Hang Lung Mathematics Awards
Vol. 4 (2010)

Hang Lung Mathematics Awards 2010

Honorable Mention

Magic Squares of Squares

Team Member: Pak Hin Li
Teacher: Mr. Chi Ming Chan
School: Po Leung Kuk Vicwood K.T. Chong Sixth Form College

Hang Lung Mathematics Awards
Vol. 4 (2010), pp. 201–224

MAGIC SQUARES OF SQUARES

TEAM MEMBER
Pak Hin Li

TEACHER
Mr. Chi Ming Chan

SCHOOL
Po Leung Kuk Vicwood K.T.Chong Sixth Form College

Abstract. In this report, we want to know whether there is a magic square whose entries are distinct perfect squares.

Firstly, we analyze the basic properties of a magic square and find that the magic sum of a magic square is equal to 3 times of the central entry and the 9 entries of a magic square contain 8 arithmetic progressions.

Secondly, we focus on our main target, magic square of squares. Investigating the properties of the prime factors of those 9 entries, we find that if the greatest common divisor of all entries is equal to 1, the prime factors of central entry are of the form $p \equiv 1 \pmod 4$, the central entry must not be a square of a prime number and the common prime factors of any two adjacent entries (if exist) are not of the form $p \equiv 3 \pmod 4$.

Thirdly, we find that this problem is equivalent to a system of Diophantine equations with ten variables. We provide a construction method of the solution to these partial equations:

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

where these nine perfect squares are distinct.

Finally, based on the theorems obtained, we find that given a positive integer N, there exists a positive integer M such that it has N essentially different representations of a sum of two perfect squares.

1. Part I

First of all, let's define what magic square is.

Definition 1. *A magic square is a $n \times n$ square of which entries are positive integers and sum in any row, column or main diagonal is the same. This sum is called magic sum.*

In this report, we only focus on 3×3 magic square. A magic square must have the form:

x_1	x_2	x_3
x_4	x_5	x_6
x_7	x_8	x_9

Property 1. *If M denotes the magic sum, $M = 3x_5$.*

Proof.

$$\begin{aligned} 4M &= (x_1 + x_5 + x_9) + (x_2 + x_5 + x_8) + (x_3 + x_5 + x_7) + (x_4 + x_5 + x_6) \\ &= (x_1 + x_2 + x_3) + (x_4 + x_5 + x_6) + (x_7 + x_8 + x_9) + 3x_5 \\ &= 3M + 3x_5 \end{aligned}$$

Therefore, $M = 3x_5$. □

Property 2. *All the entries can be expressed by 3 integers and every magic square has the form*

$c - a + b$	$c + a - 2b$	$c + b$
$c + a$	c	$c - a$
$c - b$	$c - a + 2b$	$c + a - b$

,

where $c = x_5, a = x_5 - x_6, b = x_5 - x_7$.

Proof. $x_1 + x_5 + x_9 = x_2 + x_5 + x_8 = x_3 + x_5 + x_7 = x_4 + x_5 + x_6 = 3x_5 = M$

Therefore, $x_1 = 2x_5 - x_9, x_2 = 2x_5 - x_8, x_4 = 2x_5 - x_6, x_3 = 2x_5 - x_7$.

Since $M = x_1 + x_4 + x_7 = x_3 + x_6 + x_9 = x_1 + x_2 + x_3 = 3x_5$,

$$\begin{aligned} x_1 &= 3x_5 - x_7 - (2x_5 - x_6) = x_5 + x_6 - x_7, \\ x_9 &= 3x_5 - x_3 - x_6 = 3x_5 - (2x_5 - x_7) - x_6 = x_5 - x_6 + x_7 \text{ and} \\ x_2 &= 3x_5 - x_1 - x_3 = 3x_5 - (x_5 + x_6 - x_7) - (2x_5 - x_7) = 2x_7 - x_6 \end{aligned}$$

Since $x_8 = 2x_5 - x_2, x_8 = 2x_5 - (2x_7 - x_6) = 2x_5 + x_6 - x_7$.

Let $c = x_5, a = x_5 - x_6, b = x_5 - x_7$,

x_1	x_2	x_3
x_4	x_5	x_6
x_7	x_8	x_9

can be written as

$c-a+b$	$c+a-2b$	$c+b$
$c+a$	c	$c-a$
$c-b$	$c-a+2b$	$c+a-b$

□

Property 3. *The corner entry equals the average of the two middle-side entries that are not adjacent to the corner.*

The central entry equals the average of the two entries that are in the same magic line through the central entry.

Proof. since $x_1+x_5+x_9 = x_2+x_5+x_8 = x_3+x_5+x_7 = x_4+x_5+x_6 = 3x_5 = M$,

$$x_1+x_9 = x_2+x_8 = x_3+x_7 = x_4+x_6 = 2x_5 \tag{1}$$

By property 2:

$$x_2+x_4 = 2x_9 \tag{2}$$
$$x_2+x_6 = 2x_7 \tag{3}$$
$$x_6+x_8 = 2x_1 \tag{4}$$
$$x_4+x_8 = 2x_3 \tag{5}$$

□

2. Part II

In this part, we investigate the properties of magic squares of squares, of which entries are distinct perfect squares.

A magic square of squares must have this form:

y_1^2	y_2^2	y_3^2
y_4^2	y_5^2	y_6^2
y_7^2	y_8^2	y_9^2

,

where y_i are distinct positive integer. $(i = 1, 2, \ldots, 9)$

If the greatest common divisor of $y_1, y_2, \ldots, y_9$ $(= D)$ is greater than 1,

$\frac{y_1^2}{D^2}$	$\frac{y_2^2}{D^2}$	$\frac{y_3^2}{D^2}$
$\frac{y_4^2}{D^2}$	$\frac{y_5^2}{D^2}$	$\frac{y_6^2}{D^2}$
$\frac{y_7^2}{D^2}$	$\frac{y_8^2}{D^2}$	$\frac{y_9^2}{D^2}$

is also a magic squares of square so, in this part, we only focus on the case when g.c.d $(y_1, y_2, \ldots, y_9) = 1$.

We assume all entries are relatively prime in this part.

Property 4. *$y_1, y_2, \ldots, y_9$ are odd numbers.*

Proof. Suppose $y_5 \equiv 0 \pmod 2$, we can get $y_5^2 \equiv 0 \pmod 4$ and $2y_5^2 \equiv 0 \pmod 8$,

$\therefore 2y_5^2 = y_i^2 + y_{10-i}^2 \equiv 0 \pmod 8$ for $(i = 1, 2, 3, 4, 6, 7, 8, 9)$ (By (1)).

$a^2 = \begin{cases} 0 \text{ or } 4 \pmod 8 & \text{if } a \text{ is even} \\ 1 \pmod 8 & \text{if } a \text{ is odd} \end{cases}$ (see Lemma 15 in the Appendix), so

$$a^2 + b^2 \equiv 0 \pmod 8 \iff a \equiv b \equiv 0 \pmod 2 \tag{6}$$

(by considering the positive outcome of $a^2 + b^2 \pmod 8$)

[See reviewer's comment (1)]

$\therefore y_i \equiv 0 \pmod 2$ for $(i = 1, 2, \ldots, 9)$ which contradicts our assumption:

$$\text{g.c.d } (y_1, y_2, \ldots, y_9) = 1.$$

We must have

$$y_5 \equiv 1 \pmod 2 \tag{7}$$

Suppose $y_i = 2t_i$, where $t_i \in \mathbb{Z}$ $(i \in \{1, 2, 3, 4, 6, 7, 8, 9\})$.

From (1), we get: $y_i^2 + y_{10-i}^2 = 2y_5^2, y_{10-i}^2 = 2(y_5^2 - 2t_i^2)$,

$\therefore \exists t_{10-i} \in \mathbb{Z}$ s.t. $y_{10-i} = 2t_{10-i}$, $2(t_i^2 + t_{10-i}^2) = y_5^2$.

$\therefore y_5 \equiv 0 \pmod 2$ which contradicts (7) so we must have $y_i \equiv 1 \pmod 2$.

we can get $y_i \equiv 1 \pmod 2$ for $i \in \{1, 2, 3, 4, 6, 7, 8, 9\}$. □

Property 5. *The prime factors of y_5 are of the form $p \equiv 1 \pmod 4$.*

Proof. Let p be a prime of y_5, we can get:

$$y_i^2 + y_{10-i}^2 \equiv 2y_5^2 \pmod p \text{ where } (i = 1, 2, 3, 4, 6, 7, 8, 9).$$

There exists a $i \in \{1, 2, 3, 4, 6, 7, 8, 9\}$ such that y_i is not divisible by p, otherwise all entries are divisible by p. Let $p \nmid y_i$, $y_i^2 + y_{10-i}^2 \equiv 0 \pmod p$. Since $\forall a \in \mathbb{Z}$, such that g.c.d$(a, p) = 1$, $\exists a^* \in \mathbb{Z}$, such that $aa^* \equiv 1 \pmod p$ (see Lemma 16 in the Appendix).

$$\therefore (y_i^*)^2(y_i^2 + y_{10-i}^2) \equiv 0 \pmod p, \quad (y_i^* y_{10-i})^2 \equiv -1 \pmod p,$$

We can get that $x^2 \equiv -1 \pmod p$ is solvable so $\left(\frac{-1}{p}\right) = 1$. (here $\left(\frac{a}{p}\right)$ denotes the Legendre symbol.)

By Euler's criterion:

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p$$

(where a, p are relatively prime and p is an odd prime) (see Lemma 17 in the appendix), we can get $(-1)^{\frac{p-1}{2}} = 1$, so $p \equiv 1 \pmod 4$. □

Property 6. *The common prime factors of any two adjacent entries (if exist) are not of the form $p \equiv 3 \pmod 4$.*

Proof. It is impossible for y_5 to have a prime factor p such that $p \equiv 3 \pmod 4$. Duo to the symmetry of magic square, we can suppose $y_1 \equiv y_2 \equiv 0 \pmod p$ where $p \equiv 3 \pmod 4$ and p is a prime.

If $a^2 + b^2 \equiv 0 \pmod p$ and p is a prime s.t. $p \equiv 3 \pmod 4$, then $a \equiv b \equiv 0 \pmod p$. (see Lemma 18 in the Appendix.)

By (4),

$$y_6^2 + y_8^2 = 2y_1^2 \equiv 0 \pmod{p}.$$

By Lemma 18,

$$y_6 \equiv y_8 \equiv 0 \pmod{p}.$$

By (1),

$$2y_5^2 = y_2^2 + y_8^2 \equiv 0 \pmod{p},$$

so $y_3 \equiv 0 \pmod{p}$ which contradicts Property 5. □

Property 7. *If y_5 is divisible by 5, any entries adjacent to the central entry are not divisible by 5.*

[See reviewer's comment (2)]

Proof. WLOG, let $y_2 \equiv 0 \pmod 5$, $y_8^2 \equiv 2y_5^2 - y_2^2 \equiv 0 \pmod 5$,

$$\therefore y_8 \equiv 0 \pmod 5.$$

Let $y_1^2 \equiv a \pmod 5$.

By (4), $2y_1^2 = y_8^2 + y_6^2 \equiv 0 + y_6^2 \pmod 5$, so $y_6^2 \equiv 2a \pmod 5$.

By (1), we can get:

$$y_9 \equiv -a \pmod 5 \text{ and } y_4^2 \equiv -2a \pmod 5.$$

By (3), we can get:

$$2y_7^2 = y_2^2 + y_6^2 \equiv 0 + 2a \pmod 5 \text{ so } y_7^2 \equiv a \pmod 5.$$

By (1),

$$y_3^2 \equiv -a \pmod 5,$$

$$\forall a \in \mathbb{Z}, a^2 = 0, 1 \text{ or } 4 \pmod 5 \tag{8}$$

(by considering the possible outcome of $a^2 \pmod 5$) so $a \equiv 0, 1$ or $4 \pmod 5$.

Since $y_6^2 \equiv 2a \pmod 5$, $2a \equiv 0, 1$ or $4 \pmod 5$. As a result, $5 \mid a$. This contradicts our assumption: all entries are relatively prime.

$\therefore$ any entries adjacent to the central entry are not divisible by 5. □

Property 8. *y_5 must be a composite nuymber.*

Proof. Suppose $2p^2 = a^2 + b^2 = c^2 + d^2$ has a solution such that p is a prime and a, b, c, d are distinct odd positive numbers:

WLOG let $a > c > d > b > 0$:

Let $d_0 = $ g.c.d (a, b), $a = d_0 a_0, b = d_0 b_0$, where g.c.d$(a_0, b_0) = 1$.

$2p^2 = a^2 + b^2 = d_0^2(a_0^2 + b_0^2)$ so $d_0^2 \mid 2p^2$. Since $2 \nmid a, b$, $2 \nmid d_0$,

$\therefore d_0^2 \mid p^2$ and $d_0 \mid p$. Since p is a prime, $d_0 = p$ or 1.

If $d_0 = p$, we have $2 = a_0^2 + b_0^2$ so $a_0 = b_0 = 1$. However, this is contradictory to our initial condition "a, b, c, d are distinct odd positive number".

$\therefore$ g.c.d$(a, b) = 1$. Similarly, using the same argument, we have g.c.d $(c, d) = 1$.

$$\begin{aligned} 4p^4 &= (2p^2)^2 = (a^2 + b^2)(c^2 + d^2) \\ &= (ac - bd)^2 + (ad + bc)^2 = (ac + bd)^2 + (ad - bc)^2 \end{aligned} \tag{9}$$

since

$$(ac + bd)(ad + bc) = cd(a^2 + b^2) + ab(c^2 + d^2) = 2p^2(ab + cd) \tag{10}$$

$$p^2 \mid (ac + bd)(ad + bc)$$

There are three cases:

Case A: $p^2 \mid ac + bd$, Case B: $p^2 \mid ad + bc$, Case C: $p \mid ac + bd$ and $p \mid ad + bc$.

Case A:

let $kp^2 = ac + bd$, where $k \in \mathbb{N}$.

From (9),

$$(ad - bc)^2 = 4p^4 - (ac + bd)^2 = (4 - k^2)p^4 \tag{11}$$

$\therefore p^2 \mid ad - bc$. Let $ad - bc = sp^2$, where $s \in \mathbb{Z}$.

Put it into (11), we get: $s^2 + k^2 = 4$. Since $k \in \mathbb{N}$, $k = 1$ or 2.

When $k = 1$, no solution. When $k = 2$, $s = 0$. So $ad = bc$, $\frac{a}{b} = \frac{c}{d}$.

Since g.c.d$(a, b) =$ g.c.d$(c, d) = 1$, we have $a = c$ and $b = d$, that contradicts a, b, c, d are distinct odd positive numbers.

Case B is similar to Case A.

Case C: $p \mid ac + bd$ and $p \mid ad + bc$,

let $ac + bd = s_1 p$, $ad + bc = s_2 p$, where s_1 and s_2 are positive integers.

From (9), $(ac - bd)^2 = 4p^4 - (ad + bc)^2 = 4p^4 - (s_2 p)^2 = p^2(4p^2 - s_2^2)$, and $(ad - bc)^2 = 4p^4 - (ac + bd)^2 = p^2(4p^2 - s_1^2)$, so $p \mid (ad - bc)$ and $p \mid (ac - bd)$.

Let $ad - bc = k_1 p$ and $ac - bd = k_2 p$, where $k_1, k_2 \in \mathbb{Z}$.

Hence, $ac + bd$, $ad + bc$, $ac - d$ and $ad - bc \equiv 0 \pmod{p}$.

The difference or sum of any two numbers out of these four numbers is also divisible by p.

As a result, ac, bd, ad and $bc \equiv 0 \pmod{p}$.

If $a \equiv 0 \pmod{p}$, $b^2 = 2p^2 - a^2 \equiv 0 \pmod{p}$.

Thus, $b \equiv 0 \pmod{p}$ since p is a prime.

However, it is imposiible since g.c.d$(a, b) = 1$.

Similarly, a, b, c, d are not divisible by p contradicting "ac, bd, ad and bc are divisible by p".

Combining Cases A, B and C, we conclude that it is impossible for $2p^2$ to have two essentially different representations of the sum of two squares.

Since $2y_5^2 = y_i^2 + y_{10-i}^2$ for $(i = 1, 2, 3, 4)$, $2y_5^2$ has four essentially different represntations of the sum of two squares.

$\therefore y_5$ must not be a prime.

[See reviewer's comment (3)] □

3. Part III

The existence of magic square of squares is equivalent to the existence of the solution to this set of Diophantine equations:

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

where $a, b, c, d, e, f, g, h, i$ and M are distinct positive integers.

In this part, we provide a construction method of solutions to these Diophantine equations:

$$a^2 + b^2 = c^2 + d^2 = e^2 + f^2 = g^2 + h^2 = 2k^2 \qquad (*)$$

From (1), we find that the 9 entries satisfy (*). If we can find a construction method of solutions to (*), it is possible for us to find magic square of squares.

Theorem 9.

$$(a,b) = (k_1k_3k_5 - k_2k_4k_5 - k_1k_4k_6 - k_2k_3k_6, k_1k_3k_6 - k_2k_4k_6 + k_1k_4k_5 + k_2k_3k_5)$$
$$(c,d) = (k_1k_3k_5 + k_2k_4k_5 - k_1k_4k_6 + k_2k_3k_6, k_1k_3k_6 + k_2k_4k_6 + k_1k_4k_5 - k_2k_3k_5)$$
$$(e,f) = (k_1k_3k_5 + k_2k_4k_5 + k_1k_4k_6 - k_2k_3k_6, k_1k_3k_6 + k_2k_4k_6 - k_1k_4k_5 + k_2k_3k_5)$$
$$(g,h) = (k_1k_3k_5 - k_2k_4k_5 + k_1k_4k_6 + k_2k_3k_6, k_1k_3k_6 - k_2k_4k_6 - k_1k_4k_5 - k_2k_3k_5)$$

where $(k_1,k_2,k_3,k_4,k_5,k_6) = (t_1^2-t_2^2, 2t_1t_2, t_3^2-t_4^2, 2t_3t_4, t_5^2-t_6^2-2t_5t_6, t_5^2-t_6^2+2t_5t_6)$ *and* $k = (t_1^2+t_2^2)(t_3^2+t_4^2)(t_5^2+t_6^2)$*, then* a,b,c,d,e,f,g,h,k *are solution to*

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

Proof. We have this identity:

$$(ac-bd)^2 + (ad+bc)^2 = (ac+bd)^2 + (ad-bc)^2 = (a^2+b^2)(c^2+d^2) \qquad (9)$$

Using this identity repeatedly, we get:

$$\begin{aligned}
&(k_1^2+k_2^2)(k_3^2+k_4^2)(k_5^2+k_6^2)\\
&= ((k_1k_3-k_2k_4)^2 + (k_1k_4+k_2k_3)^2)(k_5^2+k_6^2)\\
&= ((k_1k_3+k_2k_4)^2 + (k_1k_4-k_2k_3)^2)(k_5^2+k_6^2)\\
&= ((k_1k_3+k_2k_4)k_5 - (k_1k_4-k_2k_3)k_6)^2 + ((k_1k_3+k_2k_4)k_6 + (k_1k_4-k_2k_3)k_5)^2\\
&= ((k_1k_3+k_2k_4)k_5 + (k_1k_4-k_2k_3)k_6)^2 + ((k_1k_3+k_2k_4)k_6 - (k_1k_4-k_2k_3)k_5)^2\\
&= ((k_1k_3-k_2k_4)k_5 - (k_1k_4+k_2k_3)k_6)^2 + ((k_1k_3-k_2k_4)k_6 + (k_1k_4+k_2k_3)k_5)^2\\
&= ((k_1k_3-k_2k_4)k_5 - (k_1k_4+k_2k_3)k_6)^2 - ((k_1k_3-k_2k_4)k_6 + (k_1k_4+k_2k_3)k_5)^2
\end{aligned}$$

[See reviewer's comment (4)]

Let

$$(a,b) = (|k_1k_3k_5 - k_2k_4k_5 - k_1k_4k_6 - k_2k_3k_6|, |k_1k_3k_6 - k_2k_4k_6 + k_1k_4k_5 + k_2k_3k_5|)$$
$$(c,d) = (|k_1k_3k_5 + k_2k_4k_5 - k_1k_4k_6 + k_2k_3k_6|, |k_1k_3k_6 + k_2k_4k_6 + k_1k_4k_5 - k_2k_3k_5|)$$
$$(e,f) = (|k_1k_3k_5 + k_2k_4k_5 + k_1k_4k_6 - k_2k_3k_6|, |k_1k_3k_6 + k_2k_4k_6 - k_1k_4k_5 + k_2k_3k_5|)$$
$$(g,h) = (|k_1k_3k_5 - k_2k_4k_5 + k_1k_4k_6 + k_2k_3k_6|, |k_1k_3k_6 - k_2k_4k_6 - k_1k_4k_5 - k_2k_3k_5|),$$

then $a^2+b^2 = c^2+d^2 = e^2+f^2 = g^2+h^2 = (k_1^2+k_2^2)(k_3^2+k_4^2)(k_5^2+k_6^2)$.
If we let

$$(k_1,k_2,k_3,k_4,k_5,k_6) = (t_1^2-t_2^2, 2t_1t_2, t_3^2-t_4^2, 2t_3t_4, t_5^2-t_6^2-2t_5t_6, t_5^2-t_6^2+2t_5t_6),$$
$$(k_1^2+k_2^2)(k_3^2+k_4^2)(k_5^2+k_6^2) = (t_1^2+t_2^2)^2(t_3^3+t_4^2)^2(2(t_5^2+t_6^2)^2) = 2k^2,$$

where

$$k = (t_1^2+t_2^2)(t_3^2+t_4^2)(t_5^2+t_6^2).$$

[See reviewer's comment (5)] □

Example 10. *Taking* $(t_1,t_2,t_3,t_4,t_5,t_6)=(1,2,3,4,5,6)$*, we can get:*

$$2(7625)^2=10225^2+3425^2=6151^2+8857^2=10463^2+2609^2=425^2+10775^2$$

so we can find a solution of (*).

Corollary 11. $(ac-bd)^2+(ad+bc)^2=(ac+bd)^2+(ad-bc)^2$ *represent two different ways of sum of two squares and these four squares are distinct if and only if*

$$abcd(a^2-b^2)(c^2-d^2)(a^2(c-d)^2-b^2(c+d)^2)(a^2(c+d)^2-b^2(c+d)^2)\neq 0.$$

Proof. These four squares are distinct

$$\begin{aligned}
&\iff ((ac-bd)^2-(ad+bc)^2)((ac-bd)^2-(ac+bd)^2)\\
&\quad\times((ac-bd)^2-(ad-bc)^2)((ad+bc)^2-(ac+bd)^2)\\
&\quad\times((ad+bc)^2-(ad-bc)^2)((ac+bd)^2-(ad-bc)^2)\neq 0\\
&\iff 16a^2b^2c^2d^2(a^2-b^2)^2(c^2-d^2)^2(a^2(c-d)^2-b^2(c+d)^2)\\
&\quad\times(a^2(c+d)^2-b^2(c+d)^2)\neq 0\\
&\iff abcd(a^2-b^2)(c^2-d^2)(a^2(c-d)^2-b^2(c+d)^2)(a^2(c+d)^2-b^2(c+d)^2)\neq 0
\end{aligned}$$

[See reviewer's comment (6)] □

Corollary 12. *If* a,b,c,d,e,f,g,h *obtained in Theorem 9 are distinct, then*

$$\begin{aligned}
&k_1k_2k_3k_4k_5k_6(k_1k_5\pm k_2k_6)(k_2k_5\pm k_1k_5)(k_1k_3\pm k_1k_5)\\
&\times(k_2k_3\pm k_1k_4)(k_3k_5\pm k_4k_6)(k_4k_5\pm k_3k_6)\neq 0.
\end{aligned}$$

Proof. $(k_1^2+k_2^2)(k_3^2+k_4^2)(k_5^2+k_6^2)=(k_{i_1}^2+k_{i_2}^2)(k_{i_3}^2+k_{i_4}^2)(k_{i_5}^2+k_{i_6}^2)$, where sets $\{i_1,i_2\},\{i_3,i_4\},\{i_5,i_6\}$ are permutation of the sets $\{1,2\},\{3,4\},\{5,6\}$.

$$\begin{aligned}
&(k_{i_1}^2+k_{i_2}^2)(k_{i_3}^2+k_{i_4}^2)(k_{i_5}^2+k_{i_6}^2)\\
&=((k_{i_1}k_{i_3}\mp k_{i_2}k_{i_4})^2+(k_{i_1}k_{i_4}\pm k_{i_2}k_{i_3})^2)(k_{i_5}^2+k_{i_6}^2)\\
&=((k_{i_1}k_{i_3}\mp k_{i_2}k_{i_4})k_{i_5}\pm(k_{i_1}k_{i_4}\pm k_{i_2}k_{i_3})k_{i_6})^2+\\
&\quad((k_{i_1}k_{i_3}\mp k_{i_2}k_{i_4})k_{i_6}\mp(k_{i_1}k_{i_4}\pm k_{i_2}k_{i_3})k_{i_5})^2,
\end{aligned}$$

where the two red sign $\mp$ and $\pm$ are chosen in a opposite way.

[See reviewer's comment (V)]

It is not difficult to see that no matter what the permutation of $\{i_1,i_2\},\{i_3,i_4\},\{i_5,i_6\}$ we choose, the sum of two squares generated by this approach is always amount the four representations generated in Theorem 9.

By Corollary 11,

$$abcd(a^2-b^2)(c^2-d^2)(a^2(c-d)^2-b^2(c+d)^2)(a^2(c+d)^2-b^2(c+d)^2)\neq 0,$$

where $a=k_{i_1}k_{i_3}\mp k_{i_2}k_{i_4}, b=k_{i_1}k_{i_4}\pm k_{i_2}k_{i_3}, c=k_{i_5}, d=k_{i_6}$.

Since $\{i_1, i_2\}, \{i_3, i_4\}, \{i_5, i_6\}$ is a permutation of $\{1, 2\}, \{3, 4\}, \{5, 6\}$, we can get

$$k_1k_2k_3k_4k_5k_6(k_1k_5 \pm k_2k_6)(k_2k_5 \pm k_1k_5)(k_1k_3 \pm k_1k_5)$$
$$\times (k_2k_3 \pm k_1k_4)(k_3k_5 \pm k_4k_6)(k_4k_5 \pm k_3k_6) \neq 0$$

□

We investigate whether this approach can help us find magic square of squares.

Corollary 13. *If there exists 9 distinct positive integers such that*

$$2y_5^2 = y_i^2 + y_{10-i}^2 \text{ (for } i = 1, 2, 3, 4) \tag{10}$$

and

$$y_2^2 + y_4^2 = 2y_9^2, \tag{11}$$
$$y_2^2 + y_6^2 = 2y_7^2, \tag{12}$$
$$y_6^2 + y_8^2 = 2y_1^2, \tag{13}$$
$$y_4^2 + y_8^2 = 2y_3^2, \tag{14}$$

y_i^2 $(i = 1, 2, \ldots, 9)$ *are the entries of magic square of squares.*

Proof. We want to prove

y_1^2	y_2^2	y_3^2
y_4^2	y_5^2	y_6^2
y_7^2	y_8^2	y_9^2

is that magic square of squares. This suffics to prove

$$y_1^2 + y_4^2 + y_7^2 = y_7^2 + y_8^2 + y_9^2 = y_9^2 + y_6^2 + y_3^2 = y_1^2 + y_2^2 + y_3^2 = 3y_5^2$$

and

$$3y_5^2 = y_i^2 + y_{10-i}^2 + y_5^2 \quad (\text{for } i = 1, 2, 3, 4).$$

By (10),

$$3y_5^2 = y_i^2 + y_{10-i}^2 + y_5^2 \quad (\text{for } i = 1, 2, 3, 4).$$

By (12), (13):

$$y_1^2 + y_4^2 + y_7^2 = \frac{y_6^2 + y_8^2}{2} + (2y_5^2 - y_6^2) + \frac{y_2^2 + y_6^2}{2} = 2y_5^2 + \frac{y_2^2 + y_8^2}{2} = 3y_5^2.$$

Similarly,

$$y_7^2 + y_8^2 + y_9^2 = y_9^2 + y_6^2 + y_3^2 = y_1^2 + y_2^2 + y_3^2 = 3y_5^2.$$

□

There are many possible ways of distribution of $a^2, b^2, \ldots, h^2$ and k^2 in the entries of magic square. It is hard to verify all the cases so we shift our attention to an interesting fact:

Given a positive integer N, there exits a positive integer M such that it has N essentially different representations of a sum of two perfect squares.

4. Part IV

In this part, we prove an interesting fact:

Given a positive integer N, there exits a positive integer M such that it has N essentially different representations of a sum of two perfect squares.

Proof. [See reviewer's comment (7)]
$a^2 + b^2 = c^2 + d^2$ where a, b, c, d are positive distinct integers.

Let p, q be two distinct positive integers: consider

$$\begin{aligned}&(a^2+b^2)(p^2+q^2) = (ap-bq)^2 + (aq+bp)^2 = (ap+bq)^2 + (aq-bp)^2\\ =\ &(c^2+d^2)(p^2+q^2) = (cp-dq)^2 + (cq+dp)^2 = (cp+dq)^2 + (cq-dp)^2\end{aligned}$$

If $(ap-bq)^2$, $(aq+bp)^2$, $(ap+bq)^2$, $(aq-bp)^2$, $(cp-dq)^2$, $(cq+dp)^2$, $(cp+dq)^2$, $(cp+dq)^2$ and $(cq-dp)^2$ are different integers, then their pairwise difference are not equal to zero.

By Corollary 11,

$$pqcd(p^2-q^2)(c^2-d^2)(p^2(c-d)^2 - q^2(c+d)^2)(p^2(c+d)^2 - q^2(c+d)^2) \neq 0 \quad (15)$$

guarantees $(cp-dq)^2$, $(cq+dp)^2$, $(cp+dq)^2$, $(cq-dp)^2$ are distinct.

By Corollary 11,

$$pqab(p^2-q^2)(a^2-b^2)(p^2(a-b)^2 - q^2(a+b)^2)(p^2(a+b)^2 - q^2(a+b)^2) \neq 0 \quad (16)$$

guarantees $(ap-bq)^2$, $(aq+bp)^2$, $(ap+bq)^2$, $(aq-bp)^2$ are distinct.

Now we only need to consider

$$
\begin{aligned}
&((cq+dp)^2-(ap-bq)^2)((cq+dp)^2-(aq+bp)^2)\\
&\times((cq+dp)^2-(ap+bq)^2)((cq+dp)^2-(aq-bp)^2)\\
&\times((cq-dp)^2-(ap-bq)^2)((cq-dp)^2-(aq+bp)^2)\\
&\times((cq-dp)^2-(ap+bq)^2)((cq-dp)^2-(aq-bp)^2)\\
&\times((cp-dq)^2-(ap-bq)^2)((cp-dq)^2-(aq+bp)^2)\\
&\times((cp-dq)^2-(ap+bq)^2)((cp-dq)^2-(aq-bp)^2)\\
&\times((cp+dq)^2-(ap-bq)^2)((cp+dq)^2-(aq+bp)^2)\\
&\times((cp+dq)^2-(ap+bq)^2)((cp+dq)^2-(aq-bp)^2)\\
&\neq 0\\
\iff\quad & cq\pm dp\pm ap\pm bq\neq 0, cq\pm dp\pm aq\pm bp\neq 0,\\
& cp\pm dq\pm ap\pm bq\neq 0, cp\pm dq\pm aq\pm bp\neq 0, \qquad (17)
\end{aligned}
$$

where the sign can be choosen arbitrarily. Hence, these 32 numbers should be nonzero.

From (17), we can get:

$$\frac{p}{q}\neq\left|\frac{b\pm c}{a\pm d}\right|,\left|\frac{b\pm d}{a\pm c}\right|,\left|\frac{a\pm d}{b\pm c}\right| \text{ or } \left|\frac{a\pm c}{b\pm d}\right|$$

From (15) and (16), we can get:

$$\frac{p}{q}\neq\left|\frac{a+b}{a-b}\right|,\left|\frac{a-b}{a+b}\right|,\left|\frac{c+d}{c-d}\right| \text{ or } \left|\frac{c-d}{c+d}\right|$$

If we take

$$\frac{p}{q}>\max\left\{\left|\frac{b\pm c}{a\pm d}\right|,\left|\frac{b\pm d}{a\pm c}\right|,\left|\frac{a\pm d}{b\pm c}\right|,\left|\frac{a\pm c}{b\pm d}\right|,\left|\frac{a+b}{a-b}\right|,\left|\frac{a-b}{a+b}\right|,\left|\frac{c+d}{c-d}\right|,\left|\frac{c-d}{c+d}\right|\right\},$$

and have $(p^2-q^2)(c^2-d^2)(a^2-b^2)\neq 0$, we can guarantee

$$
\begin{aligned}
&(ap-bq)^2+(aq+bp)^2=(ap+bq)^2+(aq-bp)^2\\
=\;&(cp-dq)^2+(cq+dp)^2=(cp+dq)^2+(cq-dp)^2
\end{aligned}
$$

represent four representation of the sum of squares.

Since the denominators of

$$\left|\frac{b\pm c}{a\pm d}\right|,\left|\frac{b\pm d}{a\pm c}\right|,\left|\frac{a\pm d}{b\pm c}\right|,\left|\frac{a\pm c}{b\pm d}\right|,\left|\frac{a+b}{a-b}\right|,\left|\frac{a-b}{a+b}\right|,\left|\frac{c+d}{c-d}\right|,\left|\frac{c-d}{c+d}\right|$$

are positive integers,

$$\max\left\{\left|\frac{b\pm c}{a\pm d}\right|,\left|\frac{b\pm d}{a\pm c}\right|,\left|\frac{a\pm d}{b\pm c}\right|,\left|\frac{a\pm c}{b\pm d}\right|,\left|\frac{a+b}{a-b}\right|,\left|\frac{a-b}{a+b}\right|,\left|\frac{c+d}{c-d}\right|,\left|\frac{c-d}{c+d}\right|\right\}$$
$$\leq \max\{|a\pm b|,|a\pm c|,|a\pm d|,|b\pm c|,|b\pm d|,|c\pm d|\}$$

To conclude, if we take $\frac{p}{q} > \max\{|a\pm b|,|a\pm c|,|a\pm d|,|b\pm c|,|b\pm d|,|c\pm d|\}$ and have $(p^2-q^2)(c^2-d^2)(a^2-b^2)(a^2-c^2)(a^2-d^2)\neq 0$, we can guarantee

$$\begin{aligned}&(ap-bq)^2+(aq+bp)^2=(ap+bq)^2+(aq-bp)^2\\ =\ &(cp-dq)^2+(cq+dp)^2=(cp+dq)^2+(cq-dp)^2\end{aligned}$$

represent four representation of the sum of squares.

Thus,we have

Corollary 14. *If* $\frac{x}{y} > \max\limits_{(p,q)\in\{l,i,j,k\}^2}\{|r_p\pm r_q|\}$ *and* x,y,r_l,r_k,r_i,r_j *are distinct positive integers such that* $r_i^2+r_j^2=r_l^2+r_k^2$*, then*

$$\begin{aligned}&(r_lx-r_ky)^2+(r_ly+r_kx)^2=(r_lx+r_ky)^2+(r_ly-r_kx)^2\\ =\ &(r_ix-r_jy)^2+(r_iy+r_jx)^2=(r_ix+r_jy)^2+(r_iy-r_jx)^2\end{aligned}$$

represent four representation of the sum of squares.

Let $P(n)$ be "there exist positive integers $x_1,x_2,\ldots,x_{2n}$ such that $\prod\limits_{i=1}^{n}(x_{2i-1}^2+x_{2i}^2)$ can be expressed as a sum of two perfect squares in 2^{n-1} ways."

For $n=1$, it is trivial.

For $n=2$,

$$\begin{aligned}\prod_{i=1}^{2}(x_{2i-1}^2+x_{2i}^2)&=(x_1x_3-x_2x_4)^2+(x_1x_4+x_2x_3)^2\\ &=(x_1x_3+x_2x_4)^2+(x_1x_4-x_2x_3)^2\end{aligned}$$

If x_1,x_2,x_3,x_4 satisfy the condition in Corollary 11, then

$$(x_1x_3-x_2x_4)^2+(x_1x_4+x_2x_3)^2=(x_1x_3+x_2x_4)^2+(x_1x_4-x_2x_3)^2$$

represent 2 ways of sum of squares.

$\therefore$ $P(2)$ is true.

Assume $P(m)$ is true. i.e. there exist distinct positive integers $x_1, x_2, \ldots, x_{2m}$ such that $\prod_{i=1}^{m}(x_{2i-1}^2 + x_{2i}^2)$ can be expressed as a sum of two perfect squares in 2^{m-1} ways.

For $n = m + 1$,

there exist positive integers $x_1, x_2, \ldots, x_{2m}$ such that $\prod_{i=1}^{m}(x_{2i-1}^2 + x_{2i}^2) = r_{2i-1}^2 + r_{2i}^2$ $(i = 1, 2, 3, \ldots, 2^{m-1})$, where $r_i^2 \neq r_j^2$ for all $i \neq j$ (by induction assumption).

Take two distinct positive integers x_{2m+1}, x_{2m+2} such that:

$$\frac{x_{2m+1}}{x_{2m+2}} > \max_{(p,q)\in\{2i-1,2i,2j-1,2j\}^2}\{|r_p \pm r_q|\}$$

for all $0 < i < j < 2^{m-1}$ and $x_1, x_2, \ldots, x_{2m}, x_{2m+1}, x_{2m+2}$ are all distinct.

By Corollary 14, $(r_{2i-1}^2 + r_{2i}^2)(x_{2m+1}^2 + x_{2m+2}^2)$ generate 2^m ways as a sum of two perfect squares where $(i = 1, 2, 3, \ldots, 2^{m-1})$

$\therefore P(m + 1)$ is true.

By M.I., $P(n)$ is true for all positive integers n.

As a result, we have

"Given a positive integer N, there exits a positive integer M such that it has N essentially different representations of a sum of two perfect squares." □

[See reviewer's comment (7)]

5. Summary and Conclusion

After a deep investigation of this magic squares of squares probelm, we found out some interesting properties of magic squares of squares. We found that if the greatest common divisor of all entries is equal to 1, the prime factors of central entry are of the form $p \equiv 1 \pmod 4$, the central entry must not be a square of a prime number and the common prime factors of any two adjacent entries (if exist) are not of the form $p \equiv 3 \pmod 4$. These few facts which can help us rule out a large possibilities of magic squares may help us to verify whether a computer-constructed magic square is magic square of squares or not.

In addition, we found out a general (not all) solution to $a^2+b^2 = c^2+d^2 = e^2+f^2 = g^2+h^2 = 2M^2$, which also may help us to find magic square of squares. In the last part, we found out an interesting fact:

"Given a positive integer N, there exits a positive integer M such that it has N essentially different representations of a sum of two perfect squares."

without using any difficult mathematical techniques, for example, Gaussian integers.

After all, we hope that our investigation can have a little constribution to the advancement of Mathematics.

APPENDIX

Lemma 15.

$$a^2 = \begin{cases} 0 \text{ or } 4 \pmod 8 & \text{if } a \text{ is even} \\ 1 \pmod 8 & \text{if } a \text{ is odd} \end{cases}$$

Proof. If a is even, $a = 2k$ for an integer k. $a^2 = 4k^2$. If k is odd, $k = 2k_1 + 1$ where k_1 is an integer.

$$a^2 = 4k^2 = 4(2k_1 + 1)^2 = 8(2k_1^2 + 2k_1) + 1 \equiv 1 \pmod 8$$

If k is even, $k = 2k_1$,

$$a^2 = 16k_1^2 \equiv 0 \pmod 8.$$

If a is odd, $a = 2k + 1$ for an integer k.

$$a^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4k(k + 1) + 1,$$

since for any two consecutive integers there must be exactly one of them is even, $k(k + 1)$ is even for any integer k.

$$\therefore a^2 = 4k(k + 1) + 1 \equiv 1 \pmod 8$$

□

Lemma 16. *$\forall a \in \mathbb{Z}$, such that g.c.d$(a, p) = 1$, $\exists\ a^* \in \mathbb{Z}$, such that $aa^* \equiv 1 \pmod p$.*

Proof. Firstly, we prove $\{1a, 2a, \ldots, (p-1)a\}$ is a reduced residue system, where a is an integer which is relatively prime to p.

Obviously g.c.d.$(ai, p) = 1$ $(i = 1, 2, \ldots, p - 1)$.

If $ai \equiv aj \pmod p$ $(i, j \in \{1, 2, \ldots, p - 1\})$ we have, $a(i - j) \equiv 0 \pmod p$. Since $(a, p) = 1$, $i \equiv j \pmod p$.

So $1a, 2a, \ldots, (p-1)a$ represent $p - 1$ different residue classes. However, a reduced residue system of p consists of $p-1$ different residue classes. Thus, we can conclude that $\{1a, 2a, \ldots, (p-1)a\}$ is a reduced residue system.

$\forall a \in \mathbb{Z}$, such that g.c.d$(a,p) = 1$, $\{1a, 2a, \ldots, (p-1)a\}$ is a reduced residue system. $\therefore \exists a^* \in \{1, 2, \ldots, p-1\}$ such that $aa^* \equiv 1 \pmod{p}$. □

Lemma 17. $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$, *where* a, p *are relatively prime and* p *is an odd prime.*

Proof. If a is a quadratic residue modulo p, by the definition of Legendre symbol, $\left(\frac{a}{p}\right) = 1$ and $a \equiv x^2 \pmod{p}$ for an integer x where $(x,p) = 1$.

Thus, $a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p}$ (by Fermat's little theorem)

$$\therefore a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$$

If a is a quadratic non-residue modulo p, by the definition of Legendre symbol, $\left(\frac{a}{p}\right) = -1$. Let t be the primitive root of a: there exists a nonnegative integer m such that $a \equiv t^m \pmod{p}$ (for the definition and application of primitive root see website [11].)

By Fermat's little theorem, $a^{p-1} - 1 \equiv 0 \pmod{p}$.

So $(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0 \pmod{p}$.

Suppose $(a^{\frac{p-1}{2}} - 1) \equiv 0 \pmod{p}$, $(a^{\frac{p-1}{2}m} - 1) \equiv 0 \pmod{p}$. By the property of primitive root, we have $p - 1 \mid \frac{p-1}{2}m$, that implies m is even which contradicts $\left(\frac{a}{p}\right) = -1$. Hence, we have $a^{\frac{p-1}{2}} + 1 \equiv 0 \pmod{p}$. □

Lemma 18. *If* $a^2 + b^2 \equiv 0 \pmod{p}$ *and* p *is a prime s.t.* $p \equiv 3 \pmod{4}$, *then* $a \equiv b \equiv 0 \pmod{p}$.

Proof. Assume $p \nmid a$, by Lemma 16, $\exists\ a^* \in \mathbb{Z}$, such that

$$aa^* \equiv 1 \pmod{p}, \quad (a^2 + b^2)(a^*)^2 \equiv 0 \pmod{p}, \quad (a^*b)^2 \equiv -1 \pmod{p}$$

which means $x^2 \equiv -1 \pmod{p}$ is solvable $\iff \left(\frac{-1}{p}\right) = 1$.

However, by Lemma 17, $x^2 \equiv -1 \pmod{p} \iff p \equiv 1 \mod 4$, contradiction.

$\therefore p \mid a, b^2 \equiv -a^2 \pmod{p}$, so $p \mid b$. □

REFERENCES

[1] Multimagie, http://www.multimagie.com/indexengl.htm
[2] Unsolved Problems in Number Theory, Logic and Cryptography, *Magic Square of Squares*, http://unsolvedproblems.org/index_files/MagicSquare.htm
[3] Wikipedia, *Euler Criterion*, http://en.wikipedia.org/wiki/Euler%27s_criterion
[4] Wikipedia, *Primitive root modulo n*, http://en.wikipedia.org/wiki/Primitive_root_modulo_n
[5] 華羅庚, 華羅庚文集[數論卷二], 科學出版社, 2010
[6] J. Bhaskar, *Sum of Two Square*, http://www.math.uchicago.edu/∼may/VIGRE/VIGRE2008/REUPapers/Bhaskar.pdf
[7] A. Bremner, *On squares of squares II*, Acta Arith., **99** (2001), no. 3, pp. 289-308.
[8] A. Bremner, *On squares of squares*, Acta Arith., **88** (1999), no 3. pp. 289-297.
[9] C. Boyer, *Supplement to the article "Some Notes on the Magic Squares of Squares Problem"*, MATH INTELL, **27** (2005), N. 2, pp. 52-64
[10] F. W. Clarke, W. N. Everitt, L. L. Littlejohn and S. J. R. Vorster, *H. J. S. Smith and the Fermat Two Squares Theorem*, Am. Math. Mon., **106** (1999), no. 7, pp. 652-665
[11] K.Y.Li, *Primitive Roots Modulo Primes*, Mathematical Excalibur, **15** (2010), no.1, pp. 1-4.
[12] Landon W. Rabern, *Properties of magic squares of squares*, Rose-Hulman Institute of Technology Undergraduate Math Journal, **4** (2003), N.1

Reviewer's Comments

This paper investigates the property of the properties of a 3×3 magic square whose entries are all square numbers. A magic square is a 3×3 matrix such that the sums of each row, each column and each diagonals are the same. It is an open problem whether such a magic square exists. If it does exist, the entries must be rather large numbers.

The paper consists of 4 parts. Part I consists of some discussion of the properties of the classical magic square. Part II gives some properties of a magic square of squares. Part III is the main part of the paper, in which they discuss the solvability of a related system of Diophantine equations. Part IV discusses an extended problem: whether there exists arbitrary large number of distinct sum of squares representations for the same number. They show that the answer is positive. Besides modular arithmetic and some basic number theory, they make extensive and repeated use of the Lagrange identity $(a^2+b^2)(c^2+d^2) = (ac+bd)^2 + (ad-bc)^2 = (ac-bd)^2 + (ad+bc)^2$ in Part II, III and IV. Geometrically, this can be understood as the fact that there are many possibilities for the length of a vector (possibly in high-dimension Euclidean space) to be expressed as a sum of squares.

Here are the reviewer's comments concerning the style and the mathematics in this paper.

About the stylistic problems first. The typesetting in this paper is not very satisfactory. It is hard to point out all the places where there are some stylistic problems. The reviewer points out some:

I The reviewer has comments on the wordings, which have been amended in this paper.

II The reviewer suggest renaming all the "Property" to "Proposition", which is more appropriate for a mathematics paper.

III The line $\forall a \in \mathbb{Z}, a^2 \equiv \cdots$ should be changed to $\forall b \in \mathbb{Z}, b^2 \equiv \cdots$ because the symbol a has already been used (in the same sentence!) which leads to confusion.

IV The notations in the first and second paragraph are not consistent. In the first paragraph, they use the letters a to i, where immediately in the second paragraph they use a to h together with k. It is suggested that they change the $a, \cdots, i$ in the first paragraph to $y_1, \cdots, y_9$ (which is consistent with Part II), since they also use $a, b, c, \cdots, h$ and k in Theorem 9 in the same sense as the second paragraph on Part III.

V The blue color of $\pm$ is not necessary.

VI Some more advanced mathematical terms such as "reduced residue system" or "Legendre symbol" are not defined. While they use quite some pages to prove rather elementary lemmas (like Lemma 15, 16), which perhaps can be removed, it is somewhat unnatural for the author to assume that the reader knows what the "Legendre symbol" is. Indeed, all the lemmas in the Appendix

are standard and the reviewer thinks they should not reproduce the textbook proofs in the paper. So the reviewer suggests the author either shortens the proof or just cites the references for the proofs.

VII The references part is not satisfactory. First of all, except [9], they don't really cite any references in the paper. They just put a list of books, papers and websites in the "References" part, but it doesn't indicate how they are relevant. This makes the list looks rather random. E.g. they don't give any hint how the book 華羅庚文集[數論卷二] , or the paper "Properties of Magic Squares of Squares" is relavant.
Secondly, the style in the "References" is not consistent: they are not ordered in any way I can recognize. Some omit the journal names, and the entries shouldn't be capitalized. This part should be rewritten completely, and the references should be removed if they are not cited.

The followings are the reviewer's comments on the mathematics in this paper.

1. $$a^2 + b^2 \equiv 0 \pmod 8 \Leftrightarrow a \equiv b \equiv 0 \pmod 2$$
should be
$$a^2 + b^2 \equiv 0 \pmod 8 \Leftrightarrow a \equiv b \equiv 0 \pmod 4.$$
Alternatively, it can also be changed to
$$a^2 + b^2 \equiv 0 \pmod 8 \Rightarrow a \equiv b \equiv 0 \pmod 2,$$
which is all that is needed in the proof.
2. Perhaps it should be remarked that the number 5 is not that special, it can be extended to any prime p such that $S \cap 2S = \{0\}$, where S is the set of all the quadratic residues mod p and $2S := \{2n \pmod p : n \in S\}$. This in turn is equivalent to 2 being a quadratic nonresidue. By the law of quadratic reciprocity, this is equivalent to $p \not\equiv \pm 1 \pmod 8$. As it has been shown in Property 5 that $p \equiv 1 \pmod 4$, this implies $p \equiv 5 \pmod 8$. The smallest such prime is of course 5, and the next one is 13. So Property 7 can be extended as:
For a prime $p \equiv 5 \pmod 8$ which divide y_5, any entry adjacent to the central one is not divisible by p.
3. The proof is written in a slightly complicated way. The reviewer suggests the proof to be rewritten as follows.
We can assume $a > c > p > d > b > 0$. Equation (9) (Lagrange identity) states that
$$\begin{aligned} 4p^4 = (a^2 + b^2)(c^2 + d^2) &= (ad + bc)^2 + (ac - bd)^2 \\ &= (ac + bd)^2 + (ad - bc)^2. \end{aligned} \tag{**}$$
As given in (10),
$$(ac + bd)(ad + bc) = cd(a^2 + b^2) + ab(c^2 + c^2) = 2p^2(ab + cd),$$

so we have $p^2|(ac+bd)(ad+bc)$. There are three cases.
Case A: $p^2|ac+bd$.
Note that $ad-bc \neq 0$ for otherwise $(a,b) = n(c,d)$ which is impossible as $a^2+b^2 = c^2+d^2$ and $(a,b) \neq (c,d)$. So (**) implies $ac+bd < 2p^2$ and so $ac+bd = p^2$. Put this in (**), $3p^4 = (ad-bc)^2$ which is impossible as 3 is not a square.
Case B: $p^2|ad+bc$. Same proof as Case A.
Case C: $p|ac+bd$ and $p|ad+bc$.
In this case, (**) gives

$$ac - bd \equiv 0 \pmod{p},$$

which together with $ac+bd \equiv 0 \pmod{p}$ implies $bd \equiv 0 \pmod{p}$. So $d \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$, but this contradicts $0 < b < d < p$.

4. The very last line should be changed to

$$= ((k_1k_3 - k_2k_4)k_5 + (k_1k_4 - k_2k_3)k_6)^2 + ((k_1k_3 - k_2k_4)k_6 - (k_1k_4 - k_2k_3)k_5)^2$$

5. Theorem 9 is one of the highlights in this paper, in which they provide a solution to the Diophantine equations

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

While rather non-trivial, there are some concerns about this result:
   (a) It does not say anything about whether such solution constructed are distinct (say if t_i are distinct), although they compute the simplest non-trivial case (Example 10) and find that they are distinct. They also give some criteria for the solution to be distinct (Corollary 11 and Corollary 12) but they are not easy to be checked in practise.
   (b) It also does not address whether they are all solution to this problem.
   (c) Even if the solution $a, \cdots, h$ and k thus obtained are distinct, the magic square problem is still not solved because there are additional equations (equations (10) to (14) in the paper) to be satisfied, as already noticed in the paper (Corollary 13). In fact, it seems quite unlikely that the y_i obtained from Theorem 9 by choosing arbitrary t_i will solve the remaining equations (10) to (14). Nevertheless, to my knowledge, the magic square of squares is still an open problem.

6. (a) Change the second implication

$$\begin{aligned} \Leftrightarrow \quad & 16a^2b^2c^2d^2(a^2-b^2)^2(c^2-d^2)^2(a^2-b^2)^2 \\ & \times (a^2(c-d)^2 - b^2(c+d)^2) \cdot (a^2(c+d)^2 - b^2(c+d)^2) \neq 0 \end{aligned}$$

to

$$\begin{aligned} \Leftrightarrow \quad & 16a^2b^2c^2d^2(a^2-b^2)^2(c^2-d^2)^2(a^2-b^2)^2 \\ & \times (a^2(c-d)^2 - b^2(c+d)^2)(a^2(c+d)^2 - b^2(c-d)^2) \neq 0 \end{aligned}$$

(b) Change the last implication

$$abcd(a^2-b^2)(c^2-d^2)(a^2(c-d)^2-a^2(c+d)^2) \times (a^2(c+d)^2-b^2(c+d)^2) \neq 0$$

to

$$abcd(a^2-b^2)(c^2-d^2)(a^2(c-d)^2-a^2(c+d)^2) \times (a^2(c+d)^2-b^2(c-d)^2) \neq 0$$

7. They provide another non-trivial result by showing that given any positive n, there is a number which has at least n distinct sum of squares representation.

First of all, the reviewer suggests putting this "fact" in "Theorem" or "Proposition" form, for stylistic reason.

The idea of proof is essentially like this: if we already have a pair of distinct representation $a^2+b^2=c^2+d^2$, we can make use of the Lagrange identity: for any p, q,

$$\begin{aligned}(a^2+b^2)(p^2+q^2) &= (ap-bq)^2+(aq+bp)^2 \\ &= (ap+bq)^2+(aq-bp)^2. \qquad (***)\end{aligned}$$

Likewise, we also have

$$\begin{aligned}(c^2+d^2)(p^2+q^2) &= (cp-dq)^2+(cq+dp)^2 \\ &= (cp+dq)^2+(cq-dp)^2.\end{aligned}$$

If these four representations are distinct, then we have found a new number whose number of representations double the previous one! They then argue that if p, q are more carefully chosen, then these representations are distinct.

In fact, this can be seen more geometrically as follows. If we normalize (a,b) etc. to have unit length (i.e. divided by its length $\sqrt{a^2+b^2}$), then the Lagrange identity (***) is just the fact that $1=\cos^2\alpha+\sin^2\alpha=\cos^2\beta+\sin^2\beta$ where α (resp. β) is the angle between (a,b) and (p,q) (resp. (b,a) and (p,q)). Thus what they are looking for is that given finitely many vectors (say $\{(a_i,b_i)\}_{i=1}^n$), find a vector (p,q) which makes distinct angles with (a_i,b_i). They find such a vector (p,q) by requiring it to have a steeper slope than all those (a_i,b_i).

In fact, to relate this to the magic square problem, the reviewer thinks we can change the statement to the following:
Given any n, there exists integers k and $a_1,b_1,\cdots,a_n,b_n$, all distinct, such that

$$2k^2=a_1^2+b_1^2=\cdots=a_n^2+b_n^2$$

for $i=1,\cdots,n$. This can be either proved by modifying their argument, or by the following observation. It is known that there are infinitely many primitive Pythagorean triples, so for any n, we can find distinct natural numbers $x_1,y_2,\cdots,x_n,y_n$ and k such that $(\frac{x_i}{k},\frac{y_i}{k})$ all lie on the unit circle. Take

$a_i = |x_i - y_i|$ and $b_i = x_i + y_i$, we have the polarization identity

$$a_i^2 + b_i^2 = (x_i - y_i)^2 + (x_i + y_i)^2 = 2(x_i^2 + y_i^2) = 2k^2.$$

The a_i, b_i thus obtained are all distinct.

8. In fact, the method above gives all the solution to the following problem: if $a, b, k \in \mathbb{Z}$ satisfies

$$2k^2 = a^2 + b^2, \tag{***}$$

then they are of the form

$$\begin{cases} a &= m^2 + 2mn - n^2 \\ b &= m^2 - 2mn - n^2 \\ k &= m^2 + n^2 \end{cases}$$

where $m, n \in \mathbb{Z}$. The solution is nontrivial only if $|m| \neq |n|$. This follows from the fact that all rational points on the unit circle are given by $\left(\frac{m^2-n^2}{m^2+n^2}, \frac{2mn}{m^2+n^2}\right)$ and the fact that for all solution to (***), $(\frac{a+b}{2k}, \frac{a-b}{2k})$ are rational points lying on the unit circle. We notice that there is a similar construction (see k_5, k_6) in the proof of Theorem 9.

9. To go further, let us illustrate for example how to find all the solution to problem

$$k^2 = x_1^2 + y_1^2 = x_2^2 + y_2^2 = x_3^2 + y_3^2. \tag{****}$$

By the consideration in (8) above, it is easy to see that if we set

$$\begin{cases} k_i = m_i^2 + n_i^2 \\ X_i = m_i^2 - n_i^2 \\ Y_i = 2m_i n_i \\ (\cos\theta_i, \sin\theta_i) = \left(\frac{X_i}{k_i}, \frac{Y_i}{k_i}\right) = \left(\frac{m_i^2-n_i^2}{m_i^2+n_i^2}, \frac{2m_i n_i}{m_i^2+n_i^2}\right) \end{cases}$$

for $m_i, n_i \in \mathbb{Z}$, then

$$\begin{aligned} (k_1k_2k_3)^2 &= [k_1k_2k_3\cos\theta_1]^2 + [k_1k_2k_3\sin\theta_1]^2 \\ &= [k_1k_2k_3\cos(\theta_1+\theta_2)]^2 + [k_1k_2k_3\sin(\theta_1+\theta_2)]^2 \\ &= [k_1k_2k_3\cos(\theta_1+\theta_2+\theta_3)]^2 + [k_1k_2k_3\sin(\theta_1+\theta_2+\theta_3)]^2 \end{aligned}$$

are three distinct sum of square representation if and only if for distinct i, j,

$$\begin{aligned} &(\cos\alpha_i, \sin\alpha_i) \neq (\pm\cos\alpha_j, \pm\sin\alpha_j) \text{ and} \\ &(\cos\alpha_i, \sin\alpha_i) \neq (\pm\sin\alpha_j, \pm\cos\alpha_j) \end{aligned}$$

for $\alpha_i := \sum_{k=1}^{i} \theta_k$. Note also that the term inside each square bracket is an integer (by compound angle formula). By geometric reason, this would give all solution to (****).

Now, for any solution to (****), taking $a_i = x_i - y_i$ and $b_i = x_i + y_i$ will give all the integer solution to

$$2k^2 = a_1^2 + b_1^2 = a_2^2 + b_2^2 = a_3^2 + b_3^2.$$

E.g. by taking $(m_1, n_1) = (1, 2)$, $(m_2, n_2) = (2, 3)$, $(m_3, n_3) = (1, 3)$, we have

$$2 \cdot 650^2 = 910^2 + 130^2 = 230^2 + 890^2 = 350^2 + 850^2.$$

Similarly we can also find 4 pairs of distinct square representations this way, e.g. by taking one more pair $(m_4, n_4) = (1, 4)$, we find

$$\begin{aligned} 2 \cdot 11050^2 &= 15470^2 + 2210^2 = 3910^2 + 15130^2 \\ &= 5950^2 + 14450^2 = 12050^2 + 9950^2. \end{aligned}$$

It is clear that this construction can be extended to get any number of distinct square representations.

This gives a more systematic and cleaner way to represent all the solution to the problem in Theorem 9 and the "fact" in Part IV.