Properties of Magic Squares of Squares

Landon W. Rabern
Washington University, landonrabern@hotmail.com

Follow this and additional works at: https://scholar.rose-hulman.edu/rhumj

Recommended Citation
Available at: https://scholar.rose-hulman.edu/rhumj/vol4/iss1/3
Properties of Magic Squares of Squares

Landon W. Rabern
1120 NW Harlan St.
Roseburg, OR 97470
landonrabern@hotmail.com

July 2002

A problem due to Martin LaBar is to find a 3x3 magic square with 9 distinct perfect square entries or prove that such a magic square cannot exist (LaBar [1]). This problem has been tied to various domains including arithmetic progressions, rational right triangles, and elliptic curves (Robertson [2]). However, there are some interesting properties that can be derived without ever leaving the domain of magic squares. I will assume that a solution exists and prove properties of such a solution. Any solution must have the form

\[
\begin{array}{ccc}
  a^2 & b^2 & c^2 \\
  d^2 & e^2 & f^2 \\
  g^2 & h^2 & s^2 \\
\end{array}
\]

If \( M \) denotes the magic number, then \( M \) is the sum of each row, column, or main diagonal. We know from Gardner [3] that \( M \) must equal three times the middle square, so \( M = 3e^2 \).

Let \( t \) be the greatest common divisor of \( a^2, b^2, c^2, d^2, e^2, f^2, g^2, h^2 \) and \( s^2 \). If \( t \neq 1 \) then \( t \) is a square, thus we can divide all entries by \( t \) to produce a new solution with a smaller magic number (\( M/t \)). For this reason, it will be assumed throughout this paper that the entries are relatively prime (\( t = 1 \)).

**Theorem 1.1** All entries of the magic square must be odd.

Proof: Using the fact that the the entries on the left side of the square must sum to \( M \) we get

\[
a^2 + d^2 + g^2 = M = 3e^2
\]

Hence \( a^2 + g^2 = 3e^2 - d^2 \), and in particular,

\[
a^2 + g^2 \equiv 3e^2 - d^2 \pmod{4}
\]

With \( e \) odd and \( d \) even, we have \( a^2 + g^2 \equiv 3 - 0 \equiv 3 \pmod{4} \). Taking \( e \) even and \( d \) odd gives \( a^2 + g^2 \equiv 0 - 1 \equiv -1 \equiv 3 \pmod{4} \). This is impossible since
$$a^2 + g^2 \equiv 0 \text{ or } 2 \pmod{4}$$. Therefore, $e$ and $d$ must have the same parity. Both $e$ and $d$ odd gives $a^2 + g^2 \equiv 3 - 1 \equiv 2 \pmod{4}$. This implies that $a$ and $g$ must be odd. Both $e$ and $d$ even gives $a^2 + g^2 \equiv 0 - 0 \equiv 0 \pmod{4}$. This implies that $a$ and $g$ must be even. Thus $a \equiv g \equiv e \equiv d \pmod{2}$.

Arguing in a similar fashion for the other sides of the square we find that $a \equiv b \equiv c \equiv d \equiv e \equiv f \equiv g \equiv h \equiv s \pmod{2}$. Hence, all entries are odd. ■

Using the rows, columns and main diagonals that pass through the center of the square we have

$$a^2 + e^2 + s^2 = d^2 + c^2 + f^2 = b^2 + e^2 + h^2 = g^2 + e^2 + c^2 = 3e^2$$

from which it follows that

$$a^2 + s^2 = d^2 + f^2 = b^2 + h^2 = g^2 + c^2 = 2e^2$$

We can now prove the following theorem.

**Theorem 1.2** The only prime divisors of $e$ are of the form $p \equiv 1 \pmod{4}$.

Proof: We just need to show that no prime $p \equiv 3 \pmod{4}$ can divide $e$. We use the fact that the ring of Gaussian integers $\mathbb{Z}[i]$ is a Unique Factorization Domain (UFD). Factoring the left side of $a^2 + s^2 = 2e^2$ in $\mathbb{Z}[i]$, we get $(a + si)(a - si) = 2e^2$. Given an odd prime $p \in \mathbb{Z}$, then $p$ is prime in $\mathbb{Z}[i]$ if and only if $p \equiv 3 \pmod{4}$ (See Lemma 1.1 in the Appendix). Thus, assume we have a $p$ such that $p \equiv 3 \pmod{4}$ and $p \mid e$. Then we must have either $p \mid (a + si)$ or $p \mid (a - si)$. If $p \mid (a + si)$, then $a + si = pk$ and by complex conjugation $a - si = pk = \overline{p}k$. Hence $p \mid (a - si)$. But then $p$ must also divide their sum and difference: $p \mid 2si$ and $p \mid 2a$. Hence $p \mid s$ and $p \mid a$ since $p$ is odd and real.

Similarly, $p \mid d$, $p \mid f$, $p \mid b$, $p \mid h$, $p \mid g$, and $p \mid c$. Hence, $p$ divides every entry which is impossible. ■

**Theorem 1.3** If a prime $p \equiv 3, 5 \pmod{8}$ divides a non-center entry then $p$ also divides the center and the other entry in that line.

Proof: Without loss of generality we prove the result for the $a, e, s$ diagonal. We use the fact that the ring $\mathbb{Z}[\sqrt{2}]$ is a UFD. Given an odd prime $p \in \mathbb{Z}$, then $p$ is prime in $\mathbb{Z}[\sqrt{2}]$ if and only if $p \equiv 3, 5 \pmod{8}$ (See Lemma 1.2 in the Appendix).

Since $a^2 + s^2 = 2e^2$ implies $a^2 = -(s^2 - 2e^2)$, we can factor the right side of this equation in $\mathbb{Z}[\sqrt{2}]$ to get

$$a^2 = -(s + e\sqrt{2})(s - e\sqrt{2})$$

2
If $p \mid a$ and $p \equiv 3,5 \pmod{8}$, then either $p \mid (s + e\sqrt{2})$ or $p \mid (s - e\sqrt{2})$. If $p \mid (s + e\sqrt{2})$, then $s + e\sqrt{2} = pk$, and by conjugation $s - e\sqrt{2} = p\overline{k}$. Hence $p \mid (s - e\sqrt{2})$. Thus $p$ divides their sum and difference: $p \mid 2s$ and $p \mid 2e\sqrt{2}$. Hence $p \mid s$ and $p \mid e$ since $p$ is odd and rational. ■

**Corollary 1.1** No prime $p \equiv 3 \pmod{8}$ divides any entry.

Proof: If $p$ divides some non-center entry, then by Theorem 1.3, $p$ divides $e$. But from Theorem 1.2, we know that $p$ cannot divide $e$ since $p \equiv 3 \pmod{8} \Rightarrow p \equiv 3 \pmod{4}$. ■

Gardner [3] has shown that given any 3x3 magic square of distinct positive integers, there are three positive integers $x, y, z$ so that the magic square can be written in the form

$$
\begin{array}{ccc}
x + y + 2z & x & x + 2y + z \\
x + 2y & x + y + z & x + 2z \\
x + z & x + 2y + 2z & x + y
\end{array}
$$

Looking at this we quickly see that $d^2 + h^2 = 2c^2$ with similar relations holding for the other corner entries. This relation can be stated as

Twice the corner entry equals the sum of the two middle-side entries that are not adjacent to the corner.

We can now prove the following theorem.

**Theorem 1.4** No prime $p \equiv 5 \pmod{8}$ divides a middle-side entry.

Proof: Without loss of generality, let the middle-side entry be $d^2$. Again, we use the fact that the ring $\mathbb{Z}[\sqrt{2}]$ is a UFD. Given an odd prime $p \in \mathbb{Z}$, then $p$ is prime in $\mathbb{Z}[\sqrt{2}]$ if and only if $p \equiv 3, 5 \pmod{8}$ (See Lemma 1.2 in the Appendix).

Since $d^2 + h^2 = 2c^2$ implies $d^2 = -(h^2 - 2c^2)$, we can factor the right side of this equation in $\mathbb{Z}[\sqrt{2}]$ to get

$$
d^2 = -(h + c\sqrt{2})(h - c\sqrt{2})
$$

If $p \mid d$ and $p \equiv 5 \pmod{8}$ then either $p \mid (h + c\sqrt{2})$ or $p \mid (h - c\sqrt{2})$. If $p \mid (h + c\sqrt{2})$, then $h + c\sqrt{2} = pk$ and by conjugation $h - c\sqrt{2} = p\overline{k}$. Hence $p \mid (h - c\sqrt{2})$. Thus $p$ divides their sum and difference: $p \mid 2h$ and $p \mid 2c\sqrt{2}$. Hence $p \mid h$ and $p \mid c$ since $p$ is odd and rational. Since $p \mid h$ we can use the same argument to show that $p \mid f$ and $p \mid a$. But then, since $p \mid f$, we can use the same argument again to show that $p \mid b$ and $p \mid g$. Since $p$ divides both $a$ and $s, p$ must also divide $e$. Hence $p$ divides all entries, which is impossible. ■

**Theorem 1.5** If a prime $p \equiv 3 \pmod{4}$ divides a corner entry then it divides the two middle-side entries that are not adjacent to the corner.
Proof: Without loss of generality, let the corner entry be \( c^2 \). Again, we use the fact that the ring of Gaussian integers \( \mathbb{Z}[i] \) is a UFD. Factoring the left side of \( d^2 + h^2 = 2c^2 \) in \( \mathbb{Z}[i] \), we get \( (d + hi)(d - hi) = 2c^2 \). If \( p \equiv 3(\text{mod } 4) \) then \( p \) is prime in \( \mathbb{Z}[i] \) (See Lemma 1.1 in the Appendix). Thus if \( p | c \) and \( p \equiv 3(\text{mod } 4) \), then either \( p | (d + hi) \) or \( p | (d - hi) \). If \( p | (d + hi) \), then \( d + hi = pk \), and by conjugation \( d - hi = p\overline{k} \). Hence \( p | (d - hi) \). Thus \( p \) divides their sum and difference: \( p | 2d \) and \( p | 2hi \). Hence \( p | d \) and \( p | h \) since \( p \) is odd and real. ■

All of these properties taken together severely restrict the possible placement of primes that are not of the form \( p \equiv 1(\text{mod } 8) \). Given these restrictions, one might conjecture that if there is a solution, then all prime divisors of all entries are of the form \( p \equiv 1(\text{mod } 8) \). This would greatly reduce the number of possibilities. It would also be interesting to disprove this conjecture by proving the opposite; namely, that any solution must have at least one entry with prime divisor \( p \equiv 5, 7(\text{mod } 8) \).

APPENDIX

We need to know when an odd prime \( p \in \mathbb{Z} \) is also prime in the extensions \( \mathbb{Z}[i] \) and \( \mathbb{Z}[\sqrt{2}] \). The following two lemmas answer this question completely.

**Lemma 1.1** Given an odd prime \( p \in \mathbb{Z} \),

\[ p \equiv 3(\text{mod } 4) \iff p \text{ prime in } \mathbb{Z}[i] \]

Proof: We use the fact that \( \mathbb{Z}[i] \) is a UFD.

First, we assume that \( p \equiv 3(\text{mod } 4) \) and show that \( p \) must be prime in \( \mathbb{Z}[i] \). If \( p \) is composite in \( \mathbb{Z}[i] \) then \( p \) has a factorization \( p = \alpha \beta \) with \( N(\alpha) > 1 \) and \( N(\beta) > 1 \). Taking the norm of both sides we get \( p^2 = N(\alpha)N(\beta) \). It is not possible for \( p^2 \) to divide \( N(\alpha) \) or \( N(\beta) \) since this would imply \( N(\beta) = 1, N(\alpha) = 1 \) respectively. Hence \( N(\alpha) = p \) and \( N(\beta) = p \). From the former we get \( p = N(\alpha) = x^2 + y^2 \) for some \( x, y \in \mathbb{Z} \). Thus \( p \equiv 0, 1, 2(\text{mod } 4) \) which is a contradiction. ■

Now we assume that \( p \) is prime in \( \mathbb{Z}[i] \) and show that \( p \equiv 3(\text{mod } 4) \). If \( p \equiv 1(\text{mod } 4) \) then the equation \( x^2 \equiv -1(\text{mod } p) \) has a solution. Hence \( x^2 + 1 = kp \). Factoring in \( \mathbb{Z}[i] \) we get \( (x + i)(x - i) = kp \). Since \( p \) is prime, it must divide one of the factors and by complex conjugation it divides both. Therefore \( p \) divides their difference: \( p | 2i \). This is impossible since \( p \) is odd and real (Beukers [4]). ■

**Lemma 1.2** Given an odd prime \( p \in \mathbb{Z} \),

\[ p \equiv 3, 5(\text{mod } 8) \iff p \text{ prime in } \mathbb{Z}[\sqrt{2}] \]
Proof: We use the fact that $\mathbb{Z}[\sqrt{2}]$ is a UFD.

First, we assume that $p \equiv 3,5 \pmod{8}$ and show that $p$ must be prime in $\mathbb{Z}[\sqrt{2}]$. If $p$ composite in $\mathbb{Z}[\sqrt{2}]$ then $p$ has a factorization $p = \alpha \beta$ with $|N(\alpha)| > 1$ and $|N(\beta)| > 1$. Taking the norm of both sides we get $p^2 = N(\alpha)N(\beta)$. It is not possible for $p^2$ to divide $N(\alpha)$ or $N(\beta)$ since this would imply $|N(\beta)| = 1$, $|N(\alpha)| = 1$ respectively. Hence $|N(\alpha)| = p$ and $|N(\beta)| = p$. From the former we get $p = \pm N(\alpha) = \pm(x^2 - 2y^2)$ for some $x, y \in \mathbb{Z}$. Thus $p \equiv 0, 1, 2, 6, 7 \pmod{8}$ which is a contradiction. ■

Now we assume that $p$ is prime in $\mathbb{Z}[\sqrt{2}]$ and show that $p \equiv 3,5 \pmod{8}$. If $p \equiv 1, 7 \pmod{8}$ then the equation $x^2 \equiv 2 \pmod{p}$ has a solution. Hence $x^2 - 2 = kp$. Factoring in $\mathbb{Z}[\sqrt{2}]$ we get $(x + \sqrt{2})(x - \sqrt{2}) = kp$. Since $p$ is prime, it must divide one of the factors and by conjugation it divides both. Therefore $p$ divides their difference: $p \mid 2\sqrt{2}$. This is impossible since $p$ is odd and rational. ■

REFERENCES