September 5, 2009

Fermat's Last Theorem for Fractional and Irrational Exponents

Frank Morgan
Williams College

Does Fermat's Last Theorem hold for any exponents other than integers greater than two? The theorem says that for integers $n > 2$, there are no solutions to

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

among positive integers. On the first day of my senior seminar on "The Big Questions," the class asked me whether it remains true for rational exponents n. It turns out (see Proposition 4 below) that it does hold for rational exponents, although there are infinitely many irrational exponents for which it fails, that is, for which (1) has a solution among positive integers. For example, since

$$4^2 + 5^2 > 6^2 \quad \text{but} \quad 4^3 + 5^3 < 6^3,$$

by the Intermediate Value Theorem, for some $2 < n < 3$,

$$4^n + 5^n = 6^n.$$

My students tell me that $n \approx 2.487939173$. Of course there are only countably many such exponents, because there are only countably many triples x, y, z of positive integers.

On our new departmental blog [6], I asked whether anyone could find an explicit solution to (1) among positive integers for some n. One of my students, Domenico Aiello, posted infinitely many explicit solutions:

$$k^n + k^n = m^n$$

for $n = \log_{m/k} 2$; for example,

$$4^n + 4^n = 5^n$$

for $n = \log_{5/4} 2 \approx 3.106284$. Such values of n are dense. He asked for explicit examples with all three integers distinct, a challenge that remains open (for $n > 2$).

If you allow $n \le 2$, there are solutions for infinitely many rational values of n. For example,

$$(3^3)^{2/3} + (4^3)^{2/3} = (5^3)^{2/3}.$$

They all have exponent 2/m and come from Pythagorean triples $a^2 + b^2 = c^2$ by putting $x = a^m$, $y = b^m$, $z = c^m$ (or multiples thereof) or more trivially have exponent 1/n and come from some $a + b = c$ (see results below).

Son Ho, a PhD student at the University of Maryland, posted infinitely many explicit solutions to (1) with irrational $n \leq 2$ such as

$$1^n + 2^n = 4^n$$

for $n = \log_2 (1+\sqrt{5})/2 \approx .6942$, by the following proposition (with u=0, v=1, w=2, b=2, a = $(1+\sqrt{5})/2$):

Proposition 1 (Son Ho). *Fix nonnegative integers $u \leq v < w$, $b \geq 2$. Some $1 < a \leq 2$ satisfies*

$$a^u + a^v = a^w. \tag{2}$$

Let $x = b^u$, $y = b^v$, and $z = b^w$, $n = \log_b a$. Then

$$x^n + y^n = z^n. \tag{3}$$

Proof. Since $1^u + 1^v > 1^w$ and $2^u + 2^v \leq 2^{w-1} + 2^{w-1} = 2^w$, for some $1 < a \leq 2$, equation (2) holds and equation (3) follows immediately.

What about negative exponents? The class rediscovered an earlier observation of Thérond ([4], see [3, p. 272]):

Proposition 2 [4]. *Solutions of (1) for negative real exponent $-n$ are in one-to-one correspondence with solutions for positive n.*

Proof. Multiplication by $(xyz)^n$ shows that

$$x^{-n} + y^{-n} = z^{-n} \quad \Leftrightarrow \quad (yz)^n + (xz)^n = (xy)^n$$

and conversely division by $(xyz)^n$ shows that

$$x^n + y^n = z^n \quad \Leftrightarrow \quad (yz)^{-n} + (xz)^{-n} = (xy)^{-n} .$$

Going back and forth introduces common factors, but if you divide out by common factors you get a one-to-one correspondence between "primitive" solutions (without common factors) and hence between all solutions.

For example, since $3^2 + 4^2 = 5^2$,

$$20^{-2} + 15^{-2} = 12^{-2}.$$

Finally Proposition 4 will provide the proof of Fermat (no solutions to (1)) for rational exponents (given Fermat for integer exponents). Andrew Granville (University of Montreal) told me that it follows from the following lemma, which was proved before Fermat's Last Theorem.

Lemma 3 (see [1], [2], [7], and references therein). *For positive integers x, y, z, n, the only solutions to* $x^{1/n} + y^{1/n} = z^{1/n}$ *are the trivial ones* $x = ca^n$, $y = cb^n$, $z = c(a+b)^n$, *for positive integers a, b, c.*

For example,

$$(2^7)^{1/7} + (3^7)^{1/7} = (5^7)^{1/7}.$$

Proof [1]. Let $\alpha = (x/z)^{1/n}$ and $\beta = (y/z)^{1/n}$, so $\alpha + \beta = 1$. Since α^n is rational, the algebraic number α and all its conjugates have the same magnitude and hence lie on a circle about the origin in the complex plane as in Figure 1. Since the same is true for $\beta = 1-\alpha$, they also lie on a circle centered at 1. Two such circles can intersect in at most one real number, so α has no conjugates and must be rational. Similarly β is rational.

Since $\alpha + \beta = 1$, α and β must have the same denominator, relatively prime numerators a, b, and the denominator must be a + b. Consequently

$$(x, y, z) = c\left(a^n, b^n, (a+b)^n\right).$$

Since a and b are relatively prime, c must be an integer.

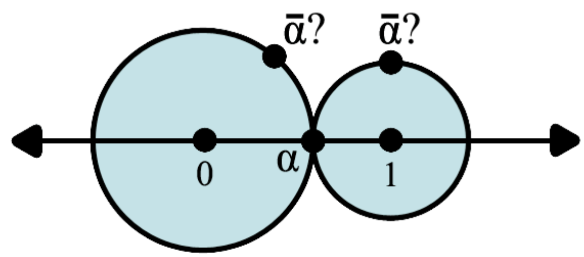

Figure 1. Since circles about 0 and 1 which intersect on the real axis cannot intersect at another point, α can have no conjugates $\bar{\alpha}$ and α must be rational. Figure by Nick Collela.

Proposition 4. *Fermat's Last Theorem holds for rational exponents greater than 2. Indeed, for rational n there are positive integer solutions to*

$$x^n + y^n = z^n$$

if and only if n is of the form ±1/m, ±2/m for positive integers m.

For example,

$$(3^3)^{2/3} + (4^3)^{2/3} = (5^3)^{2/3}.$$

Proof. By Proposition 2, we may assume that n is a positive rational k/m in lowest terms. By Lemma 3, since $(x^k)^{1/m} + (y^k)^{1/m} = (z^k)^{1/m}$,

$$x^k = ca^m, \qquad y^k = cb^m, \qquad z^k = c(a+b)^m,$$

for positive integers a, b, c. We may assume that a and b are relatively prime, by absorbing any common factor into c. Consequently c must be a perfect k^{th} power. Indeed, consider a prime p dividing c. It must fail to divide either a or b, say a. Since $x^k = ca^m$, the power of p dividing c must be a multiple of k. Therefore c must be a perfect k^{th} power: $c = C^k$.

Since k and m are relatively prime, a, b, and a+b must be perfect k^{th} powers:

$$a = A^k, \qquad b = B^k, \qquad a+b = \Gamma^k.$$

Now $x = CA^m$, $y = CB^m$, and $z = C\Gamma^m$. The original equation becomes

$$A^k + B^k = \Gamma^k,$$

and by Fermat's Last Theorem [5], k must be 1 or 2, as desired.

Remark. The proof shows that all such solutions to (1) for n = 2/m come from Pythagorean triples $A^2 + B^2 = \Gamma^2$ by putting $x = CA^m$, $y = CB^m$, $z = C\Gamma^m$.

Summary. Consider the set E of real exponents n for which $x^n + y^n = z^n$ for some positive integers x, y, z. The integers in E are precisely ±1, ±2. The rationals in E are precisely those of the form ±1/m, ±2/m for positive integers m. All of E is dense in **R**, including for example $\log_q 2$ for any positive rational q. It is apparently unknown whether E contains any algebraic irrationals.

Acknowledgements. This article grew out of Morgan's fall 2008 senior seminar on "The Big Questions." For their inspiration and contributions, he would like to thank his students Domenico Aiello, David Aitoro, Alicia Barrett, Pierre Bordeaux Jr, Carl Fred Brasz, Robert Buesing Jr, Davide Carozza, Nicholas Colella, Thomas Coleman, Clara Coughlin, Jonathan Dahlberg, Brian Dolezal, James Wes Johnson, Karin Knudson, Antoaneta Kraeva, Rachel Levy, Richard McDowell, Caitlin McGugan, Hristo Milev, Ralph Morrison, Harris Paseltiner, William A. Schmegel, Deividas Seferis, Bret Thacher, Margaret Tucker, and Corey Watts, TA Christophe Dorsey, and alum Son Ho, now a PhD student at the University of Maryland. Morgan acknowledges partial support from a National Science Foundation research grant.

References

1. H. W. Lenstra, Jr., On the inverse Fermat equation, *Discrete Math.* 106/107 (1992) 329-331.

2. M. Newman, A radical Diophantine equation, *J. Number Theory* 13 (1981) 495-498.

3. Paulo Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, New York, 1979.

4. J. D. Thérond, L'hypothèse de Fermat pour les exposants négatifs, *Enseignement Math.* 12 (1967) 247-252.

5. Andrew Wiles, Modular elliptic curves and Fermat's Last Theorem, *Ann. Math.* 141 (1995) 443–551.

6. Williams College Department of Mathematics and Statistics Blog, math.williams.edu.

7. Zhao Yu Xu, On the Diophantine equation $X^{1/m} + Y^{1/m} = Z^{1/m}$ (Chinese), *Hunan Ann. Math.* 6 (1986) 115-117.

Williamstown, MA 01267
Frank.Morgan@williams.edu

Frank Morgan works in minimal surfaces and has written six books, including The Math Chat Book, based on his former, live, call-in Math Chat TV show and Math Chat column at maa.org. Inaugural winner of the MAA Haimo teaching award, founder of the NSF SMALL Undergraduate Research Project, and a past vice-president of the MAA, he is Atwell Professor of Mathematics at Williams College. As Vice-President of the American Mathematical Society, he has launched the new AMS Graduate Student blog at mathgradblog.williams.edu.

[Picture available at http://math.williams.edu/morgan.]

Brief Descriptive Summary

Fermat's Last Theorem says that for integers n > 2, there are no solutions to

$$x^n + y^n = z^n$$

among positive integers. What about rational exponents n? Irrational n? Negative n? See what an undergraduate senior seminar discovered.

Frank.Morgan@williams.edu

MSC: 11D41

Key words and phrases: Fermat's Last Theorem, fractional exponents, irrational exponents