COMMENTS ON PROOFS THAT THERE ARE NO FOUR SQUARES IN ARITHMETIC PROGRESSION

RUSSELL A. GORDON AND SARA L. GRAHAM

ABSTRACT. It is known that there are no four distinct squares that form an arithmetic progression. We present a slightly new proof of a more general result, summarize the various proofs that there are no four squares in arithmetic progression, and carefully explain the error in an incorrect proof that persists in the literature.

Although it is relatively easy to find examples of three distinct squares in arithmetic progression (the numbers 1, 25, and 49 provide one of infinitely many examples), it is known that it is impossible to find an arithmetic progression consisting of four distinct squares. However, there is no standard proof of this result. A literature search leaves a person somewhat surprised by the variety of available proofs and puzzled by the persistence of one purported proof that is incorrect. The purpose of this article is to offer a slightly new proof (one that is shorter and clearer) of a more general result, to summarize the various proofs that there are no four squares in arithmetic progression, and to carefully explain the error in the incorrect proof.

1. INTRODUCTION

Our goal is to prove that there are no distinct positive integers a, b, c, and d for which the numbers a^2, b^2, c^2, d^2 form the terms of an arithmetic progression. We thus want to show that the pair of equations $a^2 + c^2 = 2b^2$ and $b^2 + d^2 = 2c^2$ has no positive integer solutions other than $a = b = c = d$. A slightly stronger version of this statement is to claim that there are no positive integers a, d, and x that satisfy the equation $a(a+d)(a+2d)(a+3d) = x^2$. Equations such as these, where only integer solutions are considered, are called Diophantine equations. There is a rich history behind these types of equations, but we leave such an exploration to the reader.

In order to prove this result about squares, we need a few simple facts from elementary number theory. For ease of reference, these are summarized below. Recall that an ordered triple (a, b, c) of positive integers is a Pythagorean triple if $a^2 + b^2 = c^2$. If the three integers are relatively prime, then we say that (a, b, c) is a primitive Pythagorean triple. For proofs of the following facts (primarily item (6)), the reader may consult almost any standard number theory text such as [7] or [11].

(1) If 3 divides $x^2 + y^2$, then 3 divides both x and y. Hence, if x and y are relatively prime positive integers, then 3 does not divide $x^2 + y^2$ and $\gcd(x^2 + y^2, x^2 + 4y^2) = 1$. In particular, the hypotenuse in any primitive Pythagorean triple is not a multiple of 3.
(2) If x and y are relatively prime positive integers and xy is a square, then x and y are squares.
(3) If u, v, x, and y are positive integers such that $uv = xy$ and $\gcd(u, x) = 1 = \gcd(v, y)$, then $u = y$ and $v = x$.

(4) If u, v, x, and y are positive integers such that $uv = xy$ and $\gcd(u, v) = 1 = \gcd(x, y)$, then there exist four pairwise relatively prime positive integers α, β, γ, and δ such that $u = \alpha\beta$, $v = \gamma\delta$, $x = \alpha\gamma$, and $y = \beta\delta$. Note that $\alpha = \gcd(u, x)$ and $\delta = \gcd(v, y)$.
(5) If (a, b, c) is a primitive Pythagorean triple, then c is odd, the integers a and b have opposite parity, and either a or b is divisible by 4.
(6) If (a, b, c) is a primitive Pythagorean triple and b is even, then there exist relatively prime positive integers u and v such that $v > u$, $u+v$ is odd, and $a = v^2 - u^2$, $b = 2uv$, and $c = v^2 + u^2$.

2. Primary Results

One way to prove that a Diophantine equation has no nontrivial solutions (that is, solutions where the integers are not all equal) is the method of infinite descent. For such a proof, we assume that an equation has a nontrivial solution involving positive integers, then proceed to show that the equation has a smaller nontrivial solution. Since this process involving decreasing positive integers cannot continue indefinitely, we obtain a contradiction and thus conclude that the equation has no nontrivial solutions. The method of infinite descent is equivalent to a proof that uses the Well-Ordering Property of the positive integers. This property states that a nonempty set of positive integers has a least element. It is well-known (and not difficult to establish) that this property is equivalent to the Principle of Mathematical Induction. We will use the Well-Ordering Property, rather than the method of infinite descent, to prove the following theorem.

Theorem 2.1. *There are no Pythagorean triples of the forms (a, b, c) and $(a, 2b, d)$.*

Proof. Suppose there is a pair of Pythagorean triples with the forms (a, b, c) and $(a, 2b, d)$. We first show that we may assume that the two triples are primitive. If $g = \gcd(a, b) > 1$, then the triples can be represented as (gA, gB, gC) and $(gA, 2gB, gD)$. We thus have a pair of Pythagorean triples of the form (A, B, C) and $(A, 2B, D)$, where $\gcd(A, B) = 1$. If A is odd, then both triples are primitive. If $A = 2A_1$ is even (and thus B is odd), then the triples become $(2A_1, B, C)$ and $(2A_1, 2B, 2D_1)$ or $(2A_1, B, C)$ and (A_1, B, D_1), where $\gcd(A_1, B) = 1$. We thus obtain a pair of primitive Pythagorean triples with the desired form.

With this information, suppose there is a pair of primitive Pythagorean triples of the forms (a, b, c) and $(a, 2b, d)$. By the Well-Ordering Property of the positive integers, we may assume that b is the least positive integer with this property. Note that $b \geq 4$ must be even and that a, c, and d are all odd. By fact (6), there exist positive integers u, v, x, and y such that

$\gcd(u, v) = 1$, $v > u$, $u + v$ is odd, $a = v^2 - u^2$, and $b = 2uv$;
$\gcd(x, y) = 1$, $y > x$, $x + y$ is odd, $a = y^2 - x^2$, and $2b = 2xy$.

Using a simple modulo 4 argument on the two representations of a, we find that u and x must have the same parity. We will assume that x and u are odd and thus y and v are even; the other case is similar. Since $uv = x(y/2)$, we can use fact (4) to write $u = \alpha\beta$, $v = \gamma\delta$, $x = \alpha\gamma$, and $y = 2\beta\delta$, where the four positive integers α, β, γ, and δ are pairwise relatively prime. Note that α is odd and (since b is a multiple of 4) that $\delta = \gcd(v, y/2)$ is even. Equating the two expressions for a yields $u^2 + y^2 = x^2 + v^2$ and thus

$$\beta^2(\alpha^2 + 4\delta^2) = \gamma^2(\alpha^2 + \delta^2).$$

Since $\gcd(\beta, \gamma) = 1$ and (by fact (1)) $\gcd(\alpha^2 + \delta^2, \alpha^2 + 4\delta^2) = 1$, we may use fact (3) to find that $\alpha^2 + \delta^2 = \beta^2$ and $\alpha^2 + 4\delta^2 = \gamma^2$. We thus have a pair of primitive Pythagorean triples

of the forms (α, δ, β) and $(\alpha, 2\delta, \gamma)$, where δ is an even positive integer and $\delta \leq y/2 < y \leq b$. This is a contradiction to the fact that b is the minimal such positive integer. □

A simple consequence of Theorem 2.1 is the following corollary. This statement is usually proved directly using the method of infinite descent (see [6, 10, 15]). Since almost all of the typical proofs of this fact use Pythagorean triples and their parameterizations, it seems more natural to prove our Theorem 2.1 first.

Corollary 2.2. *If p, q, and r are positive integers that satisfy $p^4 - p^2q^2 + q^4 = r^2$, then $p = q$.*

Proof. Suppose that $p \neq q$ and, without loss of generality, assume that q is greater than p. Since $p^4 - p^2q^2 + q^4 = r^2$, we find that $(q^2 - p^2, pq, r)$ and $(q^2 - p^2, 2pq, q^2 + p^2)$ are Pythagorean triples, a contradiction. □

We now prove our main result. The essential idea for this proof can be found in [5], but we have streamlined the details using Theorem 2.1 rather than give a direct proof via infinite descent.

Theorem 2.3. *The product of four distinct positive integers that form an arithmetic progression cannot be a perfect square. In other words, there are no positive integers a, d, and x that satisfy the equation $a(a + d)(a + 2d)(a + 3d) = x^2$.*

Proof. Suppose there are positive integers a, d, and x for which $a(a+d)(a+2d)(a+3d) = x^2$. Without loss of generality, we may assume that a and d are relatively prime. By basic algebra, we find that

$$x^2 = a(a + 3d)(a + d)(a + 2d) = (a^2 + 3ad)(a^2 + 3ad + 2d^2) = (a^2 + 3ad + d^2)^2 - d^4,$$

revealing that $(x, d^2, a^2 + 3ad + d^2)$ is a primitive Pythagorean triple. Suppose first that d is even. By fact (6), there exist relatively prime positive integers u and v with u even and v odd such that $d^2 = 2uv$ and $a^2 + 3ad + d^2 = u^2 + v^2$. Since $\gcd(u, v) = 1$ and the product $(u/2)v$ is a square, there exist (using fact (2)) relatively prime positive integers s and t such that $u = 2s^2$ and $v = t^2$. It then follows that

$$\Big(a + \frac{3d}{2}\Big)^2 = a^2 + 3ad + d^2 + \frac{5}{4}\,d^2 = 4s^4 + t^4 + 5s^2t^2 = (s^2 + t^2)(4s^2 + t^2).$$

Since $\gcd(s^2 + t^2, 4s^2 + t^2) = 1$ (see fact (1)), each of these numbers is a square (by fact (2)), a contradiction to Theorem 2.1.

Now suppose that d is odd. By fact (6), there exist relatively prime positive integers u and v such that $v > u$, $u + v$ is odd, $d^2 = v^2 - u^2$ and $a^2 + 3ad + d^2 = v^2 + u^2$. Note that u is even (the parity follows from a simple modulo 4 argument on the equation for d^2). We then have

$$(2a + 3d)^2 = 4(a^2 + 3ad + d^2) + 5d^2 = (4v^2 + 4u^2) + (5v^2 - 5u^2) = 9v^2 - u^2,$$

which implies that $(u, 2a + 3d, 3v)$ is a Pythagorean triple. By fact (1), it is necessary that 3 divides u and $2a + 3d$. It follows that

$$(v - u)\Big(v - \frac{u}{3}\Big)\Big(v + \frac{u}{3}\Big)(v + u) = (v^2 - u^2)\Big(\frac{9v^2 - u^2}{9}\Big) = \Big(\frac{d(2a + 3d)}{3}\Big)^2,$$

giving us four distinct positive integers that form an arithmetic progression whose product is a square. Since the common difference is an even number $2u/3$, we have a contradiction to the first part of the proof. □

Corollary 2.4. *There are no four distinct squares that form an arithmetic progression.*

Proof. This result is a simple consequence of the theorem. For the record, if we have four relatively prime squares that form an arithmetic progression, then all of the squares are odd (use a simple modulo 4 argument to verify this) and only the first half of the proof of Theorem 2.3 is needed. □

Corollary 2.5. *Suppose that a and b are positive integers. If $a^2 + b^2$ is a square, then $a^2 + 4ab + b^2$ is not a square.*

Proof. Suppose that a and b are positive integers for which both $a^2 + b^2$ and $a^2 + 4ab + b^2$ are squares. Then the numbers $(b - a)^2$, $a^2 + b^2$, $(b + a)^2$, and $a^2 + 4ab + b^2$ are four squares in arithmetic progression with common difference $2ab$. □

3. Discussion

Suppose that (a, b, c) is a Pythagorean triple with $b > a$. Then $(b - a)^2$, $c^2, (b + a)^2$ are three squares in arithmetic progression (with common difference $2ab$). For example, the triple $(8, 15, 17)$ yields the squares 7^2, 17^2, 23^2 with common difference 240. It is thus easy to find three squares in arithmetic progression. In fact, if $a^2 < b^2 < c^2$ are three relatively prime squares in arithmetic progression, then all three squares are odd (use a modulo 4 argument on $a^2 + c^2 = 2b^2$ to obtain a contradiction if b is even) and the equation $a^2 + c^2 = 2b^2$ becomes

$$\left(\frac{c-a}{2}\right)^2 + \left(\frac{c+a}{2}\right)^2 = b^2, \qquad \text{which shows that} \qquad \left(\frac{c-a}{2}, \frac{c+a}{2}, b\right)$$

is a primitive Pythagorean triple. By fact (6), there exist relatively prime positive integers u and v such that $v > u$, $u + v$ is odd, and either

$$\frac{c-a}{2} = v^2 - u^2, \quad \frac{c+a}{2} = 2uv, \quad b = v^2 + u^2$$

or

$$\frac{c+a}{2} = v^2 - u^2, \quad \frac{c-a}{2} = 2uv, \quad b = v^2 + u^2.$$

It follows that $a = |v^2 - u^2 - 2uv|$, $b = v^2 + u^2$, and $c = v^2 - u^2 + 2uv$. We can use this fact to show that one proposed proof of Corollary 2.4 that appears in the literature is not valid.

Suppose that a^2, b^2, c^2, d^2 are four squares in arithmetic progression, where the integers a, b, c, and d satisfy $0 < a < b < c < d$. As outlined in Dickson ([3, p. 440]) and appearing in various forms (see [8]), it is then claimed (see fact (4)) that there exist pairwise relatively prime positive integers α, β, γ, and δ such that

$$b - a = 2\alpha\beta,\ b + a = 2\gamma\delta, \quad c - b = 2\alpha\gamma,\ c + b = 2\beta\delta, \quad d - c = 2\alpha\delta,\ d + c = 2\beta\gamma,$$

where α and δ are defined by $\alpha = \gcd(b-a, c-b)/2$ and $\delta = \gcd(b+a, c+b)/2$. The proof then uses the numbers α, β, γ, and δ to obtain a contradiction in several elementary steps. Since all of the other proofs of Corollary 2.4 rely on a result that depends on infinite descent and usually use fact (6) at some point, this short proof is already a bit suspicious. Some authors have raised concerns about this proof (see [2] and [12]) but stop short of explicitly verifying the error. We will do so here. Before proceeding, note that the inequality $a+b < b+c < c+d$ implies that the inequality $\delta < \gamma < \beta$ must be satisfied.

We begin by factoring the quantities $b^2 - a^2$ and $c^2 - b^2$ using the known values of a, b, and c in terms of the parameters u and v listed in the opening paragraph of this section. Suppose

first that $v^2 - u^2 - 2uv > 0$. Then

$$\begin{aligned} b - a &= (v^2 + u^2) - (v^2 - u^2 - 2uv) = 2u(v + u); \\ b + a &= (v^2 + u^2) + (v^2 - u^2 - 2uv) = 2v(v - u); \\ c - b &= (v^2 - u^2 + 2uv) - (v^2 + u^2) = 2u(v - u); \\ c + b &= (v^2 - u^2 + 2uv) + (v^2 + u^2) = 2v(v + u). \end{aligned}$$

It follows that $\alpha = u$, $\beta = v + u$, $\gamma = v - u$, and $\delta = v$, which contradicts the fact that the inequality $\delta < \gamma$ is required. On the other hand, if $v^2 - u^2 - 2uv < 0$, then

$$\begin{aligned} b - a &= 2v(v - u); \\ b + a &= 2u(v + u); \\ c - b &= 2u(v - u); \\ c + b &= 2v(v + u); \end{aligned}$$

giving $\alpha = v - u$, $\beta = v$, $\gamma = u$, and $\delta = v + u$, which also contradicts the fact that $\delta < \gamma$ is required.

The contradiction reached here does not show that there are no four squares in arithmetic progression. It merely shows that the equations $d - c = 2\alpha\delta$ and $d + c = 2\beta\gamma$ do not give the correct factorization. However, there may be other ways to factor $d^2 - c^2$. To give a concrete example, suppose that $u = 3$ and $v = 10$. Using the above formulas, we find that $a = 31$, $b = 109$, and $c = 151$. Since $b^2 - a^2 = 10920 = c^2 - b^2$, we are seeking factorizations xy of 10920 with $0 < x < y$ and both x and y are even and either $x/2$ or $y/2$ is odd. (This last fact is a consequence of the fact that $(b - a)/2$ and $(b + a)/2$ have opposite parity.) Simple factoring reveals that each of the products

$$\begin{aligned} &2 \cdot 5460, \quad 4 \cdot 2730, \quad 6 \cdot 1820, \quad 10 \cdot 1092, \quad 12 \cdot 910, \quad 14 \cdot 780, \quad 20 \cdot 546, \quad 26 \cdot 420, \\ &28 \cdot 390, \quad 30 \cdot 364, \quad 42 \cdot 260, \quad 52 \cdot 210, \quad 60 \cdot 182, \quad 70 \cdot 156, \quad 78 \cdot 140, \quad 84 \cdot 130 \end{aligned}$$

has the desired properties. For our choice of integers a, b, and c, we need the factorizations $b^2 - a^2 = 78 \cdot 140$ and $c^2 - b^2 = 42 \cdot 260$. Since $d + c > c + b$, the larger of the factors must be greater than 260, giving us ten possible choices from the above list. The proof outlined in Dickson claims that exactly one of the many possible products gives $d - c$ and $d + c$. As we have seen, this particular choice leads to a contradiction, but it does not contradict the existence of four squares in arithmetic progression. It merely shows that this factorization is not an option. Hence, this approach to proving Corollary 2.4 is not valid.

A literature search for a proof of Corollary 2.4 reveals that there is no standard approach to this problem. The comments in the article [12], as well as various discussion groups found online (see [4, 9, 13, 14]), show that other mathematicians have also noticed this fact. Some authors prove Corollary 2.4 directly (see, for instance, [10, 12, 16]) while others begin with the statement of Theorem 2.3. In this case, the first step is often to use proof by cases to show that each of the four numbers (assuming that they are relatively prime) must be a square; the references [1], [6], and [17] take this approach. Some of the cases are easily dismissed and the more challenging cases can be reduced to Corollary 2.2. At this point, the references [1], [6], and [10] use the Pythagorean triple parameterization to again reduce the problem to Corollary 2.2. The reference [12] uses a direct argument by descent (on the size of the difference between squares), while [16] goes about proving that the quantity $(v^2 + u^2)^2 + 8uv(v^2 - u^2)$ cannot be a square. This may seem like an odd approach, but note that this quantity is merely the number $a^2 + b^2 + 4ab$ that appears in Corollary 2.5 after using fact (6). The details behind

this proof involve a variety of parameterizations, making the argument somewhat difficult to follow. It is interesting to note how often Pythagorean triples of the form considered in Theorem 2.1 appear in these proofs. In many cases (see [17]), using the Pythagorean triple result rather than the quartic equation would make the proofs shorter and easier to follow.

References

[1] R. Beauregard, *No arithmetic cyclic quadrilaterals*, College Mathematics Journal, **37** (2006), 110–113.
[2] K. Brown, *No four squares in arithmetic progression*, `http://archive.today/iOAd`.
[3] L. Dickson, *History of the Theory of Numbers*, Vol. 2, Chelsea, 1934.
[4] Dr. Math, `http://mathforum.org/library/drmath/view/69137.html`.
[5] T. Erdélyi, *On the equation* $a(a+d)(a+2d)(a+3d) = x^2$, Amer. Math. Monthly, **107** (2000), 166–169.
[6] K. Fogarty and C. O'Sullivan, *Arithmetic progressions with three parts in prescribed ratio and a challenge of Fermat*, Math. Mag., **77** (2004), 283–292.
[7] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 3rd ed. Oxford, England, Clarendon Press, 1954.
[8] M. Khan and H. Kwong, *Arithmetic progressions with square entries*, The Fibonacci Quarterly, **43.2** (2005), 98–103.
[9] G. McRae, `http://2000clicks.com/mathhelp/PuzzleSequenceOfSquares4.aspx`.
[10] L. Mordell, *Diophantine Equations*, Pure and Applied Mathematics, Vol. 30, Academic Press, London, 1969.
[11] I. Niven and H. Zuckerman, *An Introduction to the Theory of Numbers*, 3rd ed., Wiley, New York, 1972.
[12] A. J. van der Poorten, *Fermat's four squares theorem*, `http://arxiv.org/pdf/0712.3850.pdf`, 2007.
[13] R. Sabey, `http://www.rsabey.pwp.blueyonder.co.uk/maths/4squaresinAP1.html`.
[14] `http://math.stackexchange.com/questions/43519/squares-in-arithmetic-progression`.
[15] W. Sierpiński, *Elementary Theory of Numbers*, Państwowe Wydawnictwo Naukowe, Warsaw, 1964.
[16] M. Vasilev, *Arithmetical progressions containing only squares of natural numbers*, Bull. Number Theory Related Topics, **10** (1986), 33–39.
[17] P. Yiu, *Number Theory 2*, `http://math.fau.edu/yiu/NT2007notes.pdf`, 2007.

MSC2010: 11B25, 11D25, 11A99

Department of Mathematics, Whitman College, 345 Boyer Avenue, Walla Walla, WA 99362
E-mail address: `gordon@whitman.edu`

Department of Mathematics, Whitman College, 345 Boyer Avenue, Walla Walla, WA 99362
E-mail address: `saragraham919@gmail.com`