3x3 Magic Square of Squares Properties

Lee Morgenstern

July, 2015

Abstract

Old properties newly proved using only elementary number theory.
Proofs of new properties not covered elsewhere.
Understanding the proofs requires knowledge of only modular arithmetic and quadratic residues.

Introduction

This paper was inspired by Landon W. Rabern's "Properties of magic squares of squares" which uses algebraic number theory to prove several properties of the entries in a 3x3 magic square of distinct squares. All of Rabern's properties can be derived from the properties of three-square arithmetic progressions which require only elementary number theory.

This paper explains these old properties in a new way making the proofs more understandable to a wider audience and giving greater insight into why these properties are true.

This paper also contains proofs of properties not covered in Rabern's paper.

Lemmas that are used in the proofs

These are all provable using elementary number theory.

Lemma 1 The square of an even number is 0 (mod 4).
$(2n)^2 = 4n^2$, which is a multiple of 4.

Lemma 2 The square of an odd number is 1 (mod 4).
$(2n+1)^2 = 4n^2 + 4n + 1 = 4n(n+1) + 1$.

Lemma 3 -1 is a quadratic residue of all 1 (mod 4) primes,
but a quadratic non-residue of all 3 (mod 4) primes.

Lemma 4 2 is a quadratic residue of all 1 and 7 (mod 8) primes
but a quadratic non-residue of all 3 and 5 (mod 8) primes.

Lemma 5 If x and p have no common factor, then there exists y
such that xy = 1 (mod p).

AP Lemmas

Definition
An AP, Arithmetic Progression of three squares, $A^2 <= C^2 <= B^2$, is such that $B^2 - C^2 = C^2 - A^2$, which can also be written
$A^2 + B^2 = 2C^2$.

Lemma 6 All APs are scaled versions of primitive APs.
If d = gcd(A,B,C), then there exists a,b,c such that
A = ad, B = bd, C = cd, and
$a^2 + b^2 = 2c^2$
with a,b,c pairwise coprime.

Lemma 7 A primitive AP has the formula
$a = 2mn - m^2 + n^2$
$b = 2mn + m^2 - n^2$
$c = m^2 + n^2$
with m and n coprime, one odd, one even,

which can also be written as
$a = 2n^2 - (m - n)^2$
$b = 2m^2 - (m - n)^2$
$c = m^2 + n^2$

Note that since m and n are coprime,
m^2, n^2, and $(m-n)^2$ are also coprime.
And, a and b each have the form
$2r^2 - s^2$ with r and s coprime and s is odd.

MSS Lemmas

Definition
A 3x3 magic square consists of a 3x3 array of entries where each row, column, and diagonal has the same sum.

```
  A  B  C
  D  E  F
  G  H  I
```

In a 3x3 MSS, Magic Square of Squares, all the entries are distinct squares.

Lemma 8
Any 3x3 magic square can be represented by three terms as follows.

```
 x+y  x-y-z  x+z
x-y+z   x   x+y-z
 x-z  x+y+z  x-y
```

From the A - I array above,
let x = E, let y = A - E, and let z = C - E.

```
 x+y    B    x+z
  D     x     F
  G     H     I
```

From (x+y) + D + G = (x+z) + x + G, we have D = x-y+z.
From (x+y) + x + I = (x+z) + F + I, we have F = x+y-z.
From (x+y) + B + (x+z) = B + x + H, we have H = x+y+z.

```
 x+y   B   x+z
x-y+z  x  x+y-z
  G  x+y+z  I
```

The magic sum = (x-y+z) + x + (x+y-z) = 3x.

From (x+y) + B + (x+z) = 3x, we have B = x-y-z.
From (x+y) + (x-y+z) + G = 3x, we have G = x-z.
From (x+z) + (x+y-z) + I = 3x, we have I = x-y.

Lemma 9 Eight APs exist in a 3x3 magic square of squares,

Four of the APs run through the center and cover all nine entries.
x-y, x, x+y step y
x-z, x, x+z step z
x-y-z, x, x+y+z step y+z
x-y+z, x, x+y-z step y-z

Four more APs are on the pandiagonals.
x-y-z, x-z, x+y-z step y
x-y+z, x+z, x+y+z step y
x-y-z, x-y, x-y+z step z
x+y-z, x+y, x+y+z step z

AP Property Theorems

Theorem 1
In the AP, $A^2 + B^2 = 2C^2$,
if C^2 is even, then A^2 and B^2 are both even;
if C^2 is odd, then A^2 and B^2 are both odd.

Proof
$A^2 + B^2$ is even, thus A^2 and B^2 are both even or both odd.
If A^2 and B^2 are both even, then from Lemma 1,
their sum is a multiple of 4, thus C^2 must be even.
If A^2 and B^2 are both odd, then from Lemma 2,
their sum is 2 (mod 4), thus C^2 must be odd.
Therefore A^2,B^2,C^2 are either all even or all odd,
and thus any one of them, such as C^2,
dictates the odd-even parity of the other two.

Theorem 2
The middle term of a primitive AP,
$(m^2 + n^2)$ consists of only 1 (mod 4) primes.

Proof
Suppose the opposite: that a 3 (mod 4) prime p is a factor:
$m^2 + n^2 = pt$ or $m^2 = -n^2 \pmod p$.
p is either a factor of both m and n or a factor of neither.
If p is a factor of neither, then from Lemma 5,
there exists k such that nk = 1 (mod p), thus
$(mk)^2 = -1 \pmod p$, which states that -1 is a quadratic residue
of a 3 (mod 4) prime, contradicting Lemma 3.
Therefore, any 3 (mod 4) prime factor of $m^2 + n^2$
must be a factor of both m and n, so m and n can't be coprime.

Theorem 3
An outer term of a primitive AP,
$(2r^2 - s^2)$ consists of only 1 and 7 (mod 8) primes.

Proof
Suppose the opposite: that a 3 or 5 (mod 8) prime p is a factor:
$2r^2 - s^2 = pt$ or $s^2 = 2r^2 \pmod{p}$.
p is either a factor of both r and s or a factor of neither.
If p is a factor of neither, then from Lemma 5,
there exists k such that $rk = 1 \pmod{p}$, thus
$(sk)^2 = 2 \pmod{p}$, which states that 2 is a quadratic residue
of a 3 or 5 (mod 8) prime, contradicting Lemma 4.
Therefore, any 3 or 5 (mod 8) prime factor of $2r^2 - s^2$
must be a factor of both r and s, so r and s can't be coprime.

MSS Property Theorems

Theorem 4
In a primitive MSS, all entries are odd.

Proof
From Lemma 8, the center entry of a MSS is the center of four APs
that cover all nine entries of the MSS.
From Theorem 1, if this center entry is even, then all AP terms are even,
all nine MSS entries are even, and the MSS is not primitive.
Therefore, the center entry must be odd and all nine entries are odd.

Theorem 5.
In a primitive MSS, the central entry consists of only 1 (mod 4) primes.

Proof
From Theorem 2, the primitive part of the central entry AP must consist
of only 1 (mod 4) primes. So if you discover somehow that the central
entry has a factor of a 3 (mod 4) prime, then it must be part of its scaling.
Nothing wrong so far. But if the center entry of an AP is scaled,
then so are its outer terms, so all eight other terms must have that
3 (mod 4) prime in their scaling. But then the MSS isn't primitive.

Theorem 6
In a primitive MSS, no entry can have a 3 (mod 8) prime factor.

Proof
A 3 (mod 8) prime is also a 3 (mod 4) prime, thus from Theorem 5, a primitive MSS can't have a 3 (mod 8) prime factor in the center. What about the perimeter? All of those are outer terms of some AP that runs through the center as shown in Lemma 8. As such, according to Theorem 3, if a 3 (mod 8) prime is a factor of any of them, it must be part of its scaling, thus that prime must also be a factor of the scaling of the central entry. But that would contradict Theorem 5.

Theorem 7
In a primitive MSS, no middle-side entry can have a 5 (mod 8) prime factor.

Proof
From Lemma 8, a middle-side entry is an outer term of three different APs. If it had a 5 (mod 8) prime factor, then from Theorem 3, it must be part of its scaling and thus the other six terms of its three APs must also have that factor as part of their scalings. That's just too many entries with a common factor to make a primitive MSS.

Theorem 8
If a corner entry has a 3 (mod 4) factor,
then so does a couple of other entries.

Proof
A corner entry is the central term of one AP that is a pandiagonal. It doesn't go through the center and it doesn't affect anything else. But if a central term has a 3 (mod 4) prime factor, then from Theorem 2, it must be part of its scaling, so the other two terms of its AP must also have that prime in their scaling.

Theorem 9
If a corner entry has a 5 (mod 8) prime factor,
then so does a couple of other entries.

Proof
A corner entry is the outer term of an AP that goes through the center. But if an outer term has a 5 (mod 8) prime factor, then from Theorem 3, it must be part of its scaling, so the other two terms of its AP must also have that prime in their scaling.

More MSS Theorems

Theorem 10
In a primitive MSS, all entries are 1 (mod 3).

Proof
The square of 0 (mod 3) is 0 (mod 3).
The square of 1 (mod 3) or 2 (mod 3) is 1 (mod 3).
So in the AP, $A^2 + B^2 = 2C^2$,
$2C^2$ can only be 0 (mod 3) or 2 (mod 3).
A^2 and B^2 must be either both 0 (mod 3) or both 1 (mod 3).
So if C^2 is 0 (mod 3), so are A^2 and B^2.
If C^2 is 1 (mod 3), so are A^2 and B^2.

From Lemma 8, all nine entries are part of APs running through the center.
So if the center is 0 (mod 3), then all entries are 0 (mod 3)
and the MSS would not be primitive.
Thus the center and all entries must be 1 (mod 3).

Theorem 11
There are 84 combinations of 9 entries taken 3 at a time.
12 of those combinations are the rows, columns, diagonals, and pandiagonals.
The remaining 72 combinations are such that they can determine the values of
the other 6 entries by using just addition and subtraction. Therefore,
if there is a factor common to all 3 entries of any one of those 72 combinations,
then all 9 entries have that factor, and the MSS isn't primitive.

For the same reason, no two of the eight APs can have a common prime
in their scale factors.

Theorem 12
In the x,y,z formulation, a 3x3 MSS will have duplicated entries exactly when yz = 0.

Proof
In general, a 3x3 magic square will have duplicated entries when
y = 0, z = 0, y = z, y = -z, y = 2z, y = -2z, z = 2y, or z = -2y,
but this isn't true when the entries are squares.

By symmetry, y and z are interchangeable and negating y or z produces a mirror image solution with the same values.
So there are only 3 inequivalent duplication cases.

(1) y = z > 0, (2) y = 2z > 0, (3) y >= 0 with z = 0.

Duplication Case (1) y = z > 0

```
 x+z  x-2z  x+z
  x    x     x
 x-z  x+2z  x-z
```

x-2z, x-z, x, x+z, x+2z
represent 5 squares in arithmetic progression, which is impossible.

Duplication Case (2) y = 2z > 0

```
 x+2z  x-3z  x+z
 x-z    x    x+z
 x-z   x+3z  x-2z
```

x-3z, x-2z, x-z, x, x+z, x+2z, x+3z
represent 7 squares in arithmetic progression, which is impossible.

Duplication Case (3) y >= 0, z = 0

```
  x+y  x-y   x
  x-y   x   x+y
   x   x+y  x-y
```

x-y, x, x+y represent 3 squares in arithmetic progression,
which is possible, and other than all entries being the same,
the smallest solution is

```
  49   1  25
  1   25  49
  25  49   1
```

Remark. This yz = 0 duplication theorem is important to know both for efficient searching and as a simple goal for an impossibility proof that shows there is no 3x3 MSS having distinct entries.

MSS AP Step Value Restrictions

In the x,y,z formulation above, y and z are the step values of the APs.
If z = py, where p is an integer, there are several restrictions of the value of p.

The x,y,z formulation becomes and x,y,p formulation

x+y	x-(p+1)y	x+py		A^2	B^2	C^2
x+(p-1)y	x	x-(p-1)y	==>	D^2	E^2	F^2
x-py	x+(p+1)y	x-y		G^2	H^2	I^2

Theorem 13
The value of p can't be 0.
Proof
If p = 0, x+py = x, and we have duplicated entries.

Theorem 14
The value of p can't be 1.
Proof
If p = 1, x+y = x+py, and we have duplicated entries.

Theorem 15
The value of p can't be 2.
Proof
If p = 2, x+y = x+(p-1)y, and we have duplicated entries.

Theorem 16
The value of p can't be 3.

Proof
If p = 3, the x,y,z formulation becomes

x+y	x-4y	x+3y
x+2y	x	x-2y
x-3y	x+4y	x-3y

x-4y, x-3y, x-2y, x-y, x, x+y, x+2y, x+3y, x+4y
are nine squares in arithmetic progression.
which is impossible unless y = 0, but then we have duplicated entries.

Theorem 17
The value of p can't be 4.

Proof
If p = 4, the formulation becomes

x+y	x-5y	x+4y
x+3y	x	x-3y
x-4y	x+5y	x-y

x-5y, x-3y, x-y, x+y, x+3y, x+5y
are six squares in arithmetic progression,
which is impossible unless y = 0, but then we have duplicated entries.

Theorem 18
p can't be a 4k+3 prime.

Proof
We require

$$x - y = I^2 \qquad x + y = A^2$$
$$x - py = G^2 \qquad x + py = C^2$$
$$x - (p-1)y = F^2 \qquad x + (p-1)y = D^2$$
$$x - (p+1)y = B^2 \qquad x + (p+1)y = H^2$$

Multiplying the equations in pairs, we get

$$x^2 - y^2 = (AI)^2$$
$$x^2 - p^2y^2 = (CG)^2$$
$$x^2 - (p-1)^2y^2 = (DF)^2$$
$$x^2 - (p+1)^2y^2 = (BH)^2$$

We will prove that the first two equations are discordant,
meaning that that have no solutions in positive integers.

Let D = gcd(x,y), then x = DE, y = DF, AI = DG, CG = DH

Substituting these into the first two equations above
and dividing by D^2, we get

[1] $E^2 - F^2 = G^2$
[2] $E^2 - p^2F^2 = H^2$

Since gcd(E,F) = 1, equation [1] is a primitive pythagorean triangle,
which also means that E is a multiple of only 4k+1 primes.
Therefore, E and p have no common factor,
thus [2] is also a primitive pythagorean triangle.

From [1], $E = m^2 + n^2$, F = 2mn, m and n coprime, one odd, one even
From [2], $E = r^2 + s^2$, pF = 2rs, r and s coprime, one odd, one even

Combining the two expressions for E and F,
[3] $m^2 + n^2 = r^2 + s^2$
[4] mnp = rs

Since m and n are swappable, assume n is even.
Since r and s are swappable, assume that r has p as a factor.
Then there must exist e,f,g,h such that

m = ge, n = fh, r = pgf, s = eh
with f even and e,g,h odd
and e,f,g,h pairwise coprime.

Putting these into [3],
$g^2e^2 + f^2h^2 = p^2g^2f^2 + e^2h^2$
or
$g^2(e^2 - p^2f^2) = h^2(e^2 - f^2)$

Since g,h are coprime and e,f are coprime with e odd, f even,
$e^2 - f^2 = g^2$
$e^2 - p^2f^2 = h^2$
which matches [1] and [2] in smaller values.

Since F > f > 0, we have an infinite descent
showing that F is infinitely factorable and thus must be zero.
Since y = FD, y must be zero and there must be duplications in the MSS.

Theorem 19
p can't be one less than a 4k+3 prime.

Proof
If p is one less than a 4k+3 prime,
then p+1 is a 4k+3 prime and then
the first and last equations below are discordant by Theorem 18.

$x^2 - y^2 = (AI)^2$
$x^2 - p^2y^2 = (CG)^2$
$x^2 - (p-1)^2y^2 = (DF)^2$
$x^2 - (p+1)^2y^2 = (BH)^2$

Theorem 20
p can't be one more than a 4k+3 prime.

Proof
If p is one more than a 4k+3 prime,
then p-1 is a 4k+3 prime and then
the first and third equations above are discordant by Theorem 18.