7.B. Perfect squares in an arithmetic progression

Although Fibonacci is best known for his writings on base 10 numeration system and his discussion of the sequence which is now named after him (but were previously known to others), in many respects his most substantial contributions to mathematics are contained in his*Liber quadratorum*. This book represented the most significant advance in number theory by a Western mathematician since the work of Diophantus about 1000 years earlier, and it would be another 300 years before any comparable breakthroughs took place. Well-written modern derivations for most of the book's results appear in the following article:

> **R. B. McClendon.** *Leonardo of Pisa and His* Liber quadratorum. American Mathematical Monthly **26** (1919), 1–8.

However, Fibonacci's deepest and most difficult result — namely, a description of three term arithmetic progressions consisting of perfect squares $a^2 < b^2 < c^2$ — is only discussed briefly in this paper (there is a partial discussion on pages 280–281 of Burton, and also implicitly in Exercise 5 on page 285). In fact, finding a proof in standard books is elusive, partly because the proof is fairly long and complex, and it requires ideas that one might not initially anticipate. Since a proof of Fibonacci's result is not all that easy to find in standard references and some of the statements are somewhat imprecise, we shall state and prove a strong version of his result here. The discussion will be based upon material from the following annotated translation of Fibonacci's book:

> **Leonardo Pisano (Fibonacci).** *The Book of Squares* (An [Extensively] Annotated Translation into Modern English by L. E. Sigler). Academic Press, Boston, 1987.

There is also a brief historical discussion of the problem with further references on page 74 of this book.

Statement of the main result

If we are given an arithmetic progression of the form $\{(ka)^2, (kb)^2, (kc)^2\}$ in which k, a, b, c are positive integers and $k > 1$, then the reduced integer sequence $\{a^2, b^2, c^2\}$ is also an arithmetic progression; conversely, if the second sequence is an arithmetic progression then so is the first. Because of this, unless specifically stated otherwise we shall only consider arithmetic progressions $\{a^2, b^2, c^2\}$ such that the positive integers a, b, c have no common positive factors except 1. In this setting, we have the following strengthened form of Fibonacci's result on squares in arithmetic progressions:

THEOREM. (*i*) *Let $\{a^2, b^2, c^2\}$ be an arithmetic progression of positive integers such that the terms have no nontrivial common factors. Then there are relatively prime positive integers $n > m$ such that*

$$a \quad = \quad \frac{m^2 + 2mn - n^2}{2} \; , \quad b \quad = \quad \frac{m^2 + n^2}{2} \; , \quad c \quad = \quad \frac{n^2 + 2mn - m^2}{2}$$

if mn is odd and

$$a \quad = \quad m^2 + 2mn - n^2 \; , \quad b \quad = \quad m^2 + n^2 \; , \quad c \quad = \quad n^2 + 2mn - m^2$$

if mn is even.

(*ii*) *Conversely, if m and n are relatively prime with $n > m$ and $m^2 + 2mn - n^2 > 0$, then the formulas in* (*i*) *define an arithmetic progression whose terms have no nontrivial common factors.*

It follows that the common difference between the terms in the arithmetic progression is equal to $nm(n^2 - m^2)$ if mn is odd and $4mn(n^2 - m^2)$ if mn is even. This has an immediate consequence:

COROLLARY. *If $\{a^2, b^2, c^2\}$ is an arithmetic progression of positive integers, then the common difference between adjacent terms is divisible by* 24.

The arithmetic progression $\{1, 25, 49\} = \{1^2, 5^2, 7^2\}$ shows that this is the strongest possible divisibility property for such common differences.

Proof of the Corollary. (Compare the argument in `history07.pdf`). Suppose first that mn is odd. Then m and n are both odd and since $m^2, n^2 \equiv 1 \bmod 8$ it follows that 8 divides $n^2 - m^2$. Similarly, we know that $m^2 - n^2 \equiv 1 \bmod 3$ and hence we know that 24 divides $n^2 - m^2$.

Now suppose that mn is even. Then mn is even and therefore $4mn(n^2 - m^2)$ is divisible by 8. Also, as before we know that $m^2 - n^2$ is divisible by 3, and therefore the entire common difference is again divisible by 24.

Fibonacci's approach

The basic idea is to view the difference of two squares $u^2 - v^2$ as the sum of the $u - v$ consecutive odd numbers running from $2v + 1$ to $2u - 1$. Given an arithmetic progression of the usual form $\{a^2, b^2, c^2\}$, define the *Fibonacci ratio* of the 3-term progression to be the ratio

$$\frac{b - a}{c - b}$$

which is the ratio of the number of odd integers from $2b + 1$ to $2c - 1$ to the number of even integers from $2a + 1$ to $2b - 1$. Since we have

$$\sum_{i=b+1}^{c} 2i - 1 \quad = \quad c^2 \; - \; b^2 \quad = \quad b^2 \; - \; a^2 \quad = \quad \sum_{i=a+1}^{b} 2i - 1$$

and each term in the first summation is greater than each term in the second summation, it follows that the the second summation must have more terms, so that $b - a > c - b$ and hence the Fibonacci ratio is strictly greater than 1.

The following upper bound on the Fibonacci ratio will be very useful:

UPPER BOUND LEMMA. *Suppose we are given positive integers $a < b < c$ such that $\{a^2, b^2, c^2\}$ is an arithmetic progression with Fibonacci ratio r. Then $r < 1 + \sqrt{2}$.*

Proof. Let $q = c - b$ denote the ratio of the number of odd integers from $2b + 1$ to $2c - 1$, and let $p = b - a$ denote the number of even integers from $2a + 1$ to $2b - 1$, so that the Fibonacci ratio r is equal to p/q and $p = qr$. Since $\{a^2, b^2, c^2\}$ is an arithmetic progression we have

$$b^2 \; - \; (b - pr)^2 \quad = \quad b^2 \; - \; a^2 \quad = \quad c^2 \; - \; b^2 \quad = \quad (b + q)^2 \; - \; b^q$$

and if we solve these equations for b we obtain the formula

$$b \quad = \quad \frac{r^2 + 1}{2(r - 1)} \cdot q \; .$$

If we combine this with the equations $a = b - qr$ and $c = b + q$, we also obtain the following formulas:

$$c \quad = \quad \frac{r^2 + 2r - 1}{2(r-1)} \cdot q \ , \quad a \quad = \quad \frac{1 + 2r - r^2}{2(r-1)} \cdot q$$

Since a is positive and $r > 1$, it follows that the numerator $1+2r-r^2$ must be positive; this condition holds if and only if r lies between the two roots of the quadratic polynomial $t^2 - 2t - 1 = 0$. Now the roots of this polynomial are given by $1 \pm \sqrt{2}$, and therefore $1 + 2r - r^2 > 0$ implies that $r < 1 + \sqrt{2}$.

We can now state a modified version of Fibonacci's main result:

THEOREM. *Suppose that n and m are relatively prime positive integers such that $n > m$ but $n < (1+\sqrt{2})m$. Then there is an arithmetic progression $\{a^2, b^2, c^2\}$ such that a, b, c have no nontrivial common factors, the Fibonacci ratio is equal to r, and the terms are given explicitly by*

$$a \quad = \quad \frac{m^2 + 2mn - n^2}{2} \ , \quad b \quad = \quad \frac{m^2 + n^2}{2} \ , \quad c \quad = \quad \frac{n^2 + 2mn - m^2}{2}$$

if mn is odd and

$$a \quad = \quad m^2 + 2mn - n^2 \ , \quad b \quad = \quad m^2 + n^2 \ , \quad c \quad = \quad n^2 + 2mn - m^2$$

if mn is even.

Sketch of proof. The motivation for the displayed formulas is explained in some detail on pages 65–69 of *The Book of Squares*; observe that the condition $n < (1+\sqrt{2})m$ implies that $m^2 + 2mn - n^2$ is positive (if $n = rm$, then $r > 1$ and the given expression reduces to $m^2(1+2r-r^2)$, which is positive since r is less than $1 + \sqrt{2}$).

It is an elementary but messy exercise to verify that $b^2 - a^2$ and $c^2 - b^2$ are both given by $nm(n^2 - m^2)$ if mn is odd and by $4mn(n^2 - m^2)$ if mn is even (in fact, the main steps are given in the reference). Furthermore, if mn is odd then it follows that there are

$$b \ - \ a \quad = \quad \frac{m^2 + n^2}{2} \ - \ \frac{m^2 + 2mn - n^2}{2} \quad = \quad n(n-m)$$

odd numbers starting with $2a+1$ and running through $2b-1$, and there are

$$c \ - \ b \quad = \quad \frac{n^2 + 2mn - m^2}{2} \ - \ \frac{m^2 + n^2}{2} \quad = \quad m(n-m)$$

odd numbers starting with $2a+1$ and running through $2b-1$; similarly, if mn is even then it follows that there are $2n(n-m)$ odd numbers starting with $2a+1$ and running through $2b-1$, and there are $2m(n-m)$ odd numbers starting with $2a+1$ and running through $2b-1$. In either case the Fibonacci ratio of the sequence is equal to n/m.

The only remaining thing to check is that a, b, c have no nontrivial common factors; we shall prove this using the fact that n and m have no such factors. In any case, let $d > 0$ be the (positive) greatest common divisor of a, b and c; then every integral linear combination of these numbers is also divisible by d.

Suppose first that mn is odd. Then $c - a = n^2 - m^2$ and therefore we also have

$$2n^2 \quad = \quad 2b \ + \ c \ - \ a \ , \quad 2m^2 \quad = \quad 2b \ + \ a \ - \ c \ .$$

It follows immediately that the greatest common divisor d must also divide $2m^2$ and $2n^2$. On the other hand, we also know that d divides $b = \frac{1}{2}(m^2 + n^2)$, and this number is odd because m and n are both odd (recall that the square of an odd integer leaves a remainder of 1 when divided by 4). Therefore d must also be odd, and it follows that d must divide both m^2 and n^2. Since m and n are relatively prime, it follows that $d = 1$.

Suppose now that mn is even. Then $c - a = 2(n^2 - m^2)$ and therefore we also have

$$4n^2 \ = \ 2b \ + \ c \ - \ a \ , \quad 4m^2 \ = \ 2b \ + \ a \ - \ c \ .$$

As before, it follows that the greatest common divisor d must also divide $4m^2$ and $4n^2$. On the other hand, we also know that d divides $b = n^2 + m^2$, and this number is odd because one of m, n is even and the other is odd. Therefore d must also be odd, and it follows that d must divide the odd number in the pair $\{m^2, n^2\}$. Since d also divides $n^2 + m^2$, it follows that d must divide both m^2 and n^2. Since m and n are relatively prime, it follows that $d = 1$.

Uniqueness

To conclude the proof of the main theorem, we need to show that if $\{x^2, y^2, z^2\}$ is an arbitrary arithmetic progression whose terms have no nontrivial common factors, then it is given by the Fibonacci construction described above.

THEOREM. *If $\{a^2, b^2, c^2\}$ and $\{x^2, y^2, z^2\}$ are arithmetic progressions of positive integers whose terms have no nontrivial common factors, and if the Fibonacci ratios of these three term sequences are equal to the same number $r > 1$, then $(a, b, c) = (x, y, z)$.*

The Main Theorem follows from this result and Fibonacci's construction. By the Upper Bound Lemma and the conditions in the theorem, we know that the Fibonacci ratio satisfies $r < 1 + \sqrt{2}$.

Proof. Let q be the number of odd integers between $2b + 1$ and $2c - 1$, and let Q be the number of odd integers between $2y + 1$ and $2z - 1$.

Then the numbers of odd integers between $2a + 1$ and $2b - 1$ is equal to rq, and the number of odd integers between $2x + 1$ and $2y - 1$ is equal to rQ. Then as in the Upper Bound Lemma it follows that

$$c \ = \ b \ + \ q \ , \quad a \ = \ b \ - \ rq \ , \quad z \ = \ y \ + \ Q \ , \quad x \ = \ y \ - \ rQ$$

so that the arithmetic progression identities $c^2 - b^2 = b^2 - a^2$ and $z^2 - y^2 = y^2 - x^2$ yield the following equations:

$$y \ = \ \frac{(r^2 + 1)Q}{2(r - 1)} \ , \quad b \ = \ \frac{(r^2 + 1)q}{2(r - 1)}$$

As in the proof of the Upper Bound Lemma, these in turn yield the following additional equations:

$$z \ = \ \frac{(r^2 + 2r - 1)Q}{2(r - 1)} \ , \quad c \ = \ \frac{(r^2 + 2r - 1)q}{2(r - 1)} \ , \quad x \ = \ \frac{(1 + 2r - r^2)Q}{2(r - 1)} \ , \quad a \ = \ \frac{(1 + 2r - r^2)q}{2(r - 1)}$$

Combining these equations, we obtain the following proportionality relations:

$$\frac{Q}{q} \ = \ \frac{x}{a} \ = \ \frac{y}{b} \ = \ \frac{z}{c}$$

Express this common ratio in the form s/t where s and t are positive with no nontrivial common factors. Then we have

$$sa \quad = \quad xt\ , \quad sb \quad = \quad yt\ , \quad sc \quad = \quad zt\ .$$

If p is a prime dividing s, then p does not divide one of x, y, z because these numbers have no nontrivial common factors, and therefore it follows that p must divide t. Since we assumed that s and t had no common factors, this leads to a contradiction unless $s = 1$. But now if $t > 1$, then the equations imply that a, b, c have a nontrivial common factor, which is also false by hypothesis. Therefore the only possibility is that $t = 1$ also holds, so that $s = t$ and hence

$$\frac{Q}{q} \quad = \quad \frac{s}{t} \quad = \quad 1$$

which immediately implies $(a, b, c) = (x, y, z)$.

An alternate approach

There is a close relationship between arithmetic progressions of perfect squares are Pythagorean triples that leads to a slightly different (but certainly equivalent) statement of the main results. Our exposition will be independent of the preceding discussion, and we start with the following:

LEMMA. *Let $\{a^2, b^2, c^2\}$ be an arithmetic progression of positive integers with $a < b < c$. Then $c - a$ and $c + a$ are both even.*

Proof. The condition $c^2 - b^2 = b^2 - a^2$ is equivalent to $2b^2 = c^2 - a^2 = (c - a) \cdot (c + a)$. It follows that 2 divides either $c - a$ or $c + a$. Since

$$c \ + \ a \quad = \quad (c \ - \ a) \ + \ 2\,a$$

it follows that if one of $\{c - a, c + a\}$ is even then so is the other.

The following identities describe the relation between arithmetic progressions of perfect squares and Pythagorean triples.

THEOREM. *There is a 1–1 correspondence between triples of positive integers $a < b < c$ such that $c^2 - b^2 = b^2 - a^2$ and Pythagorean triples $x < y < z$ such that $x^2 + y^2 = z^2$. It is given by $z = b$, $y = \frac{1}{2}(c + a)$, and $x = \frac{1}{2}(c - a)$.*

Before proceeding, we note that x and y are integers by the previous lemma.

COROLLARY. *In the notation of the theorem, the common difference $c^2 - b^2 = b^2 - a^2$ is equal to $2xy$.*

Sketch of proof of Corollary. It follows from the formulas that $c = x + y$ and $a = y - x$, therefore we have $2(b^2 - a^2) \quad = \quad c^2 - a^2 \quad = \quad 4xy$ which yields the formula in the statement of the corollary.

Verification of the theorem is a straightforward and elementary exercise in algebra.

As in Burton, we say that a triple of positive integers is *primitive* if the integers have no common (integral) factors other than ± 1. We then have the following refinement of the main theorem.

THEOREM. *In the setting of the previous theorem, if $\{a, b, c\}$ corresponds to $\{x, y, z\}$, then $\{a, b, c\}$ is primitive if and only if $\{x, y, z\}$ is primitive.*

Proof. First of all, we claim that $c^2 - b^2$ and $b^2 - a^2$ are both even by a refinement of the first lemma. In that lemma we saw that $c^2 - a^2$ is the product of the even numbers $(c + a)$ and $(c - a)$, and therefore $2b^2 = c^2 - a^2$ must be divisible by 4. But this means that

$$c^2 - b^2 \quad = \quad b^2 - a^2 \quad = \quad \tfrac{1}{2}\,(c^2 - a^2)$$

must be even.

Next, we claim that if $\{a, b, c\}$ is primitive, then a, b and c are all odd. For if one were even, then its square is also even, and by the preceding paragraph it follows that all three squares must be even, and hence all three of the original integers must also be even. Since this contradicts the primitivity condition, all three integers must be odd.

Suppose now that $\{a, b, c\}$ is primitive, and let $d > 0$ be a common divisor of x, y, z. Then d divides $z = b$, $x + y = c$ and $y - x = a$. But this means that d must be equal to 1.

Suppose now that $\{x, y, z\}$ is primitive, and let $e > 0$ be a common divisor of a, b, c. Then e must be odd since a, b, c are all odd. By construction, we know that e must also divide $z = b$, $2y = a + c$, and $2x = c - a$. Since e is odd, it follows that e divides both y and x, and by the primitivity of $\{x, y, z\}$ it follows that $e = 1$.

COROLLARY. *In the setting of the theorem, the common difference $c^2 - b^2 = b^2 - a^2$ is equal to $2xy$.*

Proof of the Corollary. By construction we have $xy = \frac{1}{4}\,(c^2 - a^2)$, and we know that the right hand side is just $\frac{1}{2}$ times the common difference $c^2 - b^2 = b^2 - a^2$. Therefore the common difference is just $2xy$. If we express this in terms of s and t, we find that the common difference equals $4st(s^2 - t^2)$.

In fact, it follows that a number d is a common difference for a triple of perfect squares in arithmetic progression if and only if it can be written as $4k^2 st(s^2 - t^2)$ where k is a positive integer and s, t are relatively prime positive integers such that $s > t$ and st is even.

NOW RECALL that the theorem on pages 295–296 of Burton states that all primitive Pythagorean triples $\{x, y, z\}$ are given by pairs of relatively prime integers $s > t > 0$ such that st is even such that

$$\{x,\, y\} \quad = \quad \{2st,\, s^2 - t^2\}\ , \quad z \quad = \quad s^2 + t^2\ .$$

Our notation differs from Burton's because he assumes that x is even while we assume that $x < y$.

Using these, we can express a, b, c and the common difference in terms of s and t. Specifically, the common difference is $2xy = 4st(s^2 - t^2)$, and (as in the preceding discussion) we see that

$$a \quad = \quad |t^2 + 2st - s^2|\ , \quad b \quad = \quad t^2 + s^2\ , \quad c \quad = \quad s^2 + 2st - t^2\ .$$

Note that there is no upper bound on the ratio s/t (in contrast to the preceding discussion). Note also that $t^2 + 2st - s^2$ is positive if this ratio is less than $1 + \sqrt{2}$ and negative if this ratio is greater than $1 + \sqrt{2}$.

Uniqueness questions

We shall verify that different primitive pairs (s, t) as above will determine different primitive Pythagorean triples $\{x, y, z\}$ and different primitive arithemtic progressions $\{a, b, c\}$. By the first theorem it suffices to prove this for Pythagorean triples.

Suppose that (s, t) and (p, q) are ordered pairs of relatively prime positive integers such that $s > t$, $p > q$ and one integer in each pair is even (equivalently, both st and pq are even), and suppose that both determine the same primitive Pythagorean triple $\{x, y, z\}$. Then by the theorem on pages 295–296 of Burton we have $z = s^2 + t^2 = p^2 + q^2$ and

$$\{x,\, y\} \quad = \quad \{2st,\, s^2 - t^2\} \quad = \quad \{2pq,\, p^2 - q^2\} \;;$$

as noted earlier, our notation differs from Burton's because he assumes that x is even while we assume that $x < y$, and there are some examples for which $2st < s^2 - t^2$ and others for which $2st > s^2 - t^2$ (see the chart on page 296 of Burton).

We claim that $2st = 2pq$ and $s^2 - t^2 = p^2 - q^2$. To see this, note first that both $s^2 - t^2$ and $p^2 - q^2$ are odd because up to sign they are differences of an even integer and an odd integer (since on of $\{s, t\}$ is even and the other is odd, the same is true for their squares, and likewise for $\{p, q\}$). Since both $2st$ and $2pq$ are even, the condition $\{2st,\, s^2 - t^2\} = \{2pq,\, p^2 - q^2\}$ and the preceding observation imply that $2st = 2pq$ and $s^2 - t^2 = p^2 - q^2$.

The conditions $s^2 + t^2 = p^2 + q^2$ and $s^2 - t^2 = p^2 - q^2$ imply that $(s^2, t^2) = (p^2, q^2)$. Since all integers in sight are positive it follows that $(s, t) = (p, q)$.

Comparisons of the conclusions from the two approaches. The two approaches yield slightly different descriptions of the primitive triples of positive integers $a < b < c$ whose squares form an arithmetic progression. In the modified Fibonacci approach these are described in terms of ordered pairs of relatively prime positive integers (n, m) such that $m < n < m(1 + \sqrt{2})$, while in the approach using Pythagorean triples the same objects are described in terms of ordered pairs of positive integers (s, t) such that $s > t$ and st is even. It is possible to describe this relationship in greater detail, but we shall not do so.