1132. *Proposed by Leo Schneider, John Carroll University, Cleveland, OH*

The two parallel sides of a trapezoid are of length a and b. A segment of length m parallel to these two sides divides the trapzoid into two trapzoids, each of area equal to one half of the original trapzoid. Prove that if a, b, and m are relatively prime positive integers, then neither 2 nor 3 is a prime factor of any of these integers.

Solution by **Rex H. Wu**, *Brooklyn, NY.*

Let h be the height of the trapezoid with parallel sides a and b, h_1 be the height of the trapezoid with parallel sides a and m. Then the height for the trapezoid with parallel sides m and b is $h_2 = h - h_1$. Equating the areas, we have

$$\frac{1}{2}(a+m)h_1 = \frac{1}{2}(m+b)(h-h_1) = \frac{1}{4}(a+b)h$$

From the above, the first and the last parts give

$$h_1 = \frac{a+b}{2(a+m)}h$$

and the first two parts give

$$h_1 = \frac{m+b}{a+b+2m}h$$

Equating h_1 and simplify gives

$$a^2 + b^2 = 2m^2$$

The original problem is now reduced to showing the primitive solutions, i.e. $\gcd(a, b, m) = 1$, of the diophantine equation $a^2 + b^2 = 2m^2$ cannot be divisible by 2 or 3.

Let's show the primitive solutions are not divisible by 2. Suppose $a = 2\alpha$, for some integer α. Since $a^2+b^2 = 2m^2$, or a^2+b^2 is even, it follows that b^2 must be even. Therefore, $b = 2\beta$, for some integer β. Then $a^2 + b^2 = 4(\alpha^2 + \beta^2) = 2m^2$ which implies $m^2 = 2(\alpha^2 + \beta^2)$. So $m = 2\mu$ for some integer μ. But then 2 is a common factor of a, b and m, contradicting the assumption that $\gcd(a, b, m) = 1$. Similar argument can be applied to see b cannot be even.

Suppose $m = 2\mu$ for some integer μ. Then $a^2 + b^2 = 2(2\mu)^2 = 8\mu^2$. This implies 4 divides $a^2 + b^2$. Observe that a and b cannot be one odd and one even since the sum $a^2 + b^2$ would be odd. Therefore, a and b must be both odd or both even. Suppose a and b are both odd, $a = 2i + 1$ and $b = 2j + 1$ for some integers i and j. We have $a^2 + b^2 = 4i^2 + 4i + 4j^2 + 4j + 2$, not divisible by 4. Therefore, a and b must be both even. But then we have the contradiction again, that a, b and m have a common factor 2.

To show 3 cannot be a factor of a, b and m is more involved. I need to characterize the primitive solutions (a, b, m) of the equation $a^2+b^2 = 2m^2$. The equation $a^2+b^2 = 2m^2$ is closely related to the well-known equation $x^2+y^2 = z^2$.

Lemma 1 *$n = x^2 + y^2$ has a solution if and only if n does not contain any prime $p \equiv 3 \pmod 4$ and the exponent of p is odd.*

This is a well know fact. A proof can be found in many elementary number theory books.

Lemma 2 *If p is a prime and $p \equiv 3 \pmod 4$, then $p^2 = x^2+y^2$ has no primitive solutions in positive integers.*

PROOF: All the primitive solutions to $p^2 = x^2 + y^2$ can be generated by $p = r^2 + s^2$, $x = r^2 - s^2$ and $y = 2rs$, with $r \not\equiv s \pmod 2$ and $\gcd(r, s) = 1$. From Lemma 1, we know there is no integer solution to $p = r^2 + s^2$. ■

Lemma 3 *If p is a prime and $p \equiv 3 \pmod 4$, $Q = q_1 q_2 \cdots q_j$ where q_i is prime and $q_i \not\equiv 3 \pmod 4$, then the solution to $n = x^2 + y^2$, where $n = p^{2k}Q$, is not primitive.*

PROOF: p^{2k} can be viewed as $(p^k)^2$. If k is odd, by lemma 1, p^k cannot be expressed as the sum of two squares and therefore, $(p^k)^2$ cannot be the sum of two squares. If k is even, then the only way to express p^{2k} as the sum of two squares is $p^{2k} = 0^2 + (p^k)^2$. Suppose $Q = r^2 + s^2$, then $p^{2k}Q = p^{2k}(r^2 + s^2) = p^{2k}r^2 + p^{2k}s^2$, i.e. $\gcd(n, x, y) = \gcd(p^{2k}Q, p^{2k}r^2, p^{2k}s^2) = p^{2k}$. ■

Lemma 4 *The product of the sum of two squares is again a sum of two squares.*

PROOF:

$$(r^2 + s^2)(t^2 + u^2) = (rt + su)^2 + (ru - st)^2 = (rt - su)^2 + (ru + st)^2.$$

■

Theorem 1 *All the primitive solutions of the diophantine equation $a^2 + b^2 = 2m^2$ are generated by $(a, b, m) = (|p^2 - q^2 - 2qp|, |p^2 - q^2 + 2qp|, p^2 + q^2)$, where $\gcd(p, q) = 1$ and $p \not\equiv q \pmod 2$.*

PROOF: It is easy to verify that $(a, b, m) = (|p^2-q^2-2qp|, |p^2-q^2+2qp|, p^2+q^2)$ is a solution to $a^2 + b^2 = 2m^2$.

Suppose there is a primitive solution to $a^2 + b^2 = 2m^2$. By Lemma 1, we know $2m^2$ cannot contain a prime p such that $p \equiv 3 \pmod 4$ and the exponent of p is odd.

From Lemma 3, we know m cannot contain a prime p such that $p \equiv 3 \pmod 4$ and the exponent of p is even.

That means $2m^2$ can only contain primes p such that $p \not\equiv 3 \pmod 4$.

Since 2 is the only even prime, $m \equiv 1 \pmod 4$.

From Lemma 1, $m^2 = x^2+y^2$, for some integers x and y. This representation of m is unique if m is prime. However, from Lemma 4, if m is composite, there is at least one representation.

The primitive solutions of $m^2 = x^2+y^2$ are the Pythagorean triples, $(x, y, m) = (p^2 - q^2, 2pq, p^2 + q^2)$, where $\gcd(p, q) = 1$ and $p \not\equiv q \pmod 2$.

Going back to the original equation, $a^2 + b^2 = 2m^2 = 2(x^2 + y^2) = (1 + 1)(x^2 + y^2) = (x - y)^2 + (x + y)^2$. Thus, we have $2m^2 = 2(p^2 + q^2)^2 = (p^2 - q^2 - 2pq)^2 + (p^2 - q^2 + 2pq)^2 = a^2 + b^2$. ■

Lemma 5 *If (x, y, z) is a primitive solution of $x^2 + y^2 = z^2$, then $gcd(x, y) = gcd(x, z) = gcd(y, z) = 1$.*

Lemma 6 *If (x, y, z) is a primitive solution of $x^2 + y^2 = z^2$, then only one of x or y is a multiple of 3.*

Proofs to these two lemmas can be found in many elementary number theory textbooks.

Lemma 7 *If (x, y, z) is a primitive solution of $x^2 + y^2 = z^2$, then $x + y$ and $x - y$ cannot contain the factor 3.*

PROOF: This follows from Lemmas 5 and 6 since $\gcd(x, y) = 1$ and only one of x and y is a multiple of 3. ■

Now, we are ready to show 3 cannot be a factor of a, b and m in the equation $a^2 + b^2 = 2m^2$. Here I will also refer to the equation $x^2 + y^2 = z^2$.

a and b cannot contain a factor 3 because $a = |p^2 - q^2 - 2qp| = |x - y|$ and $b = |p^2 - q^2 + 2qp| = |x + y|$, both as a consequence of Lemma 7.

That m cannot be a multiple of 3 is already shown in the proof to Theorem 1. In fact, m cannot contain any prime p such that $p \equiv 3 \pmod 4$.

■