

On squares of squares

by

ANDREW BREMNER (Tempe, Ariz.)

0. There is a long and intriguing history of the subject of magic squares, squares whose row, column, and diagonal sums are all equal. There has recently been some interest in whether there can exist a three-by-three magic square whose nine elements are all perfect squares; the problem seems first to have been raised by LaBar [5]. The answer is of course yes, for example

$$\begin{bmatrix} 5^2 & 1^2 & 7^2 \\ 7^2 & 5^2 & 1^2 \\ 1^2 & 7^2 & 5^2 \end{bmatrix}$$

which is a particular case of the parametrized square

$$\begin{bmatrix} (m^2 + n^2)^2 & (m^2 - 2mn - n^2)^2 & (m^2 + 2mn - n^2)^2 \\ (m^2 + 2mn - n^2)^2 & (m^2 + n^2)^2 & (m^2 - 2mn - n^2)^2 \\ (m^2 - 2mn - n^2)^2 & (m^2 + 2mn - n^2)^2 & (m^2 + n^2)^2 \end{bmatrix}.$$

Martin Gardner [3] has offered \$100 for an example of a three-by-three magic square of squares in which the nine entries are distinct, or for a proof of the non-existence of such a square. See Sallows [7] for a recent discussion of this topic, in which is presented (a reflection of) the example

$$(1) \quad \begin{bmatrix} 58^2 & 46^2 & 127^2 \\ 94^2 & 113^2 & 2^2 \\ 97^2 & 82^2 & 74^2 \end{bmatrix}$$

which fails to be magic only in that the non-principal diagonal does not have the common sum (of 147^2).

There are two different problems that can be posed. The first, to find magic squares with as many as possible of the entries being perfect squares; and the second, to find squares with perfect square entries (“squared squares”) in which as many as possible of the eight row, column, and diagonal sums are equal. In this note, we do not treat the first problem, other

than to exhibit the magic square

$$\begin{bmatrix} 373^2 & 289^2 & 565^2 \\ 360721 & 425^2 & 23^2 \\ 205^2 & 527^2 & 222121 \end{bmatrix}$$

which has seven square entries; it seems that an example with eight distinct square entries is unknown. See Guy and Nowakowski [4]. For the second problem, the above example (1) of Sallows gives a squared square with seven of the eight sums equal. We here extend this example by showing how to construct parametrized families of squared squares with a similar property, namely, having all sums equal excepting that of the non-principal diagonal. (Henceforth, we are only interested in squares having distinct entries, and will refer to squares with repeated entries as *trivial*.)

The three smallest squared squares that are found have entries of degree 8, 16, 20 in the parameter, of which we give the first two. We find just one example of a magic square in which the entries are from an algebraic number field of *odd* degree.

1. Any three-by-three magic square of rational numbers has the form

$$(2) \quad \begin{bmatrix} a - b & a + b + c & a - c \\ a + b - c & a & a - b + c \\ a + c & a - b - c & a + b \end{bmatrix}$$

with $a, b, c \in \mathbb{Q}$. The square is trivial (has repeated entries) precisely when

$$bc(b^2 - c^2)(b^2 - 4c^2)(4b^2 - c^2) = 0.$$

Suppose that all the entries are perfect squares; then in particular the three triples $\{a, a \pm c\}$, $\{a + b, a + b \pm c\}$, $\{a - b, a - b \pm c\}$ are each triples of squares. Associate to the above square the elliptic curve

$$(3) \quad E: y^2 = x(x^2 - c^2).$$

A point (X, Y) in $E(\mathbb{Q})$ lies in $2E(\mathbb{Q})$ if and only if the triple $\{X, X \pm c\}$ is a triple of rational squares. Accordingly, $a - b, a, a + b$ must all be x -coordinates of points in $2E(\mathbb{Q})$. Thus the existence of a magic square of squares is equivalent to the existence of three points in $2E(\mathbb{Q})$ with x -coordinates in arithmetic progression. This observation appears first to have been noticed by Robertson [6], and seems to be a very restrictive condition, certainly when the rank of $E(\mathbb{Q})$ is small. A small computer search found very few examples of three points in $E(\mathbb{Q})$ (not $2E(\mathbb{Q})$) with x -coordinates in arithmetic progression. Indeed, the only example found where none of the three points is a torsion point on E , is the triple

$$(-528, 26136), (-363, 22869), (-198, 17424)$$

on the curve

$$y^2 = x(x^2 - 1254^2)$$

which has rank 3 over \mathbb{Q} .

For a magic square of squares it is necessary and sufficient that

$$a - b = x_{2P_0}, \quad a = x_{2P_1}, \quad a + b = x_{2P_2}$$

where x_P denotes the x -coordinate of P , and $P_0, P_1, P_2 \in E(\mathbb{Q})$. Then the square (2) becomes

$$(4) \quad \begin{bmatrix} x_{2P_0} & x_{2P_2} + c & x_{2P_1} - c \\ x_{2P_2} - c & x_{2P_1} & x_{2P_0} + c \\ x_{2P_1} + c & x_{2P_0} - c & x_{2P_2} \end{bmatrix}$$

with “magic” condition

$$x_{2P_2} - x_{2P_1} = x_{2P_1} - x_{2P_0}.$$

The curve E is known to have rational torsion group comprising just the points of order dividing 2 (see for example Silverman [9]); and observe that on replacing P_i by $P_i + T$, where T is a torsion point, the resulting square is not altered. Put $P_i = (x_i, y_i)$, so that $x_{2P_i} = (x_i^2 + c^2)/(4y_i^2)$, and (4) becomes

$$\begin{bmatrix} \frac{(x_0^2 + c^2)^2}{4y_0^2} & \frac{(x_2^2 + 2cx_2 - c^2)^2}{4y_2^2} & \frac{(x_1^2 - 2cx_1 - c^2)^2}{4y_1^2} \\ \frac{(x_2^2 - 2cx_2 - c^2)^2}{4y_2^2} & \frac{(x_1^2 + c^2)^2}{4y_1^2} & \frac{(x_0^2 + 2cx_0 - c^2)^2}{4y_0^2} \\ \frac{(x_1^2 + 2cx_1 - c^2)^2}{4y_1^2} & \frac{(x_0^2 - 2cx_0 - c^2)^2}{4y_0^2} & \frac{(x_2^2 + c^2)^2}{4y_2^2} \end{bmatrix}.$$

Equivalently, put $(x, y) = (cX, c^2Y)$ so that the equation of E takes the form

$$E: \quad cY^2 = X(X^2 - 1);$$

then the square is

$$\begin{bmatrix} \frac{(X_0^2 + 1)^2}{4Y_0^2} & \frac{(X_2^2 + 2X_2 - 1)^2}{4Y_2^2} & \frac{(X_1^2 - 2X_1 - 1)^2}{4Y_1^2} \\ \frac{(X_2^2 - 2X_2 - 1)^2}{4Y_2^2} & \frac{(X_1^2 + 1)^2}{4Y_1^2} & \frac{(X_0^2 + 2X_0 - 1)^2}{4Y_0^2} \\ \frac{(X_1^2 + 2X_1 - 1)^2}{4Y_1^2} & \frac{(X_0^2 - 2X_0 - 1)^2}{4Y_0^2} & \frac{(X_2^2 + 1)^2}{4Y_2^2} \end{bmatrix}.$$

Finally, replace c by $x_2(x_2^2 - 1)/Y_2^2$, and put $x_2 = \lambda$, with $(x, Y) = (X, Y_2Y)$. The resulting square, on multiplying by $4Y_2^2$, is

$$(5) \quad \left[\begin{array}{ccc} \frac{(X_0^2 + 1)^2}{Y_0^2} & (\lambda^2 + 2\lambda - 1)^2 & \frac{(X_1^2 - 2X_1 - 1)^2}{Y_1^2} \\ (\lambda^2 - 2\lambda - 1)^2 & \frac{(X_1^2 + 1)^2}{Y_1^2} & \frac{(X_0^2 + 2X_0 - 1)^2}{Y_0^2} \\ \frac{(X_1^2 + 2X_1 - 1)^2}{Y_1^2} & \frac{(X_0^2 - 2X_0 - 1)^2}{Y_0^2} & (\lambda^2 + 1)^2 \end{array} \right]$$

where (X_i, Y_i) , $i = 0, 1$, are points on

$$(6) \quad E : \lambda(\lambda^2 - 1)Y^2 = X(X^2 - 1).$$

This square fails to be magic only at the non-principal diagonal; the condition that it is magic has become

$$(7) \quad 2\frac{(X_1^2 + 1)^2}{Y_1^2} - \frac{(X_0^2 + 1)^2}{Y_0^2} = (\lambda^2 + 1)^2.$$

2. We can regard the equation (6) for E as defining an elliptic curve over $\mathbb{Q}(\lambda)$, obviously possessing at least one point rational over $\mathbb{Q}(\lambda)$, namely $P = (\lambda, 1)$. In fact, it is easy to verify that P is of infinite order, and consequently the multiples of P in $E(\mathbb{Q}(\lambda))$ can be used to furnish X -coordinates X_0, X_1 for substitution into the square at (5), and in this way infinitely many parametrized squared squares result. As remarked previously, it is only necessary to compute the multiples of P modulo torsion. Further, it is clear from (5) that X_0, X_1, λ must be distinct for non-repeated entries. The first non-trivial square arises from replacing X_0 and X_1 by

$$X_{2P} = \frac{(1 + \lambda^2)^2}{4(\lambda^3 - \lambda)} \quad \text{and} \quad X_{3P} = \frac{\lambda(3 - 6\lambda^2 - \lambda^4)^2}{(1 + 6\lambda^2 - 3\lambda^4)^2},$$

respectively, and gives rise to a squared square in which the entries are of degree 48.

The curve E at (6), when viewed as an elliptic fibration, has four singular fibres above $\lambda = 0, \infty, \pm 1$, each of type I_0^* with five components. It follows from a formula of Shioda [8] that

$$\text{rank}(E(\mathbb{C}(\lambda))) + 2 + 4 \cdot (5 - 1) \leq 20$$

so that $\text{rank}(E(\mathbb{C}(\lambda))) \leq 2$. But $(\lambda, 1)$ and $(-\lambda, i)$ are two independent points of E , and thus $\text{rank}(E(\mathbb{C}(\lambda))) = 2$. Quite possibly, these two points generate $E(\mathbb{C}(\lambda))$, although we have not checked this. In any event, rational squared squares that arise from multiples of P will seemingly have parametrizations of degree at least 48.

If we make the replacement

$$(8) \quad \lambda = \frac{3s^2 + s}{s - 1},$$

then the curve E at (6) over $\mathbb{Q}(s)$ now has rank 2, with independent points given by

$$(9) \quad P_0 = \left(\frac{3s^2 + s}{s - 1}, 1 \right), \quad P_1 = \left(\frac{3s^2 - s}{s + 1}, \frac{(s - 1)^2}{(s + 1)^2} \right).$$

In order to find specializations of λ such that the resulting curve will in general possess rank at least 2, it is necessary to determine a value of X other than λ such that the ratio of $X^3 - X$ to $\lambda^3 - \lambda$ is a perfect square. This is equivalent to demanding that the ratio of the area of the two Pythagorean triangles formed from generators $\{X, 1\}$ and $\{\lambda, 1\}$ be a perfect square. It is apparent that if the Pythagorean triangles formed from generators $\{p, q\}$ and $\{r, s\}$ have areas whose ratio is a square, then $(X, \lambda) = (p/q, r/s)$ have the desired property. Bremner [1] investigates the surface

$$(10) \quad xy(x^2 - y^2) = zt(z^2 - t^2)$$

representing of course the condition that the two primitive Pythagorean triangles formed from generators $\{x, y\}$ and $\{z, t\}$ have *equal* area. The table in [1] giving parametrizations of (10) can therefore be used to furnish several cases where specialization of λ results in a curve E of rank 2. The example given above at (8), $\lambda = (3s^2 + s)/(s - 1)$, corresponds to the first entry in the table,

$$(11) \quad (x, y, z, t) = (3s^2 + s, s - 1, 3s^2 - s, s + 1).$$

With P_0, P_1 as at (9), then using the X -coordinates of P_0 and of $P_0 + P_1$ in (5), we deduce the following square with entries of degree 8:

$$(12) \quad \begin{bmatrix} 4(1+2s+2s^2-6s^3+9s^4)^2 & 4(1+4s^2-12s^3-9s^4)^2 & (1-8s-10s^2-24s^3+9s^4)^2 \\ 4(1-4s-4s^2-9s^4)^2 & (1+22s^2+9s^4)^2 & 4(1+4s-4s^2-9s^4)^2 \\ (1+8s-10s^2+24s^3+9s^4)^2 & 4(1+4s^2+12s^3-9s^4)^2 & 4(1-2s+2s^2+6s^3+9s^4)^2 \end{bmatrix}.$$

The condition that the square be magic is that

$$(13) \quad 1 - 4s^2 - 170s^4 - 36s^6 + 81s^8 = 0,$$

where the polynomial is irreducible over \mathbb{Q} .

I am grateful to John Robertson for pointing out the relevant section (“Right triangles of equal area”) of Dickson [2], where a quadratic parametrization of (10) is ascribed to Hillyer. An equivalent parametrization had in fact been discovered much earlier by Euler. This parametrization is equivalent to that at (11), so in fact the case can be made that Euler was essentially aware of this family (12) of squared squares.

Other squares arising from the substitution (8) have degrees 24, 32, 40, 48, ...

The second entry in the table of [1] corresponds to

$$(14) \quad \lambda = \frac{-t^3 + 4t^2 + t}{t^3 + t + 2}$$

with the curve E possessing the two independent points

$$(15) \quad \begin{aligned} P_0 &= \left(\frac{-t^3 + 4t^2 + t}{t^3 + t + 2}, 1 \right), \\ P_1 &= \left(\frac{-t^2 + 4t + 1}{2t^3 - t^2 - 1}, \frac{(t+1)^2(t^2 - t + 2)^2}{(t-1)^2(2t^2 + t + 1)^2} \right). \end{aligned}$$

The square at (5) using the X -coordinates of P_0 and of $P_0 - P_1$ results in a square $[s_{ij}]$ of degree 16 with the following entries:

$$\begin{aligned} s_{11} &= 9(1 - 2t - t^2)^2(1 + 4t + 8t^2 - 6t^3 + t^4 - 2t^5 + 2t^6)^2, \\ s_{12} &= 9(1 - 2t - t^2)^4(2 + 4t + t^2 + 2t^3 - t^4)^2, \\ s_{13} &= (2 + 20t - 23t^2 + 20t^3 + 74t^4 - 20t^5 - 23t^6 - 20t^7 + 2t^8)^2, \\ s_{21} &= 9(1 - 2t - t^2)^2(2 + 4t + 9t^2 - 6t^4 + 8t^5 - t^6)^2, \\ s_{22} &= (2 + 2t + 49t^2 + 2t^3 - 70t^4 - 2t^5 + 49t^6 - 2t^7 + 2t^8)^2, \\ s_{23} &= 9(1 - 2t - t^2)^4(1 + 2t - t^2 + 4t^3 - 2t^4)^2, \\ s_{31} &= (2 + 4t + t^2 - 10t^3 - t^4)^2(1 - 10t - t^2 + 4t^3 - 2t^4)^2, \\ s_{32} &= 9(1 - 2t - t^2)^2(1 + 8t + 6t^2 - 9t^4 + 4t^5 - 2t^6)^2, \\ s_{33} &= 9(1 - 2t - t^2)^2(2 + 2t + t^2 + 6t^3 + 8t^4 - 4t^5 + t^6)^2. \end{aligned}$$

Further squares arising from the substitution (14) have degrees 32, 44, 48, ...

For each parametrization of (10) given in [1], two independent points P_0 and P_1 on the corresponding curve E are automatically known, and in each instance we computed the squared squares arising from substituting into (5) the X -coordinates of two of the points from the set

$$\{c_0P_0 + c_1P_1 : 0 \leq c_0 + |c_1| \leq 4\}.$$

(In two instances, an upper bound of 3 rather than 4 was taken, because the degrees of the points being computed became too large for comfortable manipulation.) Squares of the following degrees up to 300 were found:

8, 16, 20, 24, 28, 32, 34, 36, 40, 42, 44, 48, 52, 56, 58, 60, 64, 66, 68, 72, 74, 76, 80, 82, 84, 88, 90, 92, 96, 98, 100, 104, 106, 108, 112, 116, 120, 124, 128, 130, 132, 136, 138, 140, 144, 146, 148, 152, 154, 156, 160, 162, 164, 168, 172, 176, 180, 184, 186, 188, 192, 194, 196, 200, 202, 204, 208, 212, 216, 224, 228, 232, 240, 244, 248, 250, 256, 260, 264, 272, 276, 280, 288, 300.

It seems likely that squared squares exist of every degree $d \geq 16$ satisfying $d \equiv 0 \pmod{4}$, and that no squared squares exist for degrees d with $d \equiv 6 \pmod{8}$. Further, the list gives examples of squares of degrees $d \equiv 2 \pmod{8}$ in the range $34 \leq d \leq 202$ with the exceptions of $d = 50, 114, 122, 170, 178$; these latter higher degree examples may be missing simply through not searching sufficiently far.

3. For a given squared square constructed in the above manner by substituting X -coordinates of points on (6) into the square at (5), the property of being magic implies from (7), under the same substitutions, the vanishing of a polynomial of degree equal to that of the square. Substituting a root θ of this polynomial into the squared square results in a magic square with entries lying in the field $\mathbb{Q}(\theta)$. Accordingly, a linear factor results in a rational magic square. However, it turns out that finding magic squares this way in *any* odd degree extension of the rationals is far from easy. For each of the squared squares computed above, its associated polynomial determining that the square be magic was factored. The factors were almost always of even degree, and provided no example of a magic square in a field of degree less than 8, of which we already have an example at (12) and (13). In some cases, there do exist factors of odd degree, but in all but one case these lead to trivial squares with repeated entries. The only example found of a non-trivial magic square with entries in an odd-degree extension of \mathbb{Q} arises from the parametrization $\lambda = (u^2 - 1)/(u^2 + 2)$,

$$P_0 = \left(\frac{u^2 - 1}{u^2 + 2}, 1 \right), \quad P_1 = \left(\frac{u^2 - 1}{2u^2 + 1}, \frac{u(u^2 + 2)^2}{(2u^2 + 1)^2} \right)$$

and where the X -coordinates of $P_0 + P_1$ and $P_0 - P_1$ are substituted into (5). The resulting square $[m_{ij}]$ has entries:

$$\begin{aligned} m_{11} &= (1 - u^3)^2(2 + u)^2(1 + 2u)^2(10 - 32u + 94u^2 \\ &\quad - 148u^3 + 161u^4 - 148u^5 + 94u^6 - 32u^7 + 10u^8)^2, \\ m_{12} &= (2 - u)^2(1 - u)^2(1 + u)^2(2 + u)^2(1 - 2u)^2 \\ &\quad \times (1 + 2u)^2(1 - u + u^2)^2(1 + u + u^2)^2(-7 - 4u^2 + 2u^4)^2, \\ m_{13} &= (2 - u)^2(1 + u^3)^2(1 - 2u)^2(2 + 40u + 92u^2 \\ &\quad + 152u^3 + 181u^4 + 128u^5 + 80u^6 + 40u^7 + 14u^8)^2, \\ m_{21} &= (2 - u)^2(1 - u)^2(1 + u)^2(2 + u)^2(1 - 2u)^2 \\ &\quad \times (1 + 2u)^2(1 - u + u^2)^2(1 + u + u^2)^2(-1 + 8u^2 + 2u^4)^2, \\ m_{22} &= (2 - u)^2(1 + u^3)^2(1 - 2u)^2(10 + 32u + 94u^2 \\ &\quad + 148u^3 + 161u^4 + 148u^5 + 94u^6 + 32u^7 + 10u^8)^2, \end{aligned}$$

$$\begin{aligned}
m_{23} &= (1 - u^3)^2(2 + u)^2(1 + 2u)^2(14 - 40u + 80u^2 \\
&\quad - 128u^3 + 181u^4 - 152u^5 + 92u^6 - 40u^7 + 2u^8)^2, \\
m_{31} &= (2 - u)^2(1 + u^3)^2(1 - 2u)^2(14 + 40u + 80u^2 \\
&\quad + 128u^3 + 181u^4 + 152u^5 + 92u^6 + 40u^7 + 2u^8)^2, \\
m_{32} &= (1 - u^3)^2(2 + u)^2(1 + 2u)^2(2 - 40u + 92u^2 \\
&\quad - 152u^3 + 181u^4 - 128u^5 + 80u^6 - 40u^7 + 14u^8)^2, \\
m_{33} &= (2 - u)^2(1 - u^3)^2(1 + u^3)^2 \\
&\quad \times (2 + u)^2(1 - 2u)^2(1 + 2u)^2(5 + 2u^2 + 2u^4)^2
\end{aligned}$$

and is magic in the field $\mathbb{Q}(u)$ of degree 27 over \mathbb{Q} , where

$$\begin{aligned}
&-1680 - 5196u + 6768u^2 + 14545u^3 + 63864u^4 + 29940u^5 + 240u^6 - 17076u^7 \\
&\quad - 259740u^8 - 222115u^9 - 802332u^{10} - 330012u^{11} - 1202886u^{12} \\
&\quad - 343440u^{13} - 802332u^{14} - 202224u^{15} - 259740u^{16} - 28872u^{17} \\
&\quad + 240u^{18} + 36048u^{19} + 63864u^{20} + 7808u^{21} + 6768u^{22} - 1536u^{23} \\
&\quad - 1680u^{24} - 816u^{25} + 64u^{27} = 0.
\end{aligned}$$

The smallest degree extension of \mathbb{Q} in which we know an example of a magic square of squares has degree 4:

$$\begin{bmatrix}
(5 - 13\sqrt{3})^2 & (17 + 9\sqrt{3})^2 & (22 - 4\sqrt{3})^2 \\
(23 - \sqrt{3})^2 & 133 \cdot 2^2 & (23 + \sqrt{3})^2 \\
(22 + 4\sqrt{3})^2 & (17 - 9\sqrt{3})^2 & (5 + 13\sqrt{3})^2
\end{bmatrix}$$

over the field $\mathbb{Q}(\sqrt{3}, \sqrt{133})$; or indeed, the family

$$\begin{bmatrix}
(\mu^2 + 1)^2 & -(\mu^2 + 2\mu - 1)^2 & 4(\mu^3 - \mu) \\
-(\mu^2 - 2\mu - 1)^2 & 0 & (\mu^2 - 2\mu - 1)^2 \\
-4(\mu^3 - \mu) & (\mu^2 + 2\mu - 1)^2 & -(\mu^2 + 1)^2
\end{bmatrix}$$

over the field $\mathbb{Q}(i, \sqrt{\mu^3 - \mu})$.

References

- [1] A. Bremner, *Pythagorean triangles and a quartic surface*, J. Reine Angew. Math. 318 (1980), 120–125.
- [2] L. E. Dickson, *History of the Theory of Numbers*, Vol. II, Carnegie Institute, Washington, 1920.
- [3] M. Gardner, *The magic of 3×3* , Quantum, Jan.-Feb. 1996, 24–26.
- [4] R. K. Guy and R. J. Nowakowski, “*Monthly*” unsolved problems, 1969–1997, Amer. Math. Monthly 104 (1997), 967–973.
- [5] M. LaBar, *Problem 270*, College Math. J. 15 (1984), 69.

- [6] J. P. Robertson, *Magic squares of squares*, Math. Mag. 69 (1996), 289–293.
- [7] L. Sallows, *The lost theorem*, Math. Intelligencer 19 (1997), no. 4, 51–54.
- [8] T. Shioda, *On elliptic modular surfaces*, J. Math. Soc. Japan 24 (1972), 20–59.
- [9] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 151, Springer, Berlin, 1994.

Department of Mathematics
Arizona State University
Tempe, Arizona 85287-1804
U.S.A.
E-mail: bremner@asu.edu

Received on 3.8.1998
and in revised form on 16.11.1998

(3432)