Transactions of the Nigerian Association of Mathematical Physics
Vol. 6 (Jan., 2018), pp. 368– 376

In honour of Prof. Ekhaguere at 70

On the magic squares census problem

L. U. Uko
School of Science and Technology, Georgia Gwinnett College

Abstract. A magic square is a square array of order greater than two whose entries are taken from a set of consecutive whole numbers – beginning from 1 – with the property that the numbers in any row, column or diagonal of the array add up to the same sum. For centuries, they have been a source of exciting mathematical amusements and challenging unsolved problems. One of the latter is the census problem of determining the number of magic squares of order six and above. In this paper we discuss some progress that have been made in the census problem, namely the magic squares census formulas obtained recently by Kathleen Ollerenshaw and David Brée for most perfect magic square of doubly even order, and the census formula derived by Uko for uniform step magic squares of odd order. We also present a result obtained by parametrizing magic squares and show how it can be used in the study of the general magic squares census problem.

Keywords: magic square, census problem.

1. Introduction

A magic square is a square array of order greater than two whose entries are taken from a set of consecutive whole numbers – beginning from 1 – with the property that the numbers in any row, column or diagonal of the array add up to the same sum.

Magic squares were discovered in China from where they were subsequently introduced into India, Japan and – much later – Europe. The first known example of a magic square is the *lo shu*

4	9	2
3	5	7
8	1	6

which, according to an ancient Chinese legend, was discovered by Emperor Yu on the back of a divine tortoise while he was walking on the shores of the yellow river *circa* 2800 BC. For centuries, magic squares have been a source of exciting mathematical amusements and challenging unsolved problems. It is a classic topic in recreational mathematics which has aroused the interest of large numbers of people of all generations over time, most of who are not (or were not) professional mathematicians. An internet search of the term 'magic square' indicates that the number of contemporary enthusiasts currently actively involved in the subject is probably at a historical high.

It is well known that there are only 8 magic squares of order three, and that there are 7040 magic squares of order four (Bernard Freńicle de Bessy [7], 1693). In 1973 Richard Schroeppel used a computer program to obtain a census figure of 2,202,441,792 magic squares of order five. The census of magic squares of order six and above are still open problems. However, census formulae have been obtained for two major classes of magic squares, namely the most-perfect magic squares of doubly even order (Ollerenshaw and Brée [10]) and uniform step magic squares of odd order. Our main objective in this paper is to review these key results and to fill in some missing steps in the original proof of the main result. We also discuss a parametrization that we have developed for generic magic squares and it's application to the general magic squares problem.

A magic square is often considered as identical to the other seven magic squares which can be obtained from it by performing rotations and/or reflections. For simplicity, we will not make this identification in this paper, so we will regard two magic squares as identical only if they are identical in the matrix sense. In the sequel, given any integers a and b, $[a]$ will designate the largest integer less than or equal to a, a Mod b will designate the remainder when b divides a, a Div b will denote the integer $[a/b]$, (a, b) will dentoe the greatest common divisor of a and b, and we will set $Z_p\{0, 1, \ldots, p-1\}$.

2. Census of most-perfect magic squares of doubly even order

Let $p = 4k$ for some $k \in \mathbb{N}$. A magic square of order p is said to be most-perfect if any two of its entries at a distance of $p/2$ on any diagonal sum to $p^2 + 1$ and the sum of the entries in any 2×2 block of adjacent cells is $2(p^2 + 1)$. An example is the following magic square

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

which appears in a famous 1514 engraving titled 'The melancholia', due to Albrecht Dürer.

Kathleen Ollerenshaw was already in her 80s when she got the main insight of a construction that was capable of generating all magic squares of this class. Working with David Brée, she exploited this fact to obtain the following seminal formula for the number of magic squares in this class (amplified by a factor of 8 for consistency with our method of counting magic squares).

Theorem 1 (10) *Let p, a positive integer, have prime factorization $p = \prod_{i=1}^{l} q_i^{v_i}$ in which $q_1 = 2$ and $v_1 \geq 2$, so that p is doubly even. Then the number of most-perfect magic squares of order p is given by*

$$n(p) = m(p) \sum_{v=0}^{\tau(p)} w(v)(w(v) + w(v+1)),$$

where $m(p) = 2^{p+2}(p/2)!^{\,2}$, $w(v) = \sum_{i=0}^{v}(-1)^{v+i}\binom{v+1}{i+1}\prod_{j=1}^{l}\binom{v_j+1}{i}$, and $\tau(p)$ is the number of divisors of p.

3. Census of Uniform Step Magic Squares

A magic square is said to be of uniform step if it can be written in the form

$$m_{ij} = u + p(v-1), \quad u, v = 1, 2, \ldots, p$$

where

$$\begin{aligned} i &= 1 + [(\varepsilon + (u-1)\alpha + (v-1)\beta) \bmod p], \\ j &= 1 + [(\rho + (u-1)\gamma + (v-1)\delta) \bmod p], \end{aligned}$$

and ε, α, β,ρ, γ, $\delta \in Z_p$. In a previous paper [15], we showed that every uniform step magic square can be written in the form

$$\begin{aligned} m_{ij} = 1 &+ [(a_1 i + b_1 j + c_1) \bmod p] \\ &+ p[(a_2 i + b_2 j + c_2) \bmod p], \end{aligned} \tag{1}$$

for some a_1, a_2, b_1, b_2, c_1, $c_2 \in Z_p$, and vice versa. We also proved in the paper that the array (1) is a magic square if and only if

$$(a_1b_2 - b_1a_2, p) = 1, \tag{2}$$

$$(p, a_k) = (p, b_k) = 1, \qquad k = 1, 2, \tag{3}$$

$$c_k \bmod u_k = (u_k - 1)/2, \qquad k = 1, 2, \tag{4}$$

$$(b_k + c_k) \bmod v_k = (v_k - 1)/2, \qquad k = 1, 2, \tag{5}$$

where $u_k = (p, a_k + b_k)$ and $v_k = (p, a_k - b_k)$ for $k = 1, 2$.

For any odd number p, let $K(p)$ be the set of all $[a_1, b_1, c_1; a_2, b_2, c_2] \in Z_p^6$ satisfying the compatibility conditions (2) – (5). Let $\kappa(p)$ be the cardinality of $K(p)$. Then there exist precisely $\kappa(p)$ uniform step magic squares of order p. When $p = 3$ we can manually verify that $K(3)$ contains the 8 distinct elements:

$[1, 1, 0; 1, 2, 1]$, $[1, 1, 0; 2, 1, 1]$, $[1, 2, 1; 1, 1, 0]$, $[2, 1, 1; 1, 1, 0]$,
$[1, 2, 1; 2, 2, 2]$, $[2, 1, 1; 2, 2, 2]$, $[2, 2, 2; 1, 2, 1]$, $[2, 2, 2; 2, 1, 1]$.

Hence $\kappa(3) = 8$. With the aid of a computer we obtained the following table of values of $\kappa(p)$ for some sample odd values of p:

p	$\kappa(p)$
3	8
5	1,472
7	25,272
9	3,528
11	713,000
13	2,265,408
15	11,776
21	202,176
25	21,252,800
45	5,193,216
49	2,913,193,080

.

Observe that $\kappa(p)$ values are small when p is a multiple of 3. This reason for this curious phenomenon is given in the following census formula that we derived [15], thereby solving the magic square census problem for odd order uniform step magic squares.

THEOREM 2 *[15] Let $p = \prod_{i=1}^{l} q_i^{v_i}$ be the prime factorization of the odd number p. Then there exist $\kappa(p) = \prod_{i=1}^{l} \kappa(q_i^{v_i})$ uniform step magic squares of order p, where $\kappa(q_i^{v_i}) = [\tau(q_i^{v_i})]^2 - \lambda(q_i^{v_i})$, $\lambda(q_i^{v_i}) = (q_i^{v_i} - q_i^{v_i-1})^2[2(q_i^{2v_i-1}+1)^2/(q_i+1)^2 + q_i^{3v_i-1}(q_i^{v_i} - 3q_i^{v_i-1})]$ and $\tau(q_i^{v_i}) = (q_i^{v_i} - q_i^{v_i-1})(q_i^{2v_i+1} - 2q_i^{2v_i} - q_i^{2v_i-1} + 2)/(q_i + 1)$ for $i = 1, \ldots, l$.*

The idea of the proof is as follows. Let $T(p)$ be the set of all $[a, b, c] \in Z_p^3$ satisfying the conditions $(a, p) = (b, p) = 1$ and the further conditions:

$$c \bmod (a + b, p) = [(a + b, p) - 1]/2, \tag{6}$$

$$(b + c) \bmod (a - b, p) = [(a - b, p) - 1]/2. \tag{7}$$

Let $\tau(p)$ be the cardinality of $T(p)$. If we set $L(p) = (T(p) \times T(p)) \setminus K(p)$, then since

$$T(p) \times T(p) = K(p) \cup L(p)$$

is a disjoint union, it is follows immediately from definitions that

$$\kappa(p) = (\tau(p))^2 - \lambda(p).$$

Thus in order to compute $\kappa(p)$, we need only compute $\tau(p)$ and $\lambda(p)$, as was done in [15]. That computation was based on the following result.

Proposition 1 *Let $p = q^v$, where q is an odd prime. Then* $\tau(q^v) = (q^v - q^{v-1})(q^{2v+1} - 2q^{2v} - q^{2v-1} + 2)/(q+1)$.

The proof of this proposition given in [15] leaves the verification of several key details to the reader, and is therefore hard to read. A more complete proof of the proposition will be presented below.

In the sequel we will make use of Euler's ϕ_k functions. Given k integers, $d_1, \ldots, d_k$, all of which are relatively prime to p, and a collection $e_1, \ldots, e_k$ of members of Z_p, $\phi_k(p)$ is the number of distinct elements z of Z_p such that $(d_1 z + e_1, p) = \cdots = (d_k z + e_k, p) = 1$. It is well known (cf. [9, p. 539]) that $\phi_k(p)$ is given by the expression

$$\phi_k(p) = p(1 - k/q_1)^+ \ldots (1 - k/q_l)^+$$

where $q_1, \ldots, q_l$ are the distinct prime factors of p.

To prove Proposition 1, we first observe that $T(p)$ is a disjoint union of the four sets:

$$T_1(p) = \{[a,b,c] \in T(p)\ (a+b,p) = (a-b,p) = 1\}$$
$$T_2(p) = \{[a,b,c] \in T(p)\ (a+b,p) = 1 \text{ and } q \mid (a-b)\}$$
$$T_3(p) = \{[a,b,c] \in T(p)\ (a-b,p) = 1 \text{ and } q \mid (a+b)\}$$
$$T_4(p) = \{[a,b,c] \in T(p)\ q \mid (a+b) \text{ and } q \mid (a-b)\}.$$

In $T_1(p)$ we can choose a in $\phi_1(p)$ ways satisfying the condition $(a,p) = 1$. Corresponding to each of these choices, we can choose b in such a way that $(b,p) = (a+b,p) = (a-b,p) = 1$. This can be done in $\phi_3(p)$ ways. Since $(a+b,p) = (a-b,p) = 1$, conditions (6) and (7) are redundant. Therefore we can choose c in exactly p ways. Consequently the cardinality of $T_1(p)$ is given by the expression $\tau_1(p) = p\phi_1(p)\phi_3(p)$.

In $T_2(p)$ we can choose a in $\phi_1(p)$ ways satisfying $(a,p) = 1$. Once this is done, we observe that a condition of the form $(a-b, q^v) = 1$ fails to hold if and only if $q \mid (a-b)$ or, equivalently, if $(a-b, q^v) = q^l$ for some integer l such that $1 \le l \le v$. If $l = v$, then $q^l = q^v = p$, and it is easy to verify that the equation $(a-b,p) = p$ holds for some $b \in Z_p$ if and only if $b = (a-p) \bmod p = (p+a-p) \bmod p = a \bmod p = a$, and the equation $(b+c) \bmod q^v = (q^v-1)/2$ holds if and only if $c = ((p-1)/2 - b) \bmod p$. So in this case, b can be chosen in only one way, and c can be chosen in one way. If $1 \le l \le v-1$, it is also straightforward to verify that the equation $(a-b, q^v) = q^l$ holds if and only if $b = (a - \sum_{i=0}^{v-1-l} \tau_i q^{l+i}) \bmod q^v$, where the τ_i's are integers such that $1 \le \tau_0 \le q-1$ and $0 \le \tau_i \le q-1$ for $i = 1, \ldots, v-1-l$. It follows that we can choose b in $(q-1)q^{v-1-l}$ ways. Corresponding to each b, the equation $(b+c) \bmod q^l = (q^l-1)/2$ holds if and only if $c = ((q^l-1)/2 - b + \sum_{i=0}^{v-1-l} \theta_i q^{l+i}) \bmod q^v$ where the θ_i's are integers such that $0 \le \theta_i \le q-1$ for $i = 0, \ldots, v-1-l$. It follows that c can be chosen in q^{v-l} ways. Consequently, for fixed $a \in Z_p$, b and c can be chosen in $1 + \sum_{l=1}^{v-1}(q-1)q^{v-1-l}q^{v-l} = 1 + (q-1)\sum_{l=1}^{v-1} q^{2(v-l)}/q = 1 + (q-1)\sum_{l=1}^{v-1} q^{2l}/q = 1 + q(q^{2v-2}-1)/(q+1) = (1+q^{2v-1})/(q+1)$ ways. Since $q \mid (a-b)$, we must have $(b,p) = 1$ for otherwise we would have $q \mid b$, which would imply that $q \mid a$, contradicting the fact that $(a,p) = 1$. Similarly, the supposition $q \mid (a+b)$ would imply that $q \mid 2a$ which, since q is an odd prime, would imply that $q \mid a$, contradicting the fact that $(a,p) = 1$. Therefore we must have $(a+b,p) = 1$, which implies that condition (6) is redundant. Therefore the cardinality of $T_2(p)$ is given by the expression $\tau_2(p) = (q^v - q^{v-1})(1 + q^{2v-1})/(q+1)$.

The cardinality of $T_3(p)$ is computed in the same way as that of $T_2(p)$ and is given by the same expression $\tau_3(p) = (q^v - q^{v-1})(1 + q^{2v-1})/(q+1)$.

If $[a,b,c] \in T_4(p)$ then $q \mid (a \pm b)$. This implies that $q \mid 2a$ and $q \mid 2b$, and since q is an odd prime, we conclude that $q \mid a$ and $q \mid b$, contradicting the fact that $(a,q^v) = (b,q^v) = 1$. Therefore $T_4(p)$ is an empty set.

We conclude then that the cardinality of $K(q^v)$ is given by the expression

$$\begin{aligned}\tau(q^v) &= \tau_1(q^v) + \tau_2(q^v) + \tau_3(q^v) \\ &= q^v(q^v - q^{v-1})(q^v - 3q^{v-1}) + 2(q^v - q^{v-1})(1 + q^{2v-1})/(q+1) \\ &= (q^v - q^{v-1})(q^{2v+1} - 2q^{2v} - q^{2v-1} + 2)/(q+1).\end{aligned}$$

That complete the proof of Proposition 1.

When p is an odd prime, Theorem 2 becomes the following simpler result.

Corollary 1 *(cf. [16,17]) If p is a prime odd number, then there exist $\kappa(p) = (p-1)^3(p^2-6p+10)$ uniform step magic squares of order p.*

4. A parametrization of generic Magic Squares

Given a magic square $M = (m_{ij})$ of order p, if we set

$$a_{ij} = (m_{ij} - 1) \ \text{ Mod } p \tag{8}$$

$$b_{ij} = (m_{ij} - 1) \ \text{ Div } p \tag{9}$$

then it is immediately apparent that the matrices $A = (a_{ij})$ and $B = (b_{ij})$ are orthogonal in the sense that

$$\{(a_{ij}, b_{ij})\colon i, j = 1, 2, \ldots, p\} = Z_p \times Z_p \tag{10}$$

and each element of the set Z_p occurs p times in each of the sets A and B. If we let E be the order p matrix with 1 in all entries, then we obtain the representation

$$M = E + A + pB \tag{11}$$

which we refer to in the sequel as the canonical form of the magic square M.

The basic properties of the canonical components of a magic square are contained in the following result which is taken from [14].

Theorem 3 *[14] Let M be a $p \times p$ magic square with canonical form (11). Then there exist integers $r_1, r_2, \ldots, r_{2p+2}$ such that*

$$|r_i| < (p-1)/2, \quad i = 0, 1, \ldots, 2p+2 \tag{12}$$

$$\sum_{i=1}^{p} r_i = \sum_{i=1}^{p} r_{p+1+i} = 0, \tag{13}$$

$$\begin{aligned}\sum_{j=1}^{p} a_{ij} + pr_i &= \sum_{j=1}^{p} a_{ji} + pr_{p+1+i} = \sum_{j=1}^{p} a_{jj} + pr_{2p+2} \\ &= \sum_{j=1}^{p} a_{j,p+1-j} + pr_{p+1} = \frac{p(p-1)}{2},\end{aligned} \tag{14}$$

$$\begin{aligned}\sum_{j=1}^{p} b_{ij} - r_i &= \sum_{j=1}^{p} b_{ji} - r_{p+1+i} = \sum_{j=1}^{p} b_{jj} - r_{2p+2} \\ &= \sum_{j=1}^{p} b_{j,p+1-j} - r_{p+1} = \frac{p(p-1)}{2}.\end{aligned} \tag{15}$$

Moreover, each element of the set Z_p occurs p times in A and p times in B, and A and B satisfy the orthogonality condition (10).

The equations in (14) and (15) are of the form

$$\begin{aligned}\sum_{j=1}^{p} l_{ij} + zr_i = \sum_{j=1}^{p} l_{ji} + zr_{p+1+i} = \sum_{j=1}^{p} l_{jj} + zr_{2p+2} \\ = \sum_{j=1}^{p} l_{j,p+1-j} + zr_{p+1} = \frac{p(p-1)}{2}.\end{aligned} \tag{16}$$

where $z = -1$ or $z = p$ and the v_i satisfy conditions (12) and (13). This is a system of $2p+2$ linear equations. However, these equations are not independent, for if

$$\sum_{j=1}^{p} l_{ij} + zr_i = \sum_{j=1}^{p} l_{jk} + zr_{p+1+k} = p(p-1)/2 \quad i = 1, \ldots, p, \quad k = 2, \ldots, p,$$

then

$$\begin{aligned}\sum_{j=1}^{p} l_{j1} &= \sum_{i=1}^{p}\sum_{j=1}^{p} l_{ij} - \sum_{k=2}^{p}\sum_{j=1}^{p} l_{jk} \\ &= p^2(p-1)/2 - p(p-1)(p-1)/2 + z\sum_{k=2}^{p} r_{p+1+k} \\ &= p(p-1)/2 - zr_{p+2}.\end{aligned}$$

This implies that the equation $\sum_{j=1}^{p} l_{j1} = p(p-1)/2 - zr_{p+2}$ is redundant, and hence, that (14) contains only $2p+1$ independent linear equations for the p^2 unknowns (l_{ij}). The general solution will depend on z, $\mathbf{r} = (r_1, r_2, \ldots, r_{2p+2})$ and on some free parameters of the form $\mathbf{s} = (s_1, s_2, \ldots, s_q)$, where $q = p^2 - 2p - 1$. In the sequel, we will define a quasi-Latin square as any matrix $L = (l_{ij})$ satisfying the equations in (16) with $z = p$ or $p = -1$ and the property that each element of the set Z_p occurs p times in L.

It was shown in [14] that when $p = 3$, the explicit solution of (16) is given by the expression

$2-s_2+z(-r_1-r_3+r_4+r_6-2r_8)/3$	$2-s_1+z(-r_1-r_3+r_4-2r_6+r_8)/3$	$-1+s_1+s_2+z(2r_1+3r_2+5r_3-2r_4-3r_5-2r_6-3r_7+r_8)/2$
$-2+s_1+2s_2+z(r_1+4r_3-r_4-3r_5-r_6+2r_8)/3$	$1+z(r_1+r_3-r_4-r_6-r_8)/3$	$4-s_1-2s_2+z(-2r_1-3r_2-5r_3+2r_4+3r_5+2r_6-r_8)/3$
$3-s_1-s_2-zr_3$	s_1	s_2

and, when $p > 3$ by the expressions
$l_{i,j} = s_k, \quad k = 1, \ldots, (p-1)^2 - 2$
$\quad i = p - [(k-1) \text{ Div } (p-1)]$, $j = 2 + [(k-1) \text{ Mod } (p-1)]$,
$l_{i,1} = p(p-1)/2 - zr_i - \sum_{j=2}^{p} l_{i,j}, \quad i = 3, \ldots, p$
$l_{1,1} = p(p-1)/2 - zr_{2p+2} - \sum_{j=2}^{p} l_{j,j}$
$l_{2,1} = p(p-1)/2 - zr_{p+2} - l_{1,1} - \sum_{i=3}^{p} l_{i,1}$
$l_{1,j} = p(p-1)/2 - zr_{p+1+j} - \sum_{i=2}^{p} l_{i,j}, \quad j = 2, \ldots, p-2$
$l_{2,(p-1)} = \frac{1}{2}\{p(p-1)/2 - z(r_{2p} + r_{p+1} - r_1) + l_{1,1} - l_{p,1}$
$+ \sum_{j=2}^{p-2} l_{1,j} - \sum_{j=2}^{p-1} s_{(p-j)(p-1)-1} - \sum_{j=2}^{p-2} s_{p((p-1)-j)}\}$
$l_{2,p} = p(p-1)/2 - zr_2 - l_{2,1} - l_{2,(p-1)} - \sum_{j=2}^{p-2} l_{2,j}$
$l_{1,j} = p(p-1)/2 - zr_{p+1+j} - l_{2,j} - \sum_{i=3}^{p} l_{i,j}, \quad j = p-1, \ p$. If $L(\mathbf{r}; \mathbf{s}; z)$ is the generic literal quasi-Latin square that solves equation (16), then the generic magic square of order p will be expressible

in the form

$$M(\mathbf{r};\mathbf{s};\mathbf{t}) = E + L(\mathbf{r};\mathbf{s};p) + pL(\mathbf{r};\mathbf{t};-1) \tag{17}$$

where $\mathbf{s} = (s_1, \dots, s_q)$ and $\mathbf{t} = (t_1, \dots, t_q)$ are taken from the set Z_p^q, and the components of $\mathbf{r} = (r_1, \dots, r_{2p+2})$ satisfy (12) and (13).

For instance, by computing its canonical form (17) it is easy to verify that the magic square

2	23	25	7	8
4	16	9	14	22
21	11	13	15	5
20	12	17	10	6
18	3	1	19	24

has parametrization $M(\mathbf{r};\mathbf{s};\mathbf{t})$ with

$$\begin{aligned} \mathbf{r} &= (0,0,0,0,0,0,0,1,0,-1,0,0), \\ \mathbf{s} &= (2,0,3,3,1,1,4,0,0,2,4,4,0,3) \\ \mathbf{t} &= (0,0,3,4,2,3,1,1,2,2,2,0,3,1). \end{aligned}$$

Let $\mathcal{R}(p)$ be the set of all $\mathbf{r} = (r_1, \dots, r_p, r_{p+1}, r_{p+2}, \dots, r_{2p+1}, r_{2p+2})$, such that there exist $(\mathbf{s},\mathbf{t}) \in \mathbb{Z}_p \times \mathbb{Z}_p$ such that $M(\mathbf{r};\mathbf{s},\mathbf{t})$ is a magic square.

For each $\mathbf{r} \in \mathcal{R}(p)$, let $\mathcal{M}(\mathbf{r},p)$ be the set of all magic squares which are of the form $M(\mathbf{r};\mathbf{s},\mathbf{t})$ for some $(\mathbf{s},\mathbf{t}) \in \mathbb{Z}_p \times \mathbb{Z}_p$, and let $n(\mathbf{r},p)$ be cardinality of $\mathcal{M}(\mathbf{r},p)$. Then the number of magic squares of order p is given by the formula

$$N(p) = \sum_{\mathbf{r} \in \mathcal{R}(p)} n(\mathbf{r},p).$$

We believe that an understanding of the algebraic structure of the set $\mathcal{R}(p)$ will be useful in the study of the census problem for generic magic squares. The next result is an initial (simple) step in that direction which shows that the set $\mathcal{R}(p)$ is symmetric.

Theorem 4 *If $\mathbf{r} \in \mathcal{R}(p)$ then $-\mathbf{r} \in \mathcal{R}(p)$, and $n(\mathbf{r},p) = n(-\mathbf{r},p)$.*

Proof. If $M = E + A + pB \in \mathcal{M}(\mathbf{r},p)$, then $M' = (p^2+1)E - M$ is also a magic square and, for i, $j = 1, 2, \dots, p$, we have

$$\begin{aligned} m'_{ij} &= p^2 + 1 - m_{ij} = p^2 - a_{ij} - pb_{ij} \\ &= 1 + (p - 1 - a_{ij}) + p(p - 1 - b_{ij}) \equiv 1 + a'_{ij} + pb'_{ij}. \end{aligned}$$

It follows that

$$r'_{p+1} = \sum_{j=1}^{p} b'_{j,p+1-j} - \frac{p(p-1)}{2} = \sum_{j=1}^{p}(p-1-b_{j,p+1-j}) - \frac{p(p-1)}{2}$$

$$= p(p-1) - \sum_{j=1}^{p} b_{j,p+1-j} - \frac{p(p-1)}{2} = -r_{p+1},$$

$$r'_{2p+2} = \sum_{j=1}^{p} b'_{jj} - \frac{p(p-1)}{2} = \sum_{j=1}^{p}(p-1-b_{jj}) - \frac{p(p-1)}{2}$$

$$= p(p-1) - \sum_{j=1}^{p} b_{jj} - \frac{p(p-1)}{2} = -r_{2p+2}$$

and for $i = 1, 2, \ldots, p$:

$$r'_{i} = \sum_{j=1}^{p} b'_{ij} - \frac{p(p-1)}{2} = \sum_{j=1}^{p}(p-1-b_{ij}) - \frac{p(p-1)}{2}$$

$$= p(p-1) - \sum_{j=1}^{p} b_{ij} - \frac{p(p-1)}{2} = -r_{i},$$

$$r'_{p+1+i} = \sum_{j=1}^{p} b'_{ji} - \frac{p(p-1)}{2} = \sum_{j=1}^{p}(p-1-b_{ji}) - \frac{p(p-1)}{2}$$

$$= p(p-1) - \sum_{j=1}^{p} b_{ji} - \frac{p(p-1)}{2} = -r_{p+1+i}.$$

Hence $\mathbf{r}' = -\mathbf{r} \in \mathcal{R}(p)$. Finally, is easy to see that the map $M \mapsto M'$ is a bijection from $\mathcal{M}(\mathbf{r}, p)$ to $\mathcal{M}(-\mathbf{r}, p)$, and hence that $n(\mathbf{r}, p) = n(-\mathbf{r}, p)$ ■

It follows from (12) that when $p = 3$, condition $\mathbf{r} = (0, 0, 0, 0, 0, 0, 0)$ always holds. Hence $\mathcal{R}(3) = \{\mathbf{r}_0\}$, where $\mathbf{r}_0 = (0, 0, 0, 0, 0, 0, 0, 0)$. A direct verification shows that $\mathcal{M}(\mathbf{r}_0, 3) = \{M(\mathbf{r}_0; 0, 1; 0, 2),\ M(\mathbf{r}_0, 1; 2, 0),\ M(\mathbf{r}_0; 0, 2; 0, 1),\ M(\mathbf{r}_0; 0, 2; 2, 1),\ M(\mathbf{r}_0; 0, 1),\ M(\mathbf{r}_0; 2, 0; 2, 1),$ $M(\mathbf{r}_0; 2, 1; 0, 2),\ M(\mathbf{r}_0; 2, 1; 2, 0)\}$, and hence that the number of magic squares of order 3 is $N(3) = n(\mathbf{r}_0, 3) = 8$.

A lengthier verification shows that $\mathcal{R}(4) = \{\mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3\}$, where $\mathbf{r}_1 = (0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$, $\mathbf{r}_2 = (0, 0, 0, 0, -1, 0, 0, 0, 0, 1)$, and $\mathbf{r}_3 = -\mathbf{r}_2$. After calculating only $n(\mathbf{r}_1, 4) = 5248$ and $n(\mathbf{r}_2, 4) = 896$, we are able to deduce from Theorem 4 that the number of magic squares of order 4 is $N(4) = n(\mathbf{r}_1, 4) + n(\mathbf{r}_2, 4) + n(\mathbf{r}_3, 4) = n(\mathbf{r}_1, 4) + 2n(\mathbf{r}_2, 4) = 7040$. The time saved from not having to calculate $n(\mathbf{r}_3, 4)$ separately is significant.

We believe that a further study of the algebraic structure of the set $\mathcal{R}(p)$ will bring us closer to the solution of the census problem for generic magic squares. Some specific problems of immediate interest for further study are:

(1) A study of the specific characteristics of the order-4 magic square classes $\mathcal{M}(\mathbf{r}_1, 4)$, $\mathcal{M}(\mathbf{r}_2, 4)$ and $\mathcal{M}(\mathbf{r}_3, 4)$.
(2) The computation of the set $\mathcal{R}(5)$ – a task that should lead to a a detailed classification and deeper understanding of order-5 magic squares.
(3) The computation of the set $\mathcal{R}(6)$ – a task that should bring us really close to achieving the census of magic squares of order 6.

References

[1] G. Abe, *Unsolved problems on Magic Squares.* Discr. Math. 127(1994)3–13.

[2] W.S. Andrews, "Magic squares and cubes." Dover, New York, 1960.

[3] T.M. Apostol, H.S. Zuckerman. *On magic squares constructed by the uniform step method.* Proceedings of the American mathematical Society, 2(1951), 557– 565.

[4] W.W.R. Ball, "Mathematical Recreations and Essays." Dover, New York, 1987.

[5] W.H. Benson, D. Jacoby, "New Recreations with Magic squares." Dover, New York, 1976.

[6] J.L. Fults, "Magic squares." Open Court, Chicago IL, 1974.

[7] Frénicle de Bessy, B. "Des quarrez ou tables magiques. Avec table generale des quarrez magiques de quatre de cost." In Divers Ouvrages de Mathématique et de Physique, par Messieurs de l'Académie Royale des Sciences (Ed. P. de la Hire). Paris: De l'imprimerie Royale par Jean Anisson, pp. 423-507, 1693. Reprinted as Mem. de l'Acad. Roy. des Sciences 5 (pour 1666-1699), 209-354, 1729.

[8] M. Gardner, Time Travel and Other Mathematical Bewilderments. W. H. Freeman, New York, (1988)213–225.

[9] D.N. Lehmer, *On the congruences connected with certain magic squares.* Transactions of the American Mathematical Society, 31(1929) 529–551.

[10] K. Ollerenshaw, D.S. Brée, Most perfect pandiagonal magic squares: their construction and enumeration. Institute of Mathematics and its Applications, Southend-On-Sea, U.K., 1998.

[11] J. Moran, "The Wonders of Magic squares." Vintage Press, New York, 1982.

[12] L.U. Uko, Magic squares and magic formulae. *The Mathematical Scientist,* 18(1993) 67–72.

[13] L.U. Uko, *On a class of magic squares*. Journal of the Nigerian Mathematical Society, 14 (1995)1–9.

[14] L.U. Uko, *The anatomy of magic squares.*, Ars Combinatoria, 67(2003)115–128.

[15] L.U. Uko, *Uniform step magic squares revisited.* Ars Combinatoria, 71(2004)109–123.

[16] L.U. Uko, *A census of prime-order uniform step magic squares.* Abstracts Amer. Math. Soc. 24(2003), #983-05-194.

[17] L.U. Uko, Sequence A079503 in the On-Line Encyclopedia of Integer Sequences, published electronically at http://oeis.org.