On the Solution of Diophantine Equations

E. JEFF HOLDER, PH.D.

We ultimately consider the Diophantine equation

$$z^N = x^N + y^N \tag{1}$$

and show that no positive integer solution exists for all $N > 2$. We first develop the framework of propositions required to develop the final proof.

Proposition 1: If b divides a^N for $N \geq 1$, then a and b are not relatively prime.

Proof: Applying the fundamental theorem of arithmetic we have

$$a = a_1^{N_1} \cdot a_2^{N_2} \cdot \ldots \cdot a_{K_a}^{N_{K_a}}$$

$$b = b_1^{M_1} \cdot b_2^{M_2} \cdot \ldots \cdot b_{K_b}^{M_{K_b}}$$

and

$$a^N = \left(a_1^{N_1} \cdot a_2^{N_2} \cdot \ldots \cdot a_{K_a}^{N_{K_a}}\right)^N = a_1^{N \cdot N_1} \cdot a_2^{N \cdot N_2} \cdot \ldots \cdot a_{K_a}^{N \cdot N_{K_a}}$$

Now assume that b divides a^N, then

$$b = \prod_{l=1}^{K_b} b_l^{M_l} = \prod_{k_j \in I_j} a_{k_j}^{Q_{k_j}} \qquad \text{for each } j,\ 0 \leq Q_{k_j} \leq N \cdot P_j \ \text{ and } k_j \in I_j \subset \{1 \quad 2 \quad \ldots \quad K_a\}$$

By the Fundamental Theorem of Arithmetic, it follows that for some l and k_j

$$b_l = a_{k_j} \ \text{ and } \ M_l = Q_{k_j}.$$

But then b_l divides both a and b, and thus a and b are not relatively prime. $\therefore$

Proposition 2: If a and b are not relatively prime, then $a = ke$ and $b = kf$ where e and f are relatively prime.

Proof: Fundamental Theorem of Arithmetic

Proposition 3: If $u \left| (v + w) \right.$ and $u \left| v \right.$, then $u \left| w \right.$.

Proof: Let $v + w = m \cdot u$ and $v = n \cdot u$ where $m > n$, then

$$n \cdot u + w = m \cdot u$$

$$w = m \cdot u - n \cdot u = (m - n)u$$

Thus $u \mid w$. $\therefore$

Proposition 4: If *x*, *y*, and *z* is a positive integer solution to (1), and *k* is a common factor of *x*, *y*, and *z* where *z* = *ka*, *x* = *kb*, and *y* = *kc*, then *a*, *b*, and *c* is a solution to (1) with no common factor.

Proof:

$$z^N = x^N + y^N \Rightarrow$$
$$(ka)^N = (kb)^N + (kc)^N \Rightarrow$$
$$k^N a^N = k^N b^N + k^N c^N \Rightarrow$$
$$a^N = b^N + c^N$$

Thus, *a*, *b*, and *c* is a solution to (1). $\therefore$

Proposition 5: If *x*, *y*, and *z* is a solution to (1) with no common factor and *z* = *a* + *b* and *x* = *b* and *y* = *c*, then *a* is relatively prime to *b* and *b* is relatively prime to *c*.

Proof: We first show that there exists *a*, *b*, and *c* such that *a* + *b*, *b*, and *c* is a solution to (1). Let *x*, *y*, and *z* be a solution to (1). Then it follows that *z* > *x* and *z* > *y*. Now choose *a* = *z* - *x*, *b* = *x*, and *c* = *y*. The *z* = *a* + *b*, *x* = *b*, and *y* = *c* is a solution to (1).

We now prove that *a* is relatively prime to *b* and *b* is relatively prime to *c* by contradiction considering the following three cases.

Case 1: *x*, *y*, and *z* is a solution and *z* = *a* + *b*, *x* = *b*, and *y* = *c* and assume *a* and *b* are not relatively prime and *b* and *c* are relatively prime.

Case 2: *x*, *y*, and *z* is a solution and *z* = *a* + *b*, *x* = *b*, and *y* = *c* and assume *a* and *b* are relatively prime and *b* and *c* are not relatively prime.

Case 3: *x*, *y*, and *z* is a solution and *z* = *a* + *b*, *x* = *b*, and *y* = *c* and assume *a* and *b* are not relatively prime and *b* and *c* are not relatively prime.

Case 1 proof. Let *x*, *y*, and *z* be a solution and define *z* = *a* + *b*, *x* = *b*, and *y* = *c* and assume that *a* and *b* are not relatively prime and *b* and *c* are relatively prime. Then we can write *a* = *ke* and *b* = *kf* where *k* is a common factor to both *a* and *b*. We now show that *k* divides *c*.

$$(a + b)^N = b^N + c^N \tag{2}$$

$$(ke + kf)^N = (kf)^N + c^N$$

$$k^N (e + f)^N = k^N (f)^N + c^N$$

$$\left(\frac{c}{k}\right)^N = (e+f)^N - (f)^N$$

Since the right-hand side of the above equation is a positive integer, it must be that k divides c, which is a contradiction to the hypothesis for Case 1 that b and c are relatively prime.

Case 2 proof. Let x, y, and z be a solution and define $z = a + b$, $x = b$, and $y = c$ and assume that a and b are relatively prime and that b and c are not relatively prime. Then b and c have a common factor k, and we can write $b = kf$ and $c = kg$. Thus,

$$(a + k \cdot f)^N = (k \cdot f)^N + (k \cdot g)^N$$

$$(a + k \cdot f) = \left((k \cdot f)^N + (k \cdot g)^N\right)^{1/N}$$

But the right-hand side is an integer since the left-hand side is an integer, and thus

$$a = \left((k \cdot f)^N + (k \cdot g)^N\right)^{1/N} - k \cdot f$$

$$a = k\left(\left(f^N + g^N\right)^{1/N} - f\right)$$

Thus k divides a, and since k divides b, we have a contradiction to the hypothesis of Case 2 that a and b are relatively prime.

Case 3 proof. Let x, y, and z be a solution and define $z = a + b$, $x = b$, and $y = c$ and assume that a and b are not relatively prime and b and c are not relatively prime. Then we have $a = k_1 e$ and $b = k_1 f$ where e and f are relatively prime and $b = k_2 h$ and $c = k_2 g$ where h and g are relatively prime. But Case 1 showed that any factor common to a and b is also common to c. Thus k_1 divides c and is common to a, b, and c. And Case 2 showed that any factor common to b and c is also common to a. Thus k_2 divides a and is common to a, b, and c. The fact that k_1 and k_2 are common factors of a, b, and c is a contradiction to the hypothesis that all of the common factors in (1) were removed. ∴

Proposition 6: If x, y, and z is a solution to (1) with no common factor and $z = a + b$, $x = b$, and $y = c$, then x, y, and z being a solution to (1) is equivalent to the polynomial $p_N(u,v)$ having rational roots $u = a/b$ and $v = c/b$ where

$$p_N(u,v) = \sum_{i=1}^{N} \binom{N}{i} u^i - v^N .$$

Proof: We now rewrite (1) as follows,

$$(a+b)^N = b^N + c^N$$

Expanding the left-hand side we have

$$\sum_{i=0}^{N}\binom{N}{i}a^i b^{N-i} = b^N + c^N$$

$$\sum_{i=1}^{N-1}\binom{N}{i}a^i b^{N-i} = c^N$$

$$\sum_{i=1}^{N-1}\binom{N}{i}\left(\frac{a}{b}\right)^i = \left(\frac{c}{b}\right)^N$$

$$0 = \sum_{i=1}^{N-1}\binom{N}{i}\left(\frac{a}{b}\right)^i - \left(\frac{c}{b}\right)^N$$

Lemma 1: For N prime and $N > 2$, the polynomial $p_N(x,y)$, defined below, does not have a rational roots of the form $x = a/b$ and $y = c/b$ where a and b are relatively prime and b and c are relatively prime.

$$p_N(x,y) = \sum_{i=1}^{N}\binom{N}{i}y^i - x^N$$

Proof: Assume that the polynomial $p_k(x,y)$ has a rational root of the form $x = a/b$ and $y = c/b$ where a and b are relatively prime and b and c are relatively prime. Note that if a and b are not relatively prime or b and c are not relatively prime, then common factors will cancel in the quotient leaving factors that are relatively prime. Now we substitute and write,

$$0 = \sum_{i=1}^{N}\binom{N}{i}\left(\frac{a}{b}\right)^i - \left(\frac{c}{b}\right)^N$$

$$0 = \sum_{i=1}^{N}\binom{N}{i}b^N\left(\frac{a}{b}\right)^i - c^N$$

$$0 = \sum_{i=1}^{N}\binom{N}{i}a^i b^{N-i} - c^N \tag{3}$$

Assume that a and c are not relatively prime and k is a common factor.

$$c^N - a^N = \sum_{i=1}^{N-1}\binom{N}{i}a^i b^{N-i} = ab\left(\sum_{i=1}^{N-1}\binom{N}{i}a^{i-1}b^{N-i-1}\right) \Rightarrow$$

$$k^N \left| ab\left(\sum_{i=1}^{N-1}\binom{N}{i}a^{i-1}b^{N-i-1}\right) \Rightarrow k^{N-1} \right| b\left(\sum_{i=1}^{N-1}\binom{N}{i}a^{i-1}b^{N-i-1}\right) \Rightarrow$$

$$k^{N-1} \left| \left(\sum_{i=1}^{N-1}\binom{N}{i}a^{i-1}b^{N-i-1}\right) \right. \tag{4}$$

We have two cases. Either N divides k or N does not divide k.

Case 1: N divides k. Since N is prime and $N > 2$, N is odd and N divides $\binom{N}{2}$.

Since k divides a and N divides k, we have N divides a and from (4),

$$k^{N-1}\left|\left(\sum_{i=1}^{N-1}\binom{N}{i}a^{i-1}b^{N-i-1}\right)\Rightarrow N^{N-1}\right|\left(\sum_{i=1}^{N-1}\binom{N}{i}a^{i-1}b^{N-i-1}\right)\Rightarrow N^2\left|\sum_{i=1}^{N-1}\binom{N}{i}a^{i-1}b^{N-i-1}\right.$$

From Lemma 3, since N divides a,

$$N^2\left|\left(\sum_{i=3}^{N-1}\binom{N}{i}a^{i-1}b^{N-i-1}+\frac{N(N-1)}{2}ab^{N-2}+Nb^{N-2}\right)\Rightarrow N^2\right|\left(\frac{N(N-1)}{2}ab^{N-2}+Nb^{N-2}\right).$$

Thus applying Lemma 3 again,

$$N^2\left|Nb^{N-2}\Rightarrow N\right|b^{N-2}.$$

From Proposition 1, N and b are not relatively prime, and since N divides a, it follows that a and b share a common factor and are not relatively prime which is a contradiction.

Case 2: N does not divide k. From (4), we have

$$k^{N-1}\left|\left(\sum_{i=1}^{N-1}\binom{N}{i}a^{i-1}b^{N-i-1}\right)\Rightarrow k^2\right|\sum_{i=1}^{N-1}\binom{N}{i}a^{i-1}b^{N-i-1}.$$

From Lemma 3 we have,

$$k^2\left|\left(\sum_{i=3}^{N-1}\binom{N}{i}a^{i-1}b^{N-i-1}+\frac{N(N-1)}{2}ab^{N-2}+Nb^{N-2}\right)\Rightarrow k^2\right|\left(\frac{N(N-1)}{2}ab^{N-2}+Nb^{N-2}\right).$$

And again from Lemma 3 since N and k are relatively prime,

$$k\left|\left(\frac{N(N-1)}{2}ab^{N-2}+Nb^{N-2}\right)\right.\Rightarrow k\left|Nb^{N-2}\Rightarrow k\right|b^{N-2}$$

From Proposition 1, k and b are not relatively prime, and since k divides a, it follows that a and b share a common factor and are not relatively prime which again is a contradiction.

Thus a and c are relatively prime, and from (3)

$$c^N=\sum_{i=1}^{N}\binom{N}{i}a^ib^{N-i}$$

$$c^N = a\sum_{i=1}^{N}\binom{N}{i}a^{i-1}b^{N-i}$$

$$\frac{c^N}{a} = \sum_{i=1}^{N}\binom{N}{i}a^{i-1}b^{N-i}$$

The right-hand side of the above equation is an integer, but since a and c are relatively prime, the left-hand side cannot be an integer and we have a contradiction. Thus, the polynomial $p_N(x,y)$ does not have rational roots. ∴

Theorem 1: No positive integer solution exists for the equation,

$$z^N = x^N + y^N \qquad \text{where } N \text{ is prime and } N > 2 \tag{5}$$

Proof: Assume x, y, and z is a solution to (5). Then by Proposition 6, $a = z - x$, $b = x$, and $c = y$ is a solution to the following,

$$c^N = \sum_{i=1}^{N}\binom{N}{i}a^{i}b^{N-i}$$

$$\left(\frac{c}{b}\right)^N = \sum_{i=1}^{N}\binom{N}{i}\left(\frac{a}{b}\right)^{i} \tag{6}$$

By Proposition 5, a is relatively prime to b and b is relatively prime to c. By Lemma 1, (6) does not have a rational root solution where a is relatively prime to b and b is relatively prime to c. As such, (5) does not have a solution where a and b are relatively prime and b and c are relatively prime which is a contradiction. Therefore (5) does not have a positive integer solution. ∴

Theorem 2: (Fermat) No positive integer solution exists for the equation,

$$z^N = x^N + y^N \qquad \text{for all } N > 2 \tag{7}$$

Proof: Assume that (7) has an integer solution for some $N > 2$. By the Fundamental Theorem of Arithmetic we have,

$$N = p_1 p_2 \cdots p_m$$

where each p_i is prime. Now rewrite (7) as follows,

$$z^{p_1 p_2 \cdots p_m} = x^{p_1 p_2 \cdots p_m} + y^{p_1 p_2 \cdots p_m}$$

$$\left(z^{p_1 p_2 \cdots p_{m-1}}\right)^{p_m} = \left(x^{p_1 p_2 \cdots p_{m-1}}\right)^{p_m} + \left(y^{p_1 p_2 \cdots p_{m-1}}\right)^{p_m}$$

Let

$$a = z^{p_1 p_2 \cdots p_{m-1}} \qquad b = x^{p_1 p_2 \cdots p_{m-1}} \qquad c = y^{p_1 p_2 \cdots p_{m-1}}$$

Then (7) becomes,

$$a^{p_m} = b^{p_m} + c^{p_m}$$

which by Theorem 1 does not have an integer solution which is a contradiction. ∴

Corollary 1. Equation (1) has a rational solution for $N = 2$.

Note that for $N = 2$, (1) reduces to

$$(a+b)^2 = b^2 + c^2$$

where $a = z - x$, $b = x$, and $c = y$.

Then it follows that,

$$0 = a^2 + 2ab - c^2$$

and $a = 2$, $b = 3$, $c = 4$ is a solution.

Hence $x = 3$, $y = 4$, and $z = 5$ is a solution to (1). ∴

Note that a is relatively prime to b and b is relatively prime to c as dictated by Proposition 5.