ARITHMETIC PROGRESSIONS WITH SQUARE ENTRIES

M. A. Khan
c/o A. A. Khan, Regional Office, Indian Overseas Bank, Ashoka Marg, Lucknow, India

Harris Kwong
Dept. of Math. Sci., SUNY Fredonia, Fredonia, NY 14063
e-mail: kwong@fredonia.edu

(Submitted January 2001-Final Revision January 2005)

ABSTRACT

We study properties of arithmetic progressions consisting of three squares; in particular, how one arithmetic progression generates infinitely many others, by means of explicit formulas as well as a matrix method. This suggests an equivalence relation could be defined on the arithmetic progressions, which lead to interesting problems for further study.

The purpose of this paper is to investigate ordered triples of integers whose squares form an arithmetic progression. In other words, we want to study (a, b, c), where a, b, c are integers that satisfy $b^2 - a^2 = c^2 - b^2$, or equivalently,

$$2b^2 = a^2 + c^2. \tag{1}$$

We call such an ordered triple an *arithmetic progression triple*, or simply an *apt*.

Theorem 1: *The ordered triple (a, b, c) is an apt if and only if it satisfies equation (1).*

Obviously, we have an apt if its entries have the same absolute value. Consequently, for $n \neq \pm 1$, we call the ordered triple $(\pm n, \pm n, \pm n)$, for any combination of signs, the *trivial apts*. Examples of nontrivial apts include $(1, -1, -1)$, $(1, 5, 7)$, and $(-7, 13, 17)$.

Solving equation (1) is a rather standard exercise. A proof of the next result can be found in, for example, [6, pages 305 and 343]. It can also be derived from a more general result regarding solutions of $ax^2 + bxy + cy^2 = ez^2$; see, for example, [2, Theorem 42].

Theorem 2: *Let ρ be the greatest common divisor of a, b, c, then the solutions of the Diophantine equation $2b^2 = a^2 + c^2$ are of the form*

$$\begin{aligned} a &= \pm\rho(m^2 - n^2 - 2mn), \\ b &= \pm\rho(m^2 + n^2), \\ c &= \pm\rho(m^2 - n^2 + 2mn), \end{aligned} \tag{2}$$

for any integers m and n.

In light of Theorem 2, we call the apt (a, b, c) a *primitive arithmetic progression triple*, or simply a *papt*, if $\rho = 1$. Observe that

- If (a, b, c) is a papt, then so is (c, b, a).
- If (a, b, c) is a papt, then so are $(\pm a, \pm b, \pm c)$ for any combination of signs.
- Consequently, with the exception of $(\pm 1, \pm 1, \pm 1)$, finding one papt would immediately lead to fifteen other papts, which vary only in signs and order. The ordered triple $(\pm 1, \pm 1, \pm 1)$, however, leads to only seven other papts.

The next two theorems are also easy to prove.

Theorem 3: *If (a, b, c) is a papt, then a, b and c are all odd.*

Proof: Since $2b^2 = a^2 + c^2$ is even, we conclude that a^2 and c^2, hence a and c, have the same parity. If a and c are both even, then $2b^2 = a^2+c^2 \equiv 0 \pmod 4$ implies that b is also even, in which case (a, b, c) cannot be a papt. Thus both a and c are odd. Now $2b^2 = a^2 + c^2 \equiv 2 \pmod 4$ requires that b be odd as well. □

Theorem 4: *The ordered triple (a, b, c) is a papt if and only if $m \not\equiv n$ (mod 2) and* $\gcd(m, n) = 1$.

Proof: Let (a, b, c) be a papt. It is obvious that we need $\gcd(m, n) = 1$. On the other hand, Theorem 3 asserts that

$$1 \equiv m^2 - n^2 - 2mn \equiv m^2 + n^2 \equiv m^2 - n^2 + 2mn \pmod 2,$$

hence $m \not\equiv n \pmod 2$.

Conversely, assume m and n have opposite parity and are relatively prime. Let $d = \gcd(m^2 - n^2 - 2mn, m^2 + n^2)$. Suppose $d > 1$, then it has a prime factor p. Since m and n have opposite parity, p must be odd. We also know p divides the linear combination

$$(m^2 - n^2 - 2mn) + (m^2 + n^2) = 2m^2 - 2mn = 2m(m - n).$$

If p divides m, then, since p divides m^2+n^2 as well, we also have p divides n, which contradicts the assumption that m and n are relatively prime. Hence p must divide $m - n$. On the other hand, the same argument applies to the linear combination

$$(m^2 + n^2) - (m^2 - n^2 - 2mn) = 2n^2 + 2mn = 2n(m + n)$$

leads to p divides $m+n$. Consequently, p divides both $(m+n)+(m-n) = 2m$ and $(m+n)-(m-n) = 2n$, which in turn implies that p divides both m and n. This contradiction shows that $d = 1$. In a similar fashion, $\gcd(a, c) = \gcd(b, c) = 1$. Thus (a, b, c) is a papt. □

Are there any nontrivial arithmetic progression with square entries that could exceed three in length? The answer is negative.

Theorem 5: *The only four positive integers whose squares can form an arithmetic progression are those with the same absolute value. In other words, $(\pm n, \pm n, \pm n, \pm n)$ are the only ordered quadruples whose squares form an arithmetic progression.*

Proof: Suppose a^2, b^2, c^2, d^2 are relatively prime squares that form an arithmetic progression. Then $b^2 - a^2 = c^2 - b^2 = d^2 - c^2$, or equivalently,

$$(b - a)(b + a) = (c - b)(c + b) = (d - c)(d + c).$$

We know that a, b, c and d are odd, thus both $b-a$ and $c-b$ are even. Let $2\alpha = \gcd(b-a, c-b)$ so that we can write

$$b - a = 2\alpha\beta, \qquad c - b = 2\alpha\gamma, \tag{3}$$

where $\gcd(\beta, \gamma) = 1$. Likewise letting $2\delta = \gcd(b + a, c + b)$ would lead to

$$b + a = 2\gamma\delta, \qquad c + b = 2\beta\delta, \tag{4}$$

which in turn imply that

$$d - c = 2\alpha\delta, \qquad d + c = 2\beta\gamma. \tag{5}$$

¿From (3) and (4), we find $2b = 2\alpha\beta + 2\gamma\delta = 2\beta\delta - 2\alpha\gamma$. Hence we obtain

$$\gamma(\delta + \alpha) = \beta(\delta - \alpha). \tag{6}$$

Likewise, $2c = 2\alpha\gamma + 2\beta\delta = 2\beta\gamma - 2\alpha\delta$ implies that

$$\delta(\beta + \alpha) = \gamma(\beta - \alpha). \tag{7}$$

Since $\gcd(\delta \pm \alpha, \beta \pm \alpha)$ equals 1 or 2, a comparison of (6) and (7) would yield either

$$\text{(I)} \quad \begin{aligned} \delta + \alpha &= \beta \\ \delta - \alpha &= \gamma \end{aligned} \qquad \text{or} \qquad \text{(II)} \quad \begin{aligned} \delta + \alpha &= 2\beta \\ \delta - \alpha &= 2\gamma \end{aligned}$$

In a similar manner, we have either

$$\text{(III)} \quad \begin{aligned} \beta + \alpha &= \gamma \\ \beta - \alpha &= \delta \end{aligned} \qquad \text{or} \qquad \text{(IV)} \quad \begin{aligned} \beta + \alpha &= 2\gamma \\ \beta - \alpha &= 2\delta \end{aligned}$$

Substituting (I) into (7) yields

$$\beta + \alpha = \gamma.$$

Hence (I) implies (III), and similarly, (III) implies (I); and in such event we would have

$$2\delta = \beta + \gamma \qquad \text{and} \qquad \delta + \beta = 2\gamma.$$

Together they imply $2\delta - \gamma = \beta = 2\gamma - \delta$; thus $\delta = \gamma$, from which we deduce that $\alpha = 0$, which is impossible. Hence we must have (II) and (IV). It then follows that

$$\delta + \alpha = 2\beta = 2\gamma + 2\delta = (\delta - \alpha) + 2\delta,$$

which leads to $\alpha = \delta$, from which we find $\gamma = 0$, which is again impossible. Thus a^2, b^2, c^2 and d^2 cannot form an arithmetic progression without having $\gcd(a, b, c, d) > 1$. □

With Theorem 5, we can focus our attention to papts. Given a papt, we can easily generate other papts.

Lemma 6: *If (a, b, c) is a papt, then so are $(c, 3(\pm b) - 2(\pm a), 4(\pm b) - 3(\pm a))$.*

Proof: Direct computation yields

$$[4(\pm b) - 3(\pm a)]^2 - [3(\pm b) - 2(\pm a)]^2 = 7b^2 - 12(\pm b)(\pm a) + 5a^2$$

and

$$[3(\pm b) - 2(\pm a)]^2 - c^2 = [3(\pm b) - 2(\pm a)]^2 - (2b^2 - a^2) = 7b^2 - 12(\pm b)(\pm a) + 5a^2,$$

which completes the proof. □

Corollary 7: *If (a, b, c) is a papt, then so are $(4(\pm b) - 3(\pm c), 3(\pm b) - 2(\pm c), a)$.*

Proof: Since (a, b, c) is a papt, so is (c, b, a). Lemma 6 states that $(a, 3(\pm b) - 2(\pm c), 4(\pm b) - 3(\pm c))$ are also papts, hence so are $(4(\pm b) - 3(\pm c), 3(\pm b) - 2(\pm c), a)$. □

Lemma 8: *If (a, b, c) is a papt, then for $n = 0, \pm 1, \pm 2, \ldots$, the ordered triples (A_n, B_n, C_n), where*

$$A_n = 2n(n-1)b - (n^2-1)a - n(n-2)c, \tag{8}$$
$$B_n = (2n^2+1)b - n(n+1)a - n(n-1)c, \tag{9}$$
$$C_n = 2n(n+1)b - n(n+2)a - (n^2-1)c. \tag{10}$$

are also papts.

Proof: Let $A_0 = a$, $B_0 = b$, $C_0 = c$, and define recursively, for $n > 0$,

$$A_n = C_{n-1}, \quad B_n = 3B_{n-1} - 2A_{n-1}, \quad C_n = 4B_{n-1} - 3A_{n-1}.$$

It follows from Lemma 6 that (A_n, B_n, C_n) is a papt for each $n > 0$. For instance,

$A_1 =$	$B_1 = 3b - 2a$,	$C_1 = 4b - 3a$,
$A_2 = 4b - 3a$,	$B_2 = 9b - 6a - 2c$,	$C_2 = 12b - 8a - 3c$,
$A_3 = 12b - 8a - 3c$,	$B_3 = 19b - 12a - 6c$,	$C_3 = 24b - 15a - 8c$,
$A_4 = 24b - 15a - 8c$,	$B_4 = 33b - 20a - 12c$,	$C_4 = 40b - 24a - 15c$.

Newton's forward difference formula (see, for example, [3]) suggests that for all $n \geq 0$, (8)–(10) would give the formulas for A_n, B_n and C_n. These formulas can be easily verified by induction. For negative subscripts, define recursively, for $n > 0$,

$$A_{-n} = 4B_{-(n-1)} - 3C_{-(n-1)}, \quad B_{-n} = 3B_{-(n-1)} - 2C_{-(n-1)}, \quad C_{-n} = A_{-(n-1)}.$$

Corollary 7 ensures that (A_{-n}, B_{-n}, C_{-n}) is a papt for each integer $n > 0$, and it follows by induction that formulas (8)–(10) still work perfectly. □

We also discover another interesting property of the numbers A_n, B_n, C_n.

Corollary 9: *The determinant*

$$D = \begin{vmatrix} A_n & A_{n+1} & A_{n+2} \\ B_n & B_{n+1} & B_{n+2} \\ C_n & C_{n+1} & C_{n+2} \end{vmatrix} = 2(2b - a - c)^3.$$

is independent of n. Therefore, D is an invariant, and its value depends only on a, b and c.

Proof: The result follows from equations (8)–(10), the details are left to the readers. □

Let us look at a few examples. First, observe that the papt $(1, 1, 1)$ is not particularly interesting, in the sense that it generates $(A_n, B_n, C_n) = (1, 1, 1)$ for each n. The following papts are derived from the papt $(1, 5, 7)$ with the aid of Lemma 8.

n	...	-4	-3	-2	-1	0	1	2	3	4	...
A_n	...	17	7	1	-1	1	7	17	31	49	...
B_n	...	13	5	1	1	5	13	25	41	61	...
C_n	...	7	1	-1	1	7	17	31	49	71	...

It should be clear that any papt derived from $(1, 5, 7)$ will generate the same list of papts; what it amounts to is a shifting of the table listed above. Here is the reason. Note that equations (8)–(10) can be combined into a matrix equation:

$$\begin{bmatrix} A_n \\ B_n \\ C_n \end{bmatrix} = \begin{bmatrix} -(n^2-1) & 2n(n-1) & -n(n-2) \\ -n(n+1) & 2n^2+1 & -n(n-1) \\ -n(n+2) & 2n(n+1) & -(n^2-1) \end{bmatrix} \begin{bmatrix} a \\ b \\ c \end{bmatrix}. \tag{11}$$

Comparing to Lemma 6, we conclude that

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

In particular, when $n = 1, -1$, we obtain Lemma 6 and Corollary 7 respectively. The matrix equation in (11) leads to

$$\begin{bmatrix} A_h \\ B_h \\ C_h \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \\ -2 & 3 & 0 \\ -3 & 4 & 0 \end{bmatrix}^{h-k} \begin{bmatrix} A_k \\ B_k \\ C_k \end{bmatrix}.$$

Hence, given any papt (x, y, z), and any integer n, we can always find (a, b, c) such that (x, y, z) is precisely the nth papt (A_n, B_n, C_n) that can be derived from (a, b, c).

In light of what we have learned thus far, we define two papts (a, b, c) and (a', b', c') to be related, and write $(a, b, c) \sim (a', b', c')$, if one can be derived from the other; that is, if there exists an integer n such that $(a', b', c') = (A_n, B_n, C_n)$ that can be derived from (a, b, c).

It is clear that $\sim$ is an equivalence relation. For example, the equivalence class represented by $(1, 1, 1)$ contains only one papt, namely, $(1, 1, 1)$ itself. The example we discussed above is the equivalent class represented by $(1, 5, 7)$. An immediate question is whether there exists any other equivalent classes.

Suppose (a, y, z) is a papt, then by Theorem 2,

$$a = m^2 - n^2 - 2mn$$

for some integers m and n. This yields $m = n \pm \sqrt{2n^2 + a}$. Given a, choose n so that $2n^2 + a$ is a perfect square. This gives us m and in turn y and z. For example, if $a = 1$ and $n = 2$, them $m = 5$ or -1, and we obtain the papts $(1, 29, 41)$ and $(1, 5, -7)$ respectively. The following result is well-known, see, for example, [1].

Theorem 10: *If $2n^2 + a$ is a perfect square for some value of n, then it is so for infinitely many values of n.*

Consequently, there exist infinitely many equivalence classes. It would be an interesting problem to classify them according to the value of a, for which there exists an n such that $2n^2 + a$ is a perfect square. Note that if the integer a cannot be expressed in the form of $p^2 - 2q^2$ for some integers p and q, then $2n^2 + a$ can never be a perfect square for any integer n. For example, $\sqrt{2n^2 + 3}$ is always irrational if n is an integer.

For instance, one may want to count, for any papt (a, b, c), the number of equivalence classes that $(\pm a, \pm b, \pm c)$ would produce. Computational evidence suggests that the answer may depend on n and m.

ACKNOWLEDGMENT

The authors are indebted to the anonymous referee, whose patience and valuable suggestions significantly improved the presentation of this paper.

REFERENCES

[1] G. Chrystal. *Textbook of Algebra, Volume II.* Chelsea, New York, 1959.
[2] L. E. Dickson. *Introduction to the Theory of Numbers.* Dover, New York, 1957.
[3] J. D. Faires and R. Burden. *Numerical Methods, Second Edition.* Brooks/Cole, Pacific Grove, CA, 1998.
[4] S. Goldberg. *Introduction to Difference Equations.* Wiley, New York, 1958.
[5] L. J. Mordell. *Diophantine Equations.* Academic Press, New York, 1969.
[6] H. M. Stark. *An Introduction to Number Theory.* Markham, Chicago, 1970.
[7] I. M. Vinogradov. *Elements of Number Theory.* Dover, New York, 1954.

AMS Classification Numbers: 11B25, 11B37

✠ ✠ ✠