Properties of Magic Squares of Squares

Landon W. Rabern
1120 NW Harlan St.
Roseburg, OR 97470
lwr1@cec.wustl.edu

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 different 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 this solution. The solution must have the form:

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

We know from Gardner [3] that the magic number (M = the sum of each row, column, or main diagonal) must equal three times the middle square, so $M = 3e^2$.
Let gcd() mean the greatest common divisor function.
$t = gcd(a^2, b^2, c^2, d^2, e^2, f^2, g^2, h^2, s^2)$
If $t \neq 1$ then t is a square, thus we can divide all entries and M by t to have a new solution with a smaller M. 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 sum of the entries on the left side of the square must equal M we get:
$a^2 + d^2 + g^2 = M = 3e^2 \Rightarrow a^2 + g^2 = 3e^2 - d^2 \Rightarrow a^2 + g^2 \equiv 3e^2 - d^2 (\text{mod } 4)$
In this last equation, e odd and d even gives $a^2 + g^2 \equiv 3 - 0 \equiv 3(\text{mod } 4)$. e even and d odd gives $a^2 + g^2 \equiv 0 - 1 \equiv -1 \equiv 3(\text{mod } 4)$. This is impossible since $a^2 + g^2 \equiv 0$ or $2(\text{mod } 4)$. Therefore, we must have both e and d odd or both e and d even. Both e and d odd gives $a^2 + g^2 \equiv 3 - 1 \equiv 2(\text{mod } 4) \Rightarrow$ a odd, g odd. Both e and d even gives $a^2 + g^2 \equiv 0 - 0 \equiv 0(\text{mod } 4) \Rightarrow$ a even, g even. Thus $a \equiv g \equiv e \equiv d(\text{mod } 2)$.

Doing the same exact thing for all the sides of the square we find that: $a \equiv b \equiv c \equiv d \equiv e \equiv f \equiv g \equiv h \equiv s \pmod 2$. Thus, if any element is even they

are all even, but then they are all divisible by 2 and are not relatively prime. Hence, all entries are odd. ■

From all rows, columns and main diagonals that pass through the center of the square we get the following:
$a^2 + e^2 + s^2 = d^2 + e^2 + f^2 = b^2 + e^2 + h^2 = g^2 + e^2 + c^2 = 3e^2 \Rightarrow$
$a^2 + s^2 = d^2 + f^2 = b^2 + h^2 = g^2 + c^2 = 2e^2$
We can use this to prove:

Theorem 1.2 *The only prime divisors of e are of the form $p \equiv 1$(mod 4).*

Proof: We just need to show that no prime $p \equiv 3$(mod 4) can divide e. We use the fact that the ring of Gaussian integers Z[i] is a Unique Factorization Domain(UFD). Factoring the left side of $a^2 + s^2 = 2e^2$ in Z[i], we get $(a + si)(a - si) = 2e^2$. Given an odd prime $p \in Z$, then p is prime in Z[i] if and only if $p \equiv 3$(mod 4)(See Appendix). Thus, assume we have a p such that $p \equiv 3$(mod 4) and $p \mid e$ then we must have either $p \mid (a + si)$ or $p \mid (a - si)$. Say $p \mid (a + si)$, then $a + si = pk$ and by complex conjugation $a - si = \overline{pk} = p\overline{k}$. Hence $p \mid (a - si)$. But then p must also divide their sum and difference:
$p \mid 2si$, $p \mid 2a \Rightarrow p \mid s$, $p \mid a$ since p is odd and real.
Similarly, $p \mid d$, $p \mid f$, $p \mid b$, $p \mid h$, $p \mid g$, $p \mid c$. Hence, p divides every entry which is impossible. ■

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

Proof: We will only prove the theorem for the a,e,s diagonal since the same exact proof applies to the other cases. We use the fact that the ring Z[$\sqrt{2}$] is a UFD. Given an odd prime $p \in Z$, then p is prime in Z[$\sqrt{2}$] if and only if $p \equiv 3, 5$ (mod 8)(See Appendix).
$a^2 + s^2 = 2e^2 \Rightarrow a^2 = -(s^2 - 2e^2)$.
We can factor the right side of this equation in Z[$\sqrt{2}$] to get:
$a^2 = -(s + e\sqrt{2})(s - e\sqrt{2})$
If $p \mid a$ and $p \equiv 3, 5$(mod 8) then either $p \mid (s + e\sqrt{2})$ or $p \mid (s - e\sqrt{2})$. Say $p \mid (s + e\sqrt{2})$, 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:
$p \mid 2s$, $p \mid 2e\sqrt{2} \Rightarrow p \mid s$, $p \mid e$ since p is odd and rational. ■

Corollary 1.1 *No prime $p \equiv 3$(mod 8) divides any entry.*

Proof: Say 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 $p \equiv 3$(mod 8) $\Rightarrow p \equiv 3$(mod 4). ■

Gardner [3] has shown that given any 3x3 magic square made up 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 $d^2 + h^2 = 2c^2$ and similar relations for the other corner entries. The relation can be stated as: double a corner entry equals the sum of the two middle-side entries that are not adjacent to the corner. We can use this to prove the following:

Theorem 1.4 *No prime $p \equiv 5$(mod 8) divides a middle-side entry.*

Proof: We will only prove for the d^2 middle-side since the same exact proof applies to the other cases. Again, we use the fact that the ring Z[$\sqrt{2}$] is a UFD. Given an odd prime $p \in Z$, then p is prime in Z[$\sqrt{2}$] if and only if $p \equiv 3, 5$ (mod 8)(See Appendix).
$d^2 + h^2 = 2c^2 \Rightarrow d^2 = -(h^2 - 2c^2)$.
We can factor the right side of this equation in Z[$\sqrt{2}$] to get:
$d^2 = -(h + c\sqrt{2})(h - c\sqrt{2})$
If $p \mid d$ and $p \equiv 5$(mod 8) then either $p \mid (h + c\sqrt{2})$ or $p \mid (h - c\sqrt{2})$. Say $p \mid (h + c\sqrt{2})$, then $h + c\sqrt{2} = pk$ and by conjugation $h - c\sqrt{2} = p\bar{k}$. Hence $p \mid (h - c\sqrt{2})$. Thus p divides their sum and difference:
$p \mid 2h$, $p \mid 2c\sqrt{2} \Rightarrow p \mid h$, $p \mid c$ since p is odd and rational. Since $p \mid h$ we can use the same argument to show that $p \mid f$, $p \mid a$. But then, since $p \mid f$, we can use the same argument again to show that $p \mid b$, $p \mid g$. p divides both a and s, so p must also divide e. Hence p divides all entries, which is impossible. ■

Theorem 1.5 *If a prime $p \equiv 3$(mod 4) divides a corner entry then it divides the two middle-side entries that are not adjacent to the corner.*

Proof: We will only prove this for the c^2 corner entry since the same exact proof applies to the other cases. As before, we use the fact that the ring of Gaussian integers Z[i] is a UFD. Factoring the left side of $d^2 + h^2 = 2c^2$ in Z[i], we get $(d + hi)(d - hi) = 2c^2$. If $p \equiv 3$(mod 4) then p is prime in Z[i](See Appendix). Hence, as in the previous proofs, $p \mid d$, $p \mid h$. ■

All of these properties taken together severely restrict the possible placement of primes that are not $p \equiv 1$(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 $p \equiv 1$(mod 8). This would greatly lower the 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 $p \equiv 5, 7$(mod 8).

APPENDIX

Lemma 1.1 *Given an odd prime $p \in Z$:*

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

Proof: Z[i] is a UFD.
$\Rightarrow$
Given $p \equiv 3(\text{mod } 4)$. If p composite in Z[i] then p has a factorization $p = \alpha\beta$ with $N(\alpha) > 1$, $N(\beta) > 1$. Taking the norm of both sides we get $p^2 = N(\alpha)N(\beta)$. p^2 cannot divide $N(\alpha)$ or $N(\beta)$ since this would imply $N(\beta) = 1$, $N(\alpha) = 1$ respectively. Hence $N(\alpha) = p$, $N(\beta) = p$. From the former we get p=$N(\alpha) = x^2 + y^2$ for some $x, y \in Z$. Thus $p \equiv 0, 1, 2(\text{mod } 4)$ which is a contradiction. ■
$\Leftarrow$
Given p prime in Z[i]. 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 Z[i] we get $(x + i)(x - i) = kp$. p is prime, so it must divide one of the factors and by complex conjugation it divides both. Therefore p divides their sum and difference:
$p \mid 2x$, $p \mid 2i$
The latter is impossible since p is odd and real(Beukers [4]). ■

Lemma 1.2 *Given an odd prime $p \in Z$:*

$$p \equiv 3, 5 \textit{(mod 8)} \Leftrightarrow p \textit{ prime in } Z[\sqrt{2}]$$

Proof: Z[$\sqrt{2}$] is a UFD.
$\Rightarrow$
Given $p \equiv 3, 5(\text{mod } 8)$. If p composite in Z[$\sqrt{2}$] then p has a factorization $p = \alpha\beta$ with $|N(\alpha)| > 1$, $|N(\beta)| > 1$. Taking the norm of both sides we get $p^2 = N(\alpha)N(\beta)$. p^2 cannot divide $N(\alpha)$ or $N(\beta)$ since this would imply $N(\beta) = 1$, $N(\alpha) = 1$ respectively. Hence $N(\alpha) = \pm p$, $N(\beta) = \pm p$. From the former we get p=$\pm N(\alpha) = \pm(x^2 - 2y^2)$ for some $x, y \in Z$. Thus $p \equiv 0, 1, 2, 6, 7 \ (\text{mod } 8)$ which is a contradiction. ■
$\Leftarrow$
Given p prime in Z[$\sqrt{2}$]. If $p \equiv 1, 7(\text{mod } 8)$ then the equation $x^2 \equiv 2(\text{mod p})$ has a solution. Hence $x^2 - 2 = kp$. Factoring in Z[$\sqrt{2}$] we get $(x+\sqrt{2})(x-\sqrt{2}) = kp$. p is prime, so it must divide one of the factors and by conjugation it divides both. Therefore p divides their sum and difference:
$p \mid 2x$, $p \mid 2\sqrt{2}$
The latter is impossible since p is odd and rational. ■

REFERENCES

1. Martin LaBar, Problem 270, *College Math Journal*,15, p. 69.
2. John P. Robertson, *Magic Squares of Squares*, Mathematics Magazine, Vol. 69, No. 4, Oct. 1996, pp. 289-293
3. Martin Gardner, *Riddles of the Sphinx*, Mathematical Association of America, 1987, pp. 136-137.
4. Frits Beukers, *Elementary Number Theory*, Lecture Notes, Sept. 2001, p. 55.