Fermat's Last Theorem for Cubes

Before considering the integer equation x^3 + y^3 = z^3, it's worthwhile to briefly review the simple Pythagorean equation x^2 + y^2 = z^2. For primitive solutions we can assume x,y,z are pairwise coprime, x is odd and y is even. The usual approach is to re-write the equation as

$$\left(\frac{y}{2}\right)^2 = \left(\frac{z+x}{2}\right)\left(\frac{z-x}{2}\right)$$

Then, since the two integer factors on the right are coprime (and since we have unique factorization for integers), they must each individually be squares, so we have z+x = 2u^2 and z-x = 2v^2 for coprime integers u,v, (one odd and one even) from which it follows that z = u^2 + v^2, x = u^2 - v^2, and y = 2uv.

However, there is another approach to solving the Pythagorean equation that makes use of some deeper properties of integers known to Fermat, and that can be generalized to the case of cubes. This alternative approach relies on the fact that numbers of the form X^2 + Y^2 with gcd(X,Y)=1 can be "factored" uniquely into a product of primes of the same form, and that the representations of composites of this form are generated by applying the identity

(a^2 + b^2)(c^2 + d^2) = (ac +- bd)^2 + (ad -+ bc)^2

It's been speculated that Diophantus knew this identity, although he didn't give it explicitly in any of the (surviving) books of "Arithmetica". The first known explicit description was by Abu Jafar al-Khazin (circa 950 AD), and it also appears in Fibonacci's "Liber Quadratorum" (1225 AD). One could argue that this was really the first discovery of complex numbers, in the abstract sense of Hamilton's ordered pairs, because in C the product of (a,b) and (c,d) is (ac-bd,ad+bc). In any case, Fermat knew that only primes of the form 4k+1 are expressible as a sum of two coprime squares, and those are expressible in only one way. This, combined with the fact that representations of composites are given by the above formula applied to the representations of their factors, enables

us to say that if x^2 + y^2 is a square then the components x,y are given by squaring a number of the form (u^2 + v^2) using the above identity. As a result we have

$$x^2 + y^2 = (u^2 + v^2)^2 = (u^2 - v^2)^2 + (2uv)^2$$

which of course agrees with our previous solution. Thus, given the theorems about sums of two squares and their unique factorizations that were known to Fermat, this is (arguably) an even more direct solution than the original one, which is perhaps not surprising, since it is essentially employing the field of Gaussian integers, in disguised form.

Now let's consider the analagous equation for cubes, i.e., we seek all non-trivial integer solutions of x^3 + y^3 = z^3. Again we consider only primitive solutions, so without loss of generality we can assume x,y,z are coprime, one even and two odd. Changing signs if necessary we can make x and y odd and z even. Now we define x=u+v and y=u-v where (u,v)=1, and u,v have opposite parity. Substituting into x^3 + y^3 = z^3 gives

$$(2u)(u^2 + 3v^2) = z^3 \qquad (1)$$

Since z is even, u must be even and v must be odd. Now we'll consider two cases. First, assume z is not divisible by 3. In this case 2u is coprime to u^2 + 3v^2, so both of those factors must be cubes. Thus we have integers coprime m,n such that

$$u = 4m^3 \qquad (2)$$

$$u^2 + 3v^2 = n^3 \qquad (3)$$

In the case of the Pythagorean equation we had a sum of two squares equal to a square, whereas in this case we have a slightly different quadratic form, X^2 + 3Y^2, equal to a cube. Notice that we can't simply subtract u^2 from both sides of (3) and then factor the right hand side, because it is inhomogeneous, i.e., we would have a cube minus a square, which doesn't factor algenraically over the integers. We can, however, proceed to use the second approach, based on factoring the left hand side of (3) into divisors of the same form, provided we

know enough about numbers of the form X^2 + 3Y^2.

Happily, it turns out that we have a direct analog for the "Fibonacci identity". In fact, for ANY integer N we have

$$(a^2 + Nb^2)(c^2 + Nd^2) = (ac +- Nbd)^2 + N(ad -+ bc)^2$$

so we can always multiply together two numbers of the quadratic form X^2 + NY^2 to give another number of the same form. With k=3 this identity is

$$(a^2 + 3b^2)(c^2 + 3d^2) = (ac +- 3bd)^2 + 3(ad -+ bc)^2$$

With this identity in mind, we state and prove several facts about numbers of the quadratic form X^2 + 3Y^2 which are useful for continuing our search for solutions of x^3 + y^3 = z^3.

LEMMA 1: Every prime p of the form 3k+1 divides some integer of the form a^2 + 3b^2 with (a,b)=1.

PROOF: Since u^2 + uv + v^2 is an equivalent form under the substitution u=b+a and v=b-a, we need only prove that p divides such an integer, with (u,v)=1. Consider

$$u^{3k} - v^{3k} = (u^k - v^k)(u^{2k} + u^k v^k + v^{2k})$$

where 3k = p-1. Setting v=1 ensures (u,v)=1 and enables us to write

$$u^{3k} - 1 = (u^k - 1)(u^{2k} + u^k + 1)$$

The left hand side is divisible by p according to Fermat's Little Theorem for any integer u coprime to p. Therefore, the right side is also divisible by p for every such u. In order for p to NOT divide any of the number u^(2k) + u^k + 1, it must divide EACH of the numbers u^k - 1 for u = 1,2,3,..,p-1. However, the congruence u^[(p-1)/3] = 1 (mod p) can have no more than (p-1)/3 distinct roots, so it is NOT satisfied for 2/3 of the residues modulo p. Therefore, each of those non-roots is a value of u for which p

must divide u^(2k) + u^k + 1. Also, since more than half of those residues qualify, we can choose an odd u, and then a = (u-1)/2 and b = (u+1)/2. With these values, p divides a^2 + 3b^2, which completes the proof of Lemma 1.

LEMMA 2: If N is an integer of the form a^2 + 3b^2, and if the prime p = c^2 + 3d^2 divides N, then there exist integers u,v such that N/p = u^2 + 3v^2 and the repesentation of N is given by evaluating the product (p)(N/p) = (u^2 + 3v^2)(c^2 + 3d^2) using Fibonacci's formula.

PROOF: Since p divides N, it must divide Nd^2 - pb^2. Also, we have

$$Nd^2 - pb^2 = (a^2 + 3b^2)d^2 - (c^2 + 3d^2)b^2$$

$$= (ad + bc)(ad - bc)$$

which shows that the prime p must divide either ad+bc or ad-bc. Now, we can also write

$$Np = (ac +- 3bd)^2 + 3(ad -+ bc)^2$$

Depending on whether p divides ad+bc or ad-bc, we can choose the sign in the above expression so that p divides the right-most term. Then, since it also divides Np, it must divide the first term on the right. Therefore, dividing the above expression for Np by p^2, we have N/p = u^2 + 3v^2 where u,v are the integers given by

$$u = (ac +- 3bd)/p \qquad v = (ad -+ bc)/p$$

again with the choice of sign such that p divides ad-+bc. Solving these two equations for a and b gives

$$a = (cu + 3dv) \qquad b = +-(du - cv)$$

This shows that the representation of N is given by applying Fibonacci's formula to multiply (p)(N/p), which completes the proof of Lemma 2.

LEMMA 3: If we let [n\p] equal +1 or -1 accordingly as n is or is not a square (mod p), and if m,n are residues coprime to p, then [mn\p] = [m\p][n\p].

PROOF: If m,n are both squares (mod p), then obviously mn is also a square. Also, if one of m,n is a square and the other is not, then it follows that their product mn is not, because if m=x^2 and mn=y^2 we would have n = (y/x)^2, contrary to assumption that n is not square. The leaves only the case when neither m nor n is a square. To resolve this case, note that the non-zero multiplication table (modulo p) has unique inverse, so each non-zero residue appears in row and column precisely once. Also, since x^2=y^2 (mod p) implies (x-y)(x+y) mod p, it's clear that the squares of the residues 1 through (p-1)/2 are all distinct, and respectively equal to the squares of the residues (p+1)/2 to p-1. Therefore, the squares and non-squares each make up exactly half the non-zero residues. Also, each residue appears p-1 times in the table, so if fill in all the products of two squares, and all the products of a square and a non-square, we are left only with squares, which must be placed in the remaining openings, the products of two non-squares. Therefore [mn\p] = [m\p][n\p], completing the proof of Lemma 3.

LEMMA 4: If the integer N is representable in the form a^2 + 3b^2 with (a,3b)=1, then the only odd prime factors of N are of the form p = 3k+1.

PROOF: If N was divisible by a prime p, then we have a^2 = -3b^2 (mod p), which implies that (-3) is a square modulo p. It's easy to show that [-1\p] = (-1)^(p-1)/2, and by quadratic reciprocity we also have [3\p] = [p\3](-1)^(p-1)/2. From Lemma 3 and quadratic reciprocity it follows that [-3\p] = [-1\p][3\p] = [p\3]. Thus any number of the form a^2 + 3b^2 with (a,3b)=1 is divisible by only primes of the form 3k+1, which completes the proof of Lemma 4.

Notes:
1. It's possible to avoid the use of full quadratic reciprocity here, but I wonder if Fermat might have just assumed it?
2. If a^2 + 3b^2 with (a,b)=1 is even, then a,b are odd, in

which case either a+b or a-b must be divisible by 4. With that choice of sign we can set B=a+-b and A=a-+3b and then we have A^2 + 3B^2 = [a^2+3b^2]/4. Repeating if necessary, we can factor out all powers of 2, leaving an odd proper representation.

LEMMA 5: Every prime p of the form 3k+1 is expressible in the form u^2 + 3v^2 with (a,b)=1 in precisely one way.

PROOF: By Lemma 1 we know that p divides some integer of the form a^2 + 3b^2. Also, by replacing a and b with their least magnitude residues modulo p, the result is still divisible by p, but now we are assured that a and b are each less than or equal to (p-1)/2, from which it follows that a^2 + 3b^2 is strictly less than p^2. Therefore, all the prime divisors of a^2 + 3b^2 other than p are strictly smaller than p, and according to Lemma 4 all of those prime divisors are of the form 3k+1, and according to Lemma 3 they are all of the form u^2 + 3v^2. Therefore, we can apply Lemma 2 to each of these smaller prime divisors in turn, yielding a unique quotient of the form a^2 + 3b^2, until arriving at p. This completes the proof of Lemma 5.

LEMMA 6: The general primitive solution in integers of the equation x^2 + 3y^2 = N^3 for odd N is given by x = u(u^2 - 9v^2) and y = 3v(u^2 - v^2) where u,v are coprime integers.

PROOF: By Lemma 4 we know that N^3 is a product of primes of the form 3k+1, each of which by Lemma 5 has a unique proper representation of the form a^2 + 3b^2. Hence by Lemma 2 we can factor x^2 + 3y^2 uniquely into a product of primes of this form, and the representation of N^3 is given by applying the Fibonacci product formula. Also, it's easy to verify that Fibonacci multiplication is commutative, in the sense that the two representations given by AB are the same as the two given by BA. Also, we can verify that Fibonacci multiplication is associative, i.e., (AB)C = A(BC), by noting the results

$$\begin{aligned}&[(a^2 + 3b^2)(c^2 + 3d^2)](e^2 + 3f^2)\\ =\ &[ace + s1\ 3bde + s2\ 3adf - s1\ s2\ 3bcf]^2\\ &+ 3[ade - s1\ bce - s2\ acf - s1\ s2\ 3bdf]^2\end{aligned}$$

Since both components are squared, we need consider only the magnitudes of the components, so we can multiply each term of the second component by -s1 s2 and write the two components as shown below

$$ace + 3[\ s1\ bde + s2\ adf - s1\ s2\ bcf\ ]$$
$$3\ bdf\ +\ s1\ acf + s2\ bce - s1\ s2\ ade\ ]$$

Notice that the rows transpose (a,b), (c,d), and (e,f), so they have the same symmetry, and if we define s3 = -s1 s2 we have the three-way symmetry

$$s1\ s2 = -s3 \quad s1\ s3 = -s2 \quad s2\ s3 = -s1$$

Consequently, the set of proper representations given by the Fibonacci product of three proper representations is the same, regardless of the order in which the product is evaluated.

Furthermore, the number of distinct proper representations of a number equals 2^(k-1) where k is the number of distinct prime divisors, because we have two proper choices of sign when multiplying two distinct factors (whereas we have no proper choices when multiplying powers of a single prime). Since the number of distinct prime divisors of N is the same as the number of distinct prime divisors of N^3, we can produce all 2^k representations of N^3 as the cubes of the 2^k representations of N. Thus, for some coprime integers u,v we have not only

$$(u^2 + 3v^2)^3 = x^2 + 3y^2$$

but also expanding the left side by the Fibonacci formula (which gives a unique *proper* result when cubing a single representation) we have

$$x = u(u^2 - 9v^2) \quad y = 3v(u^2 - v^2)$$

completing the proof of Lemma 6.

Now (finally!) we can return to our original problem. Recall that on the assumption of the existence of integers x,y,z such that

x^3 + y^3 = z^3, and assuming first that z is not divisible by 3,
we had shown the existence of integers m,n and coprime integers
u,v such that

$$u = 4m^3 \qquad (2)$$

$$u^2 + 3v^2 = n^3 \qquad (3)$$

where n is odd. It follows from Lemma 6 that u and v can be expressed
in terms of integers r,s as follows

$$u = r^3 - 9 r s^2 = r(r-3s)(r+3s) \qquad v = 3 r^2 s - 3 s^3$$

Also, since v is odd and u is even, we must have r even and s odd.
Further, since u = 4m^3, it's clear that r is 4 times a cube, and
both r-3s and r+3s are cubes. Thus we have

$$r = 4A^3 \qquad r-3s = B^3 \qquad r+3s = C^3$$

and therefore from 2r = (r-3s) + (r+3s) we have

$$(2A)^3 = B^3 + C^3$$

which is a solution of the original equation in strictly smaller
integers. However, by applying the same argument to this new solution
we can construct a strictly smaller solution, and so on, ad infinitum.
This is clearly impossible, since there must be some absolutely
smallest integer solution. Consequently, by Fermat's principle of
infinite descent, we see that solutions with z not divisible by 3
are impossible.

For the second case, suppose z is a multiple of 3. It follows that
u is a multiple of 3, and v is not. In this case we cannot say that
2u is coprime to u^2 + 3v^2, because both are divisible by 3, but
if we factor a 3 out of the quantity in parentheses in (1) we have

$$6u[\, 3(u/3)^2 + v^2 \,] = z^3 \qquad (2)$$

so now 6u is coprime to the quantity in brackets, and so both factors
are cubes, which implies

$$u = 36m^3 \qquad v^2 + 3(u/3)^2 = n^3$$

From Lemma 6 we have coprime integers r,s with s even, such that

$$u/3 = 3r^2 s - 3s^3$$

which implies

$$u = 9s(r+s)(r-s) = 36m^3$$

so we have

$$4m^3 = s(r+s)(r-s)$$

and therefore

$$s = 4A^3 \quad r+s = B^3 \quad r-s = C^3$$

Since $2s + (r-s) = (r+s)$ we have

$$(2A)^3 + C^3 = B^3$$

so again we have a solution in smaller integers, and by the principle of infinite descent, this is impossible. Consequently, we have proven the result

THEOREM: The equation $x^3 + y^3 = z^3$ has no solution in non-zero integers.

سایت ریاضیات مقدماتی و پیشرفته
http://epmath.99k.org/BooksPapers/NumberTheoryNotes.htm

مهدی مفیدی احمدی
15 اسفند 1388

منبع: **http://www.mathpages.com/home/kmath009.htm**