Panmagic Permutations and N-ary Groups

S. Koshkin and J. Lee

Abstract - Panmagic permutations are permutations whose matrices are panmagic squares. Positions of 1-s in the latter describe maximal configurations of non-attacking queens on a toroidal chessboard. Some of them, affine panmagic permutations, can be conveniently described by linear formulas of modular arithmetic, and we show that their sets have remarkable algebraic properties when one multiplies three or more of them rather than just two. In group-theoretic terms, they are special cosets of the dihedral group in the group of all affine permutations. We also investigate decomposition of panmagic permutations into disjoint cycles and find many connections with classical topics of number theory: multiplicative orders, $4k+1$ primes, primitive roots and quadratic residues.

Keywords : magic square; pandiagonally magic square; modular n-queens; affine permutation; dihedral group; general affine group; polyadic group; Post coset theorem; Post cover

Mathematics Subject Classification (2020) **:** 05A05; 05B15; 20N15; 11A07

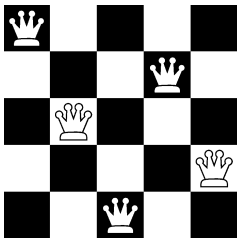
1 Introduction

Magic squares are square matrices with the same sum, called the *magic sum*, in each row, each column, the main diagonal and the main anti-diagonal. Their history goes as far back as ancient China c. 200 BC, and one appears in Albrecht Dürer's famous painting *Melencolia I* (1514). They have attracted the attention of mathematicians since Leonhard Euler's 1776 article linked them to Latin squares [3]. Magic squares that additionally have the same magic sum over all 'broken' diagonals and anti-diagonals were once called "diabolic" [15], but now are commonly known as pandiagonally magic or *panmagic* for short [1, 2]. Early work mainly focused on constructions of magic and panmagic squares, but more recently their algebraic properties also have received attention.

Back in 1950, Derek Lawden claimed that in even dimensions multiplying any three panmagic squares (and then any odd number of them) produces another panmagic square [14]. Although this only holds for panmagic squares with additional symmetry, Lawden's was the first result (that we know of) on closure under ternary multiplication for a class of magic squares. It went entirely unnoticed, but other such classes were discovered in 1990s. Anthony Thompson might have been the first to prove it in print for 3×3 magic and 5×5 panmagic squares in 1994 [21]. In 2012, known classes of magic and panmagic squares closed under ternary multiplication were codified and generalized to higher dimensions by Ronald Nordgren [18].

Thompson had even found a spanning set of 5×5 panmagic permutation matrices that is itself closed under ternary multiplication, no such spanning set exists for 3×3 magic or Lawden's panmagic squares. Moreover, this spanning set is closely associated with the well-known dihedral group D_5, the group of symmetries of the regular pentagon. The nature of this association remained mysterious, like magic, but it suggests looking deeper into permutations with panmagic matrices, which are simpler objects than the matrices themselves.

Although quite natural, the term "panmagic permutations" is rarely used (it is used in [1]), but they are classically known under a different name. A problem from the mid-19th century, often misattributed to Carl Friedrich Gauss [3], asked to place 8 non-attacking queens on the 8×8 chessboard, and it was generalized to $n \times n$ chessboards by François Lionnet in 1869. In 1900, George Carpenter proposed to fold the board into a cylinder by identifying two opposite sides of it [5], and in 1918 George Polya folded it further into a torus. Both modifications have the same effect of letting the queens attack along the entire broken diagonals, and came to be known as the *modular n-queens problem* [3]. Given its solution, replace the board with a matrix and place 1-s into the positions of the queens and 0-s elsewhere as on Figure 1. The result is a panmagic permutation matrix, and conversely, any panmagic permutation produces a modular n-queens solution. In



$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

Figure 1: Modular 5-queens solution and its permutation matrix.

this guise, panmagic permutations have been extensively studied [3], but not, it seems, for their algebraic properties. Even the connection between modular n-queens and panmagic squares [2] is little known despite being used as early as in 1900 by Charles Planck [3][p. 8].

For that matter, ternary and more general N-ary groups are also little known, but the topic is, again, classical. It goes back to Edward Kasner's talk at the 1911 International Congress of Mathematicians and was originally developed by Wilhelm Dörnte in 1920-s, at the urging of Emmy Noether [20]. It should be stressed that N-ary groups are not groups, the multiplication on them is defined for N terms only, and ordinary groups are just a special case with $N = 2$. Emil Post, better known for his work in mathematical logic, proved a key structural result about N-ary groups in 1940, the Post coset theorem. As will be explained in Section 7, it says, essentially, that N-ary groups are cosets of normal subgroups of ordinary groups when the quotient group is cyclic of order $N - 1$. This theorem demystifies the appearance of D_5 in Thompson's proof.

We will show that closure under N-ary multiplication is a general phenomenon for sets of panmagic permutations in prime dimensions $n = p > 3$ because those sets are Post cosets of the dihedral group D_p. Even for the ternary case, our descriptions are

simpler and much more explicit than those based on linear algebra in [18]. A key idea is to consider a subgroup $GA_1(\mathbb{Z}_p)$ of the symmetric group of all permutations S_p in which D_p is normal. Its elements are called *affine permutations* and they can be expressed by simple formulas of modular arithmetic in $\mathbb{Z}_p$. We will also describe the cyclic structure of panmagic affine permutations and relate it to some classical topics of number theory: primitive roots, multiplicative orders, $4k+1$ primes and quadratic residues. We only consider the case of prime dimensions to keep the exposition elementary, but most results generalize to composite n by less elementary methods, see [13].

As many authors have pointed out, magic squares provide a concrete and appealing setting for grasping non-trivial concepts of undergraduate linear algebra [7, 17, 21]. We will show that panmagic permutations are more than apt to do the same for group theory and number theory. Indeed, it is treating them as permutations encoded by simple formulas of modular arithmetic that turns out to be most fruitful for discovering and proving algebraic patterns obscured in other representations.

2 Permutations and Magic Squares

We use standard notation and terminology from group theory [8] and number theory [19]. We will identify the symmetric group of all permutations of n elements S_n with the group of permutations of $\mathbb{Z}_n = \{0, 1, \dots n-1\}$, the set of residues (congruence classes) modulo n. To recover a standard permutation of $1, \dots, n$, one simply replaces residue 0 by n. Two special permutations will play a central role in our study, even though neither of them is magic.

Definition 2.1 *Denote ϕ the flip permutation that swaps antipodal numbers, i.e. $\phi(i) := n+1-i$, and by $\varkappa$ the cyclic shift permutation $\varkappa(i) \equiv i+1 \pmod n$ that shifts numbers one unit up and n to 1. In the cyclic notation, $\phi = (1\,n)(2\,n-1)\dots$ and $\varkappa = (1\,2\dots n)$.*

As usual, $a \mid b$ means that b is an integer multiple of a, and $a \equiv b \pmod n$ means that $n \mid (b-a)$. We will often write congruence formulas for residues in a simplified notation that omits n when it is understood, and replaces $\equiv$ by $=$. For example, we may write $n \equiv 0 \pmod n$ as just $n = 0$ when no confusion results. In our simplified notation, $\phi(i) = 1 - i$ and $\varkappa(i) = i + 1$. The same convention applies to matrix indices when they go over n or under 1, for example, in an $n \times n$ matrix $a_{n+1\,1}$ is a_{11}. The *broken diagonals* of an $n \times n$ matrix A have those a_{ij} where $i - j =$ constant, and the *broken anti-diagonals* have those where $i + j =$ constant. The *main diagonal* is the one with $i - j = 0$, and the *main anti-diagonal* is the one with $i + j = 1$.

A square matrix A is called *semimagic* when all of its column sums and row sums are the same. Their common value is called the *magic sum*. A semimagic matrix is *magic (panmagic)* when the main (all) diagonal(s) and anti-diagonal(s) also have sums equal to the magic sum [7, 18]. We will be mainly interested in matrices P_σ with $\sigma \in S_n$ that permute the standard basis vectors e_i as in $P_\sigma e_i := e_{\sigma(i)}$. All of them are semimagic with the magic sum 1 because a permutation matrix must have a single entry 1 in each row and column, and the rest are 0-s. Moreover, $P_{\sigma\tau} = P_\sigma P_\tau$, where on the left we have

the composition of permutations and on the right the product of matrices. The effect of multiplying a matrix by P_ϕ is to swap i-th and $(n+1-i)$-th rows/columns. This also interchanges (broken) diagonals and anti-diagonals. In turn, multiplication of a matrix by $P_\varkappa^i = P_{\varkappa^i}$ on the left/right cyclically shifts its rows/columns by i positions and moves the main diagonal to one of the broken diagonals.

A permutation will be called magic or panmagic when its matrix is such. Note that the number of 1-s on the diagonal of P_σ is the number of *fixed points* of σ, those for which $\sigma(i) = i$. Similarly, since ϕ flips points about the middle the number of 1-s on the anti-diagonal of P_σ is the number of *flipped points* of σ, those with $\sigma(i) = n+1-i$. Thus, a permutation is magic when it has exactly one fixed and exactly one flipped point, and it is panmagic when all of its cyclic shifts $\varkappa^i\sigma$ are also magic.

3 Panmagic Permutations and Dihedral Groups

In this section, we will introduce the dihedral group in its permutational guise, relate it to panmagic permutations, and reformulate two classical results about modular n-queens solutions in the language of permutations. The subgroup of a group generated by elements of a subset S, i.e., the set of all finite products of their positive and negative powers, will be denoted $\langle S\rangle$. When $S = \{a_1, \ldots, a_k\}$, we write simply $\langle a_1, \ldots, a_k\rangle$.

Definition 3.1 *The subgroup of S_n generated by ϕ and $\varkappa$ will be called dihedral and denoted $D_n := \langle \phi, \varkappa\rangle$. Its elements will be called dihedral permutations.*

As a simple application of our trimmed down congruence notation, let us derive a commutation relation for ϕ and $\varkappa$. Note that $\varkappa^{-1}(i) = i - 1$, so

$$\phi\varkappa(i) = 1 - (i+1) = (1-i) - 1 = \varkappa^{-1}\phi(i). \tag{1}$$

It is also easy to see that $\phi^2 = \varkappa^n = \mathrm{id}$, so the commutation relation implies that all permutations in D_n are of the form $\varkappa^i$ or $\phi\varkappa^i$ with $i = 0, \ldots, n-1$. Moreover, those are all distinct, so $|D_n| = 2n$. Some authors denote D_{2n} what we denote D_n, by the number of elements in it.

Our subgroup D_n is isomorphic to the usual dihedral group defined as the group of symmetries of the regular n-gon [8][2.1]. Indeed, if we number its vertices from 1 to n

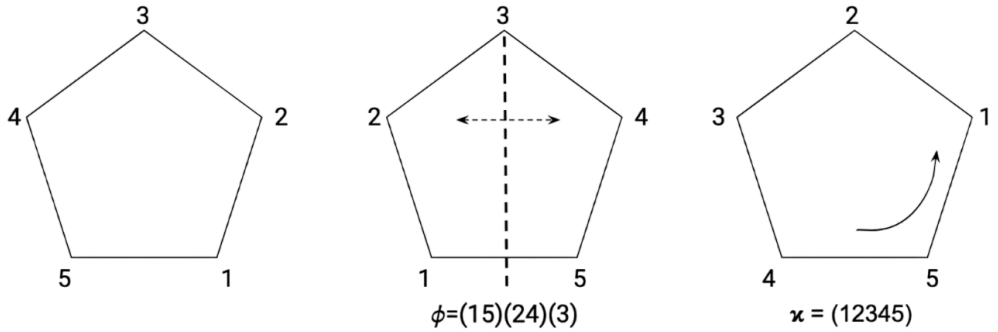


Figure 2: Flip ϕ as reflection and cyclic shift $\varkappa$ as rotation of the regular pentagon.

then ϕ is the permutation induced by the reflection about the middle perpendicular of one of its sides, and $\varkappa$ is induced by the rotation by the angle $\frac{2\pi}{n}$ around its center, see Figure 2.

We will now explain how D_n is related to panmagic squares and permutations. As multiplication by matrices P_ϕ and $P_\varkappa$ interchanges diagonals and anti-diagonals and shifts rows and columns, respectively, it preserves panmagic. The same is true of multiplication by their products and those are exactly the permutation matrices P_δ with δ from the dihedral group D_n. Moreover, multiplication by some P_δ can move any given row/column to any other, and move any given diagonal/anti-diagonal to the main one. Thus, A is a panmagic square if and only if AP_δ (or $P_\delta A$) are magic squares with the same magic sum for all $\delta \in D_n$. Accordingly, $\sigma \in S_n$ is a panmagic permutation if and only if $\sigma\delta$ (or $\delta\sigma$) are magic for all $\delta \in D_n$.

The next theorem is a modular variant of Lionnet's 1869 arithmetic reformulation of the n-queens problem [3][p.4] (see also [1][Lemmas 2.1, 2.2]), and gives convenient arithmetic characterizations of dihedral, magic, and panmagic permutations.

Theorem 3.2 (Lionnet) *Let $\sigma \in S_n$ be a permutation. Then*

(i) *σ is dihedral if and only if $\sigma(i) - i$ or $\sigma(i) + i$ is constant;*

(ii) *σ is magic if and only if 0 has a unique pre-image modulo n under $\sigma(i) - i$ and 1 has a unique pre-image modulo n under $\sigma(i) + i$;*

(iii) *σ is panmagic if and only if $i \mapsto \sigma(i) \pm i$ are both injective modulo n, and hence also permutations.*

Proof.
(i) The "only if" part is trivial from the modular formulas for ϕ and $\varkappa$. Conversely, if $\sigma(i) - i = c$ then $\sigma(i) = i + c$, so $\sigma = \varkappa^c$. And if $\sigma(i) + i = c$ then $\sigma(i) = 1 - i + c - 1$, so $\sigma = \varkappa^{c-1}\phi$. In both cases, σ is dihedral.

(ii) Let σ be magic. Since it has a single fixed point there is only one i with $\sigma(i) = i$, so 0 has a unique pre-image under $\sigma(i) - i$. Since it also has a single flipped point, there is only one j with $\sigma(j) = 1 - j$ and 1 has a unique pre-image under $\sigma(j) + j$. Running the argument in reverse, we conclude that σ has one fixed and one flipped point, and hence is magic.

(iii) Let σ be panmagic. Then $\varkappa^{-k}\sigma$ is magic for any k, and $\varkappa^{-k}\sigma(i) - i = \sigma(i) - i - k = 0$ has a unique solution modulo n by (ii). But then $\sigma(i) - i = k$ has a unique solution for any k and $\sigma(i) - i$ is injective. Similarly, $\varkappa^k\phi\sigma$ is magic for any k, $\varkappa^k\phi\sigma(i) - i = 1 - (\sigma(i) + i) + k = 1$ has a unique solution, and then so does $\sigma(i) + i = k$. Thus, $\sigma(i) + i$ is also injective.

Conversely, let $\sigma(i) \pm i$ be injective modulo n. By (ii), it is enough to show that so are $\delta\sigma(i) \pm i$ for all $\delta \in D_n$, and even just for $\delta = \varkappa, \phi$ since they generate D_n. But $\varkappa\sigma(i) \pm i = \sigma(i) \pm i + 1$ and $\phi\sigma(i) \pm i = 1 - (\sigma(i) \mp i)$, so this follows trivially. □

A sad consequence of Lionnet's characterization is that panmagic permutations do not exist in all dimensions. The 'nice' dimensions first appeared in Carpenter's construction

of modular n-queens solutions in 1900 [5], and were proved exhaustive by Polya in 1918 by tiling the plane with chessboards. The slick congruence proof of the non-trivial "only if" part below is due to Kløve, see [2]. The "if" part will easily follow from constructions in Section 5.

Theorem 3.3 (Polya) *S_n contains panmagic permutations only if $2, 3 \nmid n$.*

Proof. Let σ be a panmagic permutation. By Theorem 3.2 (iii), $\sigma(i) - i$ is also a permutation, which means that for $i = 1, \ldots, n$ it returns the same residues in a different order. Therefore, modulo n:

$$\Sigma_1 := \sum_{i=1}^{n} i = \sum_{i=1}^{n} (\sigma(i) - i) = \Sigma_1 - \Sigma_1 = 0,$$

i.e. Σ_1 is a multiple of n. But $\Sigma_1 = \frac{n(n+1)}{2}$ and this can only happen when $n+1$ is even, so $2 \nmid n$.

Similarly, let $\Sigma_2 := \sum_{i=1}^{n} i^2$. Since $\sigma(i) + i$ is also a permutation, we have modulo n:

$$2\Sigma_2 = \sum_{i=1}^{n} (\sigma(i) - i)^2 + \sum_{i=1}^{n} (\sigma(i) + i)^2 = 2\sum_{i=1}^{n} \sigma(i)^2 + 2\sum_{i=1}^{n} i^2 = 4\Sigma_2 = 0,$$

i.e. $2\Sigma_2$ is a multiple of n. But $2\Sigma_2 = \frac{n(n+1)(2n+1)}{3}$, and this can only happen when $n+1$ or $2n+1$ is divisible by 3. But both numbers are relatively prime to n, so $3 \nmid n$. □

We will refer to $n > 1$ with $2, 3 \nmid n$ as *Polya dimensions*, and n will be assumed to be Polya from now on, unless otherwise stated.

4 Panmagic Products in Dimensions 5 and 7

To motivate further developments, we will analyze products of panmagic permutations in the two lowest dimensions where they exist, $n = 5$ and $n = 7$. For the $n = 5$ case we will initially follow Thompson [21].

When H is a subgroup of a group G and $a \in G$ we will write aH for the *left coset* of H, i.e., the set of all products ah with $h \in H$. Thompson presents the space of 5×5 panmagic squares as the linear span of permutation matrices with permutations from the coset ψD_5, where $\psi := (1)(2\,4\,5\,3)$ is a particular panmagic permutation. Explicitly,

$$\psi D_5 := \{\psi, \psi\varkappa, \ldots, \psi\varkappa^4, \psi\phi, \psi\phi\varkappa, \ldots, \psi\phi\varkappa^4\}, \tag{2}$$

and there is a single independent linear relation among the matrices of ψD_5, namely, $\sum_{i=0}^{4} P_{\psi\varkappa^i} = \sum_{i=0}^{4} P_{\psi\phi\varkappa^i}$. The reader can check that both sides add up to the matrix with all entries 1. The space of 5×5 panmagic squares is known to be 9-dimensional [10], so any 9 of ψD_5 matrices form a basis of it. By direct calculation, $D_5 \cdot \psi D_5 = \psi D_5 \cdot D_5 \subseteq \psi D_5$ and $\psi D_5 \cdot \psi D_5 \subseteq D_5$, where the product of sets consists of all products of elements in them. It follows immediately that ψD_5 is closed under ternary multiplication.

We can check the above inclusions by using commutation relations. In the congruence notation, $\psi(i) = 3 - 2i$, and it is a simple exercise analogous to (1) that $\phi\psi = \psi\phi\varkappa$, $\varkappa\psi = \psi\varkappa^2$ and $\psi^2 = \phi\varkappa^4$. Therefore, products like $\phi\varkappa^i \cdot \psi\phi\varkappa^j$ are in ψD_5 because we can move ψ to the leftmost position leaving only powers of ϕ and $\varkappa$ to the right of it. Similarly, products like $\psi\phi\varkappa^i \cdot \psi\phi\varkappa^j$ are in D_5 because we can move the second ψ likewise. At the end, only powers of ϕ and $\varkappa$ remain since $\psi^2 \in D_5$.

Put this way, the exercise easily extends to ψD_7 written as in (2) but with powers of $\varkappa$ up to 6. We can again take $\psi(i) = 3-2i$, i.e., $\psi = (1)(2\,6\,5\,7\,3\,4)$, and the commutation relations for ϕ, ψ and $\varkappa, \psi$ remain the same. However, it is no longer true that $\psi D_7 \cdot \psi D_7 \subseteq D_7$ because $\psi^2 \notin D_7$. This time, $\psi^3 \in D_7$, so $\psi^3 \notin \psi D_7$ and ψD_7 is no longer ternary. It is instead *quaternary*, as the argument analogous to the one for D_5 shows, and $\psi^2 D_7$ is also quaternary by the same reasoning. But the union, $\psi D_7 \cup \psi^2 D_7$, which happens to be the set of all panmagic permutations in S_7, is neither ternary, nor quaternary, nor N-ary for any N. However, if we add D_7 itself to this union then the result is an ordinary (binary) group.

Two lessons of D_7 generalize to D_n in prime dimensions $n \geq 7$. We should expect N-arity for some N, but not necessarily ternarity, and we should expect it for parts of the panmagic permutation set rather than for the whole of it. The group we obtained by adding the dihedral group to the set of all panmagic permutations, which we will denote $\langle \psi, D_n \rangle$, is the group generated by ψ and D_n jointly. D_n is a normal subgroup in it, i.e., all of its left and and right cosets coincide, $\sigma D_n = D_n \sigma$, due to the commutation relations. It is called the Post cover of ψD_n in N-ary group theory [9, 20]. Discerning its nature will be our next task.

5 Affine Permutations and Their Group

The group $\langle \psi, D_n \rangle$, the minimal group that contained all panmagic cosets, cannot be the entire symmetric group S_n of all permutations. Indeed, D_n is never normal in S_n for $n \geq 4$ [8][2.9]. A clue to its nature is that all permutations in it, $\phi, \varkappa, \psi$ and their products and powers, are expressed by very simple congruence formulas of the form $\sigma(i) = ai + b$. These represent affine transformations of $\mathbb{Z}_n$ analogous to affine transformations of $\mathbb{R}$ when a and b are real numbers, whose graphs are straight lines with slope a.

Definition 5.1 *A permutation in S_n is called affine when it is given by an invertible affine transformation of $\mathbb{Z}_n$. Affine permutations will be denoted $\pi_{a,b}(i) \equiv ai + b \pmod{n}$ and linear ones $\pi_a := \pi_{a,0}$, with a called their slope. The group of affine permutations, also known as the general affine group of degree 1 over $\mathbb{Z}_n$, is denoted $GA_1(\mathbb{Z}_n)$.*

Aside from modular n-queens, affine permutations come up in pseudo-random number generation [11, 16], in enumerative combinatorics [4], and in pure number theory, for example, in Zolotarev's lemma. As with the dihedral group D_n, we will not distinguish between $GA_1(\mathbb{Z}_n)$ and its isomorphic representation by permutations, i.e. we will also treat it as a subgroup of S_n. Clearly, $\pi_{a,b}$ is invertible, and hence a permutation, if and

only if a is invertible in $\mathbb{Z}_n$. Let us denote $\mathbb{Z}_n^\times$ the group of invertible residues of $\mathbb{Z}_n$, called *units*, then

$$GA_1(\mathbb{Z}_n) = \{\sigma(i) = ai + b \mid a \in \mathbb{Z}_n^\times,\, b \in \mathbb{Z}_n\}. \tag{3}$$

It is a standard fact of modular arithmetic that $a \in \mathbb{Z}_n^\times$ if and only if a is relatively prime to n [19][4.2].

Linear permutations π_a will serve as convenient replacements for ψ from our examples because their powers are easier to track, $\pi_a^k = \pi_{a^k}$. Every affine permutation is a product of π_a and a power of $\varkappa$. Indeed, $\pi_{a,b} = \varkappa^b \pi_a$, so $\psi = \pi_{-2,3} = \varkappa^3 \pi_{-2}$. The commutation relations for π_a are also easy to derive as in (1), they are $\pi_a \phi = \varkappa^{a-1} \phi \pi_a$ and $\pi_a \varkappa = \varkappa^a \pi_a$. The powers of -2 generate all units of $\mathbb{Z}_n$ for $n = 5, 7$, so we can generate all affine permutations by just multiplying powers of ψ (or of π_{-2}) and powers of $\varkappa$. Thus, the group generated by ψ and D_n in these dimensions is exactly $GA_1(\mathbb{Z}_n)$.

A simple consequence of Theorem 3.2 is the following.

Corollary 5.2 *A permutation $\pi_{a,b} \in GA_1(\mathbb{Z}_n)$ is dihedral if and only if $a = \pm 1$, and is panmagic if and only if $a, a \pm 1 \in \mathbb{Z}_n^\times$. It is magic if and only if it is panmagic.*

The last claim follows from the fact that an affine transformation is injective if and only if it is injective at a single point. Since these properties of affine permutations entirely depend on their slopes a we will also call units of $\mathbb{Z}_n$ dihedral or panmagic accordingly.

It is easy to see now that the converse claim of Polya's Theorem 3.3 is true. Indeed, π_2 and π_3 are panmagic whenever $2, 3 \nmid n$ because $2, 2 \pm 1$ and $3, 3 \pm 1$ are units for any such n. And since at least one of $a-1$, a, and $a+1$ is divisible by 2 and at least one by 3 we see directly that affine panmagic permutations do not exist when n is even or divisible by 3.

By Corollary 5.2, the dihedral group D_n is a subgroup of $GA_1(\mathbb{Z}_n)$ consisting of permutations $\pi_{\varepsilon,b}$ with $\varepsilon = \pm 1$. The next theorem shows that $GA_1(\mathbb{Z}_n)$ is the largest subgroup of S_n in which D_n is normal, confirming that it is the 'right' group to consider.

Theorem 5.3 *Let $n \geq 3$ and $\sigma \in S_n$. Then $\sigma D_n = D_n \sigma$ if and only if $\sigma \in GA_1(\mathbb{Z}_n)$.*

Proof. If $\sigma D_n = D_n \sigma$ then $\sigma \varkappa = \pi_{\varepsilon,a}\, \sigma$ with $\varepsilon = \pm 1$ and $a \in \mathbb{Z}_n$. Applying both sides to i, we get $\sigma(i+1) = \varepsilon \sigma(i) + a$. If $\varepsilon = -1$ then $\sigma(i+2) = -\sigma(i+1) + a = \sigma(i)$, so σ cannot be a permutation for $n \geq 3$. If $\varepsilon = 1$ and we let $\sigma(0) = b$ then, by induction, $\sigma(i) = ai + b$. Since σ is a permutation, $a \in \mathbb{Z}_n^\times$, so $\sigma = \pi_{a,b} \in GA_1(\mathbb{Z}_n)$.

Conversely, if $\sigma \in GA_1(\mathbb{Z}_n)$ then $\sigma = \pi_{a,b} = \varkappa^b \pi_a$, and $\sigma D_n = D_n \sigma$ follows from the commutation relations for π_a. □

The number of units in $\mathbb{Z}_n$ is given by Euler's totient function $\varphi(n) := |\mathbb{Z}_n^\times|$, where $|S|$ denotes the cardinality of S. When $n = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ is the prime factorization of n, we have [19][7.1]

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_m}\right). \tag{4}$$

We now see from (3) that $|GA_1(\mathbb{Z}_n)| = \varphi(n) n$.

The number of panmagic units of $\mathbb{Z}_n$ can be similarly counted. By Corollary 5.2, a is panmagic when $a, a \pm 1 \in \mathbb{Z}_n^\times$, so panmagic units are in 1-1 correspondence with triples of consecutive units. Back in 1869, the same year when Lionnet formulated the n-queens problem, Victor Schemmel generalized Euler's totient to k-totients $\varphi_k(n)$ that count k-tuples of consecutive units, see [15][p. 539]. It can be calculated analogously to (4):

$$\varphi_k(n) = n\left(1 - \frac{k}{p_1}\right)\cdots\left(1 - \frac{k}{p_m}\right) \tag{5}$$

when all $p_i \geq k$, and 0 otherwise. The number of panmagic units is thereby $\varphi_3(n)$, and we see that there are none in non-Polya dimensions. For primes, $\varphi(p) = p - 1$ and $\varphi_3(p) = p - 3$, as expected.

Are all panmagic permutations affine? This question received much attention in the modular n-queens literature, and the answer, in general, is no. They are for $n = 5, 7, 11$, but in all Polya dimensions $n \geq 13$ there exist non-affine panmagic permutations. First examples of them were constructed only in 1975 by Bruen and Dixon, and their nature and properties are still poorly understood [3][p. 16]. We will, therefore, confine our attention to affine panmagic, which already has plenty of intricacies to offer.

6 Affine Panmagic in Prime Dimensions

Our identification of the Post cover group with $GA_1(\mathbb{Z}_n)$ for $n = 5, 7$ depended on -2 generating all units as its powers. Such units are called *primitive roots* in number theory and they do not exist for all n. Luckily, they do exist for $n = p \geq 3$ prime, by a classical theorem of Gauss [19][9.2]. If r is a primitive root then we can generate all π_a with π_r since $\pi_{r^k} = \pi_r^k$. And since any affine permutation is a product of π_a and a power of $\varkappa$ we have $GA_1(\mathbb{Z}_p) = \langle \pi_r, \varkappa \rangle$ for any odd prime p. In this long section, we use primitive roots to generalize the algebraic properties of panmagic permutations observed for $p = 5, 7$ and determine their cycle structure.

6.1 Closure Under N-ary Multiplication

When $n = p$ is prime, a linear permutation π_a from Definition 5.1 is panmagic for any $a \neq 0, \pm 1$ by Corollary 5.2. This means that among units only $a = \pm 1$ are not panmagic, and those are dihedral.

Corollary 6.1 (Panmagic/dihedral dichotomy) *When p is prime, every affine permutation is either panmagic or dihedral, and has the form $\pi_r^i \varkappa^j$, where r is a primitive root modulo p.*

Recall that when H is a normal subgroup of a group G the set of cosets of H with induced multiplication on them is called the quotient group and denoted G/H [8]. We are now ready to prove the first of our main theorems about affine panmagic cosets that generalizes the $p = 5, 7$ examples.

Theorem 6.2 *Let $p \geq 5$ be prime, r be its primitive root, $N := \frac{p+1}{2}$ and $C := \pi_r D_p$. Then for $i = 1, \ldots, N-2$ the cosets $C^i = \pi_r^i D_p$ consist of panmagic permutations and are closed under N-ary multiplication. Moreover,*

$$\langle \pi_r, D_p \rangle = \cup_{i=1}^{N-1} C^i = GA_1(\mathbb{Z}_p),$$

D_p is its normal subgroup, and the quotient group is $GA_1(\mathbb{Z}_p)/D_p \simeq \mathbb{Z}_{N-1} = \mathbb{Z}_{\frac{p-1}{2}}$.

Proof. The commutation relations, $\pi_r \phi = \varkappa^{r-1} \phi \pi_r$ and $\pi_r \varkappa = \varkappa^r \pi_r$, imply that left and right π_r-cosets of $D_p = \langle \phi, \varkappa \rangle$ are equal, so $C = \pi_r D_p = D_p \pi_r$. Since D_p is a group we have $D_p \cdot D_p = D_p$ and, by induction,

$$C^i = \pi_r D_p \pi_r D_p \cdots \pi_r D_p = \pi_r^2 D_p \cdots \pi_r D_p = \cdots = \pi_r^i D_p = D_p \pi_r^i \,.$$

Since r is a primitive root every coset of D_p in $GA_1(\mathbb{Z}_p)$ is of the form $D_p \varkappa^b \pi_{r^i} = D_p \pi_{r^i} = C^i$, so $\langle \pi_r, D_p \rangle = GA_1(\mathbb{Z}_p)$ and D_p is normal in it.

The order of r is $p-1$, the size of $\mathbb{Z}_p^\times$, so $r^{p-1} = 1$ and $p-1$ is the smallest such power. Therefore, $r^{\frac{p-1}{2}} = -1$, as -1 is the only other unit that squares to 1, and $\frac{p-1}{2}$ is the smallest power such that $r^i = \pm 1$. But $\pi_r^i = \pi_{r^i} \in D_p$ if and only if $r^i = \pm 1$, so the smallest i such that $\pi_r^i \in D_p$ is $\frac{p-1}{2} = N-1$. Therefore, $C^{N-1} = D_p$ and all cosets are exhausted by C^i with $1 \leq i \leq N-1$. Moreover, $C^i \cdot C^j = \pi_r^i \pi_r^j D_p = \pi_r^{i+j} D_p = C^{i+j}$, so $C^i \mapsto i$ is an isomorphism between the quotient group and $\mathbb{Z}_{N-1}$.

By Corollary 6.1, every permutation in $GA_1(\mathbb{Z}_p)$ is either panmagic or dihedral, and all dihedral ones are in D_p. Since cosets partition the group we conclude that C^i for $1 \leq i \leq N-2$ contain only panmagic affine permutations, and (jointly) all of them. Finally, $C^N = C C^{N-1} = C D_p = C$, so N-ary products of elements of C are again in C and it is closed under N-ary multiplication. □

Theorem 6.2 is a global one and gives us a broad algebraic picture of how affine panmagic permutations in prime dimensions behave. But, in general, the arity N it gives is not the smallest possible for every coset. Indeed, if $C^4 = D_p$ then $(C^2)^2 = D_p$, so C^2 will not just be quinternary like C, but also ternary. Conversely, if C is N'-ary then we can take a product of its N' elements, multiply it by $N'-1$ more elements, then by $N'-1$ more, and so on. All of those products will again be in C. This means that closure under N'-ary multiplication implies closure under N-ary multiplication for any $N = N' + k(N'-1)$. In particular, closure under ternary products implies closure under any odd-numbered products.

In the light of the above ambiguity, we would like to distinguish the smallest possible arity for each coset.

Definition 6.3 *A subset C of a group will be called strictly N-ary, and N its strict arity, when it is closed under N-ary multiplication, but not under N'-ary multiplication with any $N' < N$.*

To find strict arities, we will supplement Theorem 6.2 by a local theorem that treats each coset individually. Recall that the *multiplicative order* $\mathrm{ord}_p(x)$ of $x \in \mathbb{Z}_p^\times$ is the smallest positive integer i such that $x^i \equiv 1 \pmod{p}$.

Theorem 6.4 *Let $p \geq 5$ be prime, $a \in \mathbb{Z}_p^\times$ be panmagic, and $N := \mathrm{ord}_p(a^2) + 1$. Then the coset $C := \pi_a D_p$ consists of panmagic permutations and is strictly N-ary. Moreover, $\langle \pi_a, D_p \rangle = \cup_{i=1}^{N-1} C^i$, D_p is a normal subgroup in it, and the quotient group is $\langle \pi_a, D_p \rangle / D_p \simeq \mathbb{Z}_{N-1}$.*

Proof. The proof is analogous to the proof of Theorem 6.2 with a replacing r, so we only point out the differences. The group $\langle \pi_a, D_p \rangle$ is no longer necessarily the whole group $GA_1(\mathbb{Z}_p)$, but might be its proper subgroup. The smallest i such that $a^i = \pm 1$ is also the smallest i such that $(a^i)^2 = (a^2)^i = 1$, i.e. $\mathrm{ord}_p(a^2)$, which gives the formula for N. That N is the strict arity follows from the fact $a^i \neq \pm 1$ for $i < \mathrm{ord}_p(a^2)$. Indeed, $\pi_{a^i} = \pi_a^i \notin D_p$ for such i, hence $\pi_a^{i+1} \notin C$, so C is not closed under N'-ary multiplication with $N' = i + 1 < \mathrm{ord}_p(a^2) + 1 = N$. □

Theorem 6.4 allows us to find all primes p that admit strictly N-ary panmagic cosets of D_p. Those must satisfy $C^{N-1} = D_p$ and not coincide with D_p itself. Therefore, we need $\frac{p-1}{2}$ from Theorem 6.2 to be divisible by $N - 1$, meaning that $p - 1$ must be divisible by $2(N - 1)$.

Corollary 6.5 *Let $p \geq 5$ be prime and $N \geq 3$. Then strictly N-ary affine panmagic cosets of D_p exist if and only if $p = 2(N-1)k + 1$ for some integer k. When p is of this form and r is its primitive root then $\pi_{r^k} D_p$ is such a coset. In particular, strictly ternary panmagic cosets of D_p exist if and only if $p = 4k + 1$ for some integer k.*

Proof. By Theorem 6.4, strictly N-ary cosets of D_p exist if an only if there are units $a \in \mathbb{Z}_p^\times$ with $\mathrm{ord}_p(a^2) = N - 1$. Since all $a \in \mathbb{Z}_p^\times$ are powers of r, all a^2 are powers of r^2. But $\mathrm{ord}_p(r^2) = \frac{p-1}{2}$, so the orders of its powers, $(r^2)^k$, are exactly the divisors of $\frac{p-1}{2}$, which means that $\frac{p-1}{2} = (N-1)k$ for some integer k. Conversely, when this identity holds, the order of $(r^k)^2$ will be $N - 1$. Thus, $\pi_{r^k} D_p$ will be strictly N-ary by Theorem 6.4. □

Primes of the form $4k+1$, like 5, 13, 17, 29, 37, 41..., are famous in number theory. They were singled out already by Albert Girard and Pierre de Fermat, who stated that they are exactly the primes representable as the sums of two perfect squares. The first proof was given by Euler. They also happen to be the only primes for which -1 is a quadratic residue, the square of another unit [19][11.1]. Unsurprisingly, $4k + 1$ primes appear in connection with the modular queens problem as well [3][p. 15], and they will reappear in Corollary 6.9.

6.2 Panmagic Cycle Types

We will now turn from algebra to the structure of individual affine panmagic permutations. Recall that intrinsic character of a permutation is described by its *cycle type*, the number and lengths of cycles in its disjoint cycle decomposition [8][2.5]. One can easily check that all panmagic permutations in dimension 5 have one fixed point and one 4-cycle, and they also all belong to a single coset of D_5. However, in the $\pi_2 D_7$ coset, we encounter two cycle types represented by $\pi_2 = (1\,2\,4)(3\,6\,5)(7)$ and $\pi_5 = (1\,5\,4\,6\,2\,3)(7)$. Further computations

confirm that there are always at most two cycle types in each panmagic coset of D_p, and all cycles in each, other than the fixed point, have the same length. Moreover, when there are two cycle types the cycle length in one of them is twice that in the other.

A first step towards proving these observations is to recall that conjugate permutations have the same cycle types (essentially, because they permute numbers in identical ways up to relabeling). Then we observe that every affine permutation $\pi_{a,b}$ with $a \neq 1$ is conjugate to π_a. Indeed, $\sigma = \varkappa^{-t}\pi_a\varkappa^t$ with $t \equiv -(a-1)^{-1}b \pmod{p}$. Thus, we only need to consider cycle types of π_a, which is much less daunting since their powers are easily tracked. This already confirms one of the above observations. As the slopes of permutations in $\pi_a D_p$ are only $\pm a$, there can be at most two cycle types in it, that of π_a and that of π_{-a}.

Corollary 6.6 *Let $a \in \mathbb{Z}_p^\times$ be panmagic. Then the disjoint cycle decomposition of π_a consists of one fixed point and $\frac{p-1}{\operatorname{ord}_p(a)}$ cycles of equal length $\operatorname{ord}_p(a)$. Moreover, every permutation in $\pi_a D_p$ has the cycle type of π_a or of π_{-a}.*

Proof. Recall that we identify residue 0 with p for affine permutations. Clearly, $\pi_a(0) = 0$, and this gives us the fixed point p. The rest of residues are units u and $\pi_a(u) = au$, so the cycle that starts with u is of the form

$$(u\ au\ \cdots\ a^{m-1}u),$$

where m is the smallest positive integer with $a^m u = u$. Since u is a unit this is equivalent to $a^m = 1$, so $m = \operatorname{ord}_p(a)$ for all u and is their common cycle length. Since there are $p-1$ units in $\mathbb{Z}_p^\times$ there are $\frac{p-1}{m}$ such cycles. □

Thus, there are at most two cycle types in each panmagic coset. When is there just one? We already know that this happens exactly when π_a and π_{-a} have the same type. By Corollary 6.6, a necessary and sufficient condition is that $\operatorname{ord}_p(-a) = \operatorname{ord}_p(a)$. To make it more explicit, we will relate the multiplicative orders of a and a^2 (for any n).

Lemma 6.7 *If $\operatorname{ord}_n(a^2)$ is even then $\operatorname{ord}_n(a) = \operatorname{ord}_n(-a) = 2\operatorname{ord}_n(a^2)$. If $\operatorname{ord}_n(a^2)$ is odd then one of $\operatorname{ord}_n(-a)$ and $\operatorname{ord}_n(a)$ is equal to $\operatorname{ord}_n(a^2)$ and the other to $2\operatorname{ord}_n(a^2)$.*

Proof. By a standard result of group theory [8][2.4],

$$\operatorname{ord}_n(a^2) = \begin{cases} \operatorname{ord}_n(a),\ \operatorname{ord}_n(a) \text{ odd} \\ \frac{1}{2}\operatorname{ord}_n(a),\ \operatorname{ord}_n(a) \text{ even.} \end{cases} \tag{6}$$

Hence, if $\operatorname{ord}_n(a^2)$ is even then so is $\operatorname{ord}_n(a)$. Indeed, if it were odd then by (6) $\operatorname{ord}_n(a) = \operatorname{ord}_n(a^2)$ would also be odd, a contradiction. But then, by (6) again, $\operatorname{ord}_n(a) = 2\operatorname{ord}_n(a^2)$, and the same argument applies to $-a$.

Now suppose that $\operatorname{ord}_n(a^2)$ is odd. Since $\operatorname{ord}_n(a^2) = \operatorname{ord}_n\left((-a)^2\right)$, formula (6) implies that $\operatorname{ord}_n(\pm a)$ is either $\operatorname{ord}_n(a^2)$ or $2\operatorname{ord}_n(a^2)$. For definiteness, suppose $\operatorname{ord}_n(a) = \operatorname{ord}_n(a^2)$. Since it is odd $(-a)^{\operatorname{ord}_n(a^2)} = -a^{\operatorname{ord}_n(a)} = -1$, so $\operatorname{ord}_n(-a) \neq \operatorname{ord}_n(a^2)$ and it must be $2\operatorname{ord}_n(a^2)$. □

Our next result now follows easily.

Theorem 6.8 *Let $p \geq 5$ be prime, $a \in \mathbb{Z}_p^\times$ be panmagic, and $N := \mathrm{ord}_p(a^2) + 1$. If N is odd then all permutations in $\pi_a D_p$ have the same cycle type with the cycle lengths, aside from the fixed point, all equal to $2(N-1)$. If N is even then permutations in $\pi_a D_p$ have two cycle types with the cycle lengths, aside from the fixed point, all equal to $N-1$ in one of them and $2(N-1)$ in the other.*

Proof. If N is odd then $\mathrm{ord}_p(a^2) = N-1$ is even and Lemma 6.7 implies that $\mathrm{ord}_p(-a) = \mathrm{ord}_p(a) = 2\,\mathrm{ord}_p(a^2) = 2(N-1)$. If N is even then $\mathrm{ord}_p(a^2) = N-1$ is odd. By Lemma 6.7, one of $\mathrm{ord}_p(-a)$ and $\mathrm{ord}_p(a)$ is then equal to $\mathrm{ord}_p(a^2) = N-1$ and the other is twice that. □

As a simple observation, transpositions, i.e. 2-cycles, can only appear in cosets when $N = 2$, i.e. when the coset is D_p itself. In other words, affine panmagic permutations have no transpositions in prime dimensions.

Theorem 6.8 means that cosets of $\pi_a D_p$ have permutations with the same cycle type if and only if their strict arity N is odd. But then $\mathrm{ord}_p(a) = 2\,\mathrm{ord}_p(a^2) = 2(N-1)$ is divisible by 4. Since the order of any element must divide the order of $\mathbb{Z}_p^\times$ by Lagrange's theorem [8], we conclude that $4 \mid p-1$ and p is of the form $4k+1$. But this is the exact same condition as in Corollary 6.5 ! It holds if and only if strictly ternary panmagic cosets of D_p exist. In turn, Theorem 6.8 implies that all permutations in such cosets have the same cycle type. They have only 4-cycles and a single fixed point. Summarizing, we proved the following neat equivalence that highlights the special panmagic of $4k+1$ primes.

Corollary 6.9 *The following conditions on a prime p are equivalent:*

(i) *D_p has panmagic cosets with all permutations of the same cycle type;*
(ii) *D_p has panmagic cosets of strictly odd arity;*
(iii) *D_p has strictly ternary panmagic cosets;*
(iv) *$p = 4k+1$ for a positive integer k.*

7 N-ary Subgroups

Before concluding, we wish to put things into a broader algebraic perspective and tie up some loose ends. Theorems 6.2 and 6.4 provide a template for how sets closed under N-ary multiplication arise as cosets, but it is not yet clear how much of it is specific to those examples and how much is essential. Moreover, closure under multiplication does not quite entitle us to call them N-ary *groups*. If the binary case is our guide, we also need an analog of closure under taking inverses. We will briefly develop a bit of N-ary group theory to fill in those gaps.

N-ary groups can be defined abstractly, like ordinary groups, but to keep our exposition elementary we will only define N-ary *sub*groups of ordinary groups. Those are the only ones we need, and one can prove that any abstract N-ary group is isomorphic to an N-ary subgroup [9][Theorem 1.5], [20][p. 4].

Definition 7.1 *A subset $C \subseteq G$ of a group G is called an N-ary subgroup of G when for any N elements $a_1, \ldots, a_N \in C$, the product $a_1 \cdots a_N \in C$; and for any $a \in C$, the element $a^{3-2N} \in C$.*

The first condition replaces closure under the binary multiplication by an N-ary one and the second replaces closure under inversion. When $N = 2$ we recover the definition of the ordinary (binary) subgroup.

In the ternary case, $a^{3-2N} = a^{-3}$, but we still get closure under taking inverses because $a^{-1} = aaa^{-3} \in C$ as a triple product. In fact, for $N \geq 3$ we can generally replace the condition $a^{3-2N} \in C$ with a simpler equivalent one, $a^{2-N} \in C$. Indeed, $a^{2-N} = a^{N-1}a^{3-2N}$ and $a^{3-2N} = a^{N-3}\left(a^{2-N}\right)^3$, and both are N-ary products for $N \geq 3$. The element a^{2-N} is called *skew to a* and is typically used as the replacement for the inverse in N-ary group theory [9][p. 13], [20][p. 3].

We did not say anything about the identity element e, and that is by design. In the binary case, e will be in C because we can multiply any element by its inverse. But also conversely, if $e \in C$ then C is a binary subgroup because we can reproduce binary products by taking N-ary ones with $N - 2$ copies of e in them. Indeed, under Definition 7.1 any binary subgroup is also N-ary for any $N \geq 3$.

Nonetheless, there are non-binary N-ary subgroups for $N > 2$. In fact, many of them are quite familiar, albeit rarely thought about this way. For example, odd integers form a ternary (additive) subgroup of $\mathbb{Z}$. Indeed, while the sum of two odd integers is not odd, the sum of any three is. The inverse (negative) of an odd integer is also odd. Similarly, odd permutations form a non-binary ternary subgroup of S_n. Non-zero purely imaginary numbers $i\mathbb{R}^\times$ form a (multiplicative) ternary subgroup of non-zero complex numbers $\mathbb{C}^\times$. Indeed, $ia \cdot ib \cdot ic = i(-abc)$ and $(ia)^{-1} = i(-a)$.

One can check that $\psi D_5 = \pi_3 D_5$, the panmagic ternary coset from Section 4, does contain the inverses of all of its elements and is a ternary subgroup. The quaternary coset $\psi D_7 = \pi_5 D_7$ does not; in fact, its inverses belong to the other ternary panmagic coset $\pi_3 D_7$. But it does contain the skews a^{-2} of its elements and is a quaternary subgroup. Fortunately, we do not need to go back and check that our cosets closed under N-ary multiplication were also closed under skewing. This is because all of them were finite, and, as with ordinary finite subgroups, closure under multiplication is enough to be an N-ary subgroup.

Theorem 7.2 *Suppose $C \subseteq G$ is closed under N-ary multiplication and finite. Then it is an N-ary subgroup of G.*

Proof. Let C^{N-1} denote the set of $(N-1)$-element products of elements of C. We claim that it is a binary subgroup. Indeed, a product of two $(N-1)$-products of elements of C has the total of $2(N-1) = N + (N-2)$ factors. The first N multiply to an element of C by assumption, so it is again a product of $N - 1$ factors from C. If C is finite then so is C^{N-1}. Since it is closed under binary multiplication it must be a subgroup by a standard result of group theory [8][2.3].

Let $a \in C$, then $a^{N-1} \in C^{N-1}$. Since a binary subgroup contains inverses of its

elements, $a^{1-N} = (a^{N-1})^{-1} \in C^{N-1}$, i.e. is a product of $N-1$ elements of C. But then $a^{2-N} = aa^{1-N}$ is a product of N elements of C and must be in C by assumption. Thus, C is an N-ary subgroup. □

It turns out that the trick for obtaining N-ary subgroups from cosets, which we exploited in Theorems 6.2 and 6.4, is quite general. It constitutes the 'easy' direction of the Post coset theorem.

Theorem 7.3 (Post) *Let $H \subset \widetilde{H} \subseteq G$ be a pair of (binary) subgroups of G with H normal in $\widetilde{H}$ and $\widetilde{H}/H \simeq \mathbb{Z}_{N-1}$. Then every coset of H in $\widetilde{H}$ is an N-ary subgroup of G.*

Proof. Let $C = bH$ for $b \in \widetilde{H}$. Since H is normal, for any $h \in H$, we have $hb = bh'$ for some $h' \in H$, and since $\widetilde{H}/H$ is cyclic of order $N-1$, we have $b^{N-1} \in H$ for any $b \in \widetilde{H}$. Therefore, for $a_i = bh_i$ with $h_i \in H$, by induction,

$$a_1 \cdots a_N = bh_1 bh_2 \cdots bh_N = b(bh_1' h_2 b \cdots bh_N) = \cdots = b(b^{N-1}\hat{h}) \in bH = C.$$

Similarly, since $(b^{-1})^{N-1} \in H$, moving b^{-1}-s to the left we obtain for $a = bh$,

$$a^{2-N} = (h^{-1}b^{-1})^{N-2} = (b^{-1})^{N-2}\hat{h} = b\big((b^{-1})^{N-1}\hat{h}\big) \in bH = C.$$

Thus, C is an N-ary subgroup. □

In Theorem 6.2, $G = S_p$ was the symmetric group, $H = D_n$ was the dihedral group, and $\widetilde{H} = GA_1(\mathbb{Z}_p)$ was the general affine group. One can check that for the purely imaginary numbers we have $G = \mathbb{C}^\times$, $H = \mathbb{R}^\times$, and $\widetilde{H} = \langle i, \mathbb{R}^\times\rangle = \mathbb{R}^\times \cup i\mathbb{R}^\times$.

The hard direction of the Post coset theorem is that any N-ary group arises as a Post coset up to isomorphism, i.e. it is isomorphic to a coset of an index $N-1$ normal subgroup of a larger group with the cyclic quotient. It was proved by Post in his 1940 seminal paper on N-ary groups. In general, given an N-ary subgroup $C \subseteq G$, the group $H = C^{N-1}$ is called its *Post associate* and the group $\widetilde{H} = \langle C\rangle$ its *Post cover*. In our panmagic examples, the Post associate was always D_p, while the Post cover could be the entire group $GA_1(\mathbb{Z}_p)$ or its subgroup of the form $\langle \pi_a, D_p\rangle$ with a panmagic unit a.

Note that N does not, in general, have to be the strict arity of C, and that the Post cover may depend on which N it is considered under. It follows from the Post coset theorem that the strict arity is $\mathrm{ord}(C)+1$, where $\mathrm{ord}(C)$ is the order of C as an element of the quotient group $\widetilde{H}/H$. We will not elaborate further and refer the interested reader to [9, 20] and references therein.

In conclusion, let us neatly repackage Theorems 6.2 and 6.4 in terms of N-ary group theory.

Theorem 7.4 *Let $p \geq 5$ be prime. If $a \in \mathbb{Z}_p^\times$ is panmagic then $\pi_a D_p$ is a strictly N-ary panmagic subgroup of S_p with $N = \mathrm{ord}_p(a^2)+1$, the Post associate D_p and the Post cover $\langle \pi_a, D_p\rangle$. Moreover, all $\pi_a D_p$ with $a \neq 0, \pm 1$ are N-ary panmagic subgroups of S_p with common $N = \frac{p+1}{2}$, common Post associate D_p, and common Post cover $GA_1(\mathbb{Z}_p)$.*

The appearance of $GA_1(\mathbb{Z}_p)$ as the common Post cover is a consequence of the existence of primitive roots in prime dimensions. Indeed, when r is a primitive root, permutations of a single coset $\pi_r D_p$ generate the entire group of affine panmagic permutations. In turn, D_p is the common Post associate because it is the largest subgroup that preserves panmagic in those dimensions. These observations point to what should change and what should stay the same in non-prime dimensions.

8 Conclusions and Open Problems

We have developed an algebraic theory of affine panmagic permutations that focuses on their algebraic and number-theoretic properties. Their matrices are the simplest kind of panmagic squares and they also represent configurations of non-attacking queens on a toroidal chessboard. But it is treating them as permutations that unlocked many new results. We hope that our algebraic approach and its generalizations will be useful for solving other problems. Let us briefly outline some adjacent topics and open problems that lie ahead for those willing to pursue the subject further.

We generalized most of our results on N-ary groups and cycle types of panmagic permutations to composite dimensions [13]. However, proving them requires less elementary methods because the only composites satisfying the Polya condition that have primitive roots are odd prime powers. Even for them, the panmagic/dihedral dichotomy fails – there exist units that are neither panmagic nor dihedral. It turns out to be helpful to use the Post coset theorem systematically from the start. In composite dimensions, D_n is no longer the largest subgroup of S_n whose elements preserve panmagic, and we studied its extensions as Post associates instead, while $GA_1(\mathbb{Z}_n)$ is no longer the universal Post cover, and this role is passed to its proper subgroups. The cycle types of panmagic permutations are also more complex in general, and no longer have all cycles of the same length aside from the fixed point as in Theorem 6.8.

Affine panmagic permutations seem to be closely related to the uniform step method for constructing "natural" panmagic squares, those filled with natural numbers from 1 to n^2. Planck used them to construct modular queens solutions already in 1900 [3][p. 8]. The method only works in Polya dimensions, and there are intriguing parallels between Lehmer's results on it [15] and ours. More recently, constructions linking natural panmagic squares to non-affine panmagic permutations were also discovered [2][p. 225ff].

Counting all panmagic permutations in dimension n is known to be a hard problem, and even good estimates are hard to come by. It is known that there are more than $2^{\sqrt{\frac{p-1}{2}}}$ of them for prime $n = p$, and, conjecturally, the count is asymptotically $\sim n^{\alpha n}$ for some $\alpha > 0$ [3][p. 18]. Since there are only $\varphi_3(n)\, n$ affine panmagic permutations and $\varphi_3(n) \leq n$, the vast majority of panmagic permutations are non-affine for large n. While some special constructions of such permutations are known [3][p. 16], they are far from producing the entire set or revealing its algebraic structure.

Non-affine panmagic permutations present new, more complex questions. For example, are there N-ary groups consisting of them? Non-affine panmagic cosets of D_n are ruled out by Theorem 5.3, but there may be other groups that work. One would have to find

pairs of subgroups of S_n, one normal in the other, with non-affine panmagic cosets. Some candidate groups that act on general panmagic permutations are considered in [6].

The linear span of permutation matrices of any N-ary panmagic subgroup is an N-ary algebra of panmagic squares. Many such examples are provided by our Corollary 6.5. So far, only ternary panmagic algebras have been considered in the literature and they have an appealing alternative description in terms of linear algebra. Consider an invertible matrix Q that commutes with both P_ϕ and $P_\varkappa$, and let E be the square matrix with all entries 1. Matrices A such that $AQ + QA$ is a scalar multiple of E are called Q-regular, and they are panmagic squares that form a ternary algebra [18][Theorem 18]. Thompson's algebra, the linear span of $\pi_2 D_5$, is Q-regular with $Q = \frac{1}{2}I + P_\varkappa + P_\varkappa^{-1}$. Can such Q be found for other ternary groups from our Corollary 6.5? And conversely, which Q-regular algebras are spanned by ternary groups and how can those groups be recovered from Q? More generally, what is a linear algebra description of N-ary panmagic algebras, and when are they linear spans of N-ary panmagic groups?

Although affine panmagic permutations are a small fraction of all of them, this tells us little about their share of the space of panmagic squares. Indeed, there are $n!$ permutations in S_n, but the dimension of the linear span of all permutation matrices (which is the space of semimagic squares) is only $(n-1)^2 + 1$. This means that there are massively many linear relations among permutations matrices, and it is *a priori* possible that panmagic permutation matrices (or already affine ones) span the entire space of panmagic squares for Polya n. Do they?

When we consider only squares with positive entries and positive linear combinations, the answer is no for $n > 5$, as proved in [1]. For odd n, the space of panmagic squares is known to be $(n-2)^2$-dimensional [10], so we could answer the question if we counted linearly independent panmagic permutation matrices. Questions about linear relations among matrices of group elements belong to the group representation theory. For the affine case, this suggests looking into representation theory of $GA_1(\mathbb{Z}_n)$ and its subgroups. But this is a task for another day.

Acknowledgments

The authors are grateful to the anonymous referees for the helpful comments and suggestions.

References

[1] D. Alvis, M. Kinyon, Birkhoff's theorem for panstochastic matrices, *Amer. Math. Monthly*, **108** (2001), 28–37.

[2] J. Bell, B. Stevens, Constructing orthogonal pandiagonal Latin squares and panmagic squares from modular n-queens solutions, *J. Combin. Des.*, **15** (2007), 221–234.

[3] J. Bell, B. Stevens, A survey of known results and research areas for n-queens, *Discrete Math.*, **309** (2009), 1–31.

[4] V. Bozovic, Z. Kovijanić-Vukićević, The cycle index of the automorphism group of $\mathbb{Z}_n$, *Publ. Inst. Math. (Beograd)*, **101(115)** (2017), 99–108.

[5] G. Carpenter, On the n-queens problem, *Brit. Chess Mag.*, **20** (1900), 42–48.

[6] M. Engelhardt, A group-based search for solutions of the n-queens problem, *Discrete Math.*, **307** (2007), 2535–2551.

[7] A. van den Essen, Magic squares and linear algebra, *Amer. Math. Monthly*, **97** (1990), 60–62.

[8] J. Gallian, *Contemporary abstract algebra*, Cengage Learning, Boston, 2017.

[9] A. Gal'mak, V. Balan, G. Vorobiev, On Post-Gluskin-Hosszu theorem, *Appl. Sci.*, **16** (2014), 11–22.

[10] X. Hou, A. Lecuona, G. Mullen, J. Sellers, On the dimension of the space of magic squares over a field, *Linear Algebra Appl.*, **438** (2013), 3463–3475.

[11] T. Hull and A. Dobell, Random number generators, *SIAM Rev.*, **4** (1962), 230–254.

[12] K. Ireland, M. Rosen, *A classical introduction to modern number theory*, Springer-Verlag, New York-Berlin, 1982.

[13] S. Koshkin, J. Lee, N-ary groups of panmagic permutations from the Post coset theorem, *Discrete Math.*, **348** (2025), paper no. 114467.

[14] D. Lawden, Pan-Magic Squares of Even Order, *Math. Gaz.*, **34** (1950), 220–222.

[15] D. Lehmer, On the Congruences Connected with Certain Magic Squares, *Trans. Amer. Math. Soc.*, **31** (1929), 529–551.

[16] G. Marsaglia, The structure of linear congruential sequences, in *Applications of Number Theory to Numerical Analysis, S. Zaremba, editor*, 1972, 249–285.

[17] B. Mattingly, Even order regular magic squares are singular, *Amer. Math. Monthly*, **107** (2000), 777–782.

[18] R. Nordgren, On properties of special magic square matrices, *Linear Algebra Appl.*, **437** (2012), 2009–2025.

[19] K. Rosen, *Elementary number theory*, Addison-Wesley, Boston, 2005.

[20] M. Shahryari, Representations of finite polyadic groups, *Comm. Algebra*, **40** (2012), 1625–1631.

[21] A. Thompson, Odd magic powers, *Amer. Math. Monthly*, **101** (1994), 339–342.

[22] L. Weiner, The Algebra of Semi-Magic Squares, *Amer. Math. Monthly*, **62** (1955), 237–239.

Sergiy Koshkin
University of Houston-Downtown
1 Main Street
Houston, TX 77002
E-mail: koshkins@uhd.edu

Jaeho Lee
Spring Branch Academic Institute
14400 Fern Drive
Houston, TX 77079
E-mail: leejaeho0802@gmail.com

Received: January 10, 2025 **Accepted**: May 8, 2025
Communicated by Vadim Ponomarenko