So $x_n = \frac{2^{2n+2}-1}{3}$, and

$$s(2^n) = x_{(n-3)/2} + 2$$
$$= \frac{2^{n-1}-1}{3} + 2 = \frac{2^{n-1}+5}{3}.$$

A formula for the sum of the odd powers of 2 is obtained from x_n by factoring, and then $s(2^n)$ is easily computed.

REFERENCES

1. Ivan Niven and Herbert Zuckerman, *An Introduction to the Theory of Numbers*, 4th edition, John Wiley & Sons, Inc., New York, 1980.
2. David M. Burton, *Elementary Number Theory*, 3rd edition, Wm. C. Brown, Dubuque, IA, 1994.
3. John Fraleigh, *A First Course in Abstract Algebra*, 3rd edition, Addison-Wesley, Reading, MA, 1982.

Magic Squares of Squares

JOHN P. ROBERTSON
560 Bair Road
Berwyn, PA 19312

A problem in the second edition of Guy's *Unsolved Problems in Number Theory* **[1]** is to prove or disprove that a three-by-three magic square can be constructed from nine distinct integer squares (Problem D15). There are relationships between magic squares, arithmetic progressions, Pythagorean right triangles, congruent numbers, and elliptic curves. This note will follow this chain and show that the following three problems are equivalent to the original problem:

P1. Prove or disprove that there are three arithmetic progressions such that each has three terms, each has the same difference between terms as the other two, the terms are all perfect squares, and the middle terms of the three arithmetic progressions themselves form an arithmetic progression.

P2. Prove or disprove that there are three rational right triangles with the same area, such that the squares of the hypotenuses are in arithmetic progression.

P3. Prove or disprove that there is an elliptic curve, $y^2 = x^3 - n^2x$, where n is a congruent number, with three rational points on the curve, (x_1, y_1), (x_2, y_2), and (x_3, y_3), such that each point is "double" another rational point on the elliptic curve ("double" in the sense of the group structure for points on an elliptic curve), and x_1, x_2, and x_3 are in arithmetic progression.

The original problem is due to LaBar **[2]**. Guy **[1]** notes that the problem requires finding x, y, and z so that the nine quantities x^2, y^2, z^2, $y^2+z^2-x^2$, $z^2+x^2-y^2$, $x^2+y^2-z^2$, $2x^2-y^2$, $2x^2-z^2$, and $3x^2-y^2-z^2$, are distinct perfect squares.

Magic squares and arithmetic progressions For any three-by-three magic square made up of distinct positive integers, there are three positive integers a, u, and v, such that the magic square can be expressed (possibly after rotation or reflection) as:

$$\begin{array}{ccc} a+u+2v & a & a+2u+v \\ a+2u & a+u+v & a+2v \\ a+v & a+2u+2v & a+u. \end{array}$$

(See Martin Gardner [3].) Note that any such magic square can be decomposed into three arithmetic progressions:

$$a, a+u, a+2u;$$
$$a+v, a+u+v, a+2u+v;$$
$$a+2v, a+u+2v, a+2u+2v.$$

Each of these three sequences has the same difference, u, between terms. Note also that corresponding terms of the three sequences are in arithmetic progression, with common difference v. Conversely, any set of three arithmetic progressions of length three with a common difference, and corresponding terms in arithmetic progression, can be rearranged into a three-by-three magic square.

For example, if $a = 1$, $u = 1$, and $v = 3$, we get the familiar magic square:

$$\begin{array}{ccc} 8 & 1 & 6 \\ 3 & 5 & 7 \\ 4 & 9 & 2 \end{array}$$

The first equivalent formulation, **P1**, of the original problem should now be clear.

Squares in arithmetic progression It is well known that it is possible to have three squares in arithmetic progression, but not four (Dickson [4, pp. 435–440]). For any increasing three-term arithmetic progression of pairwise relatively prime squares, r^2, s^2, t^2, there are positive integers p and q such that

$$\begin{aligned} r &= |p^2 - 2pq - q^2|, \\ s &= p^2 + q^2, \\ t &= p^2 + 2pq - q^2, \end{aligned} \qquad (*)$$

p and q are relatively prime, and one of them is even (Dickson [4, pp. 437–438]). For example, if $r = 1$, $s = 5$, and $t = 7$, then $p = 2$ and $q = 1$.

If r^2, s^2, t^2 are in increasing arithmetic progression, but are not relatively prime, then there are k, p, and q, with k a positive integer, p and q as above, and

$$\begin{aligned} r &= k|p^2 - 2pq - q^2|, \\ s &= k(p^2 + q^2), \text{ and} \\ t &= k(p^2 + 2pq - q^2). \end{aligned}$$

For the r^2, s^2, t^2 just above, the difference between terms is

$$s^2 - r^2 = t^2 - s^2 = 4k^2(p^3q - pq^3).$$

Thus the original problem can be stated as find k_1, p_1, q_1, k_2, p_2, q_2, k_3, p_3, and q_3 so that

$$k_1^2(p_1^3q_1 - p_1q_1^3) = k_2^2(p_2^3q_2 - p_2q_2^3) = k_3^2(p_3^3q_3 - p_3q_3^3) > 0,$$

and

$$k_1^2(p_1^2+q_1^2)^2,\ k_2^2(p_2^2+q_2^2)^2, \text{ and } k_3^2(p_3^2+q_3^2)^2$$

are distinct and in arithmetic progression. (Note that the fact that one cannot have four squares in arithmetic progression makes unnecessary any further restrictions on the "horizontal" and "vertical" differences between terms.)

It is easy to generate any number of three-term arithmetic progressions of squares, all with the same difference between terms, as we now show. Let u^2, v^2, and w^2 be in arithmetic progression. Let $p=v^2$ and $q=v^2-u^2$. Then for the three-term arithmetic progression generated by p and q using $(*)$, the difference between terms is $4u^2v^2w^2(v^2-u^2)$, which is a perfect square times v^2-u^2. Multiplying each term of the sequence u^2, v^2, w^2 by $4u^2v^2w^2$ gives a sequence with the same difference as the sequence generated by p and q. This process of generating a new sequence from a previous one (including the step of multiplying all previous sequences by the appropriate constant so that all sequences have the same difference between terms) can be continued indefinitely. If the new sequence is always derived from the last sequence generated, then all the sequences will be different. This is not difficult to prove, but we do not do that here.

As an example, start with the sequence generated from $p=5$ and $q=2$ using $(*)$. These give the sequence $1^2, 29^2, 41^2$, with difference of terms 840. Next let $p=29^2=841$ and $q=840=29^2-1^2$. These give the sequence $1411199^2, 1412881^2, 1414561^2$, with difference of terms 840×2378^2. Not all sequences with difference a square times 840 are generated in this way. For example, the sequences generated by $p=6$ and $q=1$, and by $p=8$ and $q=7$ (and sequences generated from these two sequences) have differences between terms that are a square times 840, but are not included in the set of sequences generated from $p=5$ and $q=2$.

Pythagorean triples There are simple relationships between three-term arithmetic progressions of squares and Pythagorean triples. The latter are related to congruent numbers and rational points on elliptic curves, so these relationships will be of use to us.

Every three-term arithmetic progression of squares, r^2, s^2, t^2, can be associated with a Pythagorean triple, X, Y, Z, with $X^2+Y^2=Z^2$, by taking $X=(r+t)/2$, $Y=(t-r)/2$, and $Z=s$. Conversely, each Pythagorean triple generates a three-term arithmetic progression of squares by taking $r=X-Y$, $s=Z$, and $t=X+Y$. *Two three-term arithmetic progressions of squares have the same difference of terms if, and only if, the corresponding Pythagorean right triangles have the same area.* The second equivalent formulation, **P2**, of the original problem should now be clear.

Congruent numbers The square-free part of $XY/2$ (the result of dividing $XY/2$ by the largest possible integer square), where X, Y, Z is a Pythagorean triple, is (by definition) a *congruent number*. This is clearly also the square-free part of the difference between terms of the associated three-term arithmetic progression of squares.

It is more convenient to work with right triangles with square-free area. Note that if k is the largest integer such that k^2 divides $XY/2$, then the area of the triangle with sides X/k, Y/k, and Z/k is a square-free integer. In general, X/k, Y/k, and Z/k will not be integers.

Elliptic curves If n is a congruent number, there is a well-known mapping from rational right triangles with area n to rational points on the elliptic curve $y^2=x^3-n^2x$

given by

$$x = (Z/2)^2, y = (X^2 - Y^2)Z/8.$$

Koblitz [5] shows that for each such point, $P = (x, y)$, there is another rational point, Q, on the elliptic curve such that $2Q = P$ in the sense of the group structure (briefly described below) for points on elliptic curves. Conversely, each rational point on the elliptic curve that is the double of another point (except the point at infinity) corresponds to a rational right triangle with area n. See Koblitz [5] for further details on the correspondences between points on such elliptic curves and Pythagorean triples. The third equivalent formulation, **P3**, of the original problem should now be clear.

A group structure on an elliptic curve is described as follows. An elliptic curve consists of the points (x, y) that satisfy the defining equation, plus a *point at infinity*, which can be thought of as lying an infinite distance above the point (0, 0). The inverse, or negative, of a point $P = (x, y)$ on the elliptic curve is the point $-P = (x, -y)$. The point at infinity is its own negative and is also the identity element for the group operation. Every vertical line intersects the point at infinity, and these are the only lines that intersect the point at infinity. If a line is tangent to the curve at some point, consider the line to intersect the curve twice there, unless the line is tangent to the curve at a point of inflection, in which case consider the line to intersect the curve three times at that point. With these conventions, if a line intersects the curve twice then the line intersects the curve exactly three times. This fact can be used to define a group operation, $\oplus$, by taking $P \oplus Q \oplus R = 0$ if P, Q, and R lie on the same straight line. That is, $P \oplus Q = -R$ if P, Q, and R are collinear. To determine $P \oplus P(= 2P)$ for a point other than the point at infinity, take the tangent through P, find the other point of intersection with the curve, and take the negative of this last point. If P and Q have rational coordinates, then $P \oplus Q$ will have rational coordinates. It is easy to see that $\oplus$ is commutative, that each group element has an inverse, and that the identity behaves as it should. That $\oplus$ is associative is more difficult. See Koblitz [5], or other references on elliptic curves for more details. The operation $\oplus$, as we have defined it, is not the only way to define a group structure on the elliptic curve (see Cassels [6]).

There is a relationship between the doubling of points on elliptic curves and the method given above to generate a new three-term arithmetic progression of squares from a given one. Namely, if the point P corresponds to the three-term arithmetic progression u^2, v^2, w^2, then $2P$ corresponds to the three-term arithmetic progression generated by $(*)$ with $p = v^2$ and $q = v^2 - u^2$.

One potential usefulness of the elliptic curve formulation is that, for a given congruent number n, the group structure of rational points on elliptic curves shows there are infinitely many candidates for terms in the needed arithmetic progression. Thus, one can list as many candidates as one wants. Ideally, one "solves" the elliptic curve, finding points that generate all rational points on the curve. Failing this, one can often at least find some integral or rational points on the elliptic curve, and use these to generate others. My experience has been that there usually are several integral points with x values between $-n$ and 0, from which other points can be found.

Elliptic curves of high rank might be more likely than curves of lower rank to have three points meeting the conditions of formulation **P3**. (It is a theorem [5] that the group of rational points for an elliptic curve is $T \times Z^r$ where T is the subgroup consisting of all elements of finite order. The *rank* is r.) Wada and Taira [7] compute the ranks of all elliptic curves of the form $y^2 = x^3 - n^2x$ for all but 77 congruent

$n \leq 10{,}000$. The curve has rank three for $n = 1254$, 2605, 2774, 3502, 4199, 4669, 4895, 6286, 6671, 7230, 7766, 8005, 9015, 9430, and 9654. Noda and Wada [**8**] has a table that is an essential part of the results given in [**7**].

Martin Gardner ([**9, 10**]) also discusses this problem and gives some related results. He offers $100 to the first person who constructs a three-by-three magic square of distinct squares.

REFERENCES

1. Richard Guy, *Unsolved Problems in Number Theory*, 2nd edition, Springer-Verlag, New York, 1994, Problem D15, pp. 170–171.
2. Martin LaBar, Problem 270, *College Math. J.*, 15 (1984), 69.
3. Martin Gardner, *Riddles of the Sphinx*, Mathematical Association of America, Washington, DC, 1987, pp. 136–137.
4. Leonard Eugene Dickson, *History of the Theory of Numbers*, Volume II, Chelsea, New York, 1952.
5. Neal Koblitz, *Introduction to Elliptic Curves and Modular Forms*, 2nd edition, Springer-Verlag, New York, 1993, pp. 1–50.
6. J. W. S. Cassels, *Lectures on Elliptic Curves*, Cambridge University Press, Cambridge, UK, 1991, pp. 27–31.
7. Hideo Wada and Mayako Taira, Computations of the rank of elliptic curve $y^2 = x^3 - n^2x$, *Proc. Japan Acad.*, 70, Ser. A (1994), 154–157.
8. Kazunari Noda and Hideo Wada, All congruent numbers less than 10000, *Proc. Japan Acad.*, 69, Ser. A (1993), 175–178.
9. Martin Gardner, The magic of 3 × 3, *Quantum*, 6 (1996), January/February, pp. 24–26.
10. Martin Gardner, Letters, *Quantum*, 6 (1996), March/April, p.60.

General Russian Roulette

GUNNAR BLOM
Department of Mathematical Statistics, University of Lund,
Box 118, S-221 00 Lund, Sweden

JAN-ERIC ENGLUND
Swedish University of Agricultural Sciences,
Box 35, S-230 53 Alnarp, Sweden

DENNIS SANDELL
Biostatistics and Data Processing, Astra Draco AB,
Box 34, S-221 00 Lund, Sweden

1. Russian roulette Russian roulette provides a standard exercise in probability. Let us quote from [**1**], p. 32:

> Russian roulette is played with a revolver equipped with a rotatable magazine of six shots. The revolver is loaded with one shot. The first duellist, A, rotates the magazine at random, points the revolver at his head and presses the trigger. If, afterwards, he is still alive, he hands the revolver to the other duellist, B, who acts in the same way as A. The players shoot alternately in this manner, until a shot goes off. Determine the probability that A is killed.

The answer is 6/11.