Discrete Mathematics 106/107 (1992) 329–331
North-Holland

On the inverse Fermat equation

H.W. Lenstra Jr
Department of Mathematics, University of California, Berkeley, CA 94720, USA

Received 10 December 1991

Abstract

Lenstra Jr, H W , On the inverse Fermat equation, Discrete Mathematics 106/107 (1992) 329–331

In this paper the equation $x^{1/n} + y^{1/n} = z^{1/n}$ is solved in positive integers x, y, z, n If the nth roots are taken to be positive real numbers, then all solutions are known to be trivial in a certain sense A very short proof of this is provided The argument extends to give a complete description of all solutions when other nth roots are allowed It turns out that up to a suitable equivalence relation there are exactly four nontrivial solutions

The *inverse Fermat equation* is the diophantine equation

$$x^{1/n} + y^{1/n} = z^{1/n},$$

to be solved in positive integers x, y, z, n. When the nth roots are interpreted as positive real numbers, then it is known that the only solutions are given by $x = ca^n$, $y = cb^n$, $z = c(a+b)^n$, where a, b, c are positive integers with $\gcd(a, b) = 1$; see [1, 2] and the references listed there. Equivalently, if α, β are positive real numbers for which

$$\alpha + \beta = 1, \qquad \alpha^n \text{ and } \beta^n \text{ are rational,}$$

then α and β are rational.

The following proof is so short that it might be called a *one line* proof, had it not employed two circles as well. It relies on a fact from Euclidean geometry: *if two nonconcentric circles in the plane intersect in a point that is collinear with their centres, then they have no other intersection point.* The rationality of α^n implies that the algebraic number α and all of its conjugates have the same absolute value, so that in the complex plane they are all located on a circle centred at 0; and since the same is true for $\beta = 1 - \alpha$, they also lie on a circle centred at 1. Thus, by the geometric fact just stated, α has no conjugates different from itself, which means that it is rational.

Correspondence to H W Lenstra Jr, Department of Mathematics, University of California, Berkeley, CA 94720, USA

0012-365X/92/$05 00

When other nth roots than positive real ones are allowed in the inverse Fermat equation, then there are a few special solutions. Namely, consider the identities

$$1 + 1^{\frac{1}{4}} = 16^{\frac{1}{8}},$$

$$1 + 1^{\frac{1}{3}} = 1^{\frac{1}{6}},$$

$$1 + 9^{\frac{1}{4}} = 64^{\frac{1}{6}},$$

$$1 + 1^{\frac{1}{6}} = 729^{\frac{1}{12}},$$

where the roots are suitably chosen. The first identity leads to a solution $x = y = 1$, $z = 16$, $n = 8$ of the inverse Fermat equation. The others lead in a similar way to solutions, with $n = 6, 12, 12$, respectively.

There are essentially no other solutions. To formulate this precisely, denote by G the multiplicative group of nonzero complex numbers δ with the property that δ^n is rational for some positive integer n. Consider the equation

$$\alpha + \beta + \gamma = 0, \quad \alpha, \beta, \gamma \in G.$$

Each of the above four identities represents a solution; let the solutions obtained in this way be called *special*. In addition, there are *trivial* solutions, in which α, β, and γ are rational. Let two solutions be called *equivalent* if one is proportional to a permutation of the other, up to complex conjugation. With this terminology, *each solution is equivalent either to a trivial one or to one of the four special solutions.*

Permuting α, β, γ one can achieve that $|\gamma| = \max\{|\alpha|, |\beta|, |\gamma|\}$, and dividing by $-\gamma$ one may assume that $\gamma = -1$, so that $\alpha + \beta = 1$. If α is real, then the same proof as above shows that the solution is trivial. Suppose that α is not real. Then the same reasoning leads to two circles that intersect in two nonreal points, so α is imaginary quadratic. From $|\alpha| \leqslant 1$, $|1 - \alpha| = |\beta| \leqslant 1$ one sees that the real part of α is strictly between 0 and 1. Also, from $\alpha \in G$ it follows that the number $\zeta = \alpha/\bar{\alpha}$ is a root of unity, and it is different from ± 1. Further, ζ belongs to the quadratic field generated by α. The same statements are true for the number $\eta = \beta/\bar{\beta} = (1 - \alpha)/(1 - \bar{\alpha})$. However, the only quadratic fields that contain roots of unity different from ± 1 are the Gaussian field, generated by a primitive fourth root of unity, and the Eisenstein field, generated by a primitive cube root of unity. If α generates the Gaussian field, then ζ has order 4, and the same is true for η, so that the triangle with vertices $0, 1, \alpha$ has angles equal to $\pi/4$, $\pi/4$, $\pi/2$; in this case the solution is equivalent to the first special one. If α generates the Eisenstein field, then ζ has order 3 or 6, and the same is true for η. If both ζ and η have order 3, then the triangle with vertices $0, 1, \alpha$ is equilateral, and the solution is equivalent to the second special one. If one of ζ and η has order 6, and the other has order 3 or 6, then one finds in a similar way one of the remaining two special solutions.

Acknowledgement

The author was supported by NSF under Grant No. DMS 90-02939. He is grateful to Andrew Granville and Guoqiang Ge for their bibliographic and linguistic assistance.

References

[1] M Newman, A radical diophantine equation, J Number Theory 13 (1981) 495–498
[2] Zhao Yu Xu, On the diophantine equation $X^{1/m} + Y^{1/m} = Z^{1/m}$ (Chinese), Hunan Ann Math 6 (1) (1986) 115–117, Math Rev 88f 11019