<table>
<thead>
<tr>
<th><strong>Title</strong></th>
<th>Lupe Latin squares of order odd, 3-odd, $A^2 + 3B^2$ with $\gcd(A,B) = 1$</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Author(s)</strong></td>
<td>Azukawa, Kazuo</td>
</tr>
<tr>
<td><strong>Citation</strong></td>
<td>Toyama mathematical journal, 34: 1-22</td>
</tr>
<tr>
<td><strong>Issue Date</strong></td>
<td>2011</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>Article</td>
</tr>
<tr>
<td><strong>Text version</strong></td>
<td>publisher</td>
</tr>
<tr>
<td><strong>URL</strong></td>
<td><a href="http://hdl.handle.net/10110/9714">http://hdl.handle.net/10110/9714</a></td>
</tr>
<tr>
<td><strong>Rights</strong></td>
<td></td>
</tr>
</tbody>
</table>
Lupe Latin squares of order odd, 3-odd, $A^2 + 3B^2$
with $\text{gcm}(A, B) = 1$

Kazuo Azukawa

Abstract. Let $p$ be an odd integer which is written as $p = A^2 + 3B^2$ with $\text{gcm}(A, B) = 1$ and which is non-divisible by 3. We define (1,3)-Lupe and (3,1)-Lupe properties of a Latin $p$-square or a magic $p$-square. For any such $p$, we construct complete Latin $p$-squares $N_+^+, N_-^+$ of (1,3)-Lupe property, and $N_+^-, N_-^-$ of (3,1)-Lupe property. We show that the products $N_+^+ \times N_-^+$ and $N_+^- \times N_-^-$ are Euler squares, so that $pN_+^+ + N_-^+$ and $pN_+^- + N_-^-$ are complete magic squares of (1,3)-Lupe property (resp. (3,1)-Lupe property).

1. Odd and 3-odd numbers $A^2 + 3B^2$ with $\text{gcm}(A, B) = 1$

We start with the following lemma:

Lemma 1. If $A, B \in \mathbb{N}$ and $\text{gcm}(A, B) = 1$, then there exist unique $(a, b), (a', b') \in \{0, \ldots, A\} \times \{0, \ldots, B\} \setminus \{(0, 0), (A, B)\}$ such that $bA - aB = 1$ and $b'A - a'B = -1$. For these it holds that $(a, b) + (a', b') = (A, B)$.

Proof. To prove the existence, let

$$\frac{B}{A} = a_0 + \frac{1}{a_1 +} \frac{1}{a_2 +} \cdots \frac{1}{a_{n-1} +} \frac{1}{a_n}$$

be the continued fraction expansion of the number $B/A$ such that $a_0 \in \{0\} \cup \mathbb{N}$, $a_j \in \mathbb{N}(n \geq j \geq 1)$ and that $a_n \geq 2$ whenever $n \geq 1$. Let

$$\frac{y}{x} = a_0 + \frac{1}{a_1 +} \frac{1}{a_2 +} \cdots \frac{1}{a_{n-2} +} \frac{1}{a_{n-1}}$$

1
with \(x, y \in \mathbb{Z}, x \geq 0, \gcd(x, y) = 1\) (when \(n = 0, (x, y) = (0, 1)\))(cf. [A-Y]). Then, \((x, y) \in \{0, \ldots, A - 1\} \times \{0, \ldots, B\} \setminus \{(0, 0)\}\) and \(yA -xB = (-1)^n\); furthermore if \((x', y') := (A - x, B - y), then (x', y') \in \{1, \ldots, A\} \times \{0, \ldots, B\} \setminus \{(A, B)\}\) and \(y'A - x'B = (-1)^{n+1}\). If \(n\) is even (resp. odd), then \((a, b) = (x, y), (a', b') = (x', y')\) (resp. \((a, b) = (x', y'), (a', b') = (x, y)\) ) have the desired properties. The uniqueness and the latter half of the assertions are easy to prove.

From now on we assume that \(p \in \mathbb{N}\) and \((A, B) \in \mathbb{N}^2\) satisfy

\[(1)\quad p = A^2 + 3B^2,\]

\[(2)\quad \gcd(A, B) = 1,\]

\[(3)\quad p\text{ is odd,}\]

\[(4)\quad p\text{ is not divisible by } 3.\]

We may call property (4) \(p\) being 3-\textbf{odd}. Take \((a, b), (a', b') \in \{0, \ldots, A\} \times \{0, \ldots, B\} \setminus \{(0, 0), (A, B)\}\) satisfying

\[(5)\quad bA - aB = 1\quad \text{and}\]

\[(6)\quad b'A - a'B = -1\]

as in Lemma 1 and set

\[(7)\quad q := aA + 3bB, \quad q' := a'A + 3b'B.\]

We note that

\[(8)\quad q + q' = p,\]

\[(9)\quad qA = ap + 3B, \quad qB = bp - A,\]

\[(10)\quad q'A = a'p - 3B, \quad q'B = b'p + A.\]
It follows from (1),(2), and (3) that

\[(11) \quad A + B \text{ is odd;}
\]

especially

\[(12) \quad A \neq B.\]

**Lemma 2.** Let \(p, A, B\) satisfy (1)-(4) and \(q, q'\) be defined by (7). Then \(\gcd(q, p) = 1\) and \(\gcd(q', p) = 1\).

**Proof.** It follows from (1) and (4) that \(A\) is not divisible by 3, so that \(\gcd(A, 3B) = 1\) by (2). Take \(\ell, m \in \mathbb{Z}\) such that \(\ell A + m3B = 1\). It follows from (9) that \(\ell(bp - qB) + m(qA - ap) = 1\), so that \((-\ell B + mA)q + (\ell b - ma)p = 1\); therefore, \(\gcd(q, p) = 1\). Since \(q' = p - q\) by (8), \(\gcd(q', p) = \gcd(p - q, p) = \gcd(q, p) = 1\), as desired.

**Lemma 3.** Let \(p, a, b, q, q'\) be as in Lemma 2. Then

\[(13) \quad p(a^2 + 3b^2) - q^2 = 3, \quad p(a'^2 + 3b'^2) - q'^2 = 3,
\]

\[(14) \quad qq' \equiv 3 \pmod{p}.
\]

**Proof.** The identity

\[(A^2 + 3B^2)(x^2 + 3y^2) = (xA + 3yB)^2 + 3(yA - xB)^2
\]

implies (13). It follows from (8) and (13) that \(qq' = q(p - q) \equiv -q^2 \equiv 3 \pmod{p}\), as desired.

**Remark 4.** It is well known that for every \(p \in \mathbb{N}\), which is odd and 3-odd, the following seven statements are mutually equivalent (cf. [H]):

(i) There exists \((A, B) \in \mathbb{N}^2\) such that \(p = A^2 + 3B^2\) with \(\gcd(A, B) = 1\).

(ii) There exists \((X, Y) \in \mathbb{N}^2\) such that \(p = X^2 + Y^2 + XY\) with \(\gcd(X, Y) = 1\).

(iii) There exists \(q \in \mathbb{N}\) such that \(q^2 \equiv -3 \pmod{p}\).

(iv) For every prime \(p'\) with \(p'|p\), it holds that \(p' \equiv 1 \pmod{3}\).
(v) For every prime $p'$ with $p'|p$, there exists $(A, B) \in \mathbb{N}^2$ such that $p' = A^2 + 3B^2$ with $\gcd(A, B) = 1$.

(vi) For every prime $p'$ with $p'|p$, there exists $(X, Y) \in \mathbb{N}^2$ such that $p' = X^2 + Y^2 + XY$ with $\gcd(X, Y) = 1$.

(vii) For every prime $p'$ with $p'|p$, there exists $q \in \mathbb{N}$ such that $q^2 \equiv -3 \pmod{p'}$.

A proof of implication (i)$\Rightarrow$(iii) has been given in the proof of Lemma 3.

From (iv), every $p$ satisfying one of (i)-(vii), $p \equiv 1 \pmod{3}$.

For completeness we shall prove the equivalence of (i) and (ii), so that of (v) and (vi). We first note the following:

If $p = A^2 + 3B^2$, $A, B \in \mathbb{N}$, then $p = (A + B)^2 + 2B(B - A)$, so that

$$2|p \iff 2|(A + B); \quad \text{and}$$

$$3|p \iff 3|A.$$

If $p = X^2 + Y^2 + XY$, $X, Y \in \mathbb{N}$, then $p = (X - Y)^2 + 3XY$, so that

$$2|p \iff 2|X \text{ and } 2|Y; \quad \text{and}$$

$$3|p \iff 3|(X - Y).$$

Set

$$E_1 := \{(X, Y) \in \mathbb{N}^2 | X \text{ is odd, } Y \text{ is even}\},$$

$$E_2 := \{(X, Y) \in \mathbb{N}^2 | X, Y \text{ are odd, } Y > X\},$$

and $E := E_1 \cup E_2$. Set

$$F_1 = \{(A, B) \in \mathbb{N}^2 | A + B \text{ is odd, } A > B\},$$

$$F_2 = \{(A, B) \in \mathbb{N}^2 | A + B \text{ is odd, } A < B\},$$

and $F := F_1 \cup F_2$. Then the set

$$\{p = X^2 + Y^2 + XY | X, Y \in \mathbb{N}, X \neq Y, \ p \text{ is odd}\}$$

is uniquely parametrized by $E$, and the set

$$\{p = A^2 + 3B^2 | A, B \in \mathbb{N}, p \text{ is odd}\}$$
is by $F$. Let $\Phi : E \to F$ be defined by

$$E_1 \ni (X, Y) \mapsto (X + Y/2, Y/2) \in F_1,$$

$$E_2 \ni (X, Y) \mapsto ((Y - X)/2, (Y + X)/2) \in F_2,$$

and $\Psi : F \to E$ be by

$$F_1 \ni (A, B) \mapsto (A - B, 2B) \in E_1,$$

$$F_2 \ni (A, B) \mapsto (B - A, A + B) \in E_2.$$

Then, $\Phi \circ \Psi = \text{id}_F$ and $\Psi \circ \Phi = \text{id}_E$. Furthermore, if $\Phi(X, Y) = (A, B)$, then

$$3|(X - Y) \iff 3|A; \quad \text{and}$$

$$\gcd(X, Y) = 1 \iff \gcd(A, B) = 1.$$

This proves the equivalence of (i) and (ii).

A typical example of numbers satisfying (ii) is the hex numbers $h_n := n^2 + (n + 1)^2 + n(n + 1) = 3n^2 + 3n + 1 = (n + 1)^3 - n^3$ ($n = 1, 2, \ldots$).

2. Constructions of $N^+_\ell$ and $N^-_\ell$

Let $\ell \in \mathbb{N}$. For $\alpha \in \mathbb{Z}$, let $r_\ell(\alpha)$ denote the remainder of $\alpha$ divided by $\ell$; therefore, $r_\ell(\alpha) \in \{0, 1, \ldots, \ell - 1\}$. For $\alpha, \beta \in \mathbb{Z}$ with $\alpha < \beta$, define

$$[\alpha, \beta]_\ell := \{r_\ell(i)|i = \alpha, \alpha + 1, \ldots, \beta\}.$$

Especially, $[1, \ell]_\ell = \{0, 1, \ldots, \ell - 1\}$. An $\ell$-square matrix $M$ with entries in a set $X$ is considered as a mapping from $[1, \ell]_\ell^2$ into $X$, and written as $M = (M_{ij})_{(i,j)\in[1,\ell]_\ell^2} = (M_{ij})_{i,j}$. We also write $M_{ij} = M(i, j)$.

**Definitions.** (i) For an integer $\ell \geq 3$, a **Latin** (resp. **magic**) $\ell$-square is an $\ell$-square matrix $[1, \ell]_\ell^2 \to [1, \ell]_\ell$ (resp. an $\ell$-square bijective matrix $[1, \ell]_\ell^2 \to [1, \ell]_\ell^2$) whose restrictions to all rows and all columns are surjective (resp. are of sum $m_\ell := \ell(\ell^2 - 1)/2$).

(ii) A Latin (resp. magic) $\ell$-square is called **complete** if all $2\ell$ general
diagonals are also surjective (resp. are also of sum $m_\ell$).

Now, let $p, A, B$ satisfying (1)-(4) be fixed. Let $(a, b), (a', b') \in \{0, \ldots, A\} \times \{0, \ldots, B\}\setminus\{(0,0), (A, B)\}$ satisfy (5),(6), and $q, q'$ be given by (7). Let $N_+^\pm$, resp. $N_-^\pm$, and $N_-$ : $[1, p]^2_\ell \to [1, p]_\ell$ be defined by

\[(N_+^\pm)_{ij} := r_p(iq + j) \quad \text{(resp.)} \]
\[(N_-^\pm)_{ij} := r_p(iq' + j), \]
\[(N_-^-)_{ij} := r_p(iq + 3j), \quad \text{and} \]
\[(N_-^-)_{ij} := r_p(iq' + 3j)). \]

**Lemma 5.** Assume $A > B$. If

\[P = [0, A - 1]_\ell^2, \quad Q = [0, B - 1]_\ell \times [A, A + 3B - 1]_\ell, \]

then the image $N_+^\pm(P \cup Q) = [1, p]_\ell$.

**Proof.** As in the proof of Proposition 5 in [A], we consider an auxiliary matrix \(L = (L_{ij})_{ij} : [0, A]_{A+B} \times [0, a+b-1]_{A+B} \to [1, A+B]_{A+B}, \) defined by

\[(L_{ij}) := r_{A+B}(i(a + b) + j) \]

for $(i, j) \in [0, A]_{A+B} \times [0, a + b - 1]_{A+B}$. It follows from

\[A(a + b) - a(A + B) = 1 \]

that for $j = 0, \ldots, a + b - 2$,

\[(LA_j = L_{0,j+1}. \]

Set \(\ell := (r_{A+B}(0), r_{A+B}(a + b), \ldots, r_{A+B}((A - 1)(a + b))), \)
Because of (20), we have

\[ (\text{Image } \ell) \cup (\text{Image } s) = \{0, 1, \ldots, A + B - 1\}, \]

\[ r_{A+B}(a+b) = 1, \quad \text{and} \]

\[ s = (r_{A+B}(1), r_{A+B}((a+b) + 1), \ldots, r_{A+B}((B - 1)(a+b) + 1)). \]

By (19), \( r_{A+B}(a+b) \) coincides with the first column of \( L \), and \( s \) coincides with the first \( B \) components of the second column of \( L \). We call the numbers in \( \ell \) are of \textbf{long label} and in \( s \) of \textbf{short label}. Let \( L' \) be the restriction of \( L \) to the set \([0, A - 1]_{A+B} \times [0, a + b - 1]_{A+B} \). It follows from (19) and (20) that

\begin{equation}
\ell_j = \begin{cases} 
(u + 1, u + 2, \ldots, u + \ell), & \ell + 1 \text{ is of short label} \\
(u + 1, u + 2, \ldots, u + A), & \ell + 1 \text{ is of long label}.
\end{cases}
\end{equation}

The last row of \( L' \) have \( a + 1 \) numbers of long label, \( b - 1 \) numbers of short label and its final component is of long label. For details refer the proof of Proposition 5 in [A]. We construct vectors \( \ell_0, \ell_1, \ldots, \ell_{A+B-1} \) inductively as follows: set \( \ell_0 := (0, 1, \ldots, A - 1) \); constructed \( \ell_j = (\ldots, u) \), we set

\begin{equation}
\ell_j := \begin{cases} 
(u + 1, u + 2, \ldots, u + 3B), & j + 1 \text{ is of short label} \\
(u + 1, u + 2, \ldots, u + A), & j + 1 \text{ is of long label}.
\end{cases}
\end{equation}

Because of \( A^2 + 3B^2 = p \) we have \( \ell_{A+B-1} = (\ldots, p - 1) \). It follows that, for every \( j \in \{0, 1, \ldots, (A + 1)(a + b) - 2\} \), if \( \ell_{r_{A+B}(j)} = (\ldots, u) \), then \( \ell_{r_{A+B}(j+1)} = (r_p(u+1), \ldots) \). It follows from (22) that among \( \ell_0, \ldots, \ell_{a+b-1} \), we have \( a \) long vectors and \( b \) short ones, so that \( \ell_{a+b-1} = (\ldots, q-1) \). Hence, \( \ell_{a+b} = (q, \ldots) \). Inductively, we have \( \ell_{r_{A+B}(j(a+b)-1)} = (\ldots, r_p(jq - 1)), \)

\( \ell_{r_{A+B}(j(a+b))} = (r_p(jq), \ldots) \), for \( j = 1, \ldots, A - 1 \), so that the matrix

\[
\begin{bmatrix}
\ell_0 & \ell_1 & \ldots & \ell_{a+b-1} \\
\ell_{r_{A+B}(a+b)} & \ell_{r_{A+B}(a+b+1)} & \ldots & \ell_{r_{A+B}(2(a+b)-1)} \\
\vdots & \vdots & \ddots & \vdots \\
\ell_{r_{A+B}((A-1)(a+b))} & \ell_{r_{A+B}((A-1)(a+b)+1)} & \ldots & \ell_{r_{A+B}(A(a+b)-1)}
\end{bmatrix}
\]
coincides with \( N_+^\ast |_{[0,A-1]} \times [0,q-1] \), where \( \ell^*(A(a+b)-1) \) is \( \ell_0 |_{[0,3B-1]} \) if \( A \geq 3B \), and is \((\ell_0,\ell_1 |_{[0,3B-A-1]} )\) if \( A < 3B \) (by (20), \( r_{A+B}(A(a+b)-1) = 0 \)). It follows that
\[
N_+^\ast |_{P} = \ell(\ell_{r_{A+B}(0)}, \ell_{r_{A+B}(a+b)}, \ldots, \ell_{r_{A+B}((A-1)(a+b))})
\]
and
\[
N_+^\ast |_{Q} = \ell(\ell_{r_{A+B}(1)}, \ell_{r_{A+B}(a+b+1)}, \ldots, \ell_{r_{A+B}((B-1)(a+b)+1)}).
\]
Since the union of
\[
\{r_{A+B}(0), r_{A+B}(a+b), \ldots, r_{A+B}((A-1)(a+b))\} \quad \text{and} \quad \{r_{A+B}(1), r_{A+B}((a+b)+1), \ldots, r_{A+B}((B-1)(a+b)+1)\}
\]
coincides with
\[
(\text{Image } \ell) \cup (\text{Image } s) = \{0,1,\ldots,A+B-1\},
\]
it follows that
\[
N_+^\ast (P \cup Q) = \bigcup_{j=0}^{A+B-1} \text{Image } \ell_j = \{0,\ldots,p-1\},
\]
as desired.

**Lemma 6.** Assume \( B > A \). If
\[
Q = [0, B-1] \times [0,3B-1], \quad P = [0, A-1] \times [3B, 3B+A-1],
\]
then the image \( N_+^\ast (P \cup Q) = [1,p] \).

**Proof.** Let a matrix \( L : [0, B]_{A+B} \times [0,a'+b'-1]_{A+B} \rightarrow [1, A+B]_{A+B} \) be defined by
\[
L_{ij} := r_{A+B}(i(a'+b')+j)
\]
for \((i,j) \in [0, B]_{A+B} \times [0,a'+b'-1]_{A+B}\). Since
\[
-b'(B+A) + B(a' + b') = 1
\]
we have for \( j = 0, \ldots, a' + b' - 2 \),

\[
(25) \quad L_{Bj} = L_{0,j+1}.
\]

Set

\[
\ell := (r_{A+B}(0), r_{A+B}(a' + b'), \ldots, r_{A+B}((B - 1)(a' + b'))),
\]

\[
s := (r_{A+B}(B(a' + b')), r_{A+B}((B+1)(a' + b')), \ldots, r_{A+B}((B+A-1)(a' + b'))).
\]

By (24),

\[
(\text{Image } \ell) \cup (\text{Image } s) = \{0, 1, \ldots A + B - 1\},
\]

\[
r_{A+B}(B(a' + b')) = 1, \quad \text{and}
\]

\[
s = (r_{A+B}(1), r_{A+B}((a' + b') + 1), \ldots, r_{A+B}((A - 1)(a' + b') + 1)).
\]

By (23), \( ^t(\ell, r_{A+B}(B(a' + b'))) \) coincides with the first column of \( L \), and \( ^t s \) coincides with the first \( A \) components of the second column of \( L \). As before we call the numbers in \( \ell \) are of \textbf{long label} and in \( s \) of \textbf{short label}. Let \( L' \) be the restriction of \( L \) to the set \([0, B - 1]_{A+B} \times [0, a' + b' - 1]_{A+B} \). We have

\[
(26) \quad \left\{ \begin{array}{l}
\text{in every row of } L', \text{ except the last one, there are } \\
b' \text{ numbers of long label and } a' \text{ numbers of short label.}
\end{array} \right.
\]

As before, we set \( \ell_0 := (0, 1, \ldots, 3B - 1) \). Constructed \( \ell_j = (\ldots, u) \), we set

\[
\ell_{j+1} := \left\{ \begin{array}{l}
(u + 1, u + 2, \ldots, u + A), \quad j + 1 \text{ is of short label} \\
(u + 1, u + 2, \ldots, u + 3B), \quad j + 1 \text{ is of long label}
\end{array} \right.
\]

for \( j = 0, \ldots, A + B - 2 \), so that \( \ell_{A+B-1} = (\ldots, p - 1) \). It follows from (26) that among \( \ell_0, \ldots, \ell_{a'+b'-1} \), we have \( b' \) long vectors and \( a' \) short ones, so that \( \ell_{a'+b'-1} = (\ldots, q' - 1) \), and \( \ell_{a'+b'} = (q', \ldots) \). Hence \( \ell_{r_{A+B}(j(a'+b')-1)} = (\ldots, r_p(jq' - 1)) \), \( \ell_{r_{A+B}(j(a'+b'))} = (r_p(jq'), \ldots) \), for \( j = 1, \ldots, B - 1 \). As before, we have

\[
N^+_Q = ^t(\ell_{r_{A+B}(0)}, \ell_{r_{A+B}(a'+b')}, \ldots, \ell_{r_{A+B}((B-1)(a'+b'))})
\]

and

\[
N^+_P = ^t(\ell_{r_{A+B}(1)}, \ell_{r_{A+B}(a'+b'+1)}, \ldots, \ell_{r_{A+B}((A-1)(a'+b')+1)}).
\]
Since the union of
\[ \{r_{A+B}(0), r_{A+B}(a'+b'), \ldots, r_{A+B}((B-1)(a'+b'))\} \]
and
\[ \{r_{A+B}(1), r_{A+B}((a'+b')+1), \ldots, r_{A+B}((A-1)(a'+b')+1)\} \]
coincides with
\[ (\text{Image } \ell) \cup (\text{Image } s) = \{0, 1, \ldots, A + B - 1\}, \]
we have
\[ N_+^+(P \cup Q) = \bigcup_{j=0}^{A+B-1} \text{Image } \ell_j = \{0, \ldots, p-1\}, \]
as desired.

For \((u, v) \in \mathbb{Z}^2\), we denote by \(T_{(u, v)}\) the \((u, v)\)-translation of the space \([1, p]_p^2\), that is \([1, p]_p^2 \ni (i, j) \mapsto (r_p(i+u), r_p(j+v)) \in [1, p]_p^2\).

**Lemma 7.** Let \(D \subset [1, p]_p^2\) with \(\text{Card } D = p\). For \((u, v) \in \mathbb{Z}^2\), set \(T := T_{(u, v)}\). Let \(N\) be one of \(N_+^+, N_-^+, N_+^-, N_-\).
If \(N(D) = [1, p]_p\), then \(N(T(D)) = [1, p]_p\).

**Proof.** We have
\[
(N_+^+)_{T(i,j)} - (N_+^+)_{ij} = r_p(r_p(i+u)q + r_p(j+v)) - r_p(iq+j) \\
\equiv (i+u)q + (j+v) - (iq+j) \pmod p \\
\equiv uq + v.
\]
Hence
\[
(N_+^+)_{T(i,j)} = r_p((N_+^+)_{ij} + uq + v),
\]
so that
\[
N_+^+(T(D)) = \{(N_+^+)_{kl}(k, \ell) \in T(D)\} \\
= \{(N_+^+)_{T(i,j)}|(i, j) \in D\} \\
= \{r_p((N_+^+)_{ij} + uq + v)|(i, j) \in D\} \\
= r_p\{(N_+^+)_{ij}|(i, j) \in D\} + uq + v)
Lupe Latin squares of order odd, 3-odd, \( A^2 + 3B^2 \) with \( \gcd(A, B) = 1 \)

\[
= r_p([1, p]_p + uq + v) \\
= r_p(\{i + uq + v | i \in [1, p]_p\}) \\
= [1, p]_p.
\]

The assertion for \( N^+_1 \) has been proved. Similarly, we have

\[
(N^+_1)_{T(i, j)} = r_p((N^+_1)_{ij} + uq' + v), \\
(N^-_1)_{T(i, j)} = r_p((N^-_1)_{ij} + uq + 3v), \\
(N^-_1)_{T(i, j)} = r_p((N^-_1)_{ij} + uq' + 3v).
\]

From these, the assertions for \( N^+_1, N^-_1, N^- \) follow.

**Lemma 8.** Assume \( B > A \). If

\[
Q = [0, B - 1]_p \times [0, 3B - 1]_p, \quad P = [B - A, B - 1]_p \times [3B, 3B + A - 1]_p,
\]

then the image \( N^+_1(P \cup Q) = [1, p]_p \).

**Proof.** By Lemma 7, to prove the assertion, we may show that if

\[
Q' = [1, B]_p \times [0, 3B - 1]_p, \quad P' = [B - A + 1, B]_p \times [3B, 3B + A - 1]_p
\]

then \( N^+_1(P' \cup Q') = [1, p]_p \). Let \( R_0 : [1, p]^2_+ \rightarrow [1, p]^2_+ \) be the transformation given by

\[
(27) \quad [1, p]^2_+ \ni (i, j) \mapsto (r_p(p - i), j) \in [1, p]^2_+.
\]

Let \( CP \) be the cut-and-paste between the first row and the remainder of the space \([1, p]^2_+\), that is \([1, p]^2_+ \ni (i, j) \mapsto (r_p(i - 1), j) \in [1, p]^2_+ \), and \( R \) be the reflection of the space \([1, p]^2_+\) w.r.t. the center row of that space, that is \([1, p]^2_+ \ni (i, j) \mapsto (p - 1 - i, j) \in [1, p]^2_+ \). Since \( R_0 = R \circ CP \), the geometry of the transformations \( CR \) and \( R \) implies \( R_0(Q' \cup P') = Q_0 \cup P_0 \), where

\[
Q_0 = [p - B, p - 1]_p \times [0, 3B - 1]_p, \quad P_0 = [p - B, p - B + A - 1]_p \times [3B, 3B + A - 1]_p.
\]

Since \( R_0 \circ R_0 = \text{id} \),

\[
(28) \quad Q' \cup P' = R_0(Q_0 \cup P_0).
\]
If
\[
N_+^+ := N_+^+ \circ R_0,
\]
then in view of definitions (15),(16), and (27) we have
\[
N_+^+ = N_+^+.
\]
It follows from (28),(29),(30) that
\[
N_+^+(Q' \cup P') = N_+^+(R_0(Q_0 \cup P_0)) = N_+^+(Q_0 \cup P_0).
\]
If
\[
Q_1 = [0, B-1]_p \times [0, 3B-1]_p, \quad P_1 = [0, A-1]_p \times [3B, 3B + A-1]_p,
\]
then Lemma 6 implies $N_+^+(Q_1 \cup P_1) = [1, p]_p$. Since $Q_0 \cup P_0$ is a translation of $Q_1 \cup P_1$, Lemma 7 implies $N_+^+(Q_0 \cup P_0) = [1, p]_p$; combining (31) we have $N_+^+(Q' \cup P') = [1, p]_p$, as desired.

**Lemma 9.** Assume $A > B$. If

\[
P = [0, A-1]_p^2, \quad Q = [A-B, A-1]_p \times [A, A+3B-1]_p,
\]
then the image $N_+^+(P \cup Q) = [1, p]_p$.

**Proof.** By Lemma 7, we may show that if

\[
P' = [1, A]_p \times [0, A-1]_p, \quad Q' = [A-B+1, A]_p \times [A, A+3B-1]_p,
\]
then $N_+^+(P' \cup Q') = [1, p]_p$. As in the proof of Lemma 8, if

\[
P_0 = [p-A, p-1]_p \times [0, A-1]_p, \quad Q_0 = [p-A, p-A+B-1]_p \times [A, A+3B-1]_p,
\]
then $N_+^+(P' \cup Q') = N_+^+(P_0 \cup Q_0)$. If

\[
P_1 = [0, A-1]_p^2, \quad Q_1 = [0, B-1]_p \times [A, A+3B-1]_p,
\]
then $P_0 \cup Q_0$ is a translation of $P_1 \cup Q_1$; therefore Lemma 5 implies $N_+^+(P' \cup Q') = N_+^+(P_1 \cup Q_1) = [1, p]_p$, as desired.
Lemma 10. We have:

(32) \[ N_+^+ \circ T_{(-A,3B)} = N_+^+ \], \[ N_+^+ \circ T_{(B,A)} = N_+^+ \];
(33) \[ N_+^+ \circ T_{(-B,A)} = N_+^+ \], \[ N_+^+ \circ T_{(A,3B)} = N_+^+ \].

Proof. By (9) we have \( qA \equiv 3B, qB \equiv -A \pmod{p} \), so that (32) follows. In fact,
\[ N_+^+ \circ T_{(-A,3B)}(i, j) = r_p(q(i - A) + j + 3B) = r_p(qi + j) = N_+^+(i, j), \]
etc. By (10) we have \( q'A \equiv -3B, q'B \equiv A \pmod{p} \), so that (33) follows.

q.e.d.

Proposition 11. If
\[ P = [0, A - 1]^2_p, \quad Q = [0, B - 1]_p \times [A, A + 3B - 1]_p, \]
then \( N_+^+(P \cup Q) = [1, p]_p \).

Proof. When \( A > B \), the assertion is Lemma 5. Assume \( A < B \). By Lemma 8, combining Lemma 7 we have \( N_+^+(P' \cup Q) = [1, p]_p \), where
\[ P' = [B - A, B - 1]_p \times [A + 3B, A + 3B + A - 1]_p. \]
Since \( P' = T_{(-A,3B)} \circ T_{(B,A)}(P) \), (32) implies \( N_+^+(P \cup Q) = N_+^+(P' \cup Q) = [1, p]_p \), as desired.

Proposition 12. If
\[ P = [0, A - 1]^2_p, \quad Q = [A - B, A - 1]_p \times [A, A + 3B - 1]_p, \]
then \( N_+^+(P \cup Q) = [1, p]_p \).

Proof. When \( B < A \), the assertion is Lemma 9. Assume \( B > A \). By Lemma 6 combining Lemma 7 we get \( N_+^+(P \cup Q') = [1, p]_p \), where
\[ Q' = [0, B - 1]_p \times [p - 3B, p - 1]_p. \]
Since \( Q = T_{(-B,A)} \circ T_{(A,3B)}(Q') \), (33) implies \( N_+^+(P \cup Q) = N_+^+(P \cup Q') = [1, p]_p \), as desired.
3. Lupe properties of Latin squares and magic squares

Let $p, A, B, a, b, a', b', q,$ and $q'$ be as in the preceding section. Set

$$d := \frac{p - (A + B)}{2} = \frac{A^2 + 3B^2 - (A + B)}{2} = \frac{A(A - 1)}{2} + B^2 + B(B - 1) \in \mathbb{N},$$

and $d' := d - B$.

**Definition.** A pair $(P, Q)$ of an $A$-square

$$P = [\alpha, \alpha + A - 1]_p \times [\beta, \beta + A - 1]_p$$

and a $(B, 3B)$-rectangle

$$Q = [\gamma, \gamma + B - 1]_p \times [\delta, \delta + 3B - 1]_p$$

(resp. $(3B, B)$-rectangle

$$Q = [\gamma, \gamma + 3B - 1]_p \times [\delta, \delta + B - 1]_p)$$

in $[1, p]_p^2$ is called $(A, (B, 3B))$-antipodal (resp. $(A, (3B, B))$-antipodal) if

$$\gamma - \alpha \equiv A + d, \quad \delta - \beta \equiv A + d'(\text{mod } p)$$

(resp.

$$\gamma - \alpha \equiv A + d', \quad \delta - \beta \equiv A + d(\text{mod } p)),$$

that is if the bidistance between $P$ and $Q$ is $(d, d')$ (resp. $(d', d))$.

**Definition.** A $p$-square matrix $M : [1, p]_p^2 \rightarrow [1, p]_p^2$ is called of $(1, 3)$-Lupe (resp. $(3, 1)$-Lupe) property if for any $(A, (B, 3B))$-antipodal (resp. $(A, (3B, B))$-antipodal ) pair $(P, Q)$ in $[1, p]_p^2$, the restriction of $M$ to $P \cup Q$ is surjection.

A square matrix $M : [1, p]_p^2 \rightarrow [1, p^2]_{p^2}$ is called of $(1, 3)$-Lupe (resp. $(3, 1)$-Lupe) property if for any $(A, (B, 3B))$-antipodal (resp. $(A, (3B, B))$-antipodal ) pair $(P, Q)$ in $[1, p]_p^2$, the restriction of $M$ to $P \cup Q$ possesses the sum $m_p = p(p^2 - 1)/2$. 
We note that for a \( p \)-square matrix \( M : [1, p]_p^2 \to [1, p]_p \) or \( M : [1, p]_p^2 \to [1, p^2]_{p^2} \), \( M \) is of \((1, 3)\)-Lupe property if and only if \(^t M \) is of \((3, 1)\)-Lupe property.

**Lemma 13.** It holds that \((q + 1)d \equiv -2B, \ (q' + 1)d \equiv -A + B \pmod{p}\).

**Proof.** By definition of \( d \) as well as (9), we have

\[
(q + 1)d = \frac{1}{2}(q + 1)(p - (A + B))
\]

\[
= \frac{1}{2}((q + 1)p - q(A + B) - (A + B))
\]

\[
= \frac{1}{2}((q + 1)p - (ap + 3B + bp - A) - (A + B))
\]

\[
= -2B + \frac{1}{2}(q + 1 - (a + b))p,
\]

so that \(2((q + 1)d + 2B) = (q + 1 - (a + b))p\). Since \(\gcd(p, 2) = 1\), \(2\mid (q + 1 - (a + b))\). It follows that \((q + 1)d \equiv -2B \pmod{p}\). Similarly, using (10) we have

\[
(q' + 1)d = \frac{1}{2}(q' + 1)(p - (A + B))
\]

\[
= B - A + \frac{1}{2}(q' + 1 - (a' + b'))p,
\]

so that \(2((q' + 1)d - B + A) = (q' + 1 - (a' + b'))p\). Similar argument implies \(2((q' + 1) - (a' + b'))\), so that \((q' + 1)d \equiv -A + B \pmod{p}\), as desired.

**Lemma 14.** It holds that

\[
\gcd(q + 1, p) = 1, \quad \gcd(q' + 1, p) = 1;
\]

\[
\gcd(q - 1, p) = 1, \quad \gcd(q' - 1, p) = 1;
\]

\[
\gcd(q + 3, p) = 1, \quad \gcd(q' + 3, p) = 1;
\]

\[
\gcd(q - 3, p) = 1, \quad \gcd(q' - 3, p) = 1.
\]

**Proof.** By (9) we have

\[
(q + 1)A \equiv 3B + A \pmod{p},
\]
(35) \((q + 1)B \equiv B - A \pmod{p}\).

Since
\[
gcm(3B + A, B - A) = gcm(4B, B - A) = gcm(B, B - A) \ (\text{because } B - A \text{ is odd}) = gcm(B, -A) = gcm(A, B) = 1,
\]
there exist \(\ell, m \in \mathbb{Z}\) such that \(\ell(3B + A) + m(B - A) = 1\). Substituting (34), (35), we have
\[
\ell(q + 1)A + m(q + 1)B \equiv 1 \pmod{p}.
\]
It follows that \(gcm(q + 1, p) = 1\).

By (10) we have
\[
(q' + 1)A \equiv -3B + A, \quad (q' + 1)B \equiv A + B \pmod{p}.
\]
Since
\[
gcm(-3B + A, A + B) = gcm(-4B, A + B) = gcm(B, A + B) \ (\text{because } A + B \text{ is odd}) = gcm(A, B) = 1,
\]
similar argument as in the first part implies \(gcm(q' + 1, p) = 1\).

By (9) we have
\[
(q + 3)A \equiv 3(A + B), \quad (q + 3)B \equiv -A + 3B \pmod{p}.
\]
Since
\[
gcm(3(A + B), -A + 3B) = gcm(3(A + B), -4A) = gcm(3(A + B), A) \ (\text{because } 3(A + B) \text{ is odd}) = gcm(A + B, A) \ (\text{because } A \text{ is 3-odd}) = gcm(A, B) = 1,
\]
similarly we have $\gcd(q + 3, p) = 1$

By (10) we have

$$(q' + 3)A \equiv 3(A - B), \quad (q' + 3)B \equiv A + 3B \pmod{p}.$$ 

Since

$$\gcd(3(A - B), A + 3B) = \gcd(4A, A + 3B) = \gcd(A, A + 3B) \quad \text{(because A + 3B is odd)}$$

$$= \gcd(A, 3B) = \gcd(A, B) = 1 \quad \text{(because A is 3-odd)},$$

similarly we have $\gcd(q' + 3, p) = 1$.

The other four assertions follow from the facts

$$q - 1 \equiv -(q' + 1), \quad q' - 1 \equiv -(q + 1), \quad q - 3 \equiv -(q' + 3), \quad q' - 3 \equiv -(q + 3) \pmod{p}$$

and the first four results, as desired.

**Proposition 15.** The $p$-squares $N^+_p, N^+_q, N^-_p, N^-_q$ are complete Latin.

**Proof.** Since $\gcd(q, p) = 1$, $\gcd(q', p) = 1$, and $\gcd(3, p) = 1$, definitions (15)-(18) imply that $N^+_p, N^+_q, N^-_p, N^-_q$ are Latin squares.

Since for $i, j \in [1, p]$ it holds that

$$(N^+_p)_{ir}, r_{p(i+j)} = r_p(iq + (i + j)) = r_p(i(q + 1) + j),$$

$$(N^+_{q'})_{ir}, r_{p(i+j)} = r_p(iq' + (i + j)) = r_p(i(q' + 1) + j),$$

$$(N^-_p)_{ir}, r_{p(i+j)} = r_p(iq + 3(i + j)) = r_p(i(q + 3) + 3j),$$

$$(N^-_{q'})_{ir}, r_{p(i+j)} = r_p(iq' + 3(i + j)) = r_p(i(q' + 3) + 3j),$$

$$(N^+_p)_{ir}, r_{p(-i+j)} = r_p(iq + (-i + j)) = r_p(i(q - 1) + j),$$

$$(N^+_{q'})_{ir}, r_{p(-i+j)} = r_p(iq' + (-i + j)) = r_p(i(q' - 1) + j),$$

$$(N^-_p)_{ir}, r_{p(-i+j)} = r_p(iq + 3(-i + j)) = r_p(i(q - 3) + 3j),$$

$$(N^-_{q'})_{ir}, r_{p(-i+j)} = r_p(iq' + 3(-i + j)) = r_p(i(q' - 3) + 3j),$$

Lemma 14 implies that $N^+_p, N^+_q, N^-_p, N^-_q$ are complete. q.e.d.
Proposition 16. The $p$-squares $N^+_N$, $N^-_N$ are of $(1, 3)$-Lupe property.

Proof. By virtue of Lemma 7, to prove $(1, 3)$-Lupe property of $N := N^+_N$ or $N^-_N$ we may show that if

$$P = [0, A - 1]_p^2, \quad Q = [A + d, A + d + B - 1]_p \times [A + d', A + d' + 3B - 1]_p,$$

then $N(P \cup Q) = [1, p]_p$.

By Proposition 11, if

$$Q_1 = [0, B - 1]_p \times [A, A + 3B - 1]_p,$$

then $N(P \cup Q_1) = [1, p]_p$. We note that $Q = T_{(d + A, d - B)}(Q_1)$. We also note that $N^+_N \circ T_{(d + A, d - B)} = N^+_N$. In fact,

$$N^+_N \circ T_{(d + A, d - B)}(i, j) - N^+_N(i, j) = r_p(q(i + d + A) + (j + d - B)) - r_p(qi + j)
\quad = r_p(q(d + A) + d - B)
\quad = r_p(d(q + 1) + Aq - B)
\quad = r_p(-2B + 3B - B) = 0.$$

It follows that

$$N^+_N(Q_1) = N^+_N \circ T_{(d + A, d - B)}(Q_1) = N^+_N(Q).$$

Thus,

$$N^+_N(P \cup Q) = N^+_N(P) \cup N^+_N(Q) = N^+_N(P) \cup N^+_N(Q_1) = N^+_N(P \cup Q_1) = [1, p]_p.$$

On the other hand, by Proposition 12 if

$$Q_2 = [A - B, A - 1]_p \times [A, A + 3B - 1]_p,$$

then $N(P \cup Q_2) = [1, p]_p$. We note that $Q = T_{(d + B, d - B)}(Q_2)$. We also note that $N^-_N \circ T_{(d + B, d - B)} = N^-_N$. In fact,

$$N^-_N \circ T_{(d + B, d - B)}(i, j) - N^-_N(i, j) = r_p(q'(i + d + B) + (j + d - B)) - r_p(q'i + j)
\quad = r_p(q'(d + B) + d - B)
\quad = r_p(d(q' + 1) + Bq' - B)
\quad = r_p(-A + B + A - B) = 0.$$
It follows that
\[ N^+_+(Q_2) = N^-_+ \circ T_{(d+B,d-B)}(Q_2) = N^-_+ (Q). \]
Thus,
\[ N^+_+(P \cup Q) = N^+_+(P) \cup N^+_+(Q_2) = N^+_+(P) \cup N^+_+(Q_2) = N^+_+(P \cup Q_2) = [1,p]_p, \]
as desired.

Because of \( \gcd(q,p) = 1 \), \( \gcd(q',p) = 1 \), the functions \( y, y' : [1,p]_p \rightarrow [1,p]_p \) defined by
\[
\begin{align*}
y(j) &:= r_p(jq), \\
y'(j) &:= r_p(jq')
\end{align*}
\]
are permutations on \([1,p]_p\).

**Proposition 17.** If \( y, y' \) are the permutations defined by (36), (37), then
\[ y' \circ N^+_+ = \iota N_-, \quad y \circ N^+_+ = \iota N_+^- . \]

**Proof.** We have
\[
\begin{align*}
y'(i,j) &:= r_p(jq + j) \\
&= r_p((iq + j)q') \\
&= r_p(iqq' + jq') \\
&= r_p((3i + jq') (\text{ by (14)}) \\
&= \iota(N^-_+)(i,j).
\end{align*}
\]
Similarly, we have
\[
\begin{align*}
y(i,j) &:= r_p(iq' + j) \\
&= r_p((iq' + j)q) \\
&= r_p(iqq' + jq) \\
&= r_p((3i + jq) (\text{ by (14)}) \\
&= \iota(N^-_+)(i,j),
\end{align*}
\]
Proposition 18. The $p$-squares $N_+^-$, $N_-^-$ possess $(3, 1)$-Lupe property.

Proof. By Proposition 16, the $p$-squares $y' \circ N_+^+$, $y \circ N_+^-$ possess $(1, 3)$-Lupe property, so that by Proposition 17, the $p$-squares $N_-, N_-$ possess $(3, 1)$-Lupe property.

Proposition 19. The product

$$N_+^+ \times N_-^+ := ([1, p]_p^2 \ni (i, j) \mapsto (N_+^+(i, j), N_-^+(i, j)) \in [1, p]_p^2)$$

is an Euler square, that is $\text{Image}(N_+^+ \times N_-^+) = [1, p]_p^2$.

Proof. Let $i \in [1, p]_p$. Then for $j \in [1, p]_p$, we have

$$N_+^+(i, j) = 0 \iff qi + j \equiv 0 \pmod{p} \iff j \equiv -qi \pmod{p} \iff j \equiv q'i \pmod{p}.$$  

Then, $N_+^+(i, q'i) = 0$ and $N_+^+(i, q'i) = r_p(2q'i)$. Since $p$ is odd, $\gcd(2q', p) = \gcd(q', p) = 1$, so that

$$\{(N_+^+ \times N_-^+)(i, iq') | i \in [1, p]_p\} = \{0\} \times [1, p]_p.$$  

For $v \in [1, p]_p$, we have

$$N_+^+(i, iq' + v) = r_p(N_+^+(i, iq') + v) = v,$$

$$N_-^+(i, iq' + v) = r_p(N_-^+(i, iq') + v) = r_p(2q'i + v).$$  

Thus,

$$\{(N_+^+ \times N_-^+)(i, iq' + v) | i \in [1, p]_p\} = \{v\} \times [1, p]_p,$$

so that $\text{Image}(N_+^+ \times N_-^+)$ contains

$$\bigcup_{v \in [1, p]_p} (\{v\} \times [1, p]_p) = [1, p]_p^2,$$

as desired.
Proposition 20. The product $N_+^- \times N_-^-$ is an Euler square.

Proof. Let $j \in [1, p]$. For $i \in [1, p]$, we have

$$N_+^-(i, j) = 0 \iff qi + 3j \equiv 0 \pmod{p}$$
$$\iff q(i - qj) \equiv 0 \pmod{p} \quad \text{(by (13))}$$
$$\iff i \equiv qj \pmod{p} \quad \text{(by gcm}(q, p) = 1).$$

For $v \in [1, p]$, it follows that

$$N_+^-(qj + v, j) = N_+^-(qj, j) + r_p(vq) = r_p(vq),$$
$$N_-^-(qj + v, j) = r_p((qj + v)q' + 3j) = r_p(6j + vq').$$

Since gcm$(6, p) = 1$, it follows that

$$\{(N_+^- \times N_-^-)(qj + v, j) | j \in [1, p]\} = \{r_p(vq)\} \times [1, p].$$

It follows that $\text{Image}(N_+^- \times N_-^-)$ contains

$$\bigcup_{v \in [1, p]} \{r_p(vq)\} \times [1, p] = [1, p]^2,$$

as desired.

Theorem 21. Let $\theta, \psi : [1, p] \to [1, p]$ be permutations with $\theta(0) = 0, \psi(0) = 0$. If $N_+^+, N_-^+ : [1, p]^2 \to [1, p]$ are defined by

$$(N_+^+)_{ij} := \theta(r_p(iq + j)),
(N_-^+)_{ij} := \psi(r_p(iq' + j)),$$

then the $p$-squares $pN_+^+ + N_+^-$ and $N_+^+ + pN_-^-$ are complete $p$-magic squares of $(1, 3)$-Lupe property.

If $N_+^-, N_-^- : [1, p]^2 \to [1, p]$ are defined by

$$(N_+^-)_{ij} := \theta(r_p(iq + 3j)),
(N_-^-)_{ij} := \psi(r_p(iq' + 3j)),$$
then the $p$-squares $pN_++N_-$ and $N_++pN_-$ are complete $p$-magic squares of $(3,1)$-Lupe property.

**Proof.** Set $M^+ := pN_++N_-$ or $:= N_++pN_-$, and $M^- := pN_--N_-$ or $:= N_--pN_-$. By Proposition 19 combining Proposition 15, $M^+$ becomes a complete magic square. Proposition 20 as well as Proposition 15 implies that $M^-$ becomes a complete magic square. By Proposition 16 $M^+$ is of $(1,3)$-Lupe property and by Proposition 18 $M^-$ is of $(3,1)$-Lupe property. The proof is complete.

**References**


Department of Mathematics
University of Toyama
Gofuku, Toyama 930-8555
JAPAN
Email: azuk@sci.u-toyama.ac.jp

(Received November 4, 2010)