Rose-Hulman Undergraduate Mathematics Journal

Volume 24
Issue 1

Article 7

Some Thoughts on The 3 × 3 Magic Square of Squares Problem

Desmond Weisenberg
Case Western Reserve University, dsw65@case.edu

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

 Part of the Number Theory Commons

Recommended Citation

Weisenberg, Desmond (2023) "Some Thoughts on The 3 × 3 Magic Square of Squares Problem," *Rose-Hulman Undergraduate Mathematics Journal*: Vol. 24: Iss. 1, Article 7.
Available at: https://scholar.rose-hulman.edu/rhumj/vol24/iss1/7

Some Thoughts on The 3 × 3 Magic Square of Squares Problem

Cover Page Footnote

Thanks to Dr. Long Tran of Case Western Reserve University's Department of Mathematics for reviewing and talking through this paper with me prior to submission, and to Dr. David Singer of the same department for his support and for giving me to chance to study and present on this problem in his elementary number theory class prior to coming up with my own ideas.

This article is available in Rose-Hulman Undergraduate Mathematics Journal: https://scholar.rose-hulman.edu/rhumj/vol24/iss1/7

Rose-Hulman Undergraduate Mathematics Journal
Volume 24, Issue 1, 2023

Some Thoughts on The 3×3 Magic Square of Squares Problem

By *Desmond Weisenberg*

Abstract. A *magic square* is a square grid of numbers where each row, column, and long diagonal has the same sum (called the *magic sum*). An open problem popularized by Martin Gardner asks whether there exists a 3×3 magic square of distinct positive square numbers. In this paper, we expand on existing results about the prime factors of elements of such a square, and then provide a full list of the ways a prime factor could appear in one. We also suggest a separate possible computational approach based on the prime signature of the center entry of the square.

1 Introduction

A *magic square* is a square grid of numbers where each row, column, and long diagonal has the same sum, called the *magic sum*. (Note that *long diagonals* refer to a diagonal going from one corner entry to the opposite corner entry.) While magic squares have been an object of interest for thousands of years, an interesting unsolved problem of more recent times is whether there exists a 3×3 magic square composed of distinct positive square numbers [1]. Mentioned in 1876 by Édouard Lucas [2] and posed more recently in 1984 by Martin LaBar [7], the problem has received attention due to well-known recreational mathematician Martin Gardner offering $100 to whoever could construct such a square [5] [6]. Recreational mathematician Matt Parker's "Parker Square" from a *Numberphile* video was a well-known example of a square that didn't quite work, since there were repeated entries and one of the diagonals had the wrong sum [12]. Today, this problem is featured on Christian's Boyer magic square website multimagie.com; however, it remains unsolved. (For more information about the history of this problem, see [1] or [2].)

In fact, even the weaker problem of finding a 3×3 magic square of distinct positive integers containing at least 7 square numbers only has one known solution (see Figure 1). On multimagie.com, Christian Boyer currently offers a prize for whoever can construct or prove the impossibility of another such square with at least 7 square numbers, as well as for whoever can do the same for a square with all of its entries square numbers [1].

Mathematics Subject Classification. 11A99
Keywords. magic squares, number theory, quadratic residues, Gaussian integers

That even this seemingly-easier problem is unknown offers little hope for finding a 3 × 3 magic square of squares, or even for the existence of one.

373^2	289^2	565^2
$360,721$	425^2	23^2
205^2	527^2	$222,121$

Figure 1: The only known 3 × 3 magic square of distinct positive integers containing at least 7 square numbers (up to rotation/reflection and scaling by a square factor). The magic sum of this square is $541,875$.

However, while the 3 × 3 magic square of squares problem remains unsolved, many results are still known. Gardner has shown [4] that in any 3 × 3 magic square, the magic sum must be three times the center entry. Using this fact, he showed that every 3 × 3 magic square can be expressed in the form of Figure 2. An interesting consequence of this is as follows: define the *pandiagonals* of the square as the sets consisting of two adjacent center-side entries and the opposite corner entry. For example, in Figure 2, the elements $\{x+y, x+y-z, x+y+z\}$ form a pandiagonal. From this diagram, it is straightforward to verify that the sum of any two center-side elements in a pandiagonal is twice the corresponding corner entry.

In a 3 × 3 magic square of distinct positive square numbers, we clearly have that $x > y, z$ with all three being distinct positive integers (assuming the square is rotated/reflected as needed). Many other results are known; for example, Rabern [13] has obtained restrictions on what the prime factors of the entries can be congruent to mod 8, and Morgenstern has shown that the smallest entry of such a square must be greater than 1 [9]. Morgenstern later generalized this to devise a more general method for increasing the lower bound of the smallest element [10].

In this paper, we approach this problem in two separate ways: first, we expand the results of Rabern by deriving more restrictions on how the prime factors of the entries of a 3 × 3 magic square of squares can behave, culminating in a comprehensive list of the ways that prime factors may appear in such a square (or, at least, the ways we have not ruled out yet). Second, we describe a possible computational approach to finding

$x+z$	$x-y-z$	$x+y$
$x+y-z$	x	$x-y+z$
$x-y$	$x+y+z$	$x-z$

Figure 2: The form of all 3 × 3 magic squares.

such a square based on the prime signature of the center entry of the square. Note that these two sections are largely disjoint from each other, and the latter focuses less on presenting results and more on proposing an idea for future research on this problem.

2 Results on Prime Factors

2.1 Basics

In this section, we present some new results on the structure of the prime factors of the entries of a 3×3 magic square of squares. (Note that when we say "3×3 magic square of squares", we are specifically referring to a square whose entries are distinct positive square numbers.) After presenting these results, we will provide a comprehensive list of the ways that prime factors can appear in such a square (or, at least, the ways we have not ruled out yet). Without loss of generality, we will assume that no prime factor divides all nine entries of the square, since if one did, we could just divide it from all entries to get an even smaller 3×3 magic square of squares.

We start by describing the key known results. By taking advantage of the fact that an odd prime p has -1 as a quadratic residue if and only if $p \equiv 1 \pmod 4$ and has 2 as a quadratic residue if and only if $p \equiv 1, 7 \pmod 8$, Rabern [13] proved the following results about prime factors p of the entries of a 3×3 magic square of squares:

1. All prime factors of any entry are odd.[1]
2. If p divides the center, then $p \equiv 1 \pmod 4$.
3. If $p \equiv 3, 5 \pmod 8$ and p divides a non-center entry, then p also divides the center and the other entry in that line.
4. No prime $p \equiv 3 \pmod 8$ divides any entry.
5. No prime $p \equiv 5 \pmod 8$ divides a middle-side entry.
6. If $p \equiv 3 \pmod 4$ and p divides a corner entry, then p also divides the two non-adjacent middle-side entries.

Furthermore, it was pointed out in [11] that if a prime factor p divides at least three entries of a 3×3 magic square of squares that do not form a row, column, long diagonal, or pandiagonal, then p divides every entry of the square. To prove this, we start with the following (fairly straightforward) multi-part lemma about which entries a factor can divide:

[1] The proof of this is straightforward and uses nothing more than the fact that 0 and 1 are the only quadratic residues of 4. In fact, this logic can be used to show that even if we allowed 0 to be an element in the square, it would be impossible for it to appear.

Lemma 2.1. *First, suppose a prime factor p in a 3×3 magic square of squares divides at least two elements in a center row, center column, long diagonal, or pandiagonal. Then p divides all three elements there. Second, suppose p divides the center. Then p cannot divide exactly two elements in a non-center row or column.*

Proof. First, suppose p divides at least two elements in a center row, center column, long diagonal, or pandiagonal. Since every 3×3 magic square is of the form in Figure 2, it follows that in each center row, center column, long diagonal, or pandiagonal, there exist two elements that add up to twice the other element. Since p cannot be 2 by Rabern's theorems, it follows that if p divides two of these elements, it must divide the other one as well.

Second, suppose p divides the center. Then the magic sum is a multiple of p. However, if a non-center row or column has exactly two multiples of p, then it has exactly one element that is not a multiple of p, so its sum will not be a multiple of p, a contradiction. □

Lemma 2.2. *Suppose p is a prime factor that divides at least three entries of a 3×3 magic square of squares that do not form a row, column, long diagonal, or pandiagonal. Then p divides every entry of the square.*

Proof. We use Lemma 2.1. For any 3×3 square and prime number p, there are $2^9 = 512$ possibilities for which entries p divides. Examining all of these possibilities, it is straightforward to computationally verify that the only possibility for which a) p divides at least 3 entries that are not all in the same row, column, long diagonal, or pandiagonal, b) p does not divide exactly two entries in any center row, center column, long diagonal, or pandiagonal, and c) if p divides the center, then p does not divide exactly two entries in any non-center row or column, is the possibility in which p divides every entry.

The supplementary code in `PrimeArrangements.java` can be used to verify this statement; it is also described in the appendix. □

As stated, we are assuming without loss of generality that no prime factor divides all entries. As such, by Lemma 2.2, no prime factor can divide three entries that do not form a row, column, long diagonal, or pandiagonal — it clearly also follows that no prime factor can divide more than three entries, since if it did, at least three of those entries would have to not be contained within a single row, column, long diagonal, or pandiagonal.

As such, every prime factor p that appears in the square divides exactly one, two, or three entries. We now derive further restrictions on how the prime factors can behave in each case.

2.2 Primes That Divide Three Entries

We start by considering the case where p divides exactly three entries. By Lemma 2.2, the three entries must form a row, column, long diagonal, or pandiagonal. Observe that the three entries cannot form a non-center row or column, since then the magic sum would be a multiple of p; that is, the center element times 3 would be a multiple of p. However, if the multiples of p form a non-center row or column, then the center cannot be a multiple of p. Furthermore, p cannot be 3 by Rabern's theorems. As such, this is impossible. Therefore, we can rule out the three entries forming a non-center row or column. As such, the three entries must form either a) a center row or column, b) a long diagonal, or c) a pandiagonal.

Recall that every 3×3 magic square of squares is of the form in Figure 2, which means that in any center row/column, long diagonal, or pandiagonal, there exist two square numbers that can be added to yield twice the third square number; that is, the elements can be expressed as a^2, b^2, c^2 for distinct positive integers a, b, c where $a^2+b^2=2c^2$.

If the entries form a center row or column, then by Rabern's 2nd and 5th theorems, $p \equiv 1 \pmod 8$. If the entries form a long diagonal, then by Rabern's 2nd theorem, $p \equiv 1 \pmod 4$. If the entries form a pandiagonal, then by Rabern's 3rd theorem, $p \equiv 1,7 \pmod 8$.

One way we can expand on this is by making statements about the relative *orders* of the primes within these elements. We do so with the following theorems:

Theorem 2.3. *Suppose p is a prime factor that divides exactly three entries of a 3×3 magic square of squares. Then p attains its smallest order in at least two of these entries.*

Proof. As discussed above, there must exist distinct positive integers a, b, c such that the three entries are equal to a^2, b^2, c^2 and $a^2+b^2=2c^2$. For the sake of contradiction, suppose p attains a smaller order (call it j) in one of these entries than in the other two. Then we can divide both sides of $a^2+b^2=2c^2$ by p^j to get an equality with two multiples of p and one non-multiple of p, which is impossible. (Recall that $p \neq 2$, as the number 2 cannot divide any of the entries, so the 2 in front of the c^2 will not affect divisibility by p.) □

Theorem 2.4. *Suppose p is a prime factor dividing three entries of a 3×3 magic square of squares that form a long diagonal. If p attains a higher order in a corner entry than the other two entries, then $p \equiv 1 \pmod 8$.*

Proof. Let a^2, b^2 be the corner entries and let c^2 be the center entry; then $a^2+b^2=2c^2$. Suppose p attains a higher order in a corner entry than in the other two entries; without loss of generality, suppose p attains its highest order (call it k) in a. By Theorem 2.3, p has the same order in b and c; call it l. If we let $a' = a/p^k$, $b' = b/p^l$, and $c' = c/p^l$, then $a'^2p^{2k} + b'^2p^{2l} = 2c'^2p^{2l}$. Dividing by p^{2l}, we have $a'^2p^{2k-2l} + b'^2 = 2c'^2$. As such,

$b'^2 \equiv 2c'^2 \pmod{p}$. Since $b'^2, c'^2, 2 \not\equiv 0 \pmod{p}$, the product of two quadratic residues is also a quadratic residue, and the product of a nonzero quadratic residue and a quadratic non-residue is a non-residue, it follows that 2 is a quadratic residue (mod p), so $p \equiv 1,7 \pmod 8$. We have already established that if p divides all the entries of a long diagonal, then $p \equiv 1 \pmod 4$; as such, $p \equiv 1 \pmod 8$. □

Theorem 2.5. *Suppose p is a prime factor dividing three entries of a 3×3 magic square of squares that form a pandiagonal. If p attains a higher order in the corner entry than the other two entries, then $p \equiv 1 \pmod 8$.*

Proof. Let a^2, b^2 be the center-side entries of the pandiagonal and let c^2 be the corner entry; then $a^2 + b^2 = 2c^2$. Suppose p attains a higher order k in c than in a and b. By Theorem 2.3, p has the same order in a and b; call it l. If we let $a' = a/p^l$, $b' = b/p^l$, and $c' = c/p^k$, then $a'^2 p^{2l} + b'^2 p^{2l} = 2c'^2 p^{2k}$. Dividing by p^{2l}, we have $a'^2 + b'^2 = 2c'^2 p^{2k-2l}$. As such, $a'^2 \equiv -b'^2 \pmod{p}$. Since $a'^2, b'^2, \not\equiv 0 \pmod{p}$, the product of two quadratic residues is also a quadratic residue, and the product of a nonzero quadratic residue and a quadratic non-residue is a non-residue, it follows that -1 is a quadratic residue (mod p), so $p \equiv 1 \pmod 4$. We have already established that if p divides all the entries of a pandiagonal, then $p \equiv 1,7 \pmod 8$; as such, $p \equiv 1 \pmod 8$. □

2.3 Primes That Divide Two Entries

Suppose a prime number p divides exactly two entries of a 3×3 magic square of squares. We know from the first part of Lemma 2.1 that if the entries share a center row, center column, long diagonal, or pandiagonal, then p must divide the third entry in there as well, which we are supposing not to be the case. However, *any* two entries must share a row, column, long diagonal, or pandiagonal. (This is straightforward to verify with brute force.) As such, the only possibility is that the two multiples of p must share a non-center row or column.

As we have shown, existing results restricting prime factors generally use knowledge of which primes have -1 and 2 as a quadratic residue. In this section, we will derive a new restriction by considering which primes have 3 as a quadratic residue; namely, we will show that if p divides exactly two entries in a 3×3 magic square of squares, then $p \equiv 1 \pmod{24}$.

Lemma 2.6. *Let p be a prime dividing an entry in a 3×3 magic square of squares. Then 3 is a quadratic residue of p if and only if $p \equiv 1,11 \pmod{12}$.*

Proof. By Rabern's theorems, p cannot be 2 or 3, so we must have that $p \equiv 1,5,7,11 \pmod{12}$. We consider all four cases separately; in each case, we determine whether 3 is a quadratic residue of p by using Gauss' law of quadratic reciprocity to compute the Legendre symbol $\left(\frac{3}{p}\right)$.

If $p \equiv 1 \pmod{12}$, then $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1$.

If $p \equiv 5 \pmod{12}$, then $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1$.

If $p \equiv 7 \pmod{12}$, then $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) = -\left(\frac{1}{3}\right) = -1$.

If $p \equiv 11 \pmod{12}$, then $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) = -\left(\frac{2}{3}\right) = -(-1) = 1$.

Since $\left(\frac{3}{p}\right) = 1$ exactly in the cases where $p \equiv 1, 11 \pmod{12}$, it follows that this is exactly when 3 is a quadratic residue of p. □

Theorem 2.7. *Let p be a prime number that divides exactly two entries in a 3×3 magic square of squares. Then $p \equiv 1 \pmod{24}$.*

Proof. As explained earlier in this section, if p divides exactly two entries, then both of those entries must share a non-center row or column. We consider two cases: (i) both entries are corner entries, and (ii) one of the entries is a center-side entry. For both cases, we start by constructing the square (mod p).

For case (i), without loss of generality, suppose p divides the upper two corner entries (so they are congruent to 0 (mod p)). Let x denote the middle entry, which clearly cannot be 0 (mod p). Since the sum is three times the center entry, it must be congruent to $3x \pmod{p}$. As such, we can "fill out" the rest of the square by writing in the two zeroes and the x in the center, and then every time a row, column, or long diagonal has two entries filled in, we can set the third one appropriately to make it sum to $3x$. Doing so yields

0	$3x$	0
x	x	x
$2x$	$-x$	$2x$

.

Since every entry must be a square number, we have that x, $-x$, $2x$, and $3x$ are all quadratic residues of p.

For case (ii), without loss of generality, suppose p divides the upper-left corner entry and the top center-side entry. Letting x be the center entry and filling out the square the same way as above, we get

0	0	$3x$
$4x$	x	$-2x$
$-x$	$2x$	$2x$

.

As in the previous case, since every entry must be a square number, we have that x, $-x$, $2x$, and $3x$ are all quadratic residues of p.

We have shown that in both cases, x, $-x$, $2x$, and $3x$ are quadratic residues of p. Recall that by Rabern's theorems, p cannot be 2 or 3. Since $x, 2, 3 \not\equiv 0 \pmod{p}$, x, $-x$, $2x$, and $3x$ are thus nonzero quadratic residues of p. Recall that the product of two quadratic residues is also a quadratic residue, and the product of a nonzero quadratic residue and a quadratic non-residue is a non-residue. From this, it follows that -1, 2, and 3 are all quadratic residues of p. Recall that a prime greater than 3 in the square has -1 as a quadratic residue if and only if it is congruent to 1 (mod 4), has 2 as a quadratic residue if and only if it is congruent to 1 or 7 (mod 8), and by Lemma 2.6 has 3 as a quadratic residue if and only if it is congruent to 1 or 11 (mod 12). The only way all of these conditions can be satisfied is if $p \equiv 1 \pmod{24}$. □

2.4 Primes That Divide One Entry

If a prime p divides exactly one entry of the square, there are three possibilities: it divides a corner entry, it divides a center-side entry, or it divides the center entry. In each of these cases, we will show the existence of a certain pattern among the quadratic residues of p. (Note that Woll [15] and Labruna [8] have also used a similar idea and derived similar results.)

Theorem 2.8. *Suppose p is a prime that divides a corner entry of a 3×3 magic square of squares and divides no other entries. Then $p \equiv 1 \pmod{8}$ and p has five consecutive nonzero quadratic residues.*

Proof. That $p \equiv 1 \pmod{8}$ follows from Rabern's third and sixth theorems. We now prove that p has five consecutive nonzero quadratic residues. As in some of our previous proofs, we construct the square (mod p). Without loss of generality, suppose p divides the upper-left element, and let x be the center element. Then we start with

0		
	x	

.

Clearly, every element aside from the upper-left corner must be nonzero (mod p). Since the integers (mod p) form a field, there exists some integer m such that the top element is congruent to $mx \pmod{p}$; this gives us the square

0	mx	
	x	

.

Since the magic sum must be three times the center element, it must be $3x \pmod{p}$. As such, each time we have a row, column, or long diagonal with two elements, we can fill in the third one appropriately; doing so yields

0	mx	$(3-m)x$
$(4-m)x$	x	$(m-2)x$
$(m-1)x$	$(2-m)x$	$2x$

.

Every element aside from the upper-left entry must be a nonzero quadratic residue. As such, x is a quadratic residue. Recall that the product of two quadratic residues is also a quadratic residue, and the product of a nonzero quadratic residue and a quadratic non-residue is a non-residue. From this, it follows that m, $m-1$, $m-2$, $3-m$, and $4-m$ are all quadratic residues of p. Since $p \equiv 1 \pmod 8$, -1 is a quadratic residue of p, so we can multiply the latter two by -1 to get that m, $m-1$, $m-2$, $m-3$, and $m-4$ are all quadratic residues of p. Furthermore, since the upper-left entry is the only zero entry (mod p), these values must all be nonzero (mod p). As such, p has five consecutive nonzero quadratic residues. □

Theorem 2.9. *Suppose p is a prime that divides a center-side entry of a 3×3 magic square of squares and divides no other entries. Then either $p \equiv 1 \pmod 8$ and p has four consecutive nonzero quadratic residues, or $p \equiv 7 \pmod 8$ and p has two consecutive nonzero non-residues followed by two consecutive nonzero residues.*

Proof. That $p \equiv 1, 7 \pmod 8$ follows from Rabern's third theorem. For the rest, similarly to the last proof, we proceed by constructing the square (mod p). Without loss of generality, suppose p divides the top-side entry. If we let x be the middle entry, let m be an integer such that $mx \pmod p$ is the upper-right entry (which must exist by the same logic as the previous proof), and fill in the rest of the square to make each row, column, and long diagonal sum to $3x$, we get

$(3-m)x$	0	mx
$(2m-2)x$	x	$(4-2m)x$
$(2-m)x$	$2x$	$(m-1)x$

.

Every element aside from the top entry must be a nonzero quadratic residue. As such, x is a quadratic residue. Recall that the product of two quadratic residues is also a quadratic residue, and the product of a nonzero quadratic residue and a quadratic non-residue is a non-residue. From this, it follows that m, $m-1$, $2-m$, and $3-m$ are all quadratic residues of p. Furthermore, since the top entry is the only zero entry (mod p), these values must all be nonzero (mod p).

If $p \equiv 1 \pmod 8$, then -1 is a quadratic residue of p, so we can multiply the latter two values by -1 to get that m, $m-1$, $m-2$, and $m-3$ are all quadratic residues of p, so p has four consecutive nonzero quadratic residues. Alternatively, if $p \equiv 7 \pmod 8$, then -1 is not a quadratic residue of p, so we can multiply the latter two values by -1 to get that $m-2$ and $m-3$ are not quadratic residues of p, so p has two consecutive nonzero non-residues followed by two consecutive nonzero residues. □

The following theorem has also been proved by Woll [15] using a slightly different argument, and Labruna [8] has proved a similar result as well.

Theorem 2.10. *Suppose p is a prime that divides the center entry of a 3×3 magic square of squares and divides no other entries. Then $p \equiv 1 \pmod 4$ and p has three consecutive nonzero quadratic residues.*

Proof. That $p \equiv 1 \pmod 4$ follows from Rabern's second theorem. For the rest, as with the previous two proofs, we construct the square (mod p). If we let x be the upper-left entry, let m be an integer such that $mx \pmod p$ is the upper-right entry (which must exist by the same logic as the previous two proofs), and fill in the rest of the square to make each row, column, and long diagonal sum to 0 (since the magic sum must be three times the center and is thus also congruent to $0 \pmod p$), we get

x	$(-m-1)x$	mx
$(m-1)x$	0	$(1-m)x$
$-mx$	$(m+1)x$	$-x$

.

Every element aside from the center entry must be a nonzero quadratic residue. As such, x is a quadratic residue. Recall that the product of two quadratic residues is also a quadratic residue, and the product of a nonzero quadratic residue and a quadratic non-residue is a non-residue. From this, it follows that m, $m-1$, and $m+1$ are all quadratic residues of p. Furthermore, since the center entry is the only zero entry (mod p), these values must all be nonzero (mod p). As such, p has three consecutive nonzero quadratic residues. □

2.5 Final List

At this point, we have both described and expanded on existing results about the prime factors of the entries of a 3×3 magic square of squares. To consolidate what we know so far, we present a list of all the ways a prime factor p may appear in such a square. That is, any prime factor in such a square must appear in one of the following seven arrangements. Of course, some of these ways may end up being ruled out later on — in particular, if a 3×3 magic square of squares is eventually determined to not exist, then *all* of these ways will end up being impossible.

- p divides exactly one element.
  - p divides a corner element. If this is the case, then $p \equiv 1 \pmod 8$ and p has five consecutive nonzero quadratic residues.
  - p divides a center-side element. If this is the case, then $p \equiv 1, 7 \pmod 8$. If $p \equiv 1 \pmod 8$, then p has four consecutive nonzero quadratic residues. If $p \equiv 7 \pmod 8$, then p has two consecutive nonzero non-residues followed by two consecutive nonzero residues.

  - p divides the center element. If this is the case, then $p \equiv 1 \pmod 4$ and p has three consecutive nonzero quadratic residues.

- p divides exactly two elements.
  - p divides two elements that share a side row or side column. If this is the case, then $p \equiv 1 \pmod{24}$.

- p divides exactly three elements.
  - p divides all the elements of a center row or center column. If this is the case, then $p \equiv 1 \pmod 8$ and p attains its minimum order at least twice.
  - p divides all the elements of a long diagonal. If this is the case, then $p \equiv 1 \pmod 4$ and p attains its minimum order at least twice. If p attains a higher order in a corner entry than the other two entries, then $p \equiv 1 \pmod 8$.
  - p divides all the elements of a pandiagonal. If this is the case, then $p \equiv 1, 7 \pmod 8$ and p attains its minimum order at least twice. If p attains a higher order in the corner entry than the other two entries, then $p \equiv 1 \pmod 8$.

3 Sums of Two Squares, and The Prime Signature of the Center Entry

3.1 Finding Expressions as Sums of Two Squares

In the previous section, we classified the ways a prime factor can appear in a 3×3 magic square of squares. In this section, we explore the 3×3 magic square of squares problem from a different angle: we shift our focus away from the numerical values of the prime factors, and instead propose a possible computational approach to ruling out prime signatures of the center entry of the square. (The *prime signature* of a positive integer is the multiset of exponents in its prime factorization. That is, if $k \geq 0$, $p_1, \ldots, p_k$ are distinct primes, and $n_1, \ldots, n_k$ are positive integers, then the prime signature of $p_1^{n_1} \cdots p_k^{n_k}$ is the multiset $\{n_1, \ldots, n_k\}$.)

Recall that if a 3×3 magic square of squares is of the form

a^2	b^2	c^2
d^2	e^2	f^2
g^2	h^2	j^2

,

then $a^2 + j^2$, $b^2 + h^2$, $c^2 + g^2$, and $d^2 + f^2$ are all equal to $2e^2$. That is, $2e^2$ must have at least four ways of being written as a sum of two distinct squares, and these ways can be used to build the entire square. Let the prime factorization of e be $p_1^{n_1} \cdots p_k^{n_k}$. (Recall that $p_l \equiv 1 \pmod 4$ for all l.) Then $2e^2 = 2p_1^{2n_1} \cdots p_k^{2n_k}$. To find the ways of expressing $2e^2$ as a sum

of two distinct squares, we consider its factorization in the ring of Gaussian integers, $\mathbb{Z}[i]$.

To do so, we review some basic facts about factorization in $\mathbb{Z}[i]$. It is known that $\mathbb{Z}[i]$ is a unique factorization domain, and the norm function $\mathrm{N}(x+yi) = x^2+y^2$ is multiplicative; that is, for all $u, v \in \mathbb{Z}[i]$, $\mathrm{N}(uv) = \mathrm{N}(u)\mathrm{N}(v)$. It is also known that if $p \in \mathbb{Z}$ is a prime integer congruent to 1 (mod 4), then there exist unique (up to order and sign) nonzero distinct integers $x, y \in \mathbb{Z}$ such that the prime factorization of p in $\mathbb{Z}[i]$ is $p = (x+yi)(x-yi)$; equivalently, x and y are the unique integers (up to order and sign) such that $p = x^2+y^2$.

For each prime factor p_l of e, let x_l, y_l be the unique positive integers such that $p_l = (x_l+y_l i)(x_l-y_l i)$. (Without loss of generality, we can suppose $x_l > y_l$ for all l.) Then for the prime factorization of $2e^2$ in $\mathbb{Z}[i]$, we have

$$\begin{aligned} 2e^2 &= 2p_1^{2n_1}\cdots p_k^{2n_k} \\ &= (1+i)(1-i)(x_1+y_1 i)^{2n_1}(x_1-y_1 i)^{2n_1}\cdots(x_k+y_k i)^{2n_k}(x_k-y_k i)^{2n_k}. \end{aligned}$$

We now explain how to find the ways to express $2e^2$ as a sum of two distinct squares. Let α, β be distinct, non-opposite, nonzero integers such that $2e^2 = \alpha^2+\beta^2$. Then $2e^2 = (\alpha+\beta i)(\alpha-\beta i)$. Observe that the prime factorization of $\alpha-\beta i$ in $\mathbb{Z}[i]$ can be obtained by taking the prime factorization of $\alpha+\beta i$ and conjugating every prime factor. As such, the prime factorizations of $\alpha+\beta i$ and $\alpha-\beta i$ (up to reordering and appropriate multiplication of the prime factors by units in $\mathbb{Z}[i]$) are — not necessarily respectively — given by

$$(1+i)(x_1+y_1 i)^{a_1}(x_1-y_1 i)^{2n_1-a_1}\cdots(x_k+y_k i)^{a_k}(x_k-y_k i)^{2n_k-a_k}$$

and

$$(1-i)(x_1-y_1 i)^{a_1}(x_1+y_1 i)^{2n_1-a_1}\cdots(x_k-y_k i)^{a_k}(x_k+y_k i)^{2n_k-a_k},$$

where $0 \le a_j \le 2n_j$ for all j. As such, we can find all pairs of α and β (up to order and sign) by iterating through all possible combinations of a_j values and evaluating these expressions with those a_j values.

However, we must limit which combinations of a_j values we consider. We care that α and β be distinct; as such, we must require that $a_j \neq n_j$ for at least one j. Furthermore, observe that for any choice of a_j values, if we replace each a_j with $2n_j - a_j$, we will still obtain the same values of α and β — to avoid this repetition, we can assume without loss of generality that the first a_j value not equal to n_j is less than n_j. By iterating through all choices of a_j values satisfying these conditions, we can find all pairs α, β up to order and sign such that $2e^2 = \alpha^2+\beta^2$.

3.2 Evaluating Prime Signatures

This idea leads to an interesting and potentially useful algorithmic approach to searching for a 3×3 magic square of squares: instead of just considering numerical values of e

to search, we can search based on the prime signature of e. That is, let the multiset $\{n_1,\ldots,n_k\}$ be the possible prime signature of e we wish to evaluate. Then $e = p_1^{n_1}\cdots p_k^{n_k}$ for some distinct primes $p_1,\ldots,p_k$, but we wish to describe the possible "forms" a magic squares can have without actually considering specific numerical values for the primes.

Since we have $p_l = (x_l+y_l i)(x_l-y_l i)$ for all l, we can obtain forms of the square where each entry is a polynomial expression of the x_l and y_l values. For a given prime signature, we can obtain all of these forms in two steps: first, as described in the previous section, perform the appropriate Gaussian integer multiplication under each combination of a-values to find all the ways to express $2e^2$ as a sum of two squares in terms of the x_l and y_l values. This will result in obtaining pairs of square numbers (again, in terms of the x_l and y_l values). Second, compute all the ways to arrange these pairs in a 3×3 square with center e^2 such that the two elements of a pair are always opposite the center entry. (Of course, arrangements that are rotations/reflections/transformations of each other should not count separately.) Doing so obtains all the possible forms of a square whose center element has the specified prime signature; it would remain to find actual numerical values of x_l and y_l that would actually give the non-center rows and columns the right sum.

While we leave it at here for now, we propose that this approach might be an interesting avenue for further research on the 3×3 magic square of squares problem. For example, it may be possible to rule out specific square forms, or even rule out a prime signature in its entirety by ruling out all of its forms. Another interesting possibility might be using this idea to develop faster algorithms to search for such a 3×3 magic square of squares, as after all the forms are found for a given prime signature, they can be used for any value of e with that prime signature without having to recompute them.

4 Conclusion

At this point, we have created a list of all the ways a prime factor can appear in a 3×3 magic square of squares, as well as suggested a possible computational approach to the problem. Some avenues for further progress on the problem may be to continue searching for results on prime factors, as well as to explore this suggested computational approach. Morgenstern's results on establishing lower bounds on the smallest element of such a square indicate that there are also approaches beyond these two.

Some interesting other approaches have also been suggested by other authors. For example, Cain [3] has reformulated the problem in terms of ring extensions of $\mathbb{Z}$, and Várilly-Alvarado [14] has suggested that geometric approaches might be fruitful. It is also interesting to consider this problem over different domains; for example, Cain [3] and Labruna [8] have explored a similar problem over finite fields.

A Computer Code

The file `PrimeArrangements.java` is used to verify the statement of Lemma 2.2. It contains a method of Java code that iterates through all the ways to arrange 0s and 1s on a 3 × 3 grid, printing each arrangement where:

- There are at least three 1s, and they are not all contained within the same row, column, long diagonal, or pandiagonal.
- If a center row/column, long diagonal, or pandiagonal has at least two 1s, then it has three 1s.
- If the center has a 1 and a non-center row/column has at least two 1s, then that row or column has three 1s.

This method will end up only printing the grid where all nine entries are 1; interpreting the 1s as the entries that have the prime p as a factor proves the lemma in question.

References

[1] Boyer, Christian. *Multimagie.com*, multimagie.com. Accessed 20 Apr 2023.

[2] Boyer, Christian. "Some notes on the magic squares of squares problem." *The Mathematical Intelligencer*, vol. 27, no. 2, 2005, pp. 52-64, doi.org/10.1007/BF02985794. Accessed 20 Apr 2023.

[3] Cain, Onno. "Gaussian Integers, Rings, Finite Fields, and the Magic Square of Squares." *Arxiv.org*, 2019, doi.org/10.48550/arXiv.1908.03236. Accessed 20 Apr 2023.

[4] Gardner, Martin. *Riddles of the Sphinx: And Other Mathematical Puzzle Tales*. Washington DC, Mathematical Association of America, 1987.

[5] Gardner, Martin. "The magic of 3 × 3." *Quantum*, vol. 6, no. 3, 1996, pp. 24-26, nsta.org/quantum-magazine-math-and-science. Accessed 20 Apr 2023.

[6] Gardner, Martin. "A Quarter Century of Recreational Mathematics, by Martin Gardner." *Scientific American*, 29 May 2010, https://blogs.scientificamerican.com/observations/a-quarter-century-of-recreational-m-2010-05-26/. Accessed 20 Apr 2023.

[7] Just, Erwin, editor. "Problems". *The College Mathematics Journal*, vol. 15, no. 1, 1984, pp. 68-74, doi.org/10.2307/3027440. Accessed 20 Apr 2023.

[8] Labruna, Giancarlo. "Magic Squares of Squares of Order Three Over Finite Fields." *Montclair State University Digital Commons: Theses, Dissertations and Culminating Projects*, 2018, digitalcommons.montclair.edu/etd/138. Accessed 20 Apr 2023.

[9] Morgenstern, Lee. "Theorem 1." *Multimagie.com*, 2006, multimagie.com/English/Morgenstern01.htm. Accessed 20 Apr 2023.

[10] Morgenstern, Lee. "3 × 3 Magic Square of 7 Squares: Study 1." http://web.archive.org/web/20150511182628/http://home.earthlink.net/~morgenstern/magic/apstruc.htm. Accessed 20 Apr 2023.

[11] Morgenstern, Lee. "3 × 3 Magic Square of Squares Properties." *Multimagie.com*, 2015, multimagie.com/MorgensternMssProperties.pdf. Accessed 20 Apr 2023.

[12] Parker, Matt. "The Parker Square — Numberphile." *YouTube*, uploaded by Numberphile, 18 Apr 2016, https://www.youtube.com/watch?v=aOT_bG-vWyg. Accessed 20 Apr 2023.

[13] Rabern, Landon W. "Properties of Magic Squares of Squares". *Rose-Hulman Undergraduate Mathematics Journal*, vol. 4, no. 1, 2003, scholar.rose-hulman.edu/rhumj/vol4/iss1/3. Accessed 20 Apr 2023.

[14] Várilly-Alvarado, Anthony. "The Geometric Disposition of Diophantine Equations." *Notices of the American Mathematical Society*, vol. 68, no. 8, 2021, pp. 1291-1300, doi.org/10.1090/noti2335. Accessed 20 Apr 2023.

[15] Woll, Christian. "A Partial Residue Categorization of the Magic Square of Squares." *Arxiv.org*, 2018, https://doi.org/10.48550/arXiv.1809.03067. Accessed 20 Apr 2023.

Desmond Weisenberg
Case Western Reserve University
dsw65@case.edu