MAGIC SQUARES OF SQUARES

PAUL PIERRAT AND FRANÇOIS THIRIET AND PAUL ZIMMERMANN

In 1770 Leonhard Euler found a magic square of order 4 filled of squares.

$$\begin{array}{cccc} 68^2 & 29^2 & 41^2 & 37^2 \\ 17^2 & 31^2 & 79^2 & 32^2 \\ 59^2 & 28^2 & 23^2 & 61^2 \\ 11^2 & 77^2 & 8^2 & 49^2 \end{array}$$

All rows and columns and the two main diagonals sum up to 8515. Contrary to classical magic squares filled with consecutive integers, the only rule is that all elements are squares of *different* positive integers. We also require the magic square to be *primitive*, i.e., the gcd of all elements is one (indeed, multiplying all elements by some integer k^2 keeps the equality between sums). In 1996, Martin Gardner asked whether there exists a 3×3 magic square filled with squares, and offered a \$100 prize to the first discoverer. Euler's method, and a detailed history of this problem is presented in [2].

Lee Sallows found in 1997 the following near miss:

$$\begin{array}{ccc} 127^2 & 46^2 & 58^2 \\ 2^2 & 113^2 & 94^2 \\ 74^2 & 82^2 & 97^2 \end{array}$$

where all rows and columns and main diagonals sum up to 21609, except the descending diagonal whose sum is 38307. Christian Boyer notices in [2] that Sallows' solution is part of a family proposed by Lucas in 1876.

Duncan Buell shows in [3] that if a solution exists, its center cell is larger than $25 \cdot 10^{24}$.

In Section 1, we give a necessary condition that elements of a magic square of squares must follow. In Section 2, we extend the class of solutions found by Buell and Pech to the "magic hourglass" problem and similar configurations with 7 squares.

1. Modular Properties

Lemma 1. *For any magic* 3×3 *square of squares which is primitive, the corresponding sum must be* $s = 3 \bmod 72$*, and the (square) elements must be* $1 \bmod 24$*.*

Proof. The idea of the proof is to find all possible magic squares of squares modulo q for some prime power q. Since elements are squares, this adds some additional constraints. For example for $q = 4$, only 0 and 1 are squares. It is then easy to see that a 3×3 magic square of squares modulo 4 can be only of two possible forms:

$$\begin{array}{ccc} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{array}, \qquad \begin{array}{ccc} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{array},$$

Date: March 13, 2015.

the first one with sum 0 mod 4, the second one with sum 3 mod 4. However, the first solution will not give primitive squares, since we can divide all elements by 2^2. Modulo 8, we get solutions for sum 0 mod 8 (but non-primitive as explained above), for 3 mod 8, and for 4 mod 8 (non-primitive either). The only primitive solution is:

$$\begin{matrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{matrix}.$$

Thus a 3×3 magic square of squares must have all its (square) elements 1 mod 8, and a sum 3 mod 8.

Similarly, modulo 9, we get one non-primitive solution with all elements and sum 0 mod 9, and 27 solutions with sum 3 mod 9, filled with (square) elements 1, 4 or 7 modulo 9, which are the only squares modulo 9, apart from 0. Thus $s = 3 \bmod 8$ and $s = 3 \bmod 9$, therefore by CRT $s = 3 \bmod 72$.

The (square) elements must be 1 modulo 8, and 1, 4, or 7 modulo 9, which gives 1 mod 3, and 1 mod 24. □

Remark 1: we can also try larger q values. For example with $q = 7$ (resp. $q = 11$) we find that s should not be divisible by 7 (resp. 11).
Remark 2: the same approach applies to the "hour glass" problem [3] and to the Enigma 1 problem [2]. It suffices to relax the quadratic residue constraint on the corresponding entries (D and F for the hour glass, D and I for Enigma 1):

$$\begin{matrix} A & B & C \\ D & E & F \\ G & H & I \end{matrix}.$$

Surprisingly, despite relaxing two constraints, for both problems we get exactly the same conditions than in Lemma 1. In fact for all problems 7.I to 7.VIII from [1] we got the same constraint: all square elements must be 1 mod 24.

2. Arithmetic Progressions of Squares

In [3], Buell considers configurations called "magic hourglasses" where the central cell is $a = A^2$, with A a sum of two squares in at least 3 different ways (see also [4]). However he assumes that in each of the two diagonals and the central column, the three entries are coprime, which does not necessarily hold. We show that we can find primitive solutions with a common divisor among some rows, columns or diagonals.

Theorem 1. *Let A be a positive odd integer. Then all non-trivial arithmetic progressions of the form x^2, A^2, y^2 can be found as follows, each in a unique way. Let p be a square-free divisor of A, $p = 1 \bmod 4$. Write $A = pA'$, and search for all decompositions $A' = m^2 + n^2$ with m even and n odd, $m, n > 0$. Then write $b = 4mn(m^2 - n^2)$, $x = \sqrt{A^2 - p^2 b}$, $y = \sqrt{A^2 + p^2 b}$.*

Proof. First it can be easily checked that $A^2 - p^2 b$ and $A^2 + p^2 b$ are perfect squares, respectively of $x = p(m^2 - 2mn - n^2)$ and of $y = p(m^2 + 2mn - n^2)$.

Conversely, assume x^2, A^2, y^2 is an arithmetic progression of squares. We must prove that it can be produced in the way given by the theorem, and in a unique way.

Let us first prove the uniqueness. Assume $A = pA' = p'A''$ with p, p' square-free and distinct, $A' = m^2 + n^2$, $A'' = m'^2 + n'^2$, and $A^2 \pm 4p^2 mn(m^2 - n^2) = A^2 \pm 4p'^2 m'n'(m'^2 - n'^2)$.

If a prime q divides both m, n, m', n', we can divide all four values by q, and we will find two similar decompositions; we can thus assume that m, n, m', n' have no common factor. Without loss of generality we can assume there is a prime factor q of p' which does not divide p. Since $p(m^2+n^2) = p'(m'^2+n'^2)$, q divides m^2+n^2. But since q divides p', it also divides $x = p(m^2-2mn-n^2) = p'(m'^2-2m'n'-n'^2)$. Thus it divides $m^2-2mn-n^2$. Since q divides both m^2+n^2 and $m^2-2mn-n^2$, it divides their sum $2m^2-2mn$. Similarly, considering y, it divides both m^2+n^2 and $m^2+2mn-n^2$, thus it divides $2m^2+2mn$. Therefore q divides $4m^2$. Since q is odd (remember $p' = 1 \bmod 4$), it necessarily divides m, and then it divides n too. Now:

- if q does not divide $m'^2+n'^2$, then q divides $A = p'(m'^2+n'^2)$ with exponent 1. On the other side, since q divides both m and n, it divides $A = p(m^2+n^2)$ with exponent 2 at least, which leads to a contradiction;
- if q divides $m'^2+n'^2$, since we assumed m, n, m', n' have no common factor, it cannot divide m' (nor n', one implying the other) thus by Lemma 2 it does not divide $m'^2-2m'n'-n'^2$, thus it divides $x = p'(m'^2-2m'n'-n'^2)$ with exponent 1. On the other side since $x = p(m^2-2mn-n^2)$ and q divides both m and n it divides x with exponent 2 at least, which leads to a contradiction too.

This proves the uniqueness of a decomposition as given by the theorem.

It remains to prove that all arithmetic progressions of three squares satisfy such a decomposition. First we show (see Lemma 3) that decompositions $A = p(m^2+n^2)$ with $p = 3 \bmod 4$ cannot work (or equivalently, decompositions with $A = 3 \bmod 4$ since $m^2+n^2 = 1 \bmod 4$).

Now assume that q^2 divides all terms x, A, y of an arithmetic progression x^2, A^2, y^2 of squares. Let $x = q^2x_1$, $A = q^2A_1$, $y = q^2y_1$. Then x_1^2, A_1^2, y_1^2 is an arithmetic progression of squares. Thus by induction it can be written $A_1 = p_1(m_1^2+n_1^2)$, and $x_1 = \sqrt{A_1^2 - p_1^2b_1}$, $y_1 = \sqrt{A_1^2 + p_1^2b_1}$ with $b_1 = 4m_1n_1(m_1^2-n_1^2)$. Then x, A, y satisfy the theorem with $p_1 = p$, $m = qm_1$, $n = qn_1$.

It thus remain to deal with the case where the gcd of x, A, y is square-free. Let p be this gcd, and $x = px'$, $A = pA'$, $y = py'$. Then x'^2, A'^2, y'^2 is an arithmetic progression of squares with $\gcd(x', A', y') = 1$. According to [3, 4] we have $A' = m^2+n^2$ with m, n coprime, $x' = \sqrt{A'^2 - b}$, $y' = \sqrt{A'^2 + b}$ with $b = 4mn(m^2-n^2)$. □

Lemma 2. *If an odd prime q divides m^2+n^2 but does not divide m (or n) then it does not divide $m^2-2mn-n^2$.*

Proof. First if q does not divide m it cannot divide n, otherwise it could not divide m^2+n^2. Then assume q divides $m^2-2mn-n^2$. Then it divides $(m^2+n^2)+(m^2-2mn-n^2) = 2m(m-n)$. Since it does not divide m, it necessarily divides $m-n$. But then it divides $m^2-n^2 = (m-n)(m+n)$. And then it divides $(m^2+n^2)+(m^2-n^2) = 2m^2$, which gives a contradiction. □

Lemma 3. *Let $A > 0$ be a integer equal to $3 \bmod 4$. There exists an integer $g > 1$ such that for all decompositions $A = p(m^2+n^2)$ with p, m, n positive integers, g divides p.*

Proof. Since $A = 3 \bmod 4$, A has at least one prime factor $q = 3 \bmod 4$ appearing with odd exponent in A. Then since the exponent of q in m^2+n^2 is necessarily even (this is classical result whose proof can be found in Hardy and Wright, An introduction to the theory of numbers, instance 20.1, Theorems 367 and 368), q necessarily divides all values of p. □

Decompositions $A = p(m^2 + n^2)$ lead so arithmetic progressions of primes

$$A^2 - 4p^2mn(m^2 - n^2), A^2, A^2 + 4p^2mn(m^2 - n^2)$$

with p^2 as common divisor. However for the hourglass problem, if A decomposes in three different such ways with *coprime* values of p, then it can lead to a possible solution.

We found the following hourglass, where all 5 sums are equal modulo 2^{47}, among which the two diagonals and the central column are fully equal: in

$$\begin{array}{ccc} 711111125^2 & 1710283897^2 & 1704480209^2 \\ & 1289865125^2 & \\ 649808663^2 & 634376129^2 & 1679828875^2 \end{array}$$

This solution corresponds to:

$A = 1289865125, (m, n, p) = (13320, 8975, 5), (r, s, t) = (7666, 35087, 1), (u, v, w) = (19526, 30143, 1),$

and has a central element A of 10 digits only, whereas with $p = t = w = 1$ Buell found no solution modulo 2^{47} up to $A = 5 \cdot 10^{12}$.

Similarly Pech found no solution modulo 2^{53} up to $A = 10^{13}$, and the following is one modulo 2^{57}:

$$\begin{array}{ccc} 72545772215^2 & 1392029422601^2 & 1527110141803^2 \\ & 1081235918365^2 & \\ 77954070629^2 & 632768764193^2 & 1527376618015^2 \end{array}$$

which corresponds to A of 13 digits (less than Buell's search bound too):

$A = 1081235918365, (m, n, p) = (1306, 505, 551465), (r, s, t) = (1719, 3868, 60349), (u, v, w) = (185522, 1023141, 1).$

We performed a search up to $5 \cdot 10^{12}$, and this is the only solution modulo 2^{57} we found (we found 3 solutions modulo 2^{56}, for $A = 2112168345989, 2333130729649, 3065838349925$).

For problem 7.II we did a partial search only up to $A = 6,500,000,000$, and found no solution. Similarly for problem 7.III up $A = 16,900,000,000$, and for problem 7.V up to $A = 16,000,000,000$.

For problem 7.VI from [1] we found the following solution modulo 2^{59} (i.e., we can complete the two empty cells by numbers so that all sums are equal modulo 2^{59}):

$$\begin{array}{ccc} 11899458593932 & 18324471103132 & \\ 33953141236552 & 28307522899452 & 21208863844552 \\ & 35592772639912 & 38223482188012 \end{array}$$

This is the only solution modulo 2^{59} we found up to $A = 615,000,000,000$.

Acknowledgements. The authors thank Christian Boyer for his feedback on a preliminary version of this note.

References

[1] Boyer, C. A search for 3x3 magic squares having more than six square integers among their nine distinct integers. `http://www.multimagie.com/Search.pdf`, 2004. 5 pages.

[2] Boyer, C. Some notes on the magic squares of squares problem. *The Mathematical Intelligencer 27*, 2 (2005), 52–64.

[3] Buell, D. A. A search for a magic hourglass. http://www.multimagie.com/Buell.pdf, 2004. 4 pages.

[4] Pech, L. Carrés magiques 3×3 de carrés. `http://www.multimagie.com/Pech.pdf`, 2006. 8 pages.