4-1-2004

Fermat's Last Theorem for Rational Exponents

Curtis D. Bennett
Loyola Marymount University, cbennett@lmu.edu

A. M. W. Glass
Center for Mathematical Sciences

Gábor J. Székely
Bowling Green State University

Fermat's Last Theorem for Rational Exponents

Curtis D. Bennett, A. M. W. Glass, and Gábor J. Székely

1. INTRODUCTION. In this paper, we consider an extension of Fermat's Last Theorem to the case of rational exponents n/m with $n > 2$, an extension that admits complex roots. The use of complex roots allows for curious things to happen. For example, a "new" solution to Fermat's equation in this case is given by

$$1^{5/6} + 1^{5/6} = 1^{5/6}, \tag{1}$$

where the first $1^{5/6}$ is really $(e^{2\pi i})^{5/6} = e^{5\pi i/3}$, the second is $(e^{10\pi i})^{5/6} = e^{\pi i/3}$, and the third is $(e^0)^{5/6} = 1$. Thus the equation becomes the more believable $e^{5\pi i/3} + e^{\pi i/3} = 1$. As equation (1) makes most of us uncomfortable (and certainly leads to confusion), it behooves us to rewrite the equation $a^{n/m} + b^{n/m} = c^{n/m}$ in the form $(a^{1/m})^n + (b^{1/m})^n = (c^{1/m})^n$ and then ask: For what mth roots of positive integers a, b, and c and for what $n > 2$ with $\gcd(m, n) = 1$ do we have $a^n + b^n = c^n$?

Our main theorem is:

Theorem 1. *If m and n are coprime positive integers with $n > 2$, then solutions to $a^{n/m} + b^{n/m} = c^{n/m}$ in positive integers a, b, and c occur only if $a = b = c$, m is divisible by 6, and three different complex 6th roots are used.*

Let

$$S_m = \{z \in \mathbb{C} \mid z^m \in \mathbb{Z}, z^m > 0\},$$

the set of complex mth roots of positive integers. Then S_1 is the set of positive integers. In this notation, our main theorem becomes:

Theorem 2. *For integers n and m with $n > 2$ and $\gcd(m, n) = 1$, the numbers a, b, and c in S_m are such that $a^n + b^n = c^n$ if and only if* (1) 6 *divides m and* (2) *a, b, and c are different complex 6th roots of the same real number.*

Indeed, all solutions are given by triples of the form $(\alpha e^{i\pi/3}, \alpha e^{5i\pi/3}, \alpha)$ where α belongs to S_m or, perhaps more curiously, as triples $(\alpha e^{ni\pi/3}, \alpha e^{-ni\pi/3}, \alpha)$ (since $\gcd(m, n) = 1$ implies that $n \equiv \pm 1 (\mathrm{mod}\ 6)$).

As is standard in problems of this sort, rather than searching for solutions to $a^n + b^n = c^n$, we instead seek solutions to the equivalent equation $(a/c)^n + (b/c)^n = 1$. To this end, for each positive integer m we define

$$T_m = \{z \in \mathbb{C} \mid z^m \in \mathbb{Q}, z^m > 0\}.$$

Theorem 1 is then a corollary to the following theorem:

Theorem 3. *Let m be a positive integer, and let x_1 and x_2 in T_m be such that $x_1 + x_2 = 1$. Then either both x_1 and x_2 are rational, or $x_1 = a_1 e^{\pm i\theta_1}$ and $x_2 = a_2 e^{\mp i\theta_2}$, where a_1, a_2, θ_1, and θ_2 are as in Table 1 in section 4 (of which only the last row gives a solution to Fermat's equation).*

Surprisingly the entries in Table 1 correspond to classical triangles of interest: the equilateral triangle, the 45°-45°-90° triangle, the 30°-60°-90° triangle, and the 30°-30°-120° triangle. Moreover, the proof of this theorem can easily be presented in an abstract algebra class as an application of the fundamental theorem of Galois theory.

The proof of Theorem 3 (and hence the generalization of Fermat's Last Theorem) requires one technical result (using Galois theory) and a basic application of the sine and cosine rules from trigonometry. Of course, to obtain the generalization, we also need Fermat's Last Theorem, proved by Wiles and Taylor in [**9**] and [**6**]. Those interested in reading more about the Wiles-Taylor result will find a beautiful exposition of the problem in [**4**]. We also suggest that readers might find the extension of Fermat's Last Theorem to Gaussian integer exponents given by Zuehlke [**10**] of interest. Tomescu and Vulpescu-Jalea [**7**] consider the rational exponent case (including $n = 1, 2$) but restrict to real roots. The Galois theory argument is similar to the standard methods for reducing the Lang conjecture to the Mordel conjecture. For details the interested reader can consult [**3**].

The proof of Theorem 3 breaks into three main steps. We first treat the real case with a and b in $T_{m,\mathbb{R}} = T_m \cap \mathbb{R}$, the set of reals in T_m; we next prove the technical lemma; and we finish by proving our generalizations of Fermat's Last Theorem. A reader unfamiliar with Galois theory can read section 2 and the statement of Lemma 8 in section 3, and then skip ahead to section 4.

2. THE REAL ROOT CASE.

We begin with a well-known lemma [**5**, Lemma 3.2] on minimal polynomials.

Lemma 4. *If α is algebraic over a field F, then there is a unique monic irreducible polynomial $p_\alpha(X)$ in $F[X]$ such that $p_\alpha(\alpha) = 0$. Moreover, if $f(X)$ is a member of $F[X]$ with $f(\alpha) = 0$, then $p_\alpha(X)$ divides $f(X)$ in $F[X]$.*

We call $p_\alpha(X)$ the *minimal polynomial* for α over F, and note that the degree of the field extension $F(\alpha)$ over F satisfies $[F(\alpha) : F] = \deg(p_\alpha(X))$. In this paper, we shall be concerned primarily with the minimal polynomial for α when α^m lies in $\mathbb{Q}$. As is usual, we use $|\alpha|$ to denote the modulus of the complex number α.

Lemma 5. *If α^m is an element of $\mathbb{Q}$ and $|\alpha^k|$ is not an element of $\mathbb{Q}$ when $k < m$, then $X^m - \alpha^m$ is the minimal polynomial for α over $\mathbb{Q}$.*

Proof. Although this result is well known, we include a proof for the sake of completeness. Let ζ be a primitive mth root of unity. Then

$$X^m - \alpha^m = \prod_{j=1}^{m} (X - \zeta^j \alpha).$$

Let $p_\alpha(X)$ be the minimal polynomial for α over $\mathbb{Q}$. By Lemma 4, $p_\alpha(X) = \sum_{t=0}^{r} b_t X^t$ divides $X^m - \alpha^m$. The constant term b_0 of $p_\alpha(X)$ is a product of r roots of $X^m - \alpha^m$ by the unique factorization theorem for polynomials over $\mathbb{Q}$ [**5**, Theorem 2.3]. Hence $b_0 = \zeta^t \alpha^r$ for some integers t and r. As b_0 is rational and $|b_0| = |\alpha^r|$, it follows that $|\alpha^r|$ is rational as well. Thus by hypothesis $r \geq m$, implying that $p_\alpha(X) = X^m - \alpha^m$. ∎

We now prove the real version of Theorem 3, an important step in establishing the full complex version of the theorem.

Proposition 6. *Let m be a positive integer. If a and b are elements of $T_{m,\mathbb{R}}$ such that $a + b = 1$, then a and b are rational.*

Proof. Let k be the smallest positive integer such that $|a^k| = \pm a^k$ belongs to $\mathbb{Q}$. By Lemma 5, $p_a(X) = X^k - a^k$ and $[\mathbb{Q}(a) : \mathbb{Q}] = k$. Because $b = 1 - a$, it follows that $[\mathbb{Q}(b) : \mathbb{Q}] = k$ also. Consequently, k is the minimal positive integer such that $|b^k|$ is rational, and $p_b(X) = X^k - b^k$ belongs to $\mathbb{Q}[x]$. We observe that $a = 1 - b$ is a root of $(1 - X)^k - b^k$. On the basis of Lemma 4 we conclude that $X^k - a^k$ divides $(1 - X)^k - b^k$. Both of these polynomials have the same degree, and hence they differ by a constant multiple. This happens only if $k = 1$, for the second polynomial always has a linear term. Thus a and b are rational. ∎

At this point we can state a real version of Theorem 1 (see [7]).

Proposition 7. *Let m and n be relatively prime positive integers with $n > 2$. Then $a^n + b^n = 1$ has no solutions with a and b in $T_{m,\mathbb{R}}$.*

Proof. By way of contradiction assume a and b in $T_{m,\mathbb{R}}$ are such that $a^n + b^n = 1$. As $(a^n)^m$ and $(b^n)^m$ are both rational, Proposition 6 implies that a^n and b^n are rational. Since a^n and a^m are both rational, we deduce that $a^{\gcd(m,n)} = a$ is rational. A similar argument shows that b is rational. Consequently, $a^n + b^n = 1$ for rational numbers a and b, contrary to Fermat's Last Theorem. ∎

3. A GALOIS INTERLUDE. Allowing for complex roots adds difficulties that Galois theory will help us to circumvent. If $a^n + b^n = 1$ and $[\mathbb{Q}(a, b) : \mathbb{Q}] > 1$, then acting upon the pair (a, b) by an element of the Galois group yields other solutions. Thus our main goal in this section is to use Galois theory to identify a constraint on elements of mth cyclotomic fields whose nth powers are rational.

Lemma 8. *Let m and n be positive integers. Suppose that a is a real number in the extension field $\mathbb{Q}(e^{2\pi i/m})$ such that a^n is rational. Then a^2 is also rational.*

The proof of Lemma 8 is the one place in the paper where we need Galois theory, and the reader who already knows this lemma or is willing to take it on faith can safely skip ahead to section 4. To prove Lemma 8, we rely on the following three results from Galois theory, all of which can be found in [5]. Kummer established the first of these lemmas [5, Lemma 14.3] specifically to study Fermat's Last Theorem, Lemma 9 [5, Theorem 11.1] is the "Fundamental Theorem of Galois Theory," and Lemma 10 [5, Theorem 8.1] is important for keeping track of the roots of polynomials.

Galois theory is a typical tool in number-theoretic existence proofs. Some of the basic ideas of the theory can be traced back to J. L. Lagrange's booklet "Réflexions sur la résolution algebraique des équations" (1770–1771). In 1832 Galois developed a general theory for deciding which algebraic equalitions are "solvable" in the sense that their roots can be expressed in terms of their coefficients. Moreover, in case a concrete equation is solvable, then with the help of the Galois theory we can construct its "solutions." (For information about the interesting life of Evariste Galois see [2].) On March 30, 1796, an important special case of Galois theory was found by C. F. Gauss when he proved the constructibility of the regular 17-gon. In the past two centuries Galois theory has changed the landscape of algebra and become an indispensable tool in many existence proofs. We intend to exploit this tool. The two key insights of Galois that we use are the splitting field of a polynomial and what is now called the

Galois group of a field extension. The *splitting field* of a polynomial $p(x)$ over a field F is a smallest extension field K of F such that $p(x)$ factors into linear polynomials over K. The *Galois group* $\mathrm{Gal}(K/F)$ of an extension field K of F is the set of all field automorphisms of K that fix every element of F.

Lemma 9. *Let m be a positive integer, and let $K = \mathbb{Q}(e^{2\pi i/m})$ be the extension field of $\mathbb{Q}$ generated by adjoining $e^{2\pi i/m}$. Then $\mathrm{Gal}(K/\mathbb{Q})$ is Abelian.*

Lemma 10. *If F is a field, K is the splitting field of some polynomial over F, and L is an intermediate field ($F \subseteq L \subseteq K$), then L is the splitting field of a polynomial over F if and only if $\mathrm{Gal}(K/L)$ is a normal subgroup of $\mathrm{Gal}(K/F)$.*

Lemma 11. *Let K be the splitting field of some polynomial over F. If $p(X)$ is an irreducible polynomial in $F[X]$ that has at least one root in K, then all roots of $p(X)$ lie in K.*

Proof of Lemma 8. Let m and n be arbitrary positive integers, and suppose that a is a real number in $K = \mathbb{Q}(e^{2\pi i/m})$ such that a^n is rational. The Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$ is Abelian (Lemma 9). Consequently, every subgroup of G is normal in G. In particular, if $F = K \cap \mathbb{R}$, then $\mathrm{Gal}(K/F)$ is normal in $\mathrm{Gal}(K/\mathbb{Q})$. From the fundamental theorem of Galois theory it follows that F is the splitting field of some polynomial in $\mathbb{Q}[X]$.

Let k be the smallest positive integer such that a^k lies in $\mathbb{Q}$. By Lemma 5, the minimal polynomial for a over $\mathbb{Q}$ is $X^k - a^k$, hence this polynomial is irreducible over $\mathbb{Q}$. As a belongs to F, Lemma 11 implies that all the roots of $X^k - a^k$ are in F. Since F is a subfield of the real numbers, this ensures that every root of $X^k - a^k$ is real. Thus k is at most 2, and a^2 is rational as desired. ∎

We note that we could replace the first paragraph of the foregoing proof (and hence avoid the use of the fundamental theorem of Galois theory) by showing directly that the monic polynomial

$$\prod_{\substack{1\le k\le m/2\\ \gcd(k,m)=1}} \left(X - 2\cos\left(\frac{2k\pi}{m}\right)\right)$$

has integer coefficients (as done in [**8**]), thereby establishing that $F = \mathbb{Q}[\cos(2\pi/m)]$ is a splitting field. This method avoids Galois theory but is somewhat complicated. Because one of our goals is to provide a treatment of this problem that can be presented in an undergraduate abstract algebra class, we opted for the proof that we have given.

4. THE MAIN RESULT. For the proof of the main result, we need a lemma concerning the rational values that can be taken by $\cos(2k\pi/m)$. In particular, we record:

Lemma 12. *Suppose that k and m are positive integers. If $\cos(2k\pi/m)$ is a rational number, then $2\cos(2k\pi/m)$ is an integer.*

Proof. Let $\alpha = 2k\pi/m$. By basic manipulations, one can establish the recurrence relation

$$2\cos(n\alpha) = 2\cos\big((n-1)\alpha\big) \cdot 2\cos\alpha - 2\cos\big((n-2)\alpha\big)$$

(see [**1**, p. 137]). An easy induction argument then establishes that

$$2 = 2\cos(m\alpha) = \sum_{j=0}^{m} a_j (2\cos\alpha)^j,$$

where $a_m = 1$ and a_j is an integer for $j = 0, 1, \ldots, m$. Thus $2\cos\alpha$ is a root of a polynomial with leading coefficient 1. If $2\cos\alpha = p/q$, the rational root test implies that $q = 1$, so $2\cos\alpha$ is an integer. ∎

We are now ready to prove Theorem 3.

Proof of Theorem 3. Consider elements x_1 and x_2 of T_m with $x_1 + x_2 = 1$. If x_1 and x_2 are real, then Proposition 6 implies the result. Hence we may assume that either x_1 or x_2 is not real; since their sum is 1, we may further assume that neither is real. Using the polar representation of complex numbers we write $x_1 = a_1 e^{i\psi_1}$ and $x_2 = a_2 e^{i\psi_2}$, where a_1 and a_2 are positive real numbers and $-\pi \le \psi_1, \psi_2 < \pi$. Since $\mathrm{Im}(x_1 + x_2) = 0$, $\sin\psi_1$ and $\sin\psi_2$ have opposite signs. Accordingly, for one of the js we have $0 \le \psi_j < \pi$, while for the other $-\pi < \psi_j \le 0$. Relabeling x_1 and x_2 if necessary, we may assume that $0 \le \psi_1 \le \pi$. At this point, we let $\theta_1 = \psi_1$ and $\theta_2 = -\psi_2$, so that $x_1 = a_1 e^{i\theta_1}$ and $x_2 = a_2 e^{-i\theta_2}$. Recalling that x_j^m is a rational number ($j = 1, 2$), we infer that a_j belongs to $T_{m,R}$ and $\theta_j = 2k_j\pi/(2m)$ for some integers k_j. In this new notation, we have

$$a_1 e^{i\theta_1} + a_2 e^{-i\theta_2} = 1.$$

Figure 1 represents this complex addition graphically, with the point in the first quadrant $a_1 e^{i\theta_1}$, the point in the fourth quadrant $a_2 e^{i\theta_2}$, and the dashed line representing translation of the second vector to form the vector sum of the two complex numbers, which is equal to 1.

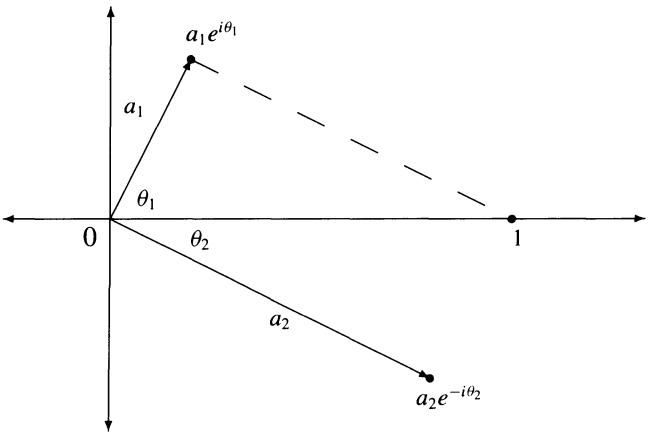

Figure 1. Complex plane representation of $x_1^n + x_2^n$.

Concentrating on the part of this figure lying in the first quadrant, we have a triangle with side-lengths the moduli of x_1, x_2, and 1 and angles given by θ_1, θ_2, and $\theta_0 = \pi - \theta_1 - \theta_2$, as in Figure 2.

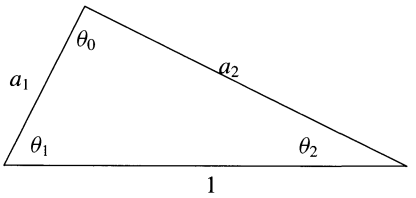

Figure 2. Triangle associated to vector sum.

Since the sum of the angles of the triangle is π, $\theta_0 = 2k_0\pi/2m$ for some integer k_0. By the law of sines, $a_2/1 = \sin\theta_1/\sin\theta_0$ and $a_1/1 = \sin\theta_2/\sin\theta_0$. Now $\sin\theta_j$ lies in $\mathbb{Q}(e^{2\pi i/4m})$, for $\sin\theta_j = (e^{i\theta_j} + e^{-i\theta_j})/2i$ and i is a fourth root of unity. Hence a_j belongs to $\mathbb{Q}(e^{2\pi i/4m}) \cap \mathbb{R}$. Lemma 8 then implies that both a_1^2 and a_2^2 are rational. We next apply the law of cosines to our triangle to obtain:

$$\begin{aligned} 1^2 &= a_1^2 + a_2^2 - 2a_1a_2\cos\theta_0, \\ a_2^2 &= a_1^2 + 1^2 - 2a_1\cos\theta_1, \\ a_1^2 &= a_2^2 + 1^2 - 2a_2\cos\theta_2. \end{aligned}$$

The first equation yields $\cos\theta_0 = (a_1^2 + a_2^2 - 1)/(2a_1a_2)$. As a_1^2 and a_2^2 are rational, it follows that $\cos(2\theta_0) = (2\cos^2\theta_0) - 1$ is rational. Consequently, $2\cos(2\theta_0)$ is an integer (Lemma 12). Similarly, $2\cos(2\theta_1)$ and $2\cos(2\theta_2)$ are integers. Hence $2\cos(2\theta_j) \in \{0, \pm1, \pm2\}$ for $j = 0, 1, 2$. Since $0 < \theta_j < \pi$ (for $j = 0, 1, 2$), we have $\theta_j = p_j\pi/12$, where $p_j \in \{2, 3, 4, 6, 8, 9, 10\}$. As $\theta_0 + \theta_1 + \theta_2 = \pi$, the possibilities for (θ_1, θ_2) under the assumption that $\theta_1 \geq \theta_2$ reduce to a short list:

$$\left(\frac{2\pi}{3}, \frac{\pi}{6}\right), \left(\frac{\pi}{6}, \frac{\pi}{6}\right), \left(\frac{\pi}{4}, \frac{\pi}{4}\right), \left(\frac{\pi}{2}, \frac{\pi}{4}\right), \left(\frac{\pi}{2}, \frac{\pi}{3}\right), \left(\frac{\pi}{2}, \frac{\pi}{6}\right), \left(\frac{\pi}{3}, \frac{\pi}{6}\right), \left(\frac{\pi}{3}, \frac{\pi}{3}\right).$$

All of these correspond to one of the classical triangles (i.e., the 30°-30°-120° triangle, the 45°-45°-90° triangle, the 30°-60°-90° triangle, or the equilateral triangle).

Solving these triangles, we arrive at the following list:

Table 1.

Triangle type	θ_1	θ_2	a_1	a_2
30°-30°-120°	$2\pi/3$	$\pi/6$	1	$\sqrt{3}$
	$\pi/6$	$\pi/6$	$1/\sqrt{3}$	$1/\sqrt{3}$
45°-45°-90°	$\pi/2$	$\pi/4$	1	$\sqrt{2}$
	$\pi/4$	$\pi/4$	$1/\sqrt{2}$	$1/\sqrt{2}$
30°-60°-90°	$\pi/2$	$\pi/3$	$\sqrt{3}$	2
	$\pi/2$	$\pi/6$	$1/\sqrt{3}$	$2/\sqrt{3}$
	$\pi/3$	$\pi/6$	1/2	$\sqrt{3}/2$
equilateral	$\pi/3$	$\pi/3$	1	1

This completes the proof of Theorem 3. (N.B. We use the upper sign in $x_1 = e^{\pm i\theta_1}$ and $x_2 = e^{\mp i\theta_2}$ when $\theta_1 \geq \theta_2$ and the lower sign in the other case.) ∎

We are now ready to prove Theorem 2, our generalization of Fermat's Last Theorem. For the sake of simplicity, we restate it in slightly modified form here.

Theorem 13. *Let m and n be relatively prime positive integers with $n > 2$. There exist x and y in T_m such that $x^n + y^n = 1$ if and only if 6 divides m, in which case $x^m = y^m = 1$. In other words, there exist x, y, and z in S_m such that $x^n + y^n = z^n$ if and only if 6 divides m, and in this case $x^m = y^m = z^m$.*

Proof. Suppose that x and y are members of T_m with $x^n + y^n = 1$. Let $\gamma = x^n$ and $\beta = y^n$. Since $\gamma^m = (x^n)^m = (x^m)^n$ is rational and positive, it follows that γ belongs to T_m. Similarly, β is in T_m, and $\gamma + \beta = 1$. Relabeling γ and β if necessary, we deduce from Theorem 3 that either both γ and β are rational or $\gamma = a_1 e^{i\theta_1}$ and $\beta = a_2 e^{-i\theta_2}$ for some choice of a_1, a_2, θ_1, and θ_2 from Table 1. If γ is rational, then x^m and x^n are also rational, whence $x = x^{\gcd(m,n)}$ is rational. A similar argument shows that y is rational. But $x^n + y^n = 1$, in contradiction with Fermat's Last Theorem. Thus we may assume that γ and β come from values provided by Table 1.

Since $a_2^{m/n} = |y^m|$ is rational, a_2^m is the nth power of some rational number. However, by inspection of the values in Table 1, this only happens if either $\gcd(m, n) = n$ or $a_1 = a_2 = 1$ and $\theta_1 = \theta_2 = \pi/3$. By hypothesis, $n > 2$ and $\gcd(m, n) = 1$, so the former case is impossible. In the latter case, $\gamma = e^{i\pi/3}$ and $\beta = e^{i\pi/3}$, and the fact that γ is a member of T_m implies that $e^{mi\pi/3}$ is a positive rational number, whence m is divisible by 6 and $\gamma^m = \beta^m = 1$. Since $x^m = \gamma^{m/n}$ is a rational positive nth root of unity, $x^m = 1$, and similarly $y^m = 1$, as desired.

We can further restrict x and y using $\gamma = e^{i\pi/3}$ and conclude that

$$x = \gamma^{1/n} = e^{(6k+1)i\pi/3n}$$

for some choice of k. As $\gcd(m, n) = 1$ and x^m is rational, it follows that $6k + 1$ must be divisible by n. Consequently, this choice of k is unique modulo n, so that x is unique. A similar argument demonstrates that y is unique.

On the other hand, if $m = 6l$, let $x = e^{ni\pi/3}$ and $y = e^{-in\pi/3}$. Then $x^m = e^{2inl\pi} = 1$ and similarly $y^m = 1$, placing x and y in T_m. Now the assumption $\gcd(m, n) = 1$ implies that $\gcd(6, n) = 1$, and thus that $n^2 \equiv 1 (\mathrm{mod}\ 6)$. It follows that $x^n + y^n = e^{i\pi/3} + e^{-i\pi/3} = 1$. Thus x and y furnish the unique (up to interchanging x and y) solutions of $x^n + y^n = 1$ with x and y in T_m. ∎

ACKNOWLEDGMENTS. The authors gratefully thank the anonymous referees for their numerous helpful suggestions leading to the improvement of this article.

REFERENCES

1. W. Beyer, ed., *CRC Standard Mathematical Tables*, CRC Press, Boca Raton FL, 1981.
2. L. Infeld, *Whom the Gods Love*, Whittlesey House, New York, 1948.
3. S. Lang, *Fundamentals of Diophantine Geometry*, Springer-Verlag, New York, 1983.
4. P. Ribenboim, *Fermat's Last Theorem for Amateurs*, Springer-Verlag, New York, 1999.
5. I. Stewart, *Galois Theory*, 2nd ed., Chapman & Hall, London, 1989.
6. R. Taylor and A. Wiles, Ring-theoretic properties of certain Hecke algebras, *Ann. Math.* **141** (1995) 553–572.
7. D. Tomescu and F. Vulpescu-Jalea, On the Fermat's equation with rational exponents, *Bull. Math. Soc. Sci. Math R.S. Roumanie (N.S.)* **34** (**82**) (1990) 187–192.
8. W. Watkins and J. Zeitlin, The minimal polynomial of $\cos(2\pi/n)$, this MONTHLY **100** (1993) 471–474.
9. A. Wiles, Modular elliptic curves and Fermat's last theorem, *Ann. Math.* **141** (1995) 443–551.
10. J. Zuehlke, Fermat's last theorem for Gaussian integer exponents, this MONTHLY **106** (1999) 49.

CURTIS BENNETT received his Ph.D. in 1990 from the University of Chicago. He was a faculty member at Bowling Green State University before moving to Loyola Marymount University in 2002, where he is currently an associate professor. His main mathematical interests are in group theory and combinatorics, although he harbors a passion for number theory. In addition, Bennett is a CASTL Fellow with the Carnegie Academy for the Scholarship of Teaching and Learning, where he has been studying the teaching and learning of future mathematics teachers.
Department of Mathematics, Loyola Marymount University, Los Angeles, CA 90045
cbennett@lmu.edu

A. M. W. GLASS was an exhibitioner and scholar at Downing College, Cambridge, where he received his B.A. (Cantab) and M.A. (Cantab). Glass received his Ph.D. from the University of Wisconsin-Madison and taught at Bowling Green State University in Ohio. In 1997, Glass returned to England. He is now a college lecturer and fellow of Queens' College, Cambridge, an honourary professor at Chonqing University of Posts and Telecommunications, and a professor emeritus from BGSU. Glass has written books on infinite permutation groups and partially ordered groups, and authored many papers in algebra, logic, and number theory.
Department of Pure Mathematics & Mathematical Statistics, Center for Mathematical Sciences, Wilberforce Rd., Cambridge CB3 0WB, England
amwg@dpmms.cam.ac.uk

GÁBOR SZÉKELY received his Ph.D. from ELTE, Budapest, and the Doctor of Science degree from the Hungarian Academy of Sciences. He is a professor at both Bowling Green State University and ELTE and a senior researcher of the Rényi Institute of the Hungarian Academy of Sciences. Between 1985 and 1995 he was the Program Manager of the Budapest Semesters in Mathematics. Székely is a past chair of the Department of Stochastics of the Budapest Institute of Technology and recipient of the Rollo Davidson Prize (Cambridge). His publications include the monographs *Paradoxes in Probability Theory and Statistics* (Reidel, 1986) and *Algebraic Probability Theory* (with I.Z. Ruzsa, Wiley, 1988).
Department of Mathematics and Statistics, Bowling Green State University, Bowling Green, OH 43403
gabors@bgnet.bgsu.edu