

King Fahd University of Petroleum & Minerals

DEPARTMENT OF MATHEMATICAL SCIENCES

Technical Report Series

TR291

April 2003

A Generalization of Fermat's Last Theorem

A. Laradji

DHAHRAN 31261 • SAUDI ARABIA • www.kfupm.edu.sa/math/ • E-mail: mathdept@kfupm.edu.sa

A Generalization of Fermat's Last Theorem

A. Laradji

The aim of this paper is to initiate a study of those complex numbers u such that $x^u + y^u = z^u$ is solvable in positive integers x, y, z. Our first step is to prove the following generalization of Fermat's Last Theorem.

Proposition 1. Let $u = \frac{m}{n} + is \in \mathbb{Q} + i (\mathbb{A} \cap \mathbb{R})$ where m and n are coprime integers with n > 0 and \mathbb{A} is the set of algebraic numbers. Then the equation $x^u + y^u = z^u$, is solvable in positive integers x, y, z if and only if $s = 0, m = \pm 1$ or ± 2 . Moreover, if m > 0 then $x = d\alpha^n, y = d\beta^n, z = d\gamma^n$, where α, β, γ are positive integers with $gcd(\alpha, \beta) = 1$ and $\alpha^m + \beta^m = \gamma^m$; and if m < 0 then $x = d\beta^n \gamma^n, y = d\alpha^n \gamma^n, z = d\alpha^n \beta^n$ for some positive integers d, α, β, γ such that $gcd(\alpha, \beta) = 1$ and $\alpha^{-m} + \beta^{-m} = \gamma^{-m}$.

In the second part of this note we address the following analytic problem (P).

Given any positive real numbers r and ε , does there exist a real number s with $|s-r| < \varepsilon$ for which $a^s + b^s = c^s$ is solvable in positive integers a, b, c?

Let us first recall some basic definitions. Any root of a nonzero polynomial with integer (or rational) coefficients is called an *algebraic number*, and the set \mathbb{A} of all such roots is a subfield of \mathbb{C} . Complex numbers that are not algebraic are called *transcendental*. A is an *algebraically closed* field, that is, all the roots of any nonzero polynomial with coefficients in \mathbb{A} are algebraic. If $t \in \mathbb{A}$ then there is a unique monic polynomial of least positive degree over \mathbb{Q} for which t is a root. Such a polynomial is called the *minimal polynomial* of t over \mathbb{Q} . Note that every nonconstant polynomial over \mathbb{Q} can be expressed as a product of linear factors over \mathbb{A} . We say that the complex numbers z_1, \ldots, z_n are \mathbb{Q} -linearly independent if, whenever q_1, \ldots, q_n are rational numbers for which the linear combination $\sum_{j=1}^n q_j z_j$ is 0, then each $q_j = 0$. Throughout, when x is a positive real number and $y \in \mathbb{C}$, $x^y = e^{y \log x}$, in the sense of principal values, and for any set $\{a_1, a_2, \ldots, a_n\}$ of nonzero integers, $gcd(a_1, a_2, \ldots, a_n)$ is simply denoted (a_1, a_2, \ldots, a_n) . For completeness, we include two theorems needed for the proof of Proposition 1. The first one follows, of course, from Fermat's Last Theorem proved by A. Wiles. The second, which provides a solution to Hilbert's seventh problem¹, was proved by Gelfond and Schneider, independently, in 1934. (See [1], for example.)

Theorem 2. Let $m \in \mathbb{Z}$. Then the equation $a^m + b^m = c^m$ is solvable in positive integers a, b, c if and only if $m = \pm 1$ or ± 2 .

Theorem 3. If $\alpha_1, \ldots, \alpha_k \in \mathbb{A} \setminus \{0, 1\}$ and $\beta_1, \ldots, \beta_k \in \mathbb{A}$ are such that $1, \beta_1, \ldots, \beta_k$ are \mathbb{Q} -linearly independent, then $\alpha_1^{\beta_1} \ldots \alpha_k^{\beta_k}$ is transcendental.

To prove Proposition 1, we first establish a few lemmas. The first is straightforward, but we include it for easy reference.

Lemma 4. The positive integers a, b, m, n satisfy $a^m = b^n$ if and only if there exists $r \in \mathbb{N}$ such that $a = r^{n/(m,n)}$ and $b = r^{m/(m,n)}$.

Proof. 'If' is clear. Next, let $m = d\mu, n = d\nu$ with $(\mu, \nu) = 1$. Then $a^m = b^n$ implies $a^{\mu} = b^{\nu}$, so that if $a = \prod_{1 \le j \le t} q_j^{a_j}$ and $b = \prod_{1 \le j \le t} q_j^{b_j}$ are prime power decompositions with $a_j, b_j \in \mathbb{N}$, then $\mu a_j = \nu b_j$ $(1 \le j \le t)$. Since μ, ν are coprime, each a_j is divisible by ν and there exist τ_j in \mathbb{N} such that $a_j = \tau_j \nu$, $b_j = \tau_j \mu$. Therefore, for some $r \in \mathbb{N}$, $a = r^{n/(m,n)}$ and $b = r^{m/(m,n)}$.

The following lemmas say more than we need for the proof of Proposition 1, but appear to be of independent interest.

Lemma 5. Let $x, y \in \mathbb{A} \cap \mathbb{R}^+$, $r, s \in \mathbb{A} \cap \mathbb{R}$ be such that $x^{ir}y^{is} \in \mathbb{A}$; then $x^ry^s = 1$.

Proof. If x = y = 1 or r = s = 0 then there is nothing to prove. We therefore assume that at least one of x, y is not equal to 1 and that not both r and s are zero. By Theorem 3, 1, ir, is are \mathbb{Q} -linearly dependent, and so there exist α, β, γ in \mathbb{Q} , not all zero, such that $\alpha + (\beta r + \gamma s)i = 0$, i.e. $\alpha = \beta r + \gamma s = 0$. Thus for some integers m, n, not both zero, mr + ns = 0. If s = 0 then $x^{ir} \in \mathbb{A}$ and so, by Theorem 3 again, x = 1 (since $ir \in \mathbb{A} \setminus \mathbb{Q}$) which means that $x^r y^s = 1$. If $s \neq 0$

¹An early version of this problem was already raised by Euler

then $(x^r y^s)^{im} = x^{irm} y^{ism} = x^{-isn} y^{ism} = (x^{-n} y^m)^{is} \in \mathbb{A}$, and since $x^{-n} y^m \in \mathbb{A}$ and $is \in \mathbb{A} \setminus \mathbb{Q}$, we get $x^{-n} y^m = 1$. Thus $(x^r y^s)^m = (x^{-n} y^m)^s = 1$ and $x^r y^s = 1$. \Box

Lemma 6. Suppose that $Ax^{ir} + By^{is} = Cz^{it}$ where $x, y, z \in \mathbb{A} \cap \mathbb{R}^+$, $r, s, t \in \mathbb{A} \cap \mathbb{R}$ and A, B, C are real numbers such that $\frac{A^2 + B^2 - C^2}{AB} \in \mathbb{A}$. Then

- (i) $x^r = y^s$ and A + B = C,
- (ii) either C = 0 or $x^r = y^s = z^t$,
- (iii) if x and y are coprime positive integers then $x^r = y^s = z^t = 1$.

Proof. Put $\alpha = r \log x$, $\beta = s \log y$, $\gamma = t \log z$, so that $Ax^{ir} + By^{is} = Cz^{it}$ can be written as $A \cos \alpha + B \cos \beta = C \cos \gamma$ and $A \sin \alpha + B \sin \beta = C \sin \gamma$. Squaring both sides of these last equations and adding gives $\cos(\alpha - \beta) = \frac{C^2 - A^2 - B^2}{2AB} \in \mathbb{A}$. Put $\tau = x^{ir}y^{-is}$, then $\tau = e^{(\alpha-\beta)i}$ and $\tau^2 - 2\cos(\alpha-\beta)\tau + 1 = 0$ so that $\tau \in \mathbb{A}$. By Lemma 5, $x^r = y^s$ and $(A+B)x^{ir} = Cz^{it}$. Suppose that $A+B \neq C$, then $C \neq 0$ and $e^{(\gamma-\alpha)i} = x^{-ir}z^{it} = \frac{A+B}{C} \in \mathbb{R}$, which implies that $x^{-ir}z^{it} = \frac{A+B}{C} = -1 \in \mathbb{A}$. By Lemma 5 again $x^r = z^t$, and hence $(A + B - C)x^{ir} = 0$, a contradiction. This proves (i). We now have $Cx^{ir} = Cz^{it}$, so that when $C \neq 0$ $x^{ir}z^{-it} = 1$ which implies that $x^r = z^t$, and (ii) follows. Assume that x, y are coprime integers greater than 1, then, by Theorem 3 and since $x^r y^{-s} = 1 \in \mathbb{A}, 1, r, s$ are Q-linearly dependent, i.e. there are integers m, n, p not all zero such that m+nr+ps=0. Hence $1=x^{pr}y^{-ps}=(x^py^n)^ry^m$ which implies that $(x^p y^n)^r \in \mathbb{A}$. If $x^p y^n \neq 1$, then r and therefore s is rational, and this happens only if r = s = 0 as x, y are coprime and positive. If $x^p y^n = 1$ then $y^m = 1$ and either y = 1 and (iii) holds, or m = 0 and at least one of n, p is nonzero, which implies, again as x, y are coprime and positive, that x = 1 or y = 1. So, in all cases, (iii) follows.

Lemma 7. Suppose that $Ax^{\frac{1}{m}} + By^{\frac{1}{n}} = z^{\frac{1}{p}}$, where A, B are nonzero rational numbers and $m, n, p \in \mathbb{N}$, is solvable in positive integers x, y, z. Then there exist positive integers a, b, β such that (a, b) = 1, $x = b^m \beta^{\frac{m}{(m,n,p)}}$, $y = a^n \beta^{\frac{n}{(m,n,p)}}$, $z = (Ab + Ba)^p \beta^{\frac{p}{(m,n,p)}}$. In particular, $x^{\frac{1}{m}}, y^{\frac{1}{n}}, z^{\frac{1}{p}} \in \mathbb{N}$ when (x, y) = 1 or (m, n, p) = 1.

Proof. Let $t = \frac{x^{\frac{1}{m}}}{y^{\frac{1}{n}}}$, $v = t^{mn}$ and $w = \left(t + \frac{B}{A}\right)^{pn}$, so that v and w are both rational numbers. Clearly t is a zero of the polynomials $X^{mn} - v$ and $\left(X + \frac{B}{A}\right)^{pn} - v$

w. We have, over \mathbb{A} , $X^{mn} - v = \prod_{0 \le j \le mn-1} (X - \varepsilon_j t)$, and $\left(X + \frac{B}{A}\right)^{\mu} - w =$ $\prod_{0 \le h \le pn-1} \left(X + \frac{B}{A} - \varepsilon'_h \left(t + \frac{B}{A} \right) \right), \text{ where the } \varepsilon_j = e^{\frac{2\pi i j}{mn}} \text{ are the } mn\text{-th roots of }$ unity and the $\varepsilon'_h = e^{\frac{2\pi i h}{pn}}$ are the *pn*-roots of unity. The minimal polynomial of t over $\mathbb{Q} \text{ is } \prod_{0 \le k \le d-1} (X - \varepsilon_{j_k} t) \text{ for some subset } \{j_k : 0 \le k \le d-1\} \text{ of } \{0, 1, \dots, mn-1\},\$ and is also $\prod_{0 \le k \le d-1} \left(X + \frac{B}{A} - \varepsilon'_{h_k} \left(t + \frac{B}{A} \right) \right)$ for some subset $\{h_k : 0 \le k \le d-1\}$ of $\{0, 1, \dots, pn-1\}$. We claim that $t \in \mathbb{Q}$. Assume to the contrary that $t \notin$ Then, by the uniqueness of minimal polynomials and of factorization in $\mathbb{A}[X]$, $X - \varepsilon_{\mu}t = X + \frac{B}{A} - \varepsilon_{\nu}'\left(t + \frac{B}{A}\right) \text{ for some } \mu \text{ and } \nu \text{ such that } 1 \le \mu < mn, 0 \le \nu < pn.$ This implies $t\left(e^{\frac{2\pi i\nu}{pn}} - e^{\frac{2\pi i\mu}{mn}}\right) = \frac{B}{4}\left(1 - e^{\frac{2\pi i\nu}{pn}}\right)$. Using the identity $e^{2\pi if} - e^{2\pi ig} =$ $2ie^{\pi i(f+g)}\sin\pi(f-g)$, we obtain $te^{\frac{2\pi i\mu}{mn}}\sin\pi\left(\frac{\nu}{pn}-\frac{\mu}{mn}\right) = -\frac{B}{A}\sin\frac{\pi\nu}{pn}$. Now $t \neq 0$, so that $\sin \pi \left(\frac{\nu}{m} - \frac{\mu}{mn}\right) \cdot \sin \frac{\pi \mu}{mn} = 0$, and since $B \neq 0$ and $1 \leq \mu \leq mn$, we get $\sin \frac{\pi \nu}{pn} = 0$. Thus $pn \mid \nu$, i.e. $\nu = 0$, as $0 \le \nu < pn$. But this means $\sin \frac{\pi \mu}{mn} = 0$, which is impossible. Hence $t = \frac{x^{\frac{1}{m}}}{u^{\frac{1}{n}}} \in \mathbb{Q}$ and there exist coprime positive integers a, b such that $ax^{\frac{1}{m}} = by^{\frac{1}{n}}$, i.e. $a^{mn}x^n = b^{mn}y^m$. Since a and b are coprime, there exist c, d in N such that $x = b^m c$ and $y = a^n d$. This implies that $c^n = d^m$, so that by Lemma 4, $c = \alpha^{\mu'}$ and $d = \alpha^{\nu'}$ for some $\alpha, \mu', \nu' \in \mathbb{N}$ with $(\mu', \nu') = 1$. Hence $x^{\frac{1}{m}} = b\alpha^{\frac{1}{\delta}}$ and $y^{\frac{1}{n}} = a\alpha^{\frac{1}{\delta}}$. This gives $(Ab + Ba)^p \alpha^{\frac{p}{\delta}} = z$, i.e. $\alpha^{\frac{p}{\delta}} \in \mathbb{Q}$. This implies that for some coprime positive integers u, v we have $v\alpha^{\frac{p}{\delta}} = u$, from which we get v = 1 and $\alpha^{\frac{p}{\delta}} = l$ for some $l \in \mathbb{N}$. Hence $\alpha^p = l^{\delta}$ and by Lemma 4, there exists $\beta \in \mathbb{N}$ such that $\alpha = \beta^{\frac{\delta}{(m,n,p)}}$ and $l = \beta^{\frac{p}{(m,n,p)}}$. We then obtain that $x^{\frac{1}{m}} = b\beta^{\frac{1}{(m,n,p)}}, y^{\frac{1}{n}} = a\beta^{\frac{1}{(m,n,p)}}$ $z^{\frac{1}{p}} = (Ab + Ba) \beta^{\frac{1}{(m,n,p)}}$. Clearly $\beta^{\frac{\min(m,n)}{(m,n,p)}}$ divides both x and y, so if (x,y) = 1 then $\beta = 1$, and $x^{\frac{1}{m}}, y^{\frac{1}{n}} \in \mathbb{N}$. In this case $z^{\frac{1}{p}} = (Ab + Ba) \in \mathbb{Q}$, so that, since $z \in \mathbb{N}$, $z^{\frac{1}{p}} \in \mathbb{N}$ as well. The case when (m, n, p) = 1 is straightforward.

The following lemma is somewhat related to Beal's Conjecture and the Fermat-Catalan's Conjecture. (See [4] and the remarkable paper of Darmon and Granville [3].)

Lemma 8. Consider the equation $\alpha x^{\frac{h}{k}+ir} + \beta y^{\frac{l}{m}+is} = z^{\frac{n}{p}+it}$, where $\alpha, \beta \in \mathbb{Q}, r, s, t \in \mathbb{A} \cap \mathbb{R}$, and where $\frac{h}{k}, \frac{l}{m}, \frac{n}{p}$ are positive rational numbers in their lowest terms. If this equation is solvable in positive integers x, y, z with (x, y) = 1, then x is a k-th power, y is an m-th power, z is a p-th power and $x^r = y^s = z^t = 1$.

Proof. Write the equation as $Ax^{ir} + By^{is} = Cz^{it}$ where $A = \alpha x^{\frac{h}{k}}, B = \beta y^{\frac{l}{m}}, C = z^{\frac{n}{p}}$. Clearly $A, B, C \in \mathbb{A} \cap \mathbb{R}$ and $C \neq 0$, so that, by Lemma 6, $x^r = y^s = z^t = 1$, and $\alpha (x^h)^{1/k} + \beta (y^l)^{1/m} = (z^n)^{1/p}$. This, by Lemma 7, implies $x^h = \rho^k, y^l = \sigma^m$, $z^n = \tau^p$ for some positive integers ρ, σ, τ . Since h and k are coprime, x is a k-th power by Lemma 4. Similarly y and z are m-th and p-th powers respectively.

Proof of Proposition 1. 'If' is clear. Next, we have $Ax^{is} + By^{is} = Cz^{is}$, where $A = x^{\frac{m}{n}}, B = y^{\frac{m}{n}}, C = z^{\frac{m}{n}} \neq 0.$ By Lemma 6, $x^s = y^s = z^s$ and $(x^m)^{1/n} + (y^m)^{1/n} =$ $(z^m)^{1/n}$. If $s \neq 0$ then x = y = z, contradicting that $x^u + y^u = z^u$. Hence s = 0. Assume first that m > 1. By Lemma 4, there are positive integers a, b, c such that $(a,b) = 1, x^m = b^n c, y^m = a^n c, z^m = (a+b)^n c$. Thus $x^m a^n = y^m b^n$, and if x = du, y = dv where $d, u, v \in \mathbb{N}$ and (u, v) = 1, then $u^m a^n = v^m b^n$, i.e. $u^m = b^n$ and $v^m = a^n$. By Lemma 4, and since (m,n) = 1, there exist $\alpha, \beta \in \mathbb{N}$ such that $a = \alpha^m, v = \alpha^n, b = \beta^m, u = \beta^n$. This means $(\alpha, \beta) = 1, c = d^m, x = d\beta^n$, and $y = d\alpha^n$, so that $z^m = d^m (\alpha^m + \beta^m)^n$, i.e. $\left(\frac{z}{d}\right)^m = (\alpha^m + \beta^m)^n$. As before, we obtain that for some positive integer γ , $z = d\gamma^n$ and $\alpha^m + \beta^m = \gamma^m$. By Theorem 2, m = 1or 2. Suppose now that $\mu = -m \ge 1$. The equation $(x^m)^{1/n} + (y^m)^{1/n} = (z^m)^{1/n}$ can be written $(xz)^{\mu/n} + (yz)^{\mu/n} = (xy)^{\mu/n}$, so that by the first part of this proof, $\mu = 1$ or 2, $xz = d\beta^n$, $yz = d\alpha^n$, $xy = d\gamma^n$, for some positive integers α, β, γ satisfying $(\alpha,\beta) = 1, \ \alpha^{\mu} + \beta^{\mu} = \gamma^{\mu}$. Thus $(\alpha,\gamma) = 1$ and we have $\frac{x}{z} = \left(\frac{\gamma}{\alpha}\right)^n$ which implies $\alpha^n \mid z$. Similarly $\beta^n \mid z$, and therefore there exists $t \in \mathbb{N}$ such that $z = t\alpha^n \beta^n$, and so $x = t\beta^n \gamma^n$, $y = t\alpha^n \gamma^n$.

Having disposed of the case of rational exponents in Fermat's Theorem, we next turn to the case when the exponents are irrational real numbers. Let a, b, c be positive integers with a, b < c. Then there exists a unique positive real number r such that $a^r + b^r = c^r$. To see this, let $f(x) = \alpha^x + \beta^x - 1$, where $\alpha = \frac{a}{c}, \beta = \frac{b}{c} \in (0, 1)$. Since f(0) = 1 and $\lim_{x\to\infty} f(x) = -1$, the existence of r is guaranteed by the intermediate value theorem. The uniqueness of r follows from the fact that f is strictly decreasing as $f'(x) = \alpha^x \ln \alpha + \beta^x \log \beta < 0$. On the other hand, consider problem (P) mentioned above. The answer to it is yes, and in fact we have the stronger

Proposition 9. For any positive integer n, and any positive real numbers r and ε , there exist infinitely many primes p, q and infinitely many real numbers s with $|s - r| < \varepsilon$ such that $p^{ns} + p^{ns} = 2p^{ns} = q^{ns}$. Such s are necessarily transcendental.

To prove Proposition 9, we use the following results.

Theorem 10 (Euclid). There are infinitely many primes.

Theorem 11 (see [2]). There exists a real number x_0 such that for all $x \ge x_0$, there is at least one prime p between $x - x^{0.525}$ and x.

Lemma 12. For any positive real numbers α, β such that $\alpha < \beta$ there exist infinitely many pairs of primes p, q such that $\alpha < \frac{p}{q} < \beta$.

Proof. Let
$$\theta = 0.525$$
, $\gamma = \frac{\alpha + \beta}{2}$. For any prime $q > \max\left(\left(\frac{\gamma^{\theta}}{\gamma - \alpha}\right)^{\frac{1}{1-\theta}}, \frac{x_0}{\gamma}\right)$ (such

q exists by Theorem 10), we have $x_0 < q\gamma$ and $q\alpha < q\gamma - (q\gamma)^{\theta}$, so that, by Theorem 11, there is a prime p with $q\alpha . Hence <math>\alpha < \frac{p}{q} < \beta$. Applying the same argument again with the pair α and $\frac{p}{q}$ yields primes p_1, q_1 satisfying $\alpha < \frac{p_1}{q_1} < \frac{p}{q} < \beta$. Continuing in this way, we obtain an infinite sequence of pairs of primes (p_n, q_n) satisfying the required inequalities.

Proof of Proposition 9. We may obviously assume that $\varepsilon < r$. By Lemma 12, there are infinitely many primes p, q such that $2^{\frac{1}{n(r+\varepsilon)}} < \frac{p}{q} < 2^{\frac{1}{n(r-\varepsilon)}}$, and clearly $p \neq q$ since $2^{\frac{1}{n(r+\varepsilon)}} > 1$. For each such pair (p,q) let $f(x) = 2^{\frac{1}{nx}}q - p$. Then $f(r-\varepsilon) > 0$ and $f(r+\varepsilon) < 0$, so that for some s with $|s-r| < \varepsilon$, and depending on p and q, we have f(s) = 0, i.e. $2p^{ns} = q^{ns}$. The real number s must be transcendental. For if it were algebraic and not rational, we would have $\left(\frac{q}{p}\right)^{ns} = 2 \in \mathbb{Q}$, contradicting the

Gelfond-Schneider Theorem; and if it were rational, $s = \frac{h}{k}$ say, then $2^k p^{nh} = q^{nh}$, which is impossible since p and q are distinct primes.

Proposition 9 implies that, although the equation $x^r + y^r = z^r$ is not solvable in \mathbb{N} for any given odd prime r, there exists a sequence (s_n) of transcendental numbers converging to r, such that $x^{s_n} + y^{s_n} = z^{s_n}$ has prime power solutions.

In view of Proposition 1 and the preceding statement, it is fitting to end this note with the following problems.

1. If r is an algebraic real number that is not rational, do there exist positive integers x, y, z such that $x^r + y^r = z^r$?

2. If r is a transcendental real number, do there exist positive integers x, y, z such that $x^{ir} + y^{ir} = z^{ir}$?

Acknowledgments. I am indebted to Dr. A. Umar who raised the question of complex exponents in Fermat's Theorem, and I gratefully acknowledge King Fahd University of Petroleum and Minerals for its support.

References

1. A. Baker, Transcendental Number Theory, Cambridge University Press, Cambridge, 1975.

2. R.C. Baker, G. Harman and J. Pintz, The difference between consecutive primes.

II, Proc. London Math. Soc. (3) 83 (2001), 532–562.

3. H. Darmon and A. Granville, On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$, Bull. London Math. Soc. 27 (1995), 513–543.

4. R.D. Mauldin, A generalization of Fermat's Last Theorem: The Beal Conjecture and prize problem, Notices Amer. Math. Soc. 44 (1997), 1436-1437.