THE SUM OF TWO POWERS IS A THIRD, SOMETIMES

R. B. KILLGROVE
California State University, Los Angeles, California 90032

1. INTRODUCTION

We seek integer solutions to the Diophantine equation

$$x^n + y^m = z^k, \tag{1}$$

where *n, m* and *k* are positive integers. We have a general algorithm which sometimes augments primitive parameters to primitive solutions regardless of the choice of *m, n, k.* We classify the types of applications of this algorithm based on the greatest common divisor of the exponents. For some types all the primitive parameters augment to all the primitive solutions. For the type which includes the famous case $n = m = k > 2$, the finding of the primitive parameters which augment to primitive solutions is equivalent to the original problem. Without gain of generality (an expression of Professor DeHardt), we could extend this approach to a Diophantine equation with more powers on the left than two but only one power on the right.

2. HISTORY OF THE PROBLEM

In 1964 we obtained the computer solution $(1176)^2 + (49)^3 = (35)^4$ and from this one example we discovered our method of augmentation as well as a type of exponents for which we determined all primitive solutions. Subsequently that year Professor E. G. Strauss pointed out to us that this method could be applied successfully (i.e., yielding solutions) to another type. At this time we found that Basu [1] and others had found rational solutions for the first type mentioned above. Recently Beerenson [2] has found a similar method for finding integer solutions for this first type. At this later time we found that Teilhet [8] in 1903 used the method of augmentation for a special case $k = 3$, $m = n = 2$.

3. TRIVIAL SOLUTIONS

For completeness as well as for illustrating a simple case of primitive solutions, we now discuss the *trivial* solutions to (1), x_0, y_0, z_0, where $x_0y_0z_0 = 0$. Let us call the case $x = y = z = 0$, the zero case, and turn our attention elsewhere. Then exactly one of x_0, y_0, z_0 is zero, and the non-zero elements are both powers with common exponent the least common multiple of their corresponding exponents (x_0 corresponds to n, y_0 to m, z_0 to k). Thus for the *non-zero trivial* solutions with $x_0 = 0$, we say y_0, z_0 form a *primitive* solution if and only if there is no integer $d > 1$ such that $d^L | y_0$ and $d^L | z_0$ where $L = [m,k]$. Thus the possible candidates for a non-zero, trivial, primitive solution are: $y_0 = \pm 1, z_0 = \pm 1$.

4. PRIMITIVE SOLUTIONS AND THE CLASSIFICATION SCHEME

The computer example indicated to us that the usual definition of primitive solution x_0, y_0, z_0, namely, one where

$$(x_0, y_0) = (x_0, z_0) = (y_0, z_0) = 1,$$

was not adequate. Thus we give a new definition which reduces to the old when appropriate.

Definition: A solution $u, v, w, uvw \neq 0$, to (1) is called a (non-trivial) *primitive solution* if and only if there is no $t > 1$ such that $t^a | u$, $t^b | v$, $t^c | w$, where

$$a = L/n, \quad b = L/m, \quad c = L/k, \quad \text{and} \quad L = [n, m, k].$$

The case $n = m = k \geqslant 3$ is referred to as Fermat's Last Theorem (F.L.T.) wherein the conjecture states that there are no non-trivial solutions. This conjecture is true for $n < 25000$ [7]. If $(n,m,k) > 2$, then (1) for this type of exponents can be reduced to F.L.T.

The type $(n,m,k) = 2$ has not yet been completely resolved. If $n = 2h$, $m = 2i$, and $k = 2j$, and if $(h,i) = (h,j) = (i,j) = 1$, then (E.G. Strauss) all possible solutions can be obtained by augmentation. If $(h,i) \geqslant 2$, we can show there are no non-trivial solutions if F.L.T. holds. We conjecture the same holds for $(h,j) \geqslant 2$ and $(i,j) \geqslant 2$.

The type $(n,m,k) = 1$, but no one of n,m,k is relatively prime to the other two, is the only known type which sometimes yields a finite number of primitive solutions. In all other cases, as far as we know, if non-trivial solutions exist, there are an infinite number of primitive solutions.

We complete our classification scheme by mentioning the remaining type where one of n, m or k is relatively prime to the others. This is the "first type" referred to in Section 2.

5. THE METHOD OF AUGMENTATION

Let $D = [m,n]$ throughout this section.

Definition: Positive integers x_0 and y_0 are *primitive parameters* for (1) if and only if there is no $t > 1$ such that $t^d | x_0$ and $t^e | y_0$, where $d = D/n$ and $e = D/m$.

Definition: A primitive solution u,v,w, $uvw \neq 0$, to (1) is *an augmentation of primitive parameters* x_0, y_0 for (1) if and only if $u = x_0 z_0^d$, $v = y_0 z_0^e$, $z_0^{dn} = z_0^{em} = z_0^D$. If $z_0 > 1$, then we have a *proper augmentation.*

Theorem 1. If positive integers u,v,w form a primitive solution to (1) then there is a unique ordered pair x_0, y_0 which are primitive parameters so that u,v,w is an augmentation of x_0, y_0.

Proof. Let t be the largest positive integer for which $t^d | u$ and $t^e | v$ and $d = D/n$, $e = D/m$. Then $x_0 = u/t^d$ and $y_0 = v/t^e$ are primitive parameters, and u,v,w is an augmentation of x_0, y_0. Suppose x_1, y_1 are primitive parameters and

$$u = x_1 z_0^d, \quad v = y_1 z_0^e.$$

Let p be a prime such that $p^q \| t$ and $p^Q \| z_0$ and $q \neq Q$. Then $p^d | x_i$ and $p^e | y_i$, where $i = 0$ if $q < Q$ and $i = 1$ if $Q < q$. This contradicts the condition $x_i y_i$ are primitive parameters. Thus $t = z_0$ and $x_0 = x_1$ and $y_0 = y_1$.

Theorem 2. If x_0, y_0 are primitive parameters for (1) and $x_0^n + y_0^m$ is written as $a_k^k a_{k-1}^{k-1} \cdots a_2^2 a_1$, where each a_i, $i \neq k$, is squarefree and $(a_i, a_j) = 1$ for each $i < k$, $j < k$, $i \neq j$, then there is an augmentation to a positive primitive solution for (1) if and only if for each i, $1 \leqslant i < k$, either $a_i = 1$ or there is a solution g_i to $Dg_i \equiv -i \pmod{k}$ and g_i is the smallest such positive solution.

Proof. Suppose we have a primitive solution $u > 0$, $v > 0$, $w > 0$. Then

$$u = x_0 z_0^d, \quad v = y_0 z_0^e \quad \text{and} \quad w^k = a_k^k a_{k-1}^{k-1} \cdots a_2^2 a_1 z_0^D .$$

Hence

$$(w/a_k)^k = a_{k-1}^{k-1} \cdots a_2^2 a_1 z_0^D .$$

Suppose there is an i, $1 \leqslant i < k$, such that $a_i \neq 1$. Then for each prime p dividing a_i we have $p^i p^{gD} = p^{qk}$, where

$$p^g \| z_0 \quad \text{and} \quad p^q \| (w/a_k).$$

Thus $Dg \equiv -i \pmod{k}$. The smallest such positive solution is $< k/(D,k)$ [2, p. 51]. If $g > k/(D,k)$, then $gD > [D,k] = L = [n,m,k]$. Thus

$$p^L | u^n, \quad p^L | v^m, \quad p^L | w^k,$$

and u,v,w is not a primitive solution.

Suppose the conditions hold, and we write b^c as $b \exp c$, then z_0^D is one if all $a_i = 1$ for $i \neq k$ and is the product of $a_i \exp D\, g_i$ for all i, $1 \leqslant i < k$ and $a_i \neq 1$, otherwise. Then

$$u = x_0 z_0^d, \quad v = y_0 z_0^e, \quad \text{and} \quad w = a_k \pi,$$

where π is the product of the positive k^{th} roots of $a_i \exp f_i$, $f_i = Dg_i + i$, $a_i \neq 1$, or one. This is a solution to (1) but it may not be primitive when $z_0 \neq 1$.

If this is not a primitive solution, then there is a prime p such that

$$p^a|x_0z_0^d, \quad p^b|y_0z_0^e \quad \text{and} \quad p^c|w,$$

where $a = L/n$, $b = L/m$, $c = L/k$. If $p \nmid a_i$ for any i, $1 \leqslant i < k$, then $p \nmid z_0$ and $p^a|x_0$ and $p^b|y_0$. Since $L = DS$ for some integer S, $a = Sd$, $b = Se$, and x_0 and y_0 are not primitive parameters.

If $p|a_i$, then $p \exp g_i \| z_0$, and $g_i < k/(D,k)$. But

$$k/(D,k) = [D,k]/D = L/D = S.$$

Then $g_i \leqslant S - 1$, so

$$g_id \leqslant dS - d = a - d, \qquad g_ie \leqslant eS - e = b - e.$$

Since

$$p^a|x_0z_0^d, \qquad \text{and} \qquad p \exp g_id \,\|\, z_0^d,$$

then $p^d|x_0$; similarly $p^e|y_0$ and x_0, y_0 are not primitive parameters.

6. THE TYPE $(n,m,k) = 2$

Here $n = 2h$, $m = 2i$, $k = 2j$. For completeness we give a proof for a theorem in the literature [4] because it is easy and not too accessible.

V. A. Lebesque Theorem: If $x^{2t} + y^{2t} = z^2$ has a non-trivial solution then t is odd and $u^t + v^t = w^t$ has a non-trivial solution.

Proof. If t is even, we use the fact [3, p. 191] that $x^4 + y^4 = z^2$ has only trivial solutions. Then $x^t = 2rs$, $y^t = r^2 - s^2$ [3, p. 190]. But $(r+s, r-s) = 1$. (In this case the new and old definition of primitive are equivalent), hence $r + s = u^t$ and $r - s = v^t$, but either $2r = w^t$ or $2s = w^t$. In the former case, by adding $r + s$ to $r - s$, we obtain $u^t + v^t = w^t$. In the latter case subtract $r - s$ from $r + s$ and rename.

Lemma 1. If $n = 2$, $m = 2$, $k = 2t$, then all the primitive solutions to (1) are obtained by augmentation of primitive Pythagorean triples.

Proof. From a primitive Pythagorean triple [3, p. 190] x_0, y_0, z_0, we can use x_0, y_0 for primitive parameters, and if

$$x_0^2 + y_0^2 = a_{2t}^{2t}a_{2t-1}^{2t-1} \cdots a_2a_1$$

under the conditions of Theorem 2, then $a_i = 1$ for all odd i and $2g_i \equiv -i \pmod{2t}$ can be solved for all needed even i. If $x_0^2 + y_0^2$ is not a square, then when written in the above form $a_i \neq 1$ form some odd i, and $2g_i \equiv -i \pmod{2t}$ has no solution, and there is no augmentation.

NOTE: Our method does not distinguish solutions 15, 20, 5, and 7, 24, 5 for $n = m = 2$, $k = 4$, except as proper or improper augmentations. For $n = k = 2$, $m = 4$ we use a general modification of Theorems 1 and 2 using

$$z_0^k - x_0^n = a_m^m a_{m-1}^{m-1} \cdots a_2^2 a_1.$$

Lemma 2. If $n = 2$, $m = 2s$, $k = 2t$, $(s,t) = 1$, then all primitive solutions to (1) are obtained from primitive solutions to (1) with $n = 2$, $k = 2$ by augmentation.

Proof. If x_0, y_0, z_0 is a primitive solution to (1) with $n = 2$, $m = 2s$, $k = 2$, then x_0, y_0 are primitive parameters for $n = 2$, $m = 2s$, $k = 2t$, $(s,t) = 1$, and the corresponding odd indexed $a_i = 1$, and $2sg_i \equiv -i \pmod{2t}$ can be solved for all even i. But if $y_0^2 + y_0^{2s}$ is not a square for x_0, y_0, primitive parameters then there is an odd i such that $a_i \neq 1$, and there is no solution to $2sg_i \equiv -i \pmod{2t}$.

Theorem 3. If

$$n = 2h, \quad m = 2i, \quad k = 2j, \quad (h,i) = (h,j) = (i,j) = 1$$

then there are an infinite number of primitive solutions to (1) obtained by none, one, or more augmentations of Pythagorean triples.

We do not give the proof since it repeats a third time essentially the proofs of the two lemmas.

7. THE TYPE $(m,n,k) = 1$ BUT NONE OF n,m,k IS RELATIVELY PRIME TO THE OTHER TWO

We know how to solve only $n = 2h$, $m = 3i$, $k = 6j$ for this type. We assume a result of Legendre [5], namely that $x^3 + y^3 = 2z^3$ implies $x = \pm y$. Using this hard to obtain result we give a proof of a theorem in the literature [6,9].

Thue-Lind Theorem. The only non-trivial primitive solutions to $x^2 + y^3 = z^6$ are $x = \pm 3$, $y = -2$, $z = \pm 1$.

Proof. First we note $(z^3 - x, z^3 + x) = 1$ or 2. In the former case, $z^3 - x = u^3$, $z^3 + x = v^3$, and $u^3 + v^3 = 2z^3$. By Legendre's result, $u = \pm v$. If $u = v$, $x = 0$, and if $u = -v$, then $z = 0$. Therefore for non-trivial solutions $(z^2 - x, z^3 + x) = 2$. Now

$$z^3 - x = 2y^3 \quad \text{and} \quad x^3 + x = 4v^3 \quad \text{or} \quad z^3 - x = 4u^3 \quad \text{and} \quad z^3 + x = 2v^3 .$$

One case can be obtained by the other by replacing x by $-x$, but x is a solution if and only if $-x$ is. Thus we consider the former case only. Then by adding, we obtain $z^3 + (-u)^3 = 2v^3$, and by Legendre's result, $z = u$ or $z = -u$. If $z = u$, then $v = 0$, and $y = 0$; thus for non-trivial solutions $z = -u$. Then $v = -u$, so, from $(u,v) = 1$, $u = \mp 1$, $v = \pm 1$; hence $y = -2$, $z = \pm 1$. Q.E.D.

Now any solution u, v, w to (1) for $n = 2h$, $m = 3i$, $k = 6j$ is a solution to the case $n = 2$, $m = 3$, $k = 6$ and hence

$$u^h = \pm 3a^3, \quad v^i = -2a^2, \quad w^j = \pm a.$$

If p is a prime greater than 3 and $p^d \| a$, then

$$h|3d, \quad i|2d, \quad \text{and} \quad j|d \quad \text{and} \quad [n,m,k]\,|6d$$

and this is not a primitive solution. Thus $a = 2^b 3^c$, and $j|b$ and $j|c$ and $h|3b$ and $i|2c$ and $h|1 + 3c$ and $i|1 + 2b$. Conversely if these conditions are met then there is a solution. Moreover, it can be shown there is a b and c if and only if $(h,i) = (h,j) = (i,j) = 1$. Note for $b = 4$ $c = 9$, we obtain 8, 9, 6 case as well as 8, 27, 6 case.

8. THE REMAINING CASE AND SUMMARY

The remaining case when one of n, m, k is relatively prime to the other two, then the conditions of Theorem 2 are always met and every set of primitive parameters augment, when the equation is written with the special exponent term being the only term of one side of the equation. For example, $n = 2$, $m = 3$, $k = 4$ then we write $z^4 - x^2 = y^3$, and, for example, 5, 24 being relatively prime are primitive parameters and $5^4 - 24^2 = 7^2$ from the Pythagorean triple, 7, 24, 25. Then we augment by 7^4 and obtain the solution we found on the computer.

Mr. Jim Grant, U.C.L.A. student, has also found an algorithm for obtaining rational solutions for this remaining case. He has made a real gain with his general approach because it not only applies to general Diophantine equations of this type but also applies to many other problems as well, including some differential equations.

REFERENCES

1. N. M. Basu, "On a Diophantine Equation," Ball, *Calcutta Math. Soc.* (1940), pp. 15–20.
2. R. G. Beerensson, "On the Equation $x^n \pm y^n = z^m$," *The Mathematical Gazette*, 54 (1970), pp. 138–139.
3. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers,* Oxford, Fourth Edition, 1960.
4. V. A. Lebesque (entry 31), L. E. Dickson, *History of the Theory of Numbers,* Vol. II, Chelsea, N.Y., 1952, p. 737.
5. A. M. Legendre (entry 184), L. E. Dickson, *ibid.,* p. 573.
6. Lind (entry 224), L. E. Dickson, *ibid,.,* p. 766.
7. J. L. Selfridge and B. W. Pollack, "Fermat's Theorem is True for any Exponent up to 25000," *Notices of AMS,* 11 (1964), p. 97.
8. P. F. Teilhet, "Cube somme de dans Carrés," *L'Intermediaire des Mathématicens,* Vol. 10, 1903, p. 210.
9. Axel Thue (entry 236), L. E. Dickson, *ibid.,* p. 580.

****