-n/2)+n/2}, \phi\rho^{k-n/2}) \in M$, because $k - \frac{n}{2} < \frac{n}{2}$. Hence $(\phi\rho^k, \phi\rho^{k+n/2}) \in M$.

Therefore, by definition, $T \subseteq M$. Furthermore, in both sets, there are n choices for i. Hence $|T| = n = |M|$. Therefore, $M \subseteq T$ as well, and so these sets are equal.

We know that the first four sets in the union are disjoint by Case 1. The fifth and sixth sets in the union are disjoint from the first and the fourth, because they contain both a reflection and a rotation. And, they are disjoint from the second and third sets because neither of their coordinates are the identity, since $|\rho| = n > \frac{n}{2}$. Finally, the seventh set in the union is equal to $(\phi\rho^i, \phi\rho^{i+n/2})$ from above, but disjoint from the first six, because it contains two reflections. So we can capture this with,

$$CP(D_n) = \begin{cases} \{(\rho^i, \rho^j) : 0 \leq i, j \leq n-1\} \cup \{(R_0, \phi\rho^i) : 0 \leq i \leq n-1\} \\ \cup\{(\phi\rho^i, R_0) : 0 \leq i \leq n-1\} \cup \{(\phi\rho^j, \phi\rho^j) : 0 \leq j \leq n-1\} \text{ if } n \text{ is odd;} \\ \\ \{(\rho^i, \rho^j) : 0 \leq i, j \leq n-1\} \cup \{(R_0, \phi\rho^i) : 0 \leq i \leq n-1\} \\ \cup\{(\phi\rho^i, R_0) : 0 \leq i \leq n-1\} \cup \{(\phi\rho^j, \phi\rho^j) : 0 \leq j \leq n-1\} \\ \cup\{(\rho^{n/2}, \phi\rho^i) : 0 \leq i \leq n-1\} \cup \{(\phi\rho^i, \rho^{n/2}) : 0 \leq i \leq n-1\} \\ \cup\{(\phi\rho^i\rho^{n/2}, \phi\rho^i) : 0 \leq i \leq n-1\} \text{ if } n \text{ is even.} \end{cases}$$

Looking at the second part to the lemma, since all of the sets are disjoint in both the odd and even case, we can add up how many elements are in each set. Note that there are n choices for i and j. So when n is odd, there are n^2 elements in the first set, and n elements in the second, third, and fourth sets. Resulting in a total of $n^2 + 3n$ elements. When n is even, there are n^2 elements in the first set again, and n elements in the second, third, fourth, fifth, sixth, and seventh sets. Resulting in a total of $n^2 + 6n$ elements. Hence, it follows that

$$Comm(D_n) = |CP(D_n)| = \begin{cases} n^2 + 3n \text{ if } n \text{ is odd;} \\ n^2 + 6n \text{ if } n \text{ is even.} \end{cases}$$

❏

The next three theorems come from [2], however the proofs are original. Theorem 7.10 is particularly interesting.

Theorem 7.9. *If n is a positive integer, then*

$$Pr(D_n) = \begin{cases} \frac{n+3}{4n} \text{ if } n \text{ is odd;} \\ \frac{n+6}{4n} \text{ if } n \text{ is even.} \end{cases}$$

Proof: Let n be a positive integer. It follows from Definition 6.2 and Lemma 7.8 that when n is odd we have $Pr(D_n) = \frac{n^2+3n}{(2n)^2} = \frac{n+3}{4n}$, and when n is even we have $Pr(D_n) = \frac{n^2+6n}{(2n)^2} = \frac{n+6}{4n}$. Hence, the theorem follows. ❏

Theorem 7.10. *For every positive integer m, there is a collection of dihedral groups, $D_{n_1}, ..., D_{n_k}$, such that*

$$Pr(D_{n_1} \oplus \cdots \oplus D_{n_k}) = \frac{1}{m}.$$

Proof: Proceed by strong induction.

1.) Base case: $m = 1$.

By Theorem 7.9, $Pr(D_1) = \frac{1+3}{4(1)} = \frac{4}{4} = 1$.

Let $m \in \mathbb{Z}^+$.

2.) Inductive hypothesis: Assume for every $m' \in \mathbb{Z}^+$ with $m' \leq m$, there exists $D_{n_1}, ..., D_{n_k}$ such that $Pr(D_{n_1} \oplus \cdots \oplus D_{n_k}) = \frac{1}{m'}$ where $m' \in \mathbb{Z}^+$.

3.) Strong Inductive Step:

Case 1: Assume $m + 1$ is even.

By definition of even, $m+1 = 2l$ and $1 \leq l < m+1$ for some $l \in \mathbb{Z}^+$. Since $l \leq m$, by our Inductive Hypothesis there exists $D_{n_1}, ..., D_{n_k}$ such that $Pr(D_{n_1} \oplus \cdots \oplus D_{n_k}) = \frac{1}{l}$. Consider $D_3,\ D_{n_1}, ..., D_{n_k}$. Then $Pr(D_3 \oplus D_{n_1} \oplus \cdots \oplus D_{n_k}) = Pr(D_3)Pr(D_{n_1} \oplus \cdots \oplus D_{n_k}) = \frac{1}{2}(\frac{1}{l})$ by Lemma 6.6 and because $Pr(D_3) = \frac{3+3}{4(3)} = \frac{1}{2}$, by Theorem 7.9. Thus $Pr(D_3 \oplus D_{n_1} \oplus \cdots \oplus D_{n_k}) = \frac{1}{2l} = \frac{1}{m+1}$ as desired.

Case 2: Assume $m + 1$ is odd.

Divide $m + 1$ by 4 using the division algorithm to obtain $m + 1 = 4q + r$ where $q, r \in \mathbb{Z}$ and $0 \leq r < 4$. Since $m+1$ is odd, it follows that r is odd. Thus $m+1 = 4q+1$ or $m + 1 = 4q + 3$.

Subcase 2a: Assume $m + 1 = 4q + 1$. Suppose to the contrary that $q + 1 > m$. Then $q + 2 > m + 1 = 4q + 1$. Subtracting $q + 1$ from both sides yields $1 > 3q \geq 3$, and a contradiction has been reached. Thus $q + 1 \leq m$.

By Theorem 7.9, we have

$$\begin{aligned} Pr(D_{m+1}) &= \frac{m+1+3}{4(m+1)} \\ &= \frac{4q+1+3}{4(m+1)} \\ &= \frac{4(q+1)}{4(m+1)} \\ &= \frac{q+1}{m+1}. \end{aligned}$$

Since $q+1 \leq m$, by our Inductive Hypothesis there exists $D_{n_1}, ..., D_{n_k}$ such that $Pr(D_{n_1} \oplus \cdots \oplus D_{n_k}) = \frac{1}{q+1}$. Consider $D_{m+1},\ D_{n_1}, ..., D_{n_k}$, then $Pr(D_{m+1} \oplus D_{n_1} \oplus \cdots \oplus D_{n_k}) = Pr(D_{m+1})Pr(D_{n_1} \oplus \cdots \oplus D_{n_k}) = \frac{q+1}{m+1}(\frac{1}{q+1})$ by Lemma 6.6.

Hence, $Pr(D_{m+1} \oplus D_{n_1} \oplus \cdots \oplus D_{n_k}) = \frac{1}{m+1}$ as desired.

Subcase 2b: Assume $m+1 = 4q+3$. Look at the odd number $3(m+1)$. By Theorem 7.9,

$$\begin{aligned} Pr(D_{3(m+1)}) &= \frac{3(m+1)+3}{4(3(m+1))} \\ &= \frac{3((m+1)+1)}{12(m+1)} \\ &= \frac{m+1+1}{4(m+1)} \\ &= \frac{4q+3+1}{4(m+1)} \\ &= \frac{4(q+1)}{4(m+1)} \\ &= \frac{q+1}{m+1}. \end{aligned}$$

Again, since $q+1 \leq m$, by our Inductive Hypothesis there exists $D_{n_1}, ..., D_{n_k}$ such that $Pr(D_{n_1} \oplus \cdots \oplus D_{n_k}) = \frac{1}{q+1}$. Consider $D_{3(m+1)},\ D_{n_1}, ..., D_{n_k}$ then $Pr(D_{3(m+1)} \oplus D_{n_1} \oplus \cdots \oplus D_{n_k}) = Pr(D_{3(m+1)})Pr(D_{n_1} \oplus \cdots \oplus D_{n_k}) = \frac{q+1}{m+1}(\frac{1}{q+1})$, by Lemma 6.6 and Theorem 7.9. Hence, $Pr(D_{3(m+1)} \oplus D_{n_1} \oplus \cdots \oplus D_{n_k}) = \frac{1}{m+1}$ as desired.

Therefore, by the Principle of Induction, for every positive integer m, there is a collection of dihedral groups, $D_{n_1}, ..., D_{n_k}$, such that $Pr(D_{n_1} \oplus \cdots \oplus D_{n_k}) = \frac{1}{m}$.

❏

Theorem 7.11. *If m is a positive integer, then there is a dihedral group D_n, such that*

$$Pr(D_n) = \frac{m}{m'}$$

where m' is an integer relatively prime to m.

Proof: Assume $m \in \mathbb{Z}^+$. Consider $n = 24m - 6$, which we observe to be a positive even integer. So by Theorem 7.9, $Pr(D_{24m-6}) = \frac{24m-6+6}{4(24m-6)} = \frac{24m}{24(4m-1)} = \frac{m}{4m-1}$. Let $m' = 4m - 1$. Thus $Pr(D_{24m-6}) = \frac{m}{m'}$. Since $4m - m' = 1$, that implies that $4m$ and m' are consecutive integers. Thus 1 is the only common factor between $4m$ and m'. Every factor of m is a factor of $4m$. Hence m and m' still only share the common factor of 1. Thus we can conclude that m and m' are relatively prime. Therefore, the theorem follows.

❏

We are headed towards calculating $Pr(GL(2,\ \mathbb{Z}_p))$, however before we do so there are some preliminaries about $\mathbb{Z}_p$ that we need to go over.

8. Preliminaries about $\mathbb{Z}_p$ and $\mathbb{Z}_p[\sqrt{D}]$

Lemma 8.1. *Suppose $< s >$ is a cyclic group of even order $n = 2^l d$ where d is odd and $l > 0$,*

1. *Let $D \coloneqq s^d$, then $|D| = |s^d| = 2^l$.*
2. *For every $y \in < s >$, if $|y|$ is odd, then there exists an $r \in < s >$ such that $y = r^2$.*
3. *Then there does not exist an $r \in < s >$ such that $r^2 = D$.*
4. *For every $y \in < s >$, if there does not exist an $r \in < s >$ such that $r^2 = y$, then $y = D\beta^2$ for some $\beta \in < s >$.*

Proof: Suppose that $< s >$ is a cyclic group of order $n = 2^l d$ where d is odd and $l > 0$.

Proof of (1). Define $D \coloneqq s^d$. Then $|D| = |s^d|$ and by Theorem 4.10, $|s^d| = \frac{2^l d}{gcd(2^l d, d)}$. Hence we have $|D| = \frac{2^l d}{d} = 2^l$.

Proof of (2). Let $y \in < s >$ and assume $|y|$ is odd. Then by Theorem 4.11 there are integers a and b such that $|y|a + 2b = gcd(|y|, 2) = 1$. It follows that $y = y^1 = y^{gcd(|y|,2)} = y^{|y|a+2b} = (y^{|y|})^a (y^b)^2$ from above and by Theorem 4.8. Since $y^{|y|}$ is the identity, it follows that $y = (y^b)^2$. Since $y \in < s >$ by closure, take $r = y^b$ and we have $y = r^2$.

Proof of (3). Suppose to the contrary that for some $r \in < s >$ such that $r^2 = D$. Then $r = s^k$ for some $k \in \mathbb{Z}$ and $D = r^2 = s^{2k}$. From Part (1) we have $2^l = |D| = |s^{2k}|$.

So by Theorem 4.10 again, we have $|s^{2k}| = \frac{2^l d}{gcd(2^l d, 2k)} = \frac{2^l d}{2c}$ for some $c \in \mathbb{Z}$, since $2^l d$ and $2k$ both share at least a factor of 2. Since $2^l = \frac{2^l d}{2c}$, it follows that $2c = d$. Since d is odd from our original hypotheses, a contradiction has been reached. Thus there does not exist an $r \in < s >$ such that $r^2 = D$. In other words, D does not have a square root in $< s >$.

Proof of (4). Let $y \in < s >$ and assume there does not exist an $r \in < s >$ such that $r^2 = y$. By Corollary 4.12, let $| < y > | = |y| = 2^k f$, where f is odd. By Corollary 4.6, $2^k f$ is a factor of $2^l d$, so $2^k f x = 2^l d$ for some $x \in \mathbb{Z}$. Looking at the prime factorization of this, it follows that $k \leq l$. Applying Theorem 4.10 to $< y >$, we get $|y^{2k}| = \frac{2^k f}{gcd(2^k f, 2^k)} = \frac{2^k f}{2^k} = f$. Therefore by Corollary 4.12, $|y^f| = 2^k = | < y^f > |$. Next, applying Part (2), since $|y^{2k}|$ is odd, because f is odd, there exists a $\gamma \in < s >$ such that $\gamma^2 = y^{2k}$ (We will use this shortly.) By Theorem 4.13 $< y^f > \leq < D >$. This is because $< D >$ has a subgroup of order 2^k, $< y^f >$ is also a subgroup of order 2^k, and there is only one such subgroup of order 2^k in $< s >$. Set $y^f = D^t$.

Apply Theorem 4.11 to $gcd(2^k, f) = 1$, so there exists integers a and b such that $2^k a + fb = 1$. Similar to Part (2), $y = y^1 = y^{2^k a + fb} = (y^{2k})^a (y^f)^b = (\gamma^2)^a (D^t)^b = (\gamma^a)^2 D^{tb}$ by Theorem 4.8 and above parts. By way of contradiction, assume tb is even, then $tb = 2c$ for $c \in \mathbb{Z}$. Then $y = (\gamma^a)^2 D^{2c} = (\gamma^a D^c)^2$, where that final equality is because $\gamma^a, D^c \in < s >$ by closure and $< s >$ is abelian. This is a contradiction because there does not exist an $r \in < s >$ such that $r^2 = y$. Hence tb is odd, so $tb = 2c_1 + 1$ for some $c_1 \in \mathbb{Z}$. Similar to before, we have $y = (\gamma^a)^2 D^{tb} = (\gamma^a)^2 D^{2c_1 + 1} = (\gamma^a)^2 (D^{c_1})^2 D = (\gamma^a D^{c_1})^2 D$, where, again, that final equality is because $\gamma^a, D^{c_1} \in < s >$ by closure and the fact that $< s >$ is abelian. If we take $\beta = \gamma^a D^{c_1}$, then we have $y = D\beta^2$.

❏

Theorem 8.2. *Assume p is an odd prime, then $\mathbb{Z}_p^*$ is a cyclic group of even order $p - 1$.*

Proof: This follows from [4, p. 383]. (Note that $\mathbb{Z}_p = GF(p)$).

Let D be the element of the cyclic group $\mathbb{Z}_p^*$ as defined in Lemma 8.1. Define a new element $\sqrt{D}$ where $(\sqrt{D})^2 = D$. By Part (3) of Lemma 8.1, $\sqrt{D}$ is "new", not in $\mathbb{Z}_p^*$, nor in $\mathbb{Z}_p$ (since $0^2 \neq D$). ❏

Definition 8.3. *Set $\mathbb{Z}_p[\sqrt{D}] \coloneqq \{\alpha + \beta\sqrt{D} : \alpha, \beta \in \mathbb{Z}_p\}$ and define addition and multiplication by $(\alpha + \beta\sqrt{D}) + (\gamma + \delta\sqrt{D}) \coloneqq (\alpha +_p \gamma) + (\beta +_p \delta)\sqrt{D}$ and $(\alpha + \beta\sqrt{D})(\gamma + \delta\sqrt{D}) \coloneqq (\alpha \times_p \gamma) + (\beta +_p \delta)D + ((\alpha \times_p \gamma) + (\beta \times_p \gamma))\sqrt{D}$.*

By analogy, think of D as -1 in $\mathbb{R}$, $\sqrt{D}$ is like $\sqrt{-1} = i$ and $\mathbb{Z}_p[\sqrt{D}]$ is like the larger field of Complex numbers.

Note: For the remainder of this paper, $+_p$ will be denoted with $+$ and $\times_p$ will be denoted with nothing.

Lemma 8.4. *$\mathbb{Z}_p[\sqrt{D}]$ with its respective operations is a field.*

Proof: Let $\mathbb{Z}_p[\sqrt{D}] = \{\alpha + \beta\sqrt{D} : \alpha, \beta \in \mathbb{Z}_p\}$. A routine calculation would show that $\mathbb{Z}_p[\sqrt{D}]$ is a commutative ring with unity equal to 1. So it remains to show that every nonzero element has a multiplicative inverse. Let $a + b\sqrt{D} \in \mathbb{Z}_p[\sqrt{D}]^*$.

Case 1: Assume $b = 0$.

Then $a + b\sqrt{D} = a \in \mathbb{Z}_p^*$. Since $\mathbb{Z}_p^*$ is a field, a has a multiplicative inverse in $\mathbb{Z}_p$, and hence in the larger field $\mathbb{Z}_p[\sqrt{D}]$ as well.

Case 2: Assume $b \neq 0$.

Consider $f \coloneqq a^2 - b^2D$. Suppose to the contrary that $f = 0$. Then $b^2D = a^2$ and since $b \neq 0$, $D = (\frac{a}{b})^2$. This implies that D has a square root in $\mathbb{Z}_p$, which is a contradiction. Hence, $f \neq 0$, so it has an inverse in $\mathbb{Z}_p$. Consider $af^{-1} - bf^{-1}\sqrt{D}$. Since $a, f^{-1}, b \in \mathbb{Z}_p$, by closure $af^{-1} - bf^{-1}\sqrt{D} \in \mathbb{Z}_p[\sqrt{D}]$. So it follows that $(a + b\sqrt{D})(af^{-1} - bf^{-1}\sqrt{D}) = (a + b\sqrt{D})(a - b\sqrt{D})f^{-1} = (a^2 - b^2D)f^{-1} = ff^{-1} = 1$ Therefore, $a + b\sqrt{D}$ has an inverse in $\mathbb{Z}_p[\sqrt{D}]$. This concludes that $\mathbb{Z}_p[\sqrt{D}]$ is a field.

❏

Lemma 8.5. *Assume $y \in \mathbb{Z}_p$. Then there exists a $\gamma \in \mathbb{Z}_p[\sqrt{D}]$ such that $\gamma^2 = y$ and if $\gamma_1, \gamma_2 \in \mathbb{Z}_p$ with $\gamma_1^2 = y = \gamma_2^2$, then $\gamma_1 = \pm\gamma_2$.*

Proof: Let $y \in \mathbb{Z}_p$. If $y = 0$, then consider $\gamma = 0 \in \mathbb{Z}_p[\sqrt{D}]$. Obviously, $0^2 = y$. So we may assume $y \in \mathbb{Z}_p^*$. If y has a square root in $\mathbb{Z}_p^*$, then we are finished since $\mathbb{Z}_p^* \subseteq \mathbb{Z}_p[\sqrt{D}]$. The remaining case is where y does not have a square root in $\mathbb{Z}_p^*$. By Lemma 8.1(4), $y = D\beta^2$ for some $\beta \in \mathbb{Z}_p^*$. Consider $\gamma = \sqrt{D}\beta$, which is in $\mathbb{Z}_p[\sqrt{D}]$ by definition. By the definition of multiplication in $\mathbb{Z}_p[\sqrt{D}]$, $(\sqrt{D}\beta)^2 = D\beta^2 = y$. In all cases, we have shown there exists a $\gamma \in \mathbb{Z}_p[\sqrt{D}]$ such that $\gamma^2 = y$.

For the second part, suppose $\gamma_1, \gamma_2 \in \mathbb{Z}_p[\sqrt{D}]$ satisfy $\gamma_1^2 = y = \gamma_2^2$. We want to show $\gamma_1 = \pm\gamma_2$.

If $y = 0$, then $\gamma_1 = 0 = \gamma_2$ because a field has no zero divisors and we are finished. Now we may assume $y \neq 0$.

Suppose $\gamma_2 = -\gamma_2$, then $2\gamma_2 = 0$. Since p is odd, $2^{-1} \in \mathbb{Z}_p^*$. Thus, $\gamma_2 = 2^{-1}0 = 0$ and so $y = \gamma_2^2 = 0$, a contradiction. Therefore, $\gamma_2 \neq -\gamma_2$. It is easy to see that both

γ_2 and $-\gamma_2$ are roots of the polynomial $x^2 - y \in \mathbb{Z}_p[\sqrt{D}][x]$. Hence, those are the only two roots of the polynomial [4, p. 304]. However, by hypothesis, γ_1 is also a root of that polynomial. Therefore, $\gamma_1 = \gamma_2$ or $\gamma_1 = -\gamma_2$ as claimed.

❏

Lemma 8.6 (Quadratic Formula)**.** *Suppose $x^2 + bx + c \in \mathbb{Z}_p[x]$, then there exists a $\gamma^2 = \frac{b^2}{4} - c$ such that $\frac{-b}{2} + \gamma$ and $\frac{-b}{2} - \gamma$ are zeros of $x^2 + bx + c$ where $\gamma \in \mathbb{Z}_p[\sqrt{D}]$.*

Proof: Suppose that $x^2+bx+c \in \mathbb{Z}_p[x]$. Consider $z_1 \coloneqq \frac{-b}{2}+\gamma$ and $z_2 \coloneqq \frac{-b}{2}-\gamma$, where $\gamma \in \mathbb{Z}_p[\sqrt{D}]$. So $z_1, z_2 \in \mathbb{Z}_p[\sqrt{D}]$ by definition. Then by Lemma 8.5, $\gamma^2 = \frac{b^2}{4} - c \in \mathbb{Z}_p$ by closure. Evaluating the polynomial at z_1 yields $(\frac{-b}{2} + \gamma)^2 + b(\frac{-b}{2} + \gamma) + c = \frac{b^2}{4} - \frac{b}{2}\gamma - \frac{b}{2}\gamma + \gamma^2 - \frac{b^2}{2} + b\gamma + c = \frac{b^2}{4} + \gamma^2 - \frac{b^2}{2} + c = \frac{b^2}{4} - \frac{2b^2}{4} + \gamma^2 + c = -\frac{b^2}{4} + \frac{b^2}{4} - c + c = 0$, by group algebra and the fact that $\gamma^2 = \frac{b^2}{4} - c$. Evaluating the polynomial at z_2 yields $(\frac{-b}{2} - \gamma)^2 + b(\frac{-b}{2} - \gamma) + c = \frac{b^2}{4} + \frac{b}{2}\gamma + \frac{b}{2}\gamma + \gamma^2 - \frac{b^2}{2} - b\gamma + c = \frac{b^2}{4} + \gamma^2 - \frac{b^2}{2} + c = \frac{b^2}{4} - \frac{2b^2}{4} + \gamma^2 + c = -\frac{b^2}{4} + \frac{b^2}{4} - c + c = 0$ by group algebra and the fact that $\gamma^2 = \frac{b^2}{4} - c$. Hence, $\frac{-b}{2} + \gamma$ and $\frac{-b}{2} - \gamma$ are zeros of $x^2 + bx + c$.

❏

Theorem 8.7. *If A is a 2×2 matrix with entries in $\mathbb{Z}_p$ and $a + b\sqrt{D}$ is an eigenvalue of A with eigenvector $\begin{pmatrix} r + s\sqrt{D} \\ u + v\sqrt{D} \end{pmatrix}$, then $a - b\sqrt{D}$ is also an eigenvalue of A with eigenvector $\begin{pmatrix} r - s\sqrt{D} \\ u - v\sqrt{D} \end{pmatrix}$.*

Proof: Copy the proof from [10, pp. 331 and 333].

❏

9. Conjugacy Classes in $GL(2,\ \mathbb{Z}_p)$

Recall that $GL(2,\ \mathbb{Z}_p)$ is the group of 2×2 invertible matrices (that is, with nonzero determinant) and entries from the field $\mathbb{Z}_p$. The following theorem is adapted from [8].

Theorem 9.1. *Let D be an element which is in $\mathbb{Z}_p$, however it does not have a square root that is in $\mathbb{Z}_p$. The conjugacy classes in $GL(2,\ \mathbb{Z}_p)$ are as follows:*

(1) $(p-1)$ classes of the form $cl(A)$, where $A \coloneqq \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$, with $\lambda \in \mathbb{Z}_p^*$.

(2) $(p-1)$ classes of the form $cl(B)$, where $B \coloneqq \begin{pmatrix} \mu & 1 \\ 0 & \mu \end{pmatrix}$, with $\mu \in \mathbb{Z}_p^*$.

(3) $\frac{1}{2}(p-1)(p-2)$ *classes of the form* $cl(C)$*, where* $C \coloneqq \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$ *with* $\lambda_1,\ \lambda_2 \in \mathbb{Z}_p^*$ *and* $\lambda_1 \neq \lambda_2$.

(4) $\frac{1}{2}(p^2-p)$ *classes of the form* $cl(E)$*, where* $E \coloneqq \begin{pmatrix} \alpha & D\beta \\ \beta & \alpha \end{pmatrix}$*, with* $\alpha,\ \beta \in \mathbb{Z}_p$ *and* $\beta \neq 0$.

In order to prove Theorem 9.1 we will use a sequence of lemmas. The first set of lemmas will give us some results about the eigenvalues associated with an upper triangular matrix as well as a matrix of the form $\begin{pmatrix} \alpha & D\beta \\ \beta & \alpha \end{pmatrix}$, with $\alpha,\ \beta \in \mathbb{Z}_p$ and $\beta \neq 0$. Then, we will show that the conjugacy classes defined above are all disjoint. Finally, we will introduce and prove the counting aspect of Theorem 9.1.

Lemma 9.2. *Every matrix of the form* $T \coloneqq \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$*, with* $a,\ b,\ c \in \mathbb{Z}_p$ *has eigenvalues* a *and* c.

Proof: Let T be a matrix of the form $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ with $a,\ b,\ c \in \mathbb{Z}_p$. The eigenvalues of T are the solutions to $Det\left[\begin{pmatrix} a-x & b \\ 0 & c-x \end{pmatrix}\right] = (a-x)(c-x) = 0$. Since $\mathbb{Z}_p$ is a field, it has no zero divisors. Thus the only eigenvalues are a and c.

❏

Since we know the eigenvalues of an upper triangular matrix, we will now look at a matrix which yields eigenvalues that are not in $\mathbb{Z}_p$.

Lemma 9.3. *Every matrix of the form* $\begin{pmatrix} \alpha & D\beta \\ \beta & \alpha \end{pmatrix}$*, with* $\alpha,\ \beta \in \mathbb{Z}_p$*,* $\beta \neq 0$ *and* D *as defined above, has eigenvalues* $\alpha \pm \sqrt{D}\beta$ *(which are not in* $\mathbb{Z}_p$*).*

Proof: Let $E \coloneqq \begin{pmatrix} \alpha & D\beta \\ \beta & \alpha \end{pmatrix}$, with $\alpha,\ \beta \in \mathbb{Z}_p$, $\beta \neq 0$ and D as defined above. The eigenvalues of E are the solutions to $Det\left[\begin{pmatrix} \alpha-x & D\beta \\ \beta & -x \end{pmatrix}\right] = (\alpha-x)^2 - D\beta^2 = 0$. Thus $\alpha \pm \sqrt{D}\beta$ are the two eigenvalues of E, because $(\alpha - (\alpha \pm \sqrt{D}\beta))^2 - D\beta^2 = (\mp\sqrt{D}\beta)(\mp\sqrt{D}\beta) - D\beta^2 = D\beta^2 - D\beta^2 = 0$. Since $\mathbb{Z}_p$ is a field, these are the only two eigenvalues of E [4, p. 299].

❏

Lemma 9.4. *Matrices of the form* $A = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$ *where* $\lambda \in \mathbb{Z}_p^*$*, have the property:* $cl(A) = \{A\}$.

Proof: Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2,\ \mathbb{Z}_\text{ı})$ and consider $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \in GL(2,\ \mathbb{Z}_p)$ where $\lambda \in \mathbb{Z}_p^*$. By matrix multiplication, $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \lambda a & \lambda b \\ \lambda c & \lambda d \end{pmatrix} = \begin{pmatrix} a\lambda & b\lambda \\ c\lambda & d\lambda \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$, because multiplication mod p is commutative. Hence, $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$. Therefore, $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \in Z(GL(2,\ \mathbb{Z}_p))$. Thus by Lemma 5.6, $cl\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$.

❏

Now, begins the sequence of lemmas which will help in proving Theorem 9.1. This first lemma states that the four conjugacy classes in Theorem 9.1 are distinct.

Lemma 9.5. *The conjugacy classes of the form $cl(A)$, $cl(B)$, $cl(C)$, $cl(E)$, where A, B, C and E are matrices as above, are all distinct.*

Proof: Part (1): $cl(A) \neq cl(B)$.

First note that $\begin{pmatrix} \mu & 1 \\ 0 & \mu \end{pmatrix} \in cl\left(\begin{pmatrix} \mu & 1 \\ 0 & \mu \end{pmatrix}\right)$ where $\mu \in \mathbb{Z}_p^*$, because every element is in its own conjugacy class. We can see that $\begin{pmatrix} \mu & 1 \\ 0 & \mu \end{pmatrix} \neq \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$ because equal matrices have equal cells. Therefore, $\begin{pmatrix} \mu & 1 \\ 0 & \mu \end{pmatrix} \notin cl\left(\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}\right)$ by Lemma 9.4. Thus we can conclude that $cl(A) \neq cl(B)$.

In the remaining parts of the proof, we will repeatedly use Lemma 5.5.

Part (2): $cl(A) \neq cl(C)$.

Suppose to the contrary that $cl\left(\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}\right) = cl\left(\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}\right)$ where $\lambda,\ \lambda_1,\ \lambda_2 \in \mathbb{Z}_p^*$ and $\lambda_1 \neq \lambda_2$. Therefore, $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$ is conjugate to $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$ by Lemma 5.5. By Theorem 5.7, those matrices have the same eigenvalues. Hence, $\lambda_1 = \lambda = \lambda_2$ by Lemma 9.2 and we have reached a contradiction because $\lambda_1 \neq \lambda_2$. Therefore, $cl(A) \neq cl(C)$.

Part (3): $cl(A) \neq cl(E)$.

Suppose to the contrary that $cl\left(\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}\right) = cl\left(\begin{pmatrix} \alpha & D\beta \\ \beta & \alpha \end{pmatrix}\right)$ where $\lambda,\ \alpha,\ \beta,\ D \in \mathbb{Z}_p,\ \lambda,\ \beta \neq 0$ and $\sqrt{D} \in \mathbb{Z}_p[\sqrt{D}]$. Therefore, $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$ is conjugate to $\begin{pmatrix} \alpha & D\beta \\ \beta & \alpha \end{pmatrix}$ by Lemma 5.5. By the Theorem 5.7 those matrices have the same

eigenvalues. However, since $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$ has eigenvalue $\lambda \in \mathbb{Z}_p^*$ by Lemma 9.2 and $\begin{pmatrix} \alpha & D\beta \\ \beta & \alpha \end{pmatrix}$ has eigenvalues $\alpha \pm \sqrt{D}\beta \notin \mathbb{Z}_p$ by Lemma 9.3, $\lambda \neq \alpha \pm \sqrt{D}\beta$. Thus we have a contradiction, so $cl(A) \neq cl(E)$.

Part(4): $cl(B) \neq (C)$.

This follows the same proof as Part (2).

Part (5): $cl(B) \neq cl(E)$.

Part (6): $cl(C) \neq cl(E)$.

The proofs of Parts (5) and (6) follow the same proof as Part (3).

Hence, the lemma follows.

❏

Lemma 9.5 showed us that there are four types of matrices that yield four different types of conjugacy classes. Note, depending on what our prime number p is, determines how many conjugacy classes we actually have of each type. We will now transition to looking at the counting aspect of Theorem 9.1. In order to count how many conjugacy classes there are of each form, we will use the following lemmas, which show that different entries into the matrices yield different conjugacy classes. Lemma 9.6 will look at (1) and (2) from Theorem 9.1.

Lemma 9.6. *For every* $\lambda_1,\ \lambda_2 \in \mathbb{Z}_p^*$ *with* $\lambda_1 \neq \lambda_2$ *and* $a = 0$ *or 1,* $cl\left(\begin{pmatrix} \lambda_1 & a \\ 0 & \lambda_1 \end{pmatrix}\right) \neq cl\left(\begin{pmatrix} \lambda_2 & a \\ 0 & \lambda_2 \end{pmatrix}\right)$.

Proof: Let $\begin{pmatrix} \lambda_1 & a \\ 0 & \lambda_1 \end{pmatrix}, \begin{pmatrix} \lambda_2 & a \\ 0 & \lambda_2 \end{pmatrix} \in GL(2,\ \mathbb{Z}_p)$ where $\lambda_1 \neq \lambda_2$ and $a = 0$ or 1. By Lemma 9.2, $\begin{pmatrix} \lambda_1 & a \\ 0 & \lambda_1 \end{pmatrix}$ has eigenvalue λ_1 and $\begin{pmatrix} \lambda_2 & a \\ 0 & \lambda_2 \end{pmatrix}$ has eigenvalue λ_2. Thus by Theorem 5.7, $\begin{pmatrix} \lambda_1 & a \\ 0 & \lambda_1 \end{pmatrix}$ and $\begin{pmatrix} \lambda_2 & a \\ 0 & \lambda_2 \end{pmatrix}$ are not conjugate. So, by Lemma 5.5, $cl\left(\begin{pmatrix} \lambda_1 & a \\ 0 & \lambda_1 \end{pmatrix}\right) \neq cl\left(\begin{pmatrix} \lambda_2 & a \\ 0 & \lambda_2 \end{pmatrix}\right)$.

❏

Now, we will look at (3) from Theorem 9.1. We have to consider two lemmas for this type of classes. Lemma 9.7 will look at when we have distinct values in the diagonals, no matter what the order is. Then Lemma 9.8 will look at when we have the same values in the diagonals, again with no fixed order.

Lemma 9.7. *For every* $\lambda_1,\ \lambda_2,\ \alpha_1,\ \alpha_2 \in \mathbb{Z}_p^*$ *with* $\{\lambda_1,\ \lambda_2\} \neq \{\alpha_1,\ \alpha_2\}$ *and* $a \neq 0$ *or*

1, $cl\left(\begin{pmatrix} \lambda_1 & a \\ 0 & \lambda_2 \end{pmatrix}\right) \neq cl\left(\begin{pmatrix} \alpha_1 & a \\ 0 & \alpha_2 \end{pmatrix}\right)$.

Proof: Let $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}, \begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix} \in GL(2,\ \mathbb{Z}_p)$ where $\lambda_1,\ \lambda_2,\ \alpha_1,\ \alpha_2 \in \mathbb{Z}_p^*$ and $\{\lambda_1,\ \lambda_2\} \neq \{\alpha_1,\ \alpha_2\}$. By Lemma 9.2, $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$ has eigenvalues λ_1 and λ_2, and $\begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix}$ has eigenvalues α_1 and α_2. Since $\{\lambda_1,\ \lambda_2\} \neq \{\alpha_1,\ \alpha_2\}$ and by Theorem 5.7, $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$ and $\begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix}$ are not conjugate. So, by Lemma 5.5, $cl\left(\begin{pmatrix} \lambda_1 & a \\ 0 & \lambda_1 \end{pmatrix}\right) \neq cl\left(\begin{pmatrix} \lambda_2 & a \\ 0 & \lambda_2 \end{pmatrix}\right)$.

❏

Lemma 9.8. *For every* $\lambda_1,\ \lambda_2,\ \alpha_1,\ \alpha_2 \in \mathbb{Z}_p^*$ *with* $\{\lambda_1,\ \lambda_2\} = \{\alpha_1,\ \alpha_2\}$ *and* $a \neq 0$ *or 1,* $cl\left(\begin{pmatrix} \lambda_1 & a \\ 0 & \lambda_2 \end{pmatrix}\right) = cl\left(\begin{pmatrix} \alpha_1 & a \\ 0 & \alpha_2 \end{pmatrix}\right)$.

Proof: Let $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}, \begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix} \in GL(2,\ \mathbb{Z}_p)$ where $\lambda_1,\ \lambda_2,\ \alpha_1,\ \alpha_2 \in \mathbb{Z}_p^*$ and $\{\lambda_1,\ \lambda_2\} = \{\alpha_1,\ \alpha_2\}$.

Case i: Assume $\lambda_1 = \alpha_1$ and $\lambda_2 = \alpha_2$. Then $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} = \begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix}$ and so $cl\left(\begin{pmatrix} \lambda_1 & a \\ 0 & \lambda_1 \end{pmatrix}\right) = cl\left(\begin{pmatrix} \lambda_2 & a \\ 0 & \lambda_2 \end{pmatrix}\right)$ by definition.

Case ii: Assume $\lambda_1 = \alpha_2$ and $\lambda_2 = \alpha_1$. Consider $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in GL(2,\ \mathbb{Z}_p)$ because $0,\ 1 \in \mathbb{Z}_p$ and $Det\left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right] = 0 - 1 = -1 \neq 0$. It is easy to see that $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. By assumption, $\begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix} = \begin{pmatrix} \lambda_2 & 0 \\ 0 & \lambda_1 \end{pmatrix}$. Therefore,

$$\begin{aligned} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1} &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \lambda_2 & 0 \\ 0 & \lambda_1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1} \\ &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \lambda_2 & 0 \\ 0 & \lambda_1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & \lambda_2 \\ \lambda_1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}. \end{aligned}$$

Thus by definition, $\begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix} \in cl\left(\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}\right)$.

Also, $\begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix} \in cl\left(\begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix}\right)$, so $cl\left(\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}\right) \bigcap cl\left(\begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix}\right) \neq$

$\emptyset$. Hence, because conjugacy is an equivalence relation,

$$cl\left(\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}\right) = cl\left(\begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix}\right).$$

❏

Lemma 9.10 will look at Part (4) from Theorem 9.1 and it is the last lemma that will deal with counting the conjugacy classes in Theorem 9.1.

Lemma 9.9. *For every* $\alpha_1,\ \alpha_2 \in \mathbb{Z}_p$ *and* $\beta_1,\ \beta_2 \in \mathbb{Z}_p^*$ *with* $\alpha_1 \neq \alpha_2$, $\begin{pmatrix} \alpha_1 & D\beta_1 \\ \beta_1 & \alpha_1 \end{pmatrix}$, $\begin{pmatrix} \alpha_2 & D\beta_2 \\ \beta_2 & \alpha_2 \end{pmatrix} \in GL(2,\ \mathbb{Z}_p)$ *and* $cl\left(\begin{pmatrix} \alpha_1 & D\beta_1 \\ \beta_1 & \alpha_1 \end{pmatrix}\right) \neq cl\left(\begin{pmatrix} \alpha_2 & D\beta_2 \\ \beta_2 & \alpha_2 \end{pmatrix}\right)$.

Proof: Let $\alpha_1,\ \alpha_2 \in \mathbb{Z}_p$ and $\beta_1,\ \beta_2 \in \mathbb{Z}_p^*$ with $\alpha_1 \neq \alpha_2$, then $\begin{pmatrix} \alpha_1 & D\beta_1 \\ \beta_1 & \alpha_1 \end{pmatrix}$, $\begin{pmatrix} \alpha_2 & D\beta_2 \\ \beta_2 & \alpha_2 \end{pmatrix} \in GL(2,\ \mathbb{Z}_p)$. By Lemma 9.3, $\begin{pmatrix} \alpha_1 & D\beta_1 \\ \beta_1 & \alpha_1 \end{pmatrix}$ has eigenvalues $\alpha_1 \pm \sqrt{D}\beta_1$ and $\begin{pmatrix} \alpha_2 & D\beta_2 \\ \beta_2 & \alpha_2 \end{pmatrix}$ has eigenvalues $\alpha_2 \pm \sqrt{D}\beta_2$. Since $\alpha_1 \neq \alpha_2$ and $\sqrt{D} \in \mathbb{Z}_p[\sqrt{D}]\backslash\mathbb{Z}_p$, by Lemma 4.14, $\alpha_1 \pm \sqrt{D}\beta_1 \neq \alpha_2 \pm \sqrt{D}\beta_2$. Thus by Theorem 5.7, $\begin{pmatrix} \alpha_1 & D\beta_1 \\ \beta_1 & \alpha_1 \end{pmatrix}$ and $\begin{pmatrix} \alpha_2 & D\beta_2 \\ \beta_2 & \alpha_2 \end{pmatrix}$ are not conjugate. And so $cl\left(\begin{pmatrix} \alpha_1 & D\beta_1 \\ \beta_1 & \alpha_1 \end{pmatrix}\right) \neq cl\left(\begin{pmatrix} \alpha_2 & D\beta_2 \\ \beta_2 & \alpha_2 \end{pmatrix}\right)$, by Lemma 5.5.

❏

Lemma 9.10. *For every* $\alpha_1,\ \alpha_2 \in \mathbb{Z}_p$ *and* $\beta_1,\ \beta_2 \in \mathbb{Z}_p^*$ *with* $\beta_1 \neq \pm\beta_2$, $\begin{pmatrix} \alpha_1 & D\beta_1 \\ \beta_1 & \alpha_1 \end{pmatrix}$, $\begin{pmatrix} \alpha_2 & D\beta_2 \\ \beta_2 & \alpha_2 \end{pmatrix} \in GL(2,\ \mathbb{Z}_p)$ *and* $cl\left(\begin{pmatrix} \alpha_1 & D\beta_1 \\ \beta_1 & \alpha_1 \end{pmatrix}\right) \neq cl\left(\begin{pmatrix} \alpha_2 & D\beta_2 \\ \beta_2 & \alpha_2 \end{pmatrix}\right)$.

Proof: Let $\alpha_1,\ \alpha_2 \in \mathbb{Z}_p$ and $\beta_1,\ \beta_2 \in \mathbb{Z}_p^*$ with $\beta_1 \neq \pm\beta_2$, then $\begin{pmatrix} \alpha_1 & D\beta_1 \\ \beta_1 & \alpha_1 \end{pmatrix}$, $\begin{pmatrix} \alpha_2 & D\beta_2 \\ \beta_2 & \alpha_2 \end{pmatrix} \in GL(2,\ \mathbb{Z}_p)$. By Lemma 9.3, $\begin{pmatrix} \alpha_1 & D\beta_1 \\ \beta_1 & \alpha_1 \end{pmatrix}$ has eigenvalues $\alpha_1 \pm \sqrt{D}\beta_1$ and $\begin{pmatrix} \alpha_2 & D\beta_2 \\ \beta_2 & \alpha_2 \end{pmatrix}$ has eigenvalues $\alpha_2 \pm \sqrt{D}\beta_2$. Since $\beta_1 \neq \pm\beta_2$, and $\sqrt{D} \in \mathbb{Z}_p[\sqrt{D}]\backslash\mathbb{Z}_p$, by Lemma 4.14, $\alpha_1 \pm \sqrt{D}\beta_1 \neq \alpha_2 \pm \sqrt{D}\beta_2$. Thus by Theorem 5.7, $\begin{pmatrix} \alpha_1 & D\beta_1 \\ \beta_1 & \alpha_1 \end{pmatrix}$ and $\begin{pmatrix} \alpha_2 & D\beta_2 \\ \beta_2 & \alpha_2 \end{pmatrix}$ are not conjugate. And so $cl\left(\begin{pmatrix} \alpha_1 & D\beta_1 \\ \beta_1 & \alpha_1 \end{pmatrix}\right) \neq cl\left(\begin{pmatrix} \alpha_2 & D\beta_2 \\ \beta_2 & \alpha_2 \end{pmatrix}\right)$, by Lemma 5.5.

❏

Lemma 9.11. *For every* $\alpha_1,\ \alpha_2 \in \mathbb{Z}_p$ *and* $\beta_1,\ \beta_2 \in \mathbb{Z}_p^*$ *with* $\alpha_1 = \alpha_2$ *and* $\beta_1 = \pm\beta_2$, $\begin{pmatrix} \alpha_1 & D\beta_1 \\ \beta_1 & \alpha_1 \end{pmatrix}, \begin{pmatrix} \alpha_2 & D\beta_2 \\ \beta_2 & \alpha_2 \end{pmatrix} \in GL(2,\ \mathbb{Z}_p)$ *and* $cl\left(\begin{pmatrix} \alpha_1 & D\beta_1 \\ \beta_1 & \alpha_1 \end{pmatrix}\right) = cl\left(\begin{pmatrix} \alpha_2 & D\beta_2 \\ \beta_2 & \alpha_2 \end{pmatrix}\right)$.

Proof: Let $\alpha_1,\ \alpha_2 \in \mathbb{Z}_p$ and $\beta_1,\ \beta_2 \in \mathbb{Z}_p^*$ with $\alpha_1 = \alpha_2$ and $\beta_1 = \pm\beta_2$, then $\begin{pmatrix} \alpha_1 & D\beta_1 \\ \beta_1 & \alpha_1 \end{pmatrix}, \begin{pmatrix} \alpha_2 & D\beta_2 \\ \beta_2 & \alpha_2 \end{pmatrix} \in GL(2,\ \mathbb{Z}_p)$.

Case (i): Assume $\beta_1 = \beta_2$.

Then, since the matrices are the same, clearly $cl\left(\begin{pmatrix} \alpha_1 & D\beta_1 \\ \beta_1 & \alpha_1 \end{pmatrix}\right) = cl\left(\begin{pmatrix} \alpha_2 & D\beta_2 \\ \beta_2 & \alpha_2 \end{pmatrix}\right)$.

Case (ii): Assume $\beta_1 = -\beta_2$.

We will show that the two matrices are conjugate in this case. Consider $S \coloneqq \begin{pmatrix} 1 & D \\ -1 & -1 \end{pmatrix}$. We can see that the determinant of S is $-1 + D$. Suppose to the contrary that $-1 + D = 0$, which implies $D = 1$ and so $|D| = 1$. Since $|D| = 2^l$ for some $l > 0$, a contradiction has been reached. Thus S has nonzero determinant. Therefore $S \in GL(2,\ \mathbb{Z}_p)$. We will show that $S\begin{pmatrix} \alpha_1 & D\beta_1 \\ \beta_1 & \alpha_1 \end{pmatrix} S^{-1} = \begin{pmatrix} \alpha_2 & D\beta_2 \\ \beta_2 & \alpha_2 \end{pmatrix}$ by showing that $S\begin{pmatrix} \alpha_1 & D\beta_1 \\ \beta_1 & \alpha_1 \end{pmatrix} = \begin{pmatrix} \alpha_2 & D\beta_2 \\ \beta_2 & \alpha_2 \end{pmatrix} S$. So by substituting, $S\begin{pmatrix} \alpha_1 & D\beta_1 \\ \beta_1 & \alpha_1 \end{pmatrix} = \begin{pmatrix} 1 & D \\ -1 & -1 \end{pmatrix}\begin{pmatrix} \alpha_2 & -D\beta_2 \\ -\beta_2 & \alpha_2 \end{pmatrix} = \begin{pmatrix} \alpha_2 - D\beta_2 & -D\beta_2 + D\alpha_2 \\ -\alpha_2 + \beta_2 & D\beta_2 - \alpha_2 \end{pmatrix}$. Calculating the other side we have $\begin{pmatrix} \alpha_2 & D\beta_2 \\ \beta_2 & \alpha_2 \end{pmatrix} S = \begin{pmatrix} \alpha_2 & D\beta_2 \\ \beta_2 & \alpha_2 \end{pmatrix}\begin{pmatrix} 1 & D \\ -1 & -1 \end{pmatrix}$ $= \begin{pmatrix} \alpha_2 - D\beta_2 & -D\beta_2 + D\alpha_2 \\ -\alpha_2 + \beta_2 & D\beta_2 - \alpha_2 \end{pmatrix}$. Hence $\begin{pmatrix} \alpha_1 & D\beta_1 \\ \beta_1 & \alpha_1 \end{pmatrix}$ is conjugate to $\begin{pmatrix} \alpha_2 & D\beta_2 \\ \beta_2 & \alpha_2 \end{pmatrix}$. Therefore, following the same strategy as in the proof of Lemma 9.8, we have $cl\left(\begin{pmatrix} \alpha_1 & D\beta_1 \\ \beta_1 & \alpha_1 \end{pmatrix}\right) = cl\left(\begin{pmatrix} \alpha_2 & D\beta_2 \\ \beta_2 & \alpha_2 \end{pmatrix}\right)$.

❏

Lemma 9.12. *The number of conjugacy classes in* $GL(2,\ \mathbb{Z}_p)$ *are as follows:*

(1) $(p-1)$ *classes of the form* $cl(A)$, *where* $A \coloneqq \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$, *with* $\lambda \in \mathbb{Z}_p^*$.

(2) $(p-1)$ *classes of the form* $cl(B)$, *where* $B \coloneqq \begin{pmatrix} \mu & 1 \\ 0 & \mu \end{pmatrix}$, *with* $\mu \in \mathbb{Z}_p^*$.

(3) $\frac{1}{2}(p-1)(p-2)$ *classes of the form* $cl(C)$, *where* $C \coloneqq \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$ *with* $\lambda_1,\ \lambda_2 \in \mathbb{Z}_p^*$ *and* $\lambda_1 \neq \lambda_2$.

(4) $\frac{1}{2}(p^2-p)$ *classes of the form* $cl(E)$*, where* $E \coloneqq \begin{pmatrix} \alpha & D\beta \\ \beta & \alpha \end{pmatrix}$*, with* $\alpha,\ \beta \in \mathbb{Z}_p$ *and* $\beta \neq 0$*.*

Proof: Parts (1) and (2): From Lemma 9.6, different λ's in $\mathbb{Z}_p^*$ yield different conjugacy classes. Since there are $(p-1)$ choices for λ, we have $(p-1)$ classes of type A matrices when $a=0$ and $(p-1)$ classes of type B matrices when $a=1$.

Part (3): From Lemma 9.7 and Lemma 9.8, different subsets of order 2 in $\mathbb{Z}_p^*$ yield different conjugacy classes. Since there are $\begin{pmatrix} p-1 \\ 2 \end{pmatrix}$ choices for subsets of order 2, we have $\begin{pmatrix} p-1 \\ 2 \end{pmatrix} \coloneqq \frac{1}{2}(p-1)(p-2)$ classes of type C matrices.

Part (4): From Lemma 9.9, different α's in $\mathbb{Z}_p$ yield different conjugacy classes. So we have p choices for α. Next, from Lemmas 9.10 and 9.11, different subsets of the form $\{\beta, -\beta\}$ with $\beta \in \mathbb{Z}_p^*$ yield different conjugacy classes. Since there are $p-1$ choices for β, we have $\frac{1}{2}(p-1)$ choices for such subsets. So we have $p\frac{1}{2}(p-1) = \frac{1}{2}(p^2-p)$ total classes of type E matrices.

❏

Finally, we will show that there are no more conjugacy classes in $GL(2,\ \mathbb{Z}_p)$.

Lemma 9.13. *Every matrix in* $GL(2,\ \mathbb{Z}_p)$ *will fall into one of the types of conjugacy classes from Theorem 9.1.*

Proof: Let $L = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2,\ \mathbb{Z}_p)$. Note that L has two eigenvalues in $\mathbb{Z}_p[\sqrt{D}]$, by Lemma 8.6 and the fact that $Det\left[\begin{pmatrix} a-x & b \\ c & d-x \end{pmatrix}\right] = (a-x)(d-x) - bc = x^2 + (-a+(-d))x + (ad-bc)$ is a quadratic polynomial in $\mathbb{Z}_p[x]$.

Proceed by cases.

Case 1: Assume the eigenvalues are in $\mathbb{Z}_p$ and they are distinct.

Let λ_1 and λ_2 be the corresponding eigenvalues, so by Theorem 5.8, L is conjugate to $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$. Thus L is in a class of type (3) matrices.

Case 2: Assume the eigenvalues are in $\mathbb{Z}_p$ and they are the same.

Consider the eigenvalue of L to be λ. Let u be an eigenvector for λ. From Linear Algebra, there exists a vector v such that $\{u, v\}$ is a basis for $\mathbb{Z}_p^2$. Let T be the matrix with u and v as columns, denoted $T = L[u\ v]$. Then T is invertible [10, p. 173]. Thus $T \in GL(2,\ \mathbb{Z}_p)$. Following the same strategy that Strang uses for diagonalization, we will show that $T^{-1}LT = \begin{pmatrix} \lambda & x \\ 0 & y \end{pmatrix}$ where $\begin{bmatrix} x \\ y \end{bmatrix} = T^{-1}Lv$. To do this we will first

show that $LT = T\begin{pmatrix} \lambda & x \\ 0 & y \end{pmatrix}$. Looking at the left side, we have $LT = L[u\ v] = [Lu\ Lv]$ by definition of T and matrix multiplication. Then $[Lu\ Lv] = [\lambda u\ Lv]$ since u is an eigenvector for the eigenvalue λ. Moving onto the right side, because $\begin{bmatrix} x \\ y \end{bmatrix} = T^{-1}Lv$, $T\begin{pmatrix} \lambda & x \\ 0 & y \end{pmatrix} = T\begin{pmatrix} \begin{bmatrix} \lambda \\ 0 \end{bmatrix} & T^{-1}Lv \end{pmatrix} = \begin{pmatrix} T\begin{bmatrix} \lambda \\ 0 \end{bmatrix} & T(T^{-1}Lv) \end{pmatrix}$. Knowing that u is an eigenvector for the eigenvalue λ, we have that $\begin{pmatrix} T\begin{bmatrix} \lambda \\ 0 \end{bmatrix} & T(T^{-1}Lv) \end{pmatrix} = [\lambda u\ Lv]$. Thus $LT = T\begin{pmatrix} \lambda & x \\ 0 & y \end{pmatrix}$. Since T is invertible, we obtain $T^{-1}LT = \begin{pmatrix} \lambda & x \\ 0 & y \end{pmatrix}$, as desired. Hence, by Theorem 5.7 and Lemma 9.2, $y = \lambda$. So, $T^{-1}LT = \begin{pmatrix} \lambda & x \\ 0 & \lambda \end{pmatrix}$.

Subcase 2a: Assume $x = 0$.

Then, $T^{-1}LT = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$ and L is in a conjugacy class of type (1) matrices.

Subcase 2b: Assume $x \neq 0$.

Let $C = \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}$. Since $x \neq 0$, $Det(C) \neq 0$. Hence $C \in GL(2,\ \mathbb{Z}_p)$. It is easy to check that $C^{-1} = \begin{pmatrix} x^{-1} & 0 \\ 0 & 1 \end{pmatrix}$. By Theorem 4.3, substitution and matrix multiplication we obtain, $(TC)^{-1}L(TC) = C^{-1}T^{-1}LTC = C^{-1}\begin{pmatrix} \lambda & x \\ 0 & \lambda \end{pmatrix}C = \begin{pmatrix} x^{-1} & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \lambda & x \\ 0 & \lambda \end{pmatrix}\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \lambda x^{-1} & 1 \\ 0 & \lambda \end{pmatrix}\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$. This concludes that L is in a conjugacy class of type (2).

Case 3: Assume the eigenvalues are not in $\mathbb{Z}_p$ and they are distinct.

From above, the eigenvalues of L are the roots of $x^2+(-a+(-d))x+(ad-bc) = 0$ which is an element in $\mathbb{Z}_p[x]$, because of closure and the fact that $a, b, c, d \in \mathbb{Z}_p$. Lemma 8.6 states that these eigenvalues are $-(-a+(-d))2^{-1} \pm \gamma$ where $\gamma^2 = (-a-d)^2 2^{-2} - (ad-bc)$. Let's define $\alpha \coloneqq -(-a+(-d))2^{-1}$.

We want to show that $\gamma = \pm\sqrt{D}\beta$ for some $\beta \in < s >$, so that our eigenvalues have the same form as in Part (4).

First, suppose to the contrary that $\gamma^2 = 0$. It follows that $\gamma = 0$, and so the eigenvalue of L is α, which is in $\mathbb{Z}_p$ by closure. Since the eigenvalues of L are not in $\mathbb{Z}_p$ from above, a contradiction has been reached. Thus $\gamma^2 \in \mathbb{Z}_p^*$. Next, assume to the contrary that γ^2 has a square root in $\mathbb{Z}_p^*$. Hence, $\gamma \in \mathbb{Z}_p^*$, thus by closure $\alpha \pm \gamma \in \mathbb{Z}_p$. Again, the same contradiction has been reached. Thus there does not exist a square root of γ^2 that is in $\mathbb{Z}_p^*$. So, it follows from Part (4) that $\gamma^2 = D\beta^2$ for some $\beta \in < s >$. By the definition of multiplication in $\mathbb{Z}_p^*[\sqrt{D}]$, $\gamma^2 = (\sqrt{D}\beta)^2$.

Hence, $\gamma = \pm\sqrt{D}\beta$. Either way, the eigenvalues of L are $\alpha \pm \sqrt{D}\beta$. If $\beta = 0$, then the eigenvalues are both α, which is an element in $\mathbb{Z}_p$. This contradicts our original assumption, thus $\beta \neq 0$. Furthermore, by the Corollary 4.14, since $\beta \neq -\beta$, because $\beta \in \mathbb{Z}_p$ where p is an odd prime, we can say that these two eigenvalues are distinct.

Let z and w be eigenvectors in $\mathbb{Z}_p[\sqrt{D}]^2$ for $\alpha \pm \sqrt{D}\beta$ respectively. Let $z = \begin{pmatrix} r+\sqrt{D}s \\ u+\sqrt{D}v \end{pmatrix}$ where $r, s, u, v \in \mathbb{Z}_p$, then by Theorem 8.7 $w = \begin{pmatrix} r-\sqrt{D}s \\ u-\sqrt{D}v \end{pmatrix}$. Let T be the matrix with z and w as columns. Hence, $T = [z\ w]$. Furthermore, $T^{-1}LT = \begin{pmatrix} \alpha+\sqrt{D}\beta & 0 \\ 0 & \alpha-\sqrt{D}\beta \end{pmatrix}$ by Theorem 5.8.

Notice $\begin{pmatrix} \alpha & D\beta \\ \beta & \alpha \end{pmatrix}\begin{pmatrix} \sqrt{D} \\ 1 \end{pmatrix} = \begin{pmatrix} \sqrt{D}\alpha + D\beta \\ \sqrt{D}\beta + \alpha \end{pmatrix} = (\alpha+\sqrt{D}\beta)\begin{pmatrix} \sqrt{D} \\ 1 \end{pmatrix}$ and $\begin{pmatrix} \alpha & D\beta \\ \beta & \alpha \end{pmatrix}\begin{pmatrix} -\sqrt{D} \\ 1 \end{pmatrix} = \begin{pmatrix} -\sqrt{D}\alpha + D\beta \\ -\sqrt{D}\beta + \alpha \end{pmatrix} = (\alpha-\sqrt{D}\beta)\begin{pmatrix} -\sqrt{D} \\ 1 \end{pmatrix}$. Therefore, $\alpha \pm D\beta$ are eigenvalues of $\begin{pmatrix} \alpha & D\beta \\ \beta & \alpha \end{pmatrix}$, with corresponding eigenvectors $\begin{pmatrix} \pm\sqrt{D} \\ 1 \end{pmatrix}$. Consider the matrix $S = \begin{pmatrix} \sqrt{D} & -\sqrt{D} \\ 1 & 1 \end{pmatrix}$. Then by Theorem 5.8, $S^{-1}\begin{pmatrix} \alpha & D\beta \\ \beta & \alpha \end{pmatrix}S = \begin{pmatrix} \alpha+\sqrt{D}\beta & 0 \\ 0 & \alpha-\sqrt{D}\beta \end{pmatrix}$, which implies that $\begin{pmatrix} \alpha & D\beta \\ \beta & \alpha \end{pmatrix} = S\begin{pmatrix} \alpha+\sqrt{D}\beta & 0 \\ 0 & \alpha-\sqrt{D}\beta \end{pmatrix}S^{-1}$. Therefore,

$$(TS^{-1})^{-1}L(TS^{-1}) = ST^{-1}LTS^{-1} = S\begin{pmatrix} \alpha+\sqrt{D}\beta & 0 \\ 0 & \alpha-\sqrt{D}\beta \end{pmatrix}S^{-1} = \begin{pmatrix} \alpha & D\beta \\ \beta & \alpha \end{pmatrix}.$$

Computing TS^{-1} we get

$$\begin{aligned} TS^{-1} &= \begin{pmatrix} r+\sqrt{D}s & r-\sqrt{D}s \\ u+\sqrt{D}v & u-\sqrt{D}v \end{pmatrix}\begin{pmatrix} \frac{1}{2\sqrt{D}} & \frac{1}{2} \\ \frac{1}{2\sqrt{D}} & -\frac{1}{2} \end{pmatrix} \\ &= \begin{pmatrix} \frac{1}{2\sqrt{D}}(r+\sqrt{D}s) - \frac{1}{2\sqrt{D}}(r-\sqrt{D}s) & \frac{1}{2}(r+\sqrt{D}s) + \frac{1}{2}(r-\sqrt{D}s) \\ \frac{1}{2\sqrt{D}}(u+\sqrt{D}v)\frac{1}{2\sqrt{D}}(u-\sqrt{D}v) & \frac{1}{2}(r+\sqrt{D}s) + \frac{1}{2}(r-\sqrt{D}s) \end{pmatrix} \\ &= \begin{pmatrix} s & r \\ u & v \end{pmatrix}. \end{aligned}$$

As noted before, $s, u, r, v \in \mathbb{Z}_p$. Therefore, $\begin{pmatrix} s & r \\ u & v \end{pmatrix} = TS^{-1} \in GL(2,\ \mathbb{Z}_p)$. Thus L is in a conjugacy class of type (4) matrices.

❏

Theorem 9.14. *Let p be a prime, then $|GL(2,\ \mathbb{Z}_p)| = (p^2-1)(p^2-p)$.*

Proof: The columns of any matrix in $GL(2,\ \mathbb{Z}_p)$ must be linearly independent. So calculating how many choices for column one, we can obtain any combination of entries, except for the zero vector. Thus there are $p^2 - 1$ options for this column in total. Since the second column is linearly independent from the first, it cannot be any scalar multiple of it. Hence, since there are p scalar multiples in $\mathbb{Z}_p$, we have $(p^2 - p)$ choices for the entries in column two. Hence, the theorem follows.

❏

Theorem 9.15. *If p is an odd prime number, then $Pr(GL(2,\ \mathbb{Z}_p)) = \frac{1}{(p-1)p}$.*

Proof: Suppose that p is an odd prime number. From Theorem 9.1, we can compute the total number of conjugacy classes in $GL(2,\ \mathbb{Z}_p)$. This results in $(p-1)+(p-1)+\frac{1}{2}(p-1)(p-2)+\frac{1}{2}(p^2-p) = (p-1)(1+1+\frac{1}{2}(p-2)+\frac{1}{2}p) = (p-1)(p+1)$. Hence, it follows from Theorem 6.3 and Theorem 9.14 that $Pr(GL(2,\ \mathbb{Z}_p)) = \frac{(p-1)(p+1)}{(p^2-1)(p^2-p)} = \frac{(p-1)(p+1)}{(p-1)(p+1)(p-1)p} = \frac{1}{(p-1)p}$.

❏

We will end with an interesting example comparing two diverse groups. Consider the following groups, $GL(2,\ \mathbb{Z}_5)$ and $(D_3 \oplus D_3 \oplus D_5 \oplus D_3)$. If we compute the probability of each, we obtain $Pr(GL(2,\ \mathbb{Z}_5)) = \frac{1}{(5-1)5} = \frac{1}{20}$ from Theorem 9.15, and $Pr(D_3 \oplus D_3 \oplus D_5 \oplus D_3) = \frac{1}{20}$ from Theorem 7.9 and Lemma 6.6. So, it is interesting to see how two very distinct groups, one a set of matrices and the other a direct sum of dihedral groups, yet both yield the same probability that two elements when chosen at random will commute.

REFERENCES

---

1. A. Castelaz, Commutativity Degree of Finite Groups, Master of Arts Thesis, Wake Forest University, 2010.

2. C. Clifton, D Guichard, P. Keef, How Commutative Are Direct Product of Dihedral Groups, *Math. Mag.* **84** (2011) 137-140.

3. P. Erdos and P. Turan, On some problems of statistical group theory, *Acta Math. Acad. Sci. Hung.* **19** (1968) 413-435.

4. J. Gallian, *Contemporary Abstract Algebra*. Eighth Edition. Brooks/Cole, Boston, MA, 2013.

5. R. M. Guralnick, G. R. Robinson, On the commuting probability in finite groups, *J. Algebra* **300** (2006) 509-528.

6. W.H. Gustafson, What is the probability that two group elements commute?, *Amer. Math. Monthly* **80** (1973) 1031-1034.

7. D. MacHale, How Commutative Can a Non-Commutative Group Be?, *Math. Gaz.* **58** (1974) 199-202.

8. A. Prasad, $GL_2(\mathbf{F}_p)$, `http://www.imsc.res.in/~amri/GL2p.pdf`.

9. S. Rogers, On Some Problems in Group Theory of Probabilistic Nature, Master of Arts Thesis, State University of New York at Binghamton, 1993.

10. G. Strang, *Introduction to Linear Algebra*. Fourth Edition. Wellesley-Cambridge Press, Wellesley, MA, 2009.