THE DIOPHANTINE EQUATION $x^2 + a^2y^m = z^{2n}$ WITH $(x, ay) = 1$

Konstantine Dabmian Zelator (formerly K. Spyropoulos)
Carnegie Mellon University, Pittsburgh, PA 15213
(Submitted December 1990)

As it is well known, the equation

(1) $$x^2 + y^4 = z^4$$

has no solutions in the set of positive integers (one can find this equation in a number of sources including Dickson's *History of the Theory of Numbers* [2]). The equation $x^2 + y^4 = z^4$ serves as a classic result in the history of diophantine analysis, and one of the first known examples where Fermat's method of infinite descent is employed.

Therefore, if $m \equiv 0 \pmod 4$ and n is even, the equation $x^2 + y^m = z^{2n}$ has no solution in positive integers x, y, and z.

Now consider the diophantine equation $x^2 + a^2y^m = z^{2n}$ with m even. We will show that if a is a positive odd integer and if it has a prime divisor $p \equiv \pm 3 \pmod 8$, then the above equation has no solution with $(x, ay) = 1$ and y odd, provided that $n \equiv 0 \pmod 2$. This author has shown in [3] that the equation $x^4 + p^2y^4 = z^2$, p a prime with $p \equiv 5 \pmod 8$, has no solution in the set of positive integers. It is known, however, that for certain primes of the form $p \equiv 1$, 3, or 7 (mod 8), the latter equation does have a solution over the set of positive integers (for fruther details, refer to [3]).

To start, we have

Theorem 1: Let a be a positive odd integer with a prime factor p of the form $p \equiv \pm 3 \pmod 8$. Also, let m and n be positive integers with m and n both even. Then the diophantine equation $x^2 + a^2y^m = z^{2n}$ with $(x, ay) = 1$ and y odd has no solution in the set of positive integers.

Proof: Assume (x, y, z) to be a solution to the equation

(2) $$x^2 + a^2y^m = z^{2n}$$

with $(x, ay) = 1$.

Since m is even, $m = 2k$, the equation

(3) $$x^2 + a^2y^{2k} = z^{2n},$$

describes a Pythagorean triangle with side lengths x, ay^k, and z^n. Accordingly, there must exist positive integers t and ℓ of different parity, i.e., $t + \ell \equiv 1 \pmod 2$, with $(t, \ell) = 1$ (t and ℓ relatively prime), such that

(4) $$x = 2t\ell, \quad ay^k = t^2 - \ell^2, \quad z^n = t^2 + \ell^2.$$

From the second equation of (4), we obtain

(5) $$ay^k = (t - \ell)(t + \ell).$$

In view of the fact that the integers t and ℓ are relatively prime and of different parity, we conclude that $t - \ell$ and $t + \ell$ must be relatively prime and both odd; thus, (5) implies

(6) $$t - \ell = a_1y_1^k, \quad t + \ell = a_2y_2^k$$

with y_1, y_2 both odd and $(y_1, y_2) = 1 = (a_1, a_2)$ and $a_1a_2 = a$.

Equations (6) yield

$$t = \frac{a_1y_1^k + a_2y_2^k}{2}, \quad \ell = \frac{a_2y_2^k - a_1y_1^k}{2}$$

and by substituting in the third equation of (4), we obtain

$$2z^n = a_1^2y_1^{2k} + a_2^2y_2^{2k}.$$

By the hypothesis of the Theorem, n is even, $n = 2\beta$, and so we obtain

$$(7) \qquad 2z^{2\beta} = a_1^2y_1^{2k} + a_2^2y_2^{2k}.$$

According to the general solution of the diophantine equation

$$2Z^2 = X^2 + Y^2 \text{ with } (X, Y) = 1$$

(refer to [2] and also to the Remark at the end of the proof for comment on this equation), (7) implies

$$(8) \qquad z^\beta = r^2 + s^2, \quad a_1y_1^k = r^2 + 2rs - s^2, \quad a_2y_2^k = -r^2 + 2rs + s^2$$

with $(r, s) = 1$ (and, in fact, r and s are of different parity).

According to the hypothesis of the Theorem, $a = a_1a_2$ is divisible by a prime $p = \pm 3 \pmod 8$. Thus, a_1 or a_2 is divisible by p, say a_1. Then the second equation in (8) gives $r^2 + 2rs - s^2 = 0 \pmod p$; $(r + s)^2 - 2s^2 = 0$; and so

$$(9) \qquad (r + s)^2 \equiv 2s^2 \pmod p.$$

But s and $r + s$ are relatively prime, since r and s are; thus, neither of them is divisible by p [by (9)] and so congruence (9) shows that 2 is a quadratic residue modulo p, which is impossible according to the quadratic reciprocity law and since $p = \pm 3 \pmod 8$ [recall that $p = \pm 1 \pmod 8$ iff 2 is a quadratic residue mod p]. The argument is identical when a_2 is divisible by p; the congruence that yields the contradiction is

$$(r + s)^2 \equiv 2r^2 \pmod p.$$

Remark: Given two positive integers a and b which are relatively prime, it can be shown through elementary means that every solution (with X, Y, and Z relatively prime) (X, Y, Z) in $\mathbb{Z}$, to the diophantine equation

$$(a^2 + b^2)Z^2 = X^2 + Y^2,$$

must satisfy

$$X = \frac{-am^2 + 2bmn + an^2}{D}, \quad Y = \frac{bm^2 + 2amn - bn^2}{D}, \quad Z = \frac{m^2 + n^2}{D},$$

where D is the greatest common divisor of the three numerators and where the integers m and n are relatively prime. In the case of the equation

$$2Z^2 = X^2 + Y^2$$

we have, of course, $a = b = 1$; so the parametric solution takes the form

$$X = -m^2 + 2mn + n^2, \quad Y = m^2 + 2mn - n^2, \quad Z = m^2 + n^2$$

with $(X, Y) = 1$, $(m, n) = 1$, and m, n of different parity. If we set $a = b = 1$ in the above formulas and require $(X, Y) = 1$, then it is not hard to see that $D = 1$ or 2 according to whether m and n are of different parity or both odd with $(m, n) = 1$; but the case $D = 2$ reduces to $D = 1$ when m and n are both odd. To see this, we may set $m = m' - n'$ and $n = m' + n'$ with $(m', n') = 1$ and m', n' of different parity. By solving the above formulas for m' and n' in terms of m and n, substituting for $a = b = 1$ and $D = 2$ in the above formulas, we do see indeed that the case $(m, n) = 1$ and $m + n = 0 \pmod 2$ reduces to that of $(m, n) = 1$ and $m + n \equiv 1 \pmod 2$ (and so $D = 1$).

These elementary derivations of parametric solutions make essential use of the fact that the equation $(a^2 + b^2)Z^2 = X^2 + Y^2$ is homogeneous. For further reading, you may refer to [1].

Corollary 1: If a satisfies the hypothesis of Theorem 1, there is no primitive Pythagoran triangle (primitive means that any two sides are relatively prime) whose odd perpendicular side is divisible by a and whose hypotenuse is an integer square.

Proof: Suppose, to the contrary, that there is such a primitive Pythagorean triple, say (x_1, y_1, z_1), so that $x_1^2 + y_1^2 = z_1^2$, $(x_1, y_1) = 1$, y_1 odd. Then we must, accordingly, have $y_1 = ay$ and $z_1 = z^2$, where y and z are positive integers. Substituting into the above equation, we obtain $x_1^2 + a^2y^2 = z^4$; since y_1 is odd, so must be y in view of $y_1 = ay$. But $(x_1, y_1) = (x_1, ay) = 1$, which, together with the last equation, violate Theorem 1 for $n = m = 2$. Thus, a contradiction.

Comment: It is not very difficult to show that, given any positive integer ρ, there is an infinitude of Pythagorean triangles with a perpendicular side being a ρ^{th} integer power; or with the hypotenuse a ρ^{th} integer power. A construction of such families of Pythagorean triangles can be done elementarily and explicitly. Specifically, if a and b are odd positive integers which are relatively prime, define the positive integers

$$M = \frac{a^\rho + b^\rho}{2} \quad \text{and} \quad N = \frac{a^\rho - b^\rho}{2}; \quad a > b.$$

Then the triple $(M^2 - N^2, 2MN, M^2 + N^2)$ is a primitive Pythagorean triple such that $M^2 - N^2$ is the ρ^{th} power of an integer. That the triple is Pythagorean is well known and established by a straightforward computation. To show that it is primitive, it is enough to observe that, in view of the fact that a and b are both odd (and so are a^ρ and b^ρ), M and N must have different parity (to see this, consider $a^\rho + b^\rho$ and $a^\rho - b^\rho$ modulo 4). If p is a prime divisor of M and N one easily shows that p must divide both a^ρ and b^ρ, an impossibility in view of $(a, b) = 1$. This establishes that $(M, N) = 1$. Finally, a computation shows $M^2 - N^2 = a^\rho b^\rho = (ab)^\rho$.

To construct a primitive Pythagorean triangle whose even side is the ρ^{th} power of an integer, it would suffice to take $M = a^\rho$ and $N = 2^{\rho-1}\cdot b^\rho$ (or vice versa), with $(a, b) = 1$, a and b positive integers and a odd. Here we assume $\rho \geq 2$ (for $\rho = 1$ the problem is trivial, in which case one must assume b to be even). By inspection, we have $(M, N) = 1$. And $2MN = 2a^\rho \cdot 2^{\rho-1}b^\rho = (2ab)^\rho$; the triangle $(M^2 - N^2, 2MN, M^2 + N^2)$ is a primitive one whose even side is a ρ^{th} integer power.

Now, let us discuss the construction of a primitive Pythagorean triangle whose hypotenuse is the ρ^{th} power of an integer. In the special case $\rho = 2^n$, the following procedure can be applied. We form the sequence

$$(x_0, y_0, z_0), \ldots, (x_n, y_n, z_n)$$

by first defining

$$x_0 = M_0^2 - N_0^2, \quad y_0 = 2M_0N_0, \quad z_0 = M_0^2 + N_0^2,$$

where M_0 and N_0 are given positive integers, relatively prime, of different parity, and $M_0 > N_0$. Then recursively define

$$M_i = M_{i-1}^2 - N_{i-1}^2 \quad \text{and} \quad N_i = 2M_{i-1}N_{i-1}, \text{ for } i = 1, \ldots, n.$$

It can easily be shown by induction that $(M_i, N_i) = 1$ and that (x_i, y_i, z_i) is a Pythagorean triple, where

$$x_i = M_i^2 - N_i^2, \quad y_i = 2M_iN_i, \quad z_i = M_i^2 + N_i^2.$$

It is also easily shown that $z_i = z_{i-1}^2$, which eventually leads to $z_n = z_0^{2n}$. The Pythagorean triple (x_n, y_n, z_n) would then be a primitive one, with z_n the ρ^{th}

power of an integer $\rho = 2^n$. More generally, if $\rho \geq 2$ is any integer, a primitive Pythagorean triangle can be constructed such that the hypotenuse is the ρ^{th} power of a prime $p \equiv 1 \pmod 4$.

Specifically, if p is any prime such that $p = 1 \pmod 4$, then $p = a^2 + b^2$, where the relatively prime integers a and b are uniquely determined.

We have

$$p^2 = p \cdot p = (a^2 + b^2)(a^2 + b^2) = (a^2 - b^2)^2 + (2ab)^2;$$

one can easily check that $a^2 - b^2$ and $2ab$ must be relatively prime. Now, suppose that $p^{\rho-1} = M^2 + N^2$, $\rho \geq 3$, for some positive integers M and N such that $(M, N) = 1$.

We have

$$p^\rho = p^{\rho-1} \cdot p = (M^2 + N^2)(a^2 + b^2) = (Mb - Na)^2 + (Ma + Nb)^2$$
$$= (Mb + Na)^2 + (Ma - Nb)^2.$$

We claim that

$$(Mb - Na, Ma + Nb) = 1 \quad \text{or} \quad (Mb + Na, Ma - Nb) = 1.$$

For, otherwise, there would be a prime q dividing $Mb - Na$ and $Ma + Nb$ and a prime r dividing $Mb + Na$ and $Ma + Nb$. But then, according to the above equation, both q and r would divide p^ρ; hence, $q = r = p$. But this would imply that p must divide $2Mb$, $2Na$, $2Ma$, and $2Nb$; consequently, p must divide (since p is odd) Mb, Na, Ma, and Nb; however, this is impossible by virtue of $(M, N) = (a, b) = 1$. Thus, we have shown that, for given $\rho \geq 2$ and prime $p \equiv 1 \pmod 4$, there exist integers M, N, $(M, N) = 1$ such that $p^\rho = M^2 + N^2$. Then the desired Pythagorean triple is $(M^2 - N^2, 2MN, p^\rho)$.

Corollary 2: If in a primitive Pythagorean triangle the hypotenuse is an integer square, then each prime factor p of its odd perpendicular side must be congruent to ± 1 modulo 8.

Proof: The result is an immediate consequence of Corollary 1. Indeed, if it were otherwise, that is, if the odd perpendicular side y had a prime factor $p = \pm 3 \pmod 8$, then by setting $y = py_1$, we would obtain

$$x^2 + p^2 \cdot y_1^2 = z^2, \text{ with } (x, py_1) = 1.$$

But $z = R^2$ by hypothesis, and so the last equation produces

$$x^2 + p^2y_1^2 = R^4,$$

which is contrary to Corollary 1 with $a = p$.

Theorem 2: Let m be a (positive) even integer, $m = 2k$, with k odd, $k \geq 3$, and n even. Also, let a be an odd positive integer that contains a prime divisor $p \equiv \pm 3 \pmod 8$, and assume that b is a non-k^{th} residue modulo q, while 2 is a k^{th} residue of q, where q is some prime divisor of a; b some positive integer relatively prime to a. Moreover, assume that each divisor ρ of a/q^e, where q^e is the highest power of q dividing a, is a k^{th} residue modulo q. Then the diophantine equation

$$b^2x^m + a^2y^m = z^{2n}; \; (bx^k)^2 + (ay^k)^2 = (z^n)^2$$

has no solution in positive integers x, y, z with $(bx, ay) = 1$.

Proof: By Theorem 1, there is nothing to prove when y is odd. If, on the other hand, y is even and x odd, with $(bx, ay) = 1$ and $b^2x^m + a^2y^m = z^{2n}$, we see that bx^k, ay^k, and z^n form a primitive Pythagorean triple, where $k = m/2$. In that case, of course, bx is odd and ay is even, and so we must have

(10) $\quad bx^k = M^2 - N^2, \quad ay^k = 2MN, \quad z^n = M^2 + N^2$

with $(M, N) = 1$ and M, N being positive integers of different parity.

Let q be the prime divisor of a, as stated in the hypothesis. The second equation of (10) shows that q must divide M or N. Certainly the above coprimeness conditions show that q does not divide bx. On the other hand, by virtue of the fact that k is odd, we have $(-1)^k = -1$. First, suppose $M \equiv 0 \pmod{q}$. Then, if q^e is the highest power of q dividing a, then since $(M, N) = 1$, the second equation in (1) shows that q^e divides M; and

$$N = N_1^k \rho 2^f,$$

where ρ is a divisor of a/q^e and the exponent f equals 0 or $k - 1$, depending on whether N is odd or even, respectively. Thus,

$$N^2 = N_1^{2k} \rho^2 \cdot 2^{2f};$$

but ρ is a k^{th} residue of q by hypothesis; hence, so is ρ^2. Also 2^{k-1} is a k^{th} residue of q, since 2 is (by hypothesis) and $2 \cdot 2^{k-1} = 2^k$. Consequently, N^2 is a k^{th} residue and since $(-1)^k = -1$, the first equation in (10) clearly implies that b is also a k^{th} residue of q, contrary to the hypothesis.

A similar argument settles the case $N \equiv 0 \pmod{q}$.

Example: Take $k = 3$, and so $m = 6$, $p = 29$, $q = 31$, $e = 1$, and $a = p \cdot q = 899$; then $p \equiv 5 \pmod{8}$ and the cubic residues of 31 are ±1, ±2, ±4, ±8, and ±15; $p = 29$ is a cubic residue of q. Thus, if $b \not\equiv \pm 1, \pm 2, \pm 4, \pm 15 \pmod{31}$, the diophantine equation $(bx^3)^2 + (899y^3)^2 = z^4$ has no solution over the set of positive integers.

Corollary 3 (to Th. 2): Let a, b, and k be positive integers satisfying the hypothesis of Theorem 2. Then, there is no primitive Pythagorean triangle with one perpendicular side equal to a times a k^{th} integer power, the other b times a k^{th} power, and the hypotenuse a perfect square.

Proof: Apply Theorem 2 with $m = n = 2$. We omit the details.

References

1. L. J. Mordell. *Diophantine Euqations*. London: Academic Press, 1969.
2. L. E. Dickson. *History of the Theory of Numbers*, Vol. II. New York: Chelsea, 1952.
3. K. Spyropoulos. "On a Property of Pythagorean Triangles and Its Application to Two Diophantine Equations." *Congressus Numerantium* 57 (March 1987):281-88.
4. W. Sierpinski. *Elementary Theory of Numbers*. Warsaw, 1964.

AMS Classification number: 11NT (number theory)

*****