UNIFORM STEP MAGIC SQUARES REVISITED

LIVINUS U. UKO
Laboratôrio de Ciências Matemáticas – CCT
Universidade Estadual do Norte Fluminense
Campos dos Goytacazes – RJ 2805015-620
Brazil
e-mail: uko@zappa.uenf.br

ABSTRACT

We derive an alternative rule for generating uniform step magic squares. The compatibility conditions for the proposed rule are simpler than the analogous conditions for the classical uniform step rule. We exploit this fact to enumerate all uniform-step magic squares of every given odd order. Our main result states that if $p = \prod_{i=1}^{l} q_i^{r_i}$ is the prime factorization of a positive odd number p, then there exist $\kappa(p) = \prod_{i=1}^{l} \kappa(q_i^{r_i})$ uniform step magic squares of order p, where $\kappa(q_i^{r_i}) = [\tau(q_i^{r_i})]^2 - \lambda(q_i^{r_i})$, $\lambda(q_i^{r_i}) = (q_i^{r_i} - q_i^{r_i-1})^2[2(q_i^{2r_i-1}+1)^2/(q_i+1)^2 + q_i^{3r_i-1}(q_i^{r_i} - 3q_i^{r_i-1})]$ and $\tau(q_i^{r_i}) = (q_i^{r_i} - q_i^{r_i-1})(q_i^{2r_i+1} - 2q_i^{2r_i} - q_i^{2r_i-1} + 2)/(q_i+1)$ for $i = 1, \ldots, l$.

Key words: Magic Square, Enumerative Combinatorics, Uniform Step.
2000 Mathematics Subject Classification: Primary 05A99, 00A08.

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. For centuries, magic squares have been a source of exciting mathematical amusements and challenging problems, many of which have remained unsolved to this day (cf. [1]).

In the sequel, for any integers p, s and t, with p positive, Z_p designates the set $\{0, 1, \ldots, p-1\}$, N_p designates the index set $\{1, 2, \ldots, p\}$; $s \bmod t$ is the remainder when t divides s, the expression $t \mid s$ means that $s \bmod t = 0$, and (s, t) designates the largest common factor of s and t. The expression $s \equiv t \pmod{p}$ means that $s - t$ is a multiple of p.

Classical methods for making magic squares can be found in [2,4,5,7]. One of the most popular methods for odd-order squares is the uniform step rule:

$$m^*_{ij} = u + p(v-1), \quad u,v = 1,2,\ldots,p \tag{1.1}$$

with

$$i = 1 + [(\varepsilon + (u-1)\alpha + (v-1)\beta) \bmod p],$$
$$j = 1 + [(\rho + (u-1)\gamma + (v-1)\delta) \bmod p],$$

where ε, α, β, ρ, γ, δ are elements of Z_p satisfying the compatibility conditions (cf. [1]):

$$(p,\alpha) = (p,\beta) = (p,\delta) = (p,\gamma) = (\theta,p) = 1, \tag{1.2}$$
$$\beta\rho - \delta\varepsilon \equiv \theta(u-1)/2 \pmod{u}, \tag{1.3}$$
$$\beta\rho - \delta\varepsilon - \delta \equiv \theta(v-1)/2 \pmod{v}, \tag{1.4}$$
$$\gamma\varepsilon - \alpha\rho \equiv \theta(s-1)/2, \pmod{s}, \tag{1.5}$$
$$\gamma\varepsilon - \alpha\rho + \gamma \equiv \theta(t-1)/2 \pmod{t}, \tag{1.6}$$

with $\theta = \alpha\delta - \gamma\beta$, $u = (p,\delta-\beta)$, $v = (p,\delta+\beta)$, $s = (p,\alpha-\gamma)$ and $t = (p,\alpha+\gamma)$.

In order to enumerate uniform step magic squares we have to determine the number of distinct elements $[\alpha,\beta,\varepsilon;\gamma,\delta,\rho]$ in Z_p^6 satisfying conditions (1.2) – (1.6). Unfortunately these compatibility conditions are discouragingly complicated and give the impression that this combinatorial enumeration problem is extremely difficult.

In the present paper we will adopt a completely different approach to the problem. We begin by studying odd-order magic squares of the form:

$$m_{ij} = 1 + [(a_1 i + b_1 j + c_1) \bmod p] + p[(a_2 i + b_2 j + c_2) \bmod p], \ i,j \in N_p, \tag{1.7}$$

where the a_k, b_k and c_k are elements of Z_p satisfying some compatibility conditions. In the sequel, we will refer to such arrays as regular magic squares. It turns out that every regular magic square can be expressed in uniform step form, and vice versa. Thus the two classes of magic squares coincide. However, the compatibility conditions for the regular magic square rule turn out to be very much simpler than the conditions (1.2) – (1.6) for the uniform step rule. By exploiting this fact it is possible to reformulate and solve the uniform step magic square enumeration problem.

Similar enumeration problems have been studied in [6] for pandiagonal magic squares – also referred to as 'Nasik' or 'diabolic' – that are magic

also in their broken diagonals, and semi-magic squares that are not required to be magic in their diagonals. It is well known (cf. [6]) that the array (1.1) is semi-magic if and only if (1.2) holds, and pandiagonal if and only if $(p, \alpha \pm \gamma) = (p, \delta \pm \beta) = 1$ and (1.2) holds. Such squares can be easily enumerated (cf. [6]) with the aid of Euler's ϕ_k functions (defined in the next section). However, the enumeration of conventional uniform-step magic squares is more difficult and apparently has not yet been done.

This paper will be organized as follows. In section 2 we collect together several ancillary results which will be used in the sequel. In section 3 we derive compatibility conditions for the regular square rule and show that all regular magic squares are uniform step magic squares, and vice versa. In Section 4 – the most important part of the paper – we use the regular square compatibility conditions to resolve the uniform step magic square enumeration problem.

2. Ancillary Results.

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. [6, 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, provided that none of the terms on the right hand side is negative.

We will make repeated use of the following simple Lemmas. Some of the proofs are given for the sake of completeness.

Lemma 2.1. *If* $(m, n) = 1$, $z \bmod n = 0$ *and* $z \bmod m = 0$, *then* $z \bmod mn = 0$.

Proof. It follows from the hypotheses that there exist integers s, t, α and β such that $(m, n) = 1 = m\alpha + n\beta$, $z = ns$ and $z = mt$. Hence $z = ns = mns\alpha + nsn\beta = mn(s\alpha + t\beta)$. □

Lemma 2.2. *Let* m *and* n *be relatively prime positive integers and set* $\psi(z) = [z \bmod m, z \bmod n]$, *for all* $z \in Z_{mn}$. *Then the map* $\psi\colon Z_{mn} \mapsto Z_m \times Z_n$ *is bijective.*

Proof. If $\psi(z) = \psi(z')$, then it follows from Lemma 2.1 that $z - z' \equiv 0 \pmod{mn}$ and, since $z, z' \in Z_{mn}$, that $z = z'$. Thus ψ is injective.

Given $[u, v] \in Z_m \times Z_n$, let $s = (v - u)\alpha$, where α and β are integers such that $1 = (m, n) = m\alpha + n\beta$, and let $z = u + ms$. Then, it is evident that

$z \bmod m = u$. Moreover, since $z = u + (v-u)m\alpha = u + v - u - (v-u)n\beta = v - n(v-u)\beta$, we see that $z \bmod n = v$. Hence $\psi(z) = [u, v]$. Therefore ψ is also surjective. □

Lemma 2.3. *Let m and n be odd numbers such that $(m, n) = 1$. Then the equation $z \bmod mn = (mn-1)/2$ holds if and only if $z \bmod m = (m-1)/2$ and $z \bmod n = (n-1)/2$.*

Proof. Let $z' = (mn-1)/2$. Then since $z' = m(n-1)/2 + (m-1)/2$ and $z' = n(m-1)/2 + (n-1)/2$, we see that $z' \bmod m = (m-1)/2$ and $z' \bmod n = (n-1)/2$.

Thus if $z \bmod mn = z'$ then $z \bmod m = z' \bmod m = (m-1)/2$ and $z \bmod n = z' \bmod n = (n-1)/2$. Conversely, if $z \bmod m = (m-1)/2$ and $z \bmod n = (n-1)/2$ then it follows from the remarks in the previous paragraph that $(z - z') \bmod m = 0$ and $(z - z') \bmod n = 0$. Therefore, on applying Lemma 2.1 we see that $z \bmod mn = z' \bmod mn = z'$. That completes the proof. □

Lemma 2.4. *For all integers z, m and n, we have $(mn, z) = (m, z)(n, z)$.*

Proof. It is evident that $(m, z)(n, z)$ is a common factor of mn and z. Now there exist integers α, β, s and t such that $(m, z) = m\alpha + z\beta$ and $(n, z) = ns + zt$. Hence $(m, z)(n, z) = mns\alpha + z(ns\beta + tm\alpha + tz\beta)$. This shows that every divisor of mn and z divides $(m, z)(n, z)$, and hence that $(m, z)(n, z)$ is in fact the highest common factor of mn and z. □

Lemma 2.5. *Let $\theta \in Z_p$. Then the Diophantine equation*

$$\theta z \equiv b \pmod{p}$$

has one unique solution $z \in Z_p$ associated with each integer b, if and only if $(p, \theta) = 1$. This solution, when it exists, is given by the explicit expression: $z = (b\theta^{\phi_1(p)-1}) \bmod p$.

Proof. Cf. [3]. □

Lemma 2.6. *Let a, b, c, $d \in Z_p$, $\theta = ad - bd$ and $\sigma = \theta^{\phi_1(p)-1}$. Then the Diophantine system of simultaneous equations:*

$$ax + by \equiv e \pmod{p}$$
$$cx + dy \equiv f \pmod{p}$$

has one unique solution $[x, y] \in Z_p^2$ associated to each pair $[e, f]$ of integers, if and only if $(\theta, p) = 1$. This solution, when it exists, is given by the expressions: $x = \sigma(ed - bf) \bmod p$, $y = \sigma(af - ce) \bmod p$.

Proof. These equations imply that

$$\theta x \equiv (ed - bf) \pmod{p}$$
$$\theta y \equiv (af - ce) \pmod{p}.$$

The result follows immediately from Lemma 2.5. □

The following is the basic result from which the compatibility conditions of the regular magic square rule (1.7) will be derived.

Proposition 2.1. *Let p be a positive odd number, let q and z be any integers and let $\alpha = (p, q)$. Then the equation*

$$\sum_{i=1}^{p} [(qi + z) \bmod p] = p(p-1)/2$$

holds if and only if $z \bmod \alpha = (\alpha - 1)/2$.

Proof. Let $p = \alpha s$, $q = \alpha t$, $u = z \bmod \alpha$ and $z = u + l\alpha$. Since $\alpha = (p, q)$, we must have $(s, t) = 1$.

Given any $i \in N_p$, if we set $j = (ti + l) \bmod s$, then the integer $(qi + z) - (\alpha j + u) = \alpha[(ti + l) - (ti + l) \bmod s]$ is a multiple of p, since $(ti + l) - [(ti + l) \bmod s]$ is a multiple of s. For all $j = 0, \ldots, s - 1$, we have $\alpha j + u \leq \alpha(s-1) + u = p + u - \alpha < p$. Therefore $(qi + z) \bmod p = (\alpha j + u) \bmod p = \alpha j + u$, and hence

$$\{(qi + z) \bmod p \mid i = 1, \ldots, p\} \subseteq \{\alpha j + u \mid j = 0, \ldots, s - 1\}.$$

On the other hand, for any fixed $j \in Z_s$, the equation $kt \equiv (j - t - l) \pmod{s}$ has a unique solution $k \in Z_p$, and if we set $i = k + 1 \in N_p$, we see that $(it - j + l) \equiv 0 \pmod{s}$. It follows that

$$(qi + z) - (\alpha j + u) = \alpha(ti - j + l) \equiv 0 \pmod{p},$$

since $ti - j + l$ is a multiple of s. Thus $\alpha j + u = (\alpha j + u) \bmod p = (qi + z) \bmod p$. This shows that in fact we have

$$\{(qi + z) \bmod p \mid i = 1, \ldots, p\} = \{\alpha j + u \mid j = 0, \ldots, s - 1\}. \tag{2.1}$$

Given any $i \in N_p$ we set $i_j = i + js$ for $j = 0, \ldots, \alpha - 1$. Then $(qi_j + z) - (qi + z) = \alpha(tsj) \equiv 0 \pmod{p}$. Therefore each element of the set on the right hand side of (2.1) is repeated α times on the left hand side. Hence

$$\sum_{i=1}^{p} [(qi + z) \bmod p] = \alpha \sum_{j=0}^{s-1} (\alpha j + u) = \alpha[su + \alpha s(s-1)/2]$$
$$= \alpha s[u + \alpha(s-1)/2] = p[u + (p - \alpha)/2].$$

It is easy to show that this sum coincides with $p(p-1)/2$ if and only if $u = (\alpha - 1)/2$. □

3. Regular and Uniform Step Magic Squares.

We now give compatibility conditions for the regular magic square rule (1.7). All through this section, p will designate a generic odd number.

Theorem 3.1. *Let $[a_k, b_k, c_k] \in Z_p^3$ for $k = 1, 2$. Then the $p \times p$ matrix $M = (m_{ij})$ defined in equation (1.7) is a magic square if and only if*

$$(a_1 b_2 - b_1 a_2, p) = 1, \tag{3.1}$$

$$(p, a_k) = (p, b_k) = 1, \qquad k = 1, 2, \tag{3.2}$$

$$c_k \bmod u_k = (u_k - 1)/2, \qquad k = 1, 2, \tag{3.3}$$

$$(b_k + c_k) \bmod v_k = (v_k - 1)/2, \qquad k = 1, 2, \tag{3.4}$$

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

Proof. Let $a_{ij}^{(k)} \equiv (a_k i + b_k j + c_k) \bmod p$. It follows from Proposition 2.1 that the equations

$$\sum_{i=1}^{p} a_{ii}^{(k)} = \sum_{i=1}^{p} [(a_k + b_k)i + c_k] \bmod p = p(p-1)/2$$

$$\sum_{i=1}^{p} a_{i\,p+1-i}^{(k)} = \sum_{i=1}^{p} [(a_k - b_k)i + b_k p + b_k + c_k] \bmod p = p(p-1)/2$$

$$\sum_{i=1}^{p} a_{ij}^{(k)} = \sum_{i=1}^{p} (a_k i + b_k j + c_k) \bmod p = p(p-1)/2$$

$$\sum_{i=1}^{p} a_{ji}^{(k)} = \sum_{i=1}^{p} (b_k i + a_k j + c_k) \bmod p = p(p-1)/2$$

hold, for $k = 1$, 2 and for all $j \in N_p$, if and only if the conditions (3.2) – (3.4) hold. The definition of m_{ij} shows that these conditions hold if and only if $\sum_{i=1}^{p} m_{ii} = \sum_{i=1}^{p} m_{i\,p+1-i} = \sum_{i=1}^{p} m_{ij} = \sum_{i=1}^{p} m_{ji} = p(p^2+1)/2$, $\forall j \in N_p$.

Next, we observe from the definition of (m_{ij}) that the identity

$$\{m_{ij} \mid i, j = 1, \ldots, p\} = \{1, 2, \ldots, p^2\}$$

holds if and only if the equation $m_{ij} = 1 + u + pv$ has a unique solution $[i, j] \in N_p^2$, for any given $[u, v] \in Z_p^2$. This is the case if and only if the Diophantine system:

$$a_1 i + b_1 j + c_1 \equiv u \pmod{p}$$
$$a_2 i + b_2 j + c_2 \equiv v \pmod{p}$$

has a unique solution $[i,j] \in N_p^2$, for any given $[u,v] \in Z_p^2$ or, equivalently, if the Diophantine system:

$$a_1(i-1) + b_1(j-1) \equiv (u - c_1 - a_1 - b_1) \pmod{p}$$
$$a_2(i-1) + b_2(j-1) \equiv (v - c_2 - a_2 - b_2) \pmod{p}$$

has a unique solution $[i,j] \in N_p^2$, for any given $[u,v] \in Z_p^2$. By Lemma 2.6, this condition holds if and only if (3.1) holds. That completes the proof. □

In the sequel, $M_p(a_1, b_1, c_1; a_2, b_2, c_2)$ will designate the regular magic square (1.7). Thus, for instance,

$$m_{ij} = 1 + [(i + 2j) \bmod 5] + 5[(i + 3j) \bmod 5],$$

is the order-5 magic square

$$M_5(1,2,0;1,3,0) = \begin{bmatrix} 24 & 11 & 3 & 20 & 7 \\ 5 & 17 & 9 & 21 & 13 \\ 6 & 23 & 15 & 2 & 19 \\ 12 & 4 & 16 & 8 & 25 \\ 18 & 10 & 22 & 14 & 1 \end{bmatrix}.$$

The next result shows that the regular magic square $M_p(a_1, b_1, c_1; a_2, b_2, c_2)$ is uniquely defined by its coefficients $[a_1, b_1, c_1; a_2, b_2, c_2]$.

Theorem 3.2. *If* $M_p(a_1, b_1, c_1; a_2, b_2, c_2) = M_p(a_1', b_1', c_1'; a_2', b_2', c_2')$ *then* $[a_1, b_1, c_1; a_2, b_2, c_2] = [a_1', b_1', c_1'; a_2', b_2', c_2']$.

Proof. For all $i, j = 1, 2, \ldots, p$, we have

$$[(a_1'i + b_1'j + c_1') \bmod p] + p[(a_2'i + b_2'j + c_2') \bmod p]$$
$$= [(a_1 i + b_1 j + c_1) \bmod p] + p[(a_2 i + b_2 j + c_2) \bmod p].$$

Hence

$$[(a_1' - a_1)i + (b_1' - b_1)j + (c_1' - c_1)] \equiv 0 \pmod{p}$$
$$[(a_2' - a_2)i + (b_2' - b_2)j + (c_2' - c_2)] \equiv 0 \pmod{p}.$$

On taking $i = j = p$, we obtain the relations $|c_1' - c_1| \equiv 0 \pmod{p}$ and $|c_2' - c_2| \equiv 0 \pmod{p}$, which imply (since $|c_1' - c|$ and $|c_2' - c_2|$ are elements of Z_p) that $c_1' = c_1$ and $c_2' = c_2$. On taking $i = 1$ and $j = p$, we obtain the relations $|a_1' - a_1| \equiv 0 \pmod{p}$ and $|a_2' - a_2| \equiv 0 \pmod{p}$, which imply (since $|a_1' - a_1|$ and $|a_2' - a_2|$ are elements of Z_p) that $a_1' = a_1$ and $a_2' = a_2$. Finally, we set $j = 1$ to obtain the relations $|b_1' - b_1| \equiv 0 \bmod p$ and $|b_2' - b_2| \equiv 0 \pmod{p}$, which imply (since $|b_1' - b_1|$ and $|b_2' - b_2|$ are elements of Z_p) that $b_1' = b_1$ and $b_2' = b_2$. That completes the proof. □

We now show the equivalence between regular magic squares generated with equation (1.7) and uniform step squares generated with equation (1.1).

Proposition 3.1. *Every regular magic square of the form (1.7) is a uniform step square of the form (1.1).*

Proof. Given a regular magic square (m_{ij}) of the form (1.7), we set $d = a_1b_2 - b_1a_2$, $\omega = d^{\phi_1(p)-1} \bmod p$, $\alpha = (\omega b_2) \bmod p$, $\beta = (-\omega b_1) \bmod p$, $\varepsilon = [\omega(b_1c_2 - b_2c_1 - d)] \bmod p$, $\gamma = (-\omega a_2) \bmod p$, $\delta = (\omega a_1) \bmod p$ and $\rho = [\omega(a_2c_1 - a_1c_2 - d)] \bmod p$. Then we define a matrix (m^*_{ij}) by substituting these values in (1.1).

Since $(p, d) = 1$, Euler's Theorem ([3, Thm. 13]) implies that $(d\omega) \bmod p = 1$. Therefore, for any $[i, j] \in N_p^2$, if we set

$$\begin{aligned} u &= 1 + [(a_1i + b_1j + c_1) \bmod p] \\ v &= 1 + [(a_2i + b_2j + c_2) \bmod p], \end{aligned}$$

and substitute the values of the α, β, γ, δ, ε and ρ, and rearrange, we see that

$$\begin{aligned} \alpha(u-1) + \beta(v-1) + \varepsilon &\equiv \omega[i(a_1b_2 - b_1a_2) + b_2c_1 - b_1c_2] + \varepsilon \pmod p \\ &\equiv d\omega(i-1) \pmod p \\ &\equiv [(d\omega) \bmod p](i-1) \pmod p \\ &\equiv (i-1) \pmod p \\ \gamma(u-1) + \delta(v-1) + \rho &\equiv \omega[j(a_1b_2 - b_1a_2) + a_1c_2 - a_2c_1] + \rho \pmod p \\ &\equiv d\omega(j-1) \pmod p \\ &\equiv [(d\omega) \bmod p](j-1) \pmod p \\ &\equiv (j-1) \pmod p. \end{aligned}$$

It follows from this that

$$\begin{aligned} m_{ij} &= 1 + [(a_1i + b_1j + c_1) \bmod p] + p[(a_2i + b_2j + c_2) \bmod p] \\ &= u + p(v-1) = m^*_{ij}, \quad \forall i, j \in N_p. \end{aligned}$$

That completes the proof. □

Proposition 3.2. *Every uniform step magic square of the form (1.1) is a regular square of the form (1.7).*

Proof. Given a uniform step magic square (m^*_{ij}) of the form (1.1), let $\theta = \alpha\delta - \gamma\beta$, $\sigma = \theta^{\phi_1(p)-1} \bmod p$, $a_1 = (\sigma\delta) \bmod p$, $b_1 = (-\sigma\beta) \bmod p$, $c_1 = (\sigma[\beta(\rho+1) - \delta(\varepsilon+1)]) \bmod p$, $a_2 = (-\sigma\gamma) \bmod p$, $b_2 = (\sigma\alpha) \bmod p$ and $c_2 = (\sigma[\gamma(\varepsilon+1) - \alpha(\rho+1)]) \bmod p$. Let (m_{ij}) be the matrix obtained by substituting these values in (1.7).

In (1.1), the pairs $1+[(\varepsilon+(u-1)\alpha+(v-1)\beta) \bmod p]$ and $1+[(\lambda+(u-1)\gamma+(v-1)\delta) \bmod p]$ with $[u,v] \in N_p^2$, must exhaust with N_p^2. Therefore, corresponding to any $[s,t] \in Z_p^2$, the Diophantine system

$$\begin{aligned} \alpha k + \beta l + \varepsilon &\equiv s \pmod p \\ \gamma k + \delta l + \lambda &\equiv t \pmod p \end{aligned}$$

has a unique solution $[k,l] \in Z_p^2$. Therefore it follows from Lemma 2.6 that $(p,\theta) = 1$.

Euler's Theorem ([3, Thm. 13]) implies that $(\theta\sigma) \bmod p = 1$. Therefore, for any $[i,j] \in N_p^2$, if we set

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

and substitute the values of the a_k, b_k, c_k, and rearrange, we see that

$$\begin{aligned} \alpha(u-1)+\beta(v-1)+\varepsilon &\equiv \sigma[i(\alpha\delta-\gamma\beta)+\alpha(\beta(\rho+1)-\delta(\varepsilon+1)) \\ &\quad +\beta(\gamma(\varepsilon+1)-\alpha(\rho+1))]+\varepsilon \pmod p \\ &\equiv \sigma\theta(i-1-\varepsilon)+\varepsilon \pmod p \\ &\equiv [\sigma\theta \bmod p](i-1-\varepsilon)+\varepsilon \pmod p \\ &\equiv (i-1) \pmod p \\ \gamma(u-1)+\delta(v-1)+\rho &\equiv \sigma[j(\alpha\delta-\gamma\beta)+\gamma(\beta(\rho+1)-\delta(\varepsilon+1)) \\ &\quad +\delta(\gamma(\varepsilon+1)-\alpha(\rho+1))]+\rho \pmod p \\ &\equiv \sigma\theta(j-1-\rho)+\rho \pmod p \\ &\equiv [\sigma\theta \bmod p](j-1-\rho)+\rho \pmod p \\ &\equiv (j-1) \pmod p \end{aligned}$$

It follows from this that

$$\begin{aligned} m_{ij} &= 1 + [(a_1 i + b_1 j + c_1) \bmod p] + p[(a_2 i + b_2 j + c_2) \bmod p] \\ &= u + p(v-1) = m^*_{ij}, \quad \forall i,j \in N_p. \end{aligned}$$

That completes the proof. □

In the next result we prove, for the sake of completeness, that equations (1.2) – (1.6) are the compatibility conditions for uniform step magic squares of the form (1.1).

Corollary 3.1. *The uniform step array in (1.1) is a magic square if and only if the compatibility conditions (1.2) - (1.6) hold.*

Proof. Let (m^*_{ij}) be a uniform step array of the form (1.1), let the parameters a_1, b_1, c_1, a_2, b_2, c_2, θ and σ be defined as in the proof of Proposition 3.2, and let (m_{ij}) be the regular array obtained by substituting these values in equation (1.7). The resulting array will be a magic square if and only if the compatibility conditions (3.1) - (3.4) hold. On substituting the values of a_1, b_1, c_1, a_2, b_2, c_2 in (3.1) - (3.4) we obtain the equivalent conditions:

$$(p, \delta\sigma) = (p, \beta\sigma) = (p, \gamma\sigma) = (p, \alpha\sigma) = (p, \sigma^2\theta) = 1, \tag{3.5}$$

$$\sigma(\beta\rho - \delta\varepsilon + \beta - \delta) \bmod u = (u-1)/2, \tag{3.6}$$

$$\sigma(\beta\rho - \delta\varepsilon - \delta) \bmod v = (v-1)/2, \tag{3.7}$$

$$\sigma(\gamma\varepsilon - \alpha\rho + \gamma - \alpha) \bmod s = (s-1)/2, \tag{3.8}$$

$$\sigma(\gamma\varepsilon - \alpha\rho + \gamma) \bmod t = (t-1)/2, \tag{3.9}$$

where $\sigma = \theta^{\phi_1(p)-1} \bmod p$, $u = (p, \sigma(\delta - \beta))$, $v = (p, \sigma(\delta + \beta))$, $s = (p, \sigma(\alpha - \gamma))$ and $t = (p, \sigma(\alpha + \gamma))$. It suffices to show that equations (3.5) - (3.9) are equivalent to equations (1.2) - (1.6).

Suppose that conditions (3.5) - (3.9) hold. Then it follows from (3.5) and Lemma 2.4 that $(p, \delta)(p, \sigma) = (p, \beta)(p, \sigma) = (p, \gamma)(p, \sigma) = (p, \alpha)(p, \sigma) = (p, \sigma^2)(p, \theta) = 1$. Since all quantities appearing are positive integers, we see that $(p, \sigma) = 1$ and that (1.2) holds. Euler's Theorem ([3, Thm. 13]) implies that $\theta\sigma \equiv 1 \pmod{p}$. Therefore, on multiplying both sides of the congruence equations in (3.6) - (3.9) with θ and observing that $(\beta - \delta) \bmod u = (\gamma - \alpha) \bmod s = 0$, $(p, \sigma(\delta \pm \beta)) = (p, \sigma)(p, \delta \pm \beta) = (p, \delta \pm \beta)$ and $(p, \sigma(\alpha \pm \gamma)) = (p, \sigma)(p, \alpha \pm \gamma) = (p, \alpha \pm \gamma)$, we see that (1.2) - (1.6) hold.

Now suppose that (1.2) - (1.6) hold. Then since $(p, \theta) = (p, \sigma) = 1$, Lemma 2.4 shows that (3.5) holds. Euler's Theorem implies that $\theta\sigma \equiv 1 \pmod{p}$. Therefore, on multiplying both sides of the congruence equations in (1.3) - (1.6) with σ and applying Lemma 2.4, we obtain equations (3.6) - (3.9).

Thus the compatibility conditions (1.2) - (1.6) and (3.5) - (3.9) are equivalent. □

4. Enumeration of Uniform Step Magic Squares.

If we compare the regular square compatibility conditions (3.1) - (3.4) with their analogues (1.2) - (1.6) for the uniform step rule, we see that the

regular square conditions are very much simpler. In this section we exploit this fact to solve the enumeration problem for uniform step magic squares.

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 (3.1) – (3.4). Let $\kappa(p)$ be the cardinality of $K(p)$. Then there exist precisely $\kappa(p)$ uniform step magic squares of order p. Let $T(p)$ be the set of all $[a, b, c] \in Z_p^3$ satisfying the condition $(a, p) = (b, p) = 1$ and the two conditions:

$$c \bmod (a+b, p) = [(a+b, p) - 1]/2, \tag{4.1}$$

$$(b+c) \bmod (a-b, p) = [(a-b, p) - 1]/2. \tag{4.2}$$

Let $\tau(p)$ be the cardinality of $T(p)$.

It is evident from (3.1) – (3.4) that if $[a_1, b_1, c_1; a_2, b_2, c_2] \in K(p)$, then $[a_1, b_1, c_1] \in T(p)$ and $[a_2, b_2, c_2] \in T(p)$. However, the converse may be false since condition (3.1) may fail to hold. Let $L(p) = [T(p) \times T(p)] \setminus K(p)$. Then $[a_1, b_1, c_1; a_2, b_2, c_2]$ belongs to $L(p)$ precisely when (3.2) – (3.4) hold but (3.1) does not. If we let $\lambda(p)$ be the cardinality of $L(p)$, then since

$$T(p) \times T(p) = K(p) \cup L(p) \tag{4.3}$$

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

$$\kappa(p) = [\tau(p)]^2 - \lambda(p). \tag{4.4}$$

Thus in order to compute $\kappa(p)$, we need only compute $\tau(p)$ and $\lambda(p)$.

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.

In the next series of results we derive a general formula for $\kappa(p)$ when p is an arbitrary odd positive integer.

Proposition 4.1. *Let $p = q^r$, where q is an odd prime. Then* $\tau(q^r) = (q^r - q^{r-1})(q^{2r+1} - 2q^{2r} - q^{2r-1} + 2)/(q+1)$.

Proof. It is easy to see that a condition of the form $(q^r, z) = 1$ fails to hold if and only if $q \mid z$ or, equivalently, if $(q^r, z) = q^l$ for some integer l such that $1 \le l \le r$. On using this fact we easily see that $T(p)$ is a disjoint union of the four sets:

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

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 (4.1) and (4.2) are redundant. Therefore we can choose c in exactly p ways. Consequently the cardinality of $T_1(p)$ is given by the expression $\tau_1(p) = p\phi_1(p)\phi_3(p) = q^r(q^r - q^{r-1})(q^r - 3q^{r-1})$.

In $T_2(p)$ we can choose b in $\phi_1(p)$ ways satisfying $(b,p) = 1$. Since $(a+b,p) = 1$, condition (4.1) is redundant. For each integer l such that $1 \le l \le r$, we can choose a in $\phi_1(q^{r-l})$ ways such that $(a-b,q^r) = q^l$ (or, equivalently, $(a-b,q^{r-l}) = 1$). Corresponding to each such choice of a, we can choose c in q^{r-l} ways satisfying $(b+c) \bmod q^l = (q^l - 1)$. Consequently, a and c can be chosen in $\sum_{l=1}^{r} q^{r-l}\phi_1(q^{r-l}) = \sum_{l=0}^{r-1} q^l(q^l - q^{l-l}) = (1 + q^{2r-1})/(q+1)$ ways. Therefore the cardinality of $T_2(p)$ is given by the expression $\tau_2(p) = (q^r - q^{r-1})(1 + q^{2r-1})/(q+1)$.

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 $\tau_3(p) = (q^r - q^{r-1})(1 + q^{2r-1})/(q+1)$.

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 $(a,q^r) = (b,q^r) = 1$. Therefore $T_4(p)$ is an empty set.

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

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

Proposition 4.2. *Let $p = q^r$, where q is an odd prime. Then* $\lambda(q^r) = (q^r - q^{r-1})^2[2(q^{2r-1}+1)^2/(q+1)^2 + q^{3r-1}(q^r - 3q^{r-1})]$.

Proof. Let $T_i(p)$ be defined as in the proof of Proposition 4.1, with cardinality $\tau_i(p)$, for $i = 1, \ldots, 3$ (we recall that $T_4(p) = \emptyset$). It follows from (4.3) that the set $L(p)$ is a disjoint union of the nine sets

$$L_{ij}(p) \equiv \{[a_1, b_1, c_1; a_2, b_2, c_2] \in T_i(p) \times T_j(p) \colon q \mid (a_1 b_2 - b_1 a_2)\},$$

with cardinalities $\lambda_{ij}(p)$, respectively, for $i, j = 1, \ldots, 3$.

If $[a_1, b_1, c_1; a_2, b_2, c_2] \in L_{12}(p)$, then since $a_2 \bmod q = b_2 \bmod q$ we see that $(a_1 b_2) \bmod q = (b_1 a_2) \bmod q = (b_1 b_2) \bmod q$. Since $(b_2, q) = 1$, it follows that $a_1 \bmod q = b_1 \bmod q$, and hence that $q \mid (a_1 - b_1)$, contradicting the fact that $(a_1 - b_1, p) = 1$. Consequently, $L_{12}(p) = \emptyset$.

In a similar manner we can show that $L_{13}(p) = L_{21}(p) = L_{23}(p) = L_{31}(p) = L_{32}(p) = \emptyset$.

If $[a_1, b_1, c_1; a_2, b_2, c_2] \in L_{11}(p)$, then b_1 can be chosen in $\phi_1(p)$ ways satisfying $(b_1, p) = 1$. Corresponding to each of these choices, a_1 is chosen in such a way that $(a_1, p) = (a_1 + b_1, p) = (a_1 - b_1, p) = 1$. This can be done in $\phi_3(p)$ ways. Furthermore, we can choose b_2 in $\phi_1(p)$ ways such that $(b_2, p) = 1$.

Once b_1, b_2 and a_1 have been chosen it suffices to choose a_2 in such a way that $a_2 b_1 \equiv b_2 a_1 \pmod q$, for then we automatically have $(q, a_2) = (q, a_2 \pm b_2) = 1$. In fact, if a_2 is chosen in this way and $(q, a_2) \neq 1$, then $a_2 \bmod q = 0$. This implies that $(a_2 b_1) \equiv (b_2 a_1) \equiv 0 \pmod q$ and hence that either $(q, b_2) = q$ or $(q, a_1) = q$, contradicting the earlier hypotheses. Hence $(q, a_2) = 1$. Furthermore, if $(q, a_2 \pm b_2) \neq 1$, then $a_2 \equiv \mp b_2 \pmod q$, and hence $(a_2 b_1) \equiv (b_2 a_1) \equiv \mp a_2 a_1 \pmod q$. Since $(q, a_2) = 1$ this implies that $(b_1 \pm a_1) \pmod q = 0$, again contradicting the previous hypotheses.

Therefore when b_1, b_2 and a_1 have been chosen we only need to choose $a_2 \in Z_p$ in such a way that $a_2 b_1 \equiv b_2 a_1 \pmod q$. All possible choices are of the form $a_2 = z + q\alpha$ where z is the unique element in Z_q that solves the Diophantine equation $z b_1 \equiv a_1 b_2 \pmod q$. Therefore a_2 can be chosen in p/q ways.

Since $(a_1 \pm b_1, p) = (a_2 \pm b_2, p) = 1$, conditions (3.3) - (3.4) on c_1 and c_2 are redundant. Therefore we can choose c_1 in p ways and c_2 in p ways. Hence $\lambda_{11}(p) = [p\phi_1(p)]^2 \phi_3(p)[p/q] = q^{3r-1}(q^r - q^{r-1})^2(q^r - 3q^{r-1})]$.

The two conditions $a_1 \bmod q = b_1 \bmod q$ and $a_2 \bmod q = b_2 \bmod q$ automatically imply the condition $(a_1 b_2) \bmod q = (b_1 a_2) \bmod q$. Therefore the condition $q \mid (a_1 b_2 - b_1 a_2)$ in the definition of $L_{22}(p)$ is redundant. Thus $L_{22}(p)$ is given by the simpler expression $L_{22}(p) = T_2(p) \times T_2(p)$. Hence $\lambda_{22}(p) = \tau_2(p)^2 = [\phi_1(q^r)(1 + q^{2r-1})/(q+1)]^2$.

In a similar manner we can show that $L_{33}(p) = T_3(p) \times T_3(p)$ and hence, that $\lambda_{33}(p) = \tau_3(p)^2 = [\phi_1(q^r)(1+q^{2r-1})/(q+1)]^2$.

Consequently, the cardinality of $L(p)$ is given by the expression:

$$\begin{aligned}\lambda(q^r) &= \lambda_{11}(q^r) + \lambda_{22}(q^r) + \lambda_{33}(q^r) \\ &= [q^r\phi_1(q^r)]^2 q^{r-1}\phi_3(q^r) + 2[\phi_1(q^r)(1+q^{2r-1})/(q+1)]^2 \\ &= (q^r - q^{r-1})^2[2(1+q^{2r-1})^2/(q+1)^2 + q^{3r-1}(q^r - 3q^{r-1})]. \quad \square\end{aligned}$$

Corollary 4.1. *Let $p = q^r$, where q is an odd prime. Then there exist $\kappa(q^r) = [\tau(q^r)]^2 - \lambda(q^r)$ uniform step magic squares of order p, where $\lambda(q^r) = (q^r - q^{r-1})^2[2(q^{2r-1}+1)^2/(q+1)^2 + q^{3r-1}(q^r - 3q^{r-1})]$ and $\tau(q^r) = (q^r - q^{r-1})(q^{2r+1} - 2q^{2r} - q^{2r-1} + 2)/(q+1)$.*

Corollary 4.2. *Let p be an odd prime number. Then there exist $\kappa(p) = (p-1)^3[(p-2)^3 - 2(p-3)]$ uniform step magic squares of order p.*

The next result will enables us compute the cardinality of $K(p)$ for values of p that are not prime powers.

Proposition 4.3. *Let m and n be relatively prime odd numbers. Then $\kappa(mn) = \kappa(m)\kappa(n)$.*

Proof. It follows from Lemma 2.2 that the map from Z^6_{mn} to $Z^6_m \times Z^6_n$ that takes $[a_1, b_1, c_1; a_2, b_2, c_2] \in Z^6_{mn}$ to the elements $[a'_1, b'_1, c'_1; a'_2, b'_2, c'_2] \in Z^6_m$ and $[a''_1, b''_1, c''_1; a''_2, b''_2, c''_2] \in Z^6_n$ defined by $a'_i = a_i \bmod m$, $b'_i = b_i \bmod m$, $c'_i = c_i \bmod m$, $a''_i = a_i \bmod n$, $b''_i = b_i \bmod n$, $c''_i = c_i \bmod n$, $i = 1, 2$, is a bijective map.

On the other hand, it follows from Lemma 2.4 that

$$\begin{aligned}(a_1b_2 - b_1a_2, mn) &= (a_1b_2 - b_1a_2, m)(a_1b_2 - b_1a_2, n) \\ &= (a'_1b'_2 - b'_1a'_2, m)(a''_1b''_2 - b''_1a''_2, n) \\ (a_i, mn) &= (a_i, m)(a_i, n) = (a'_i, m)(a''_i, n), \qquad i = 1, 2 \\ (b_i, mn) &= (b_i, m)(b_i, n) = (b'_i, m)(b''_i, n), \qquad i = 1, 2.\end{aligned}$$

These relations show that the condition

$$(a_1, mn) = (b_1, mn) = (a_2, mn) = (b_2, mn) = (a_1b_2 - b_1a_2, mn) = 1$$

holds if and only if the conditions

$$(a'_1, m) = (b'_1, m) = (a'_2, m) = (b'_2, m) = (a'_1b'_2 - b'_1a'_2, m) = 1$$

$$(a_1'', n) = (b_1'', n) = (a_2'', n) = (b_2'', n) = (a_1''b_2'' - b_1''a_2'', n) = 1$$

hold.

If we set $u_i = (a_i + b_i, mn)$, $u_i' = (a_i' + b_i', m)$, $u_i'' = (a_i'' + b_i'', n)$, $v_i = (a_i - b_i, mn)$, $v_i' = (a_i' - b_i', m)$ and $v_i'' = (a_i'' - b_i'', n)$, then it follows from Lemma 2.4 that

$$u_i = (a_i + b_i, m)(a_i + b_i, n) = (a_i' + b_i', m)(a_i'' + b_i'', n) = u_i'u_i'',$$
$$v_i = (a_i - b_i, m)(a_i - b_1, n) = (a_i' - b_i', m)(a_i'' - b_i'', n) = v_i'v_i'',$$

for $i = 1, 2$. Moreover, $c_i' \bmod u_i' = c_i \bmod u_i'$ and $c_i'' \bmod u_i'' = c_i \bmod u_i''$. It follows from Lemma 2.3 that the condition $c_i \bmod u_i = (u_i - 1)/2$ holds if and only if the two conditions $c_i' \bmod u_i' = (u_i' - 1)/2$ and $c_i'' \bmod u_i'' = (u_i'' - 1)/2$ hold. Similarly, we can show that the condition $(b_i + c_i) \bmod v_i = (v_i - 1)/2$ holds if and only if the two conditions $(b_i' + c_i') \bmod v_i' = (v_i' - 1)/2$ and $(b_i'' + c_i'') \bmod v_i'' = (v_i'' - 1)/2$ hold.

Thus $[a_1, b_1, c_1; a_2, b_2, c_2] \in K(mn)$ if and only if $[a_1', b_1', c_1'; a_2', b_2', c_2'] \in K(m)$ and $[a_1'', b_1'', c_1''; a_2'', b_2'', c_2''] \in K(n)$, and conversely. This shows that $K(mn)$ and $K(m) \times K(n)$ have the same cardinality and completes the proof. □

Corollary 4.3. *Let $p = \prod_{i=1}^{l} q_i^{r_i}$ be the prime factorization of the odd number p. Then there exist $\kappa(p) = \prod_{i=1}^{l} \kappa(q_i^{r_i})$ uniform step magic squares of order p, where the $\kappa(q_i^{r_i})$ are defined as in Corollary 4.1.*

References

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

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

[3] L.E. Dickson, "Introduction to the Theory of Numbers." Dover, New York, 1950.

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

[5] M. Kraitchik, "Mathematical Recreations." George Allen & Unwin, London, 1955.

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

[7] L.U. Uko, *Magic Squares and Magic Formulae.* The Mathematical Scientist, 18 (1993) 67–72.