On the inverse Fermat equation

H.W. Lenstra Jr

Department of Mathematics, University of California, Berkeley, CA 94720, USA

Received 10 December 1991

Abstract


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 $n$th 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 $n$th 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 $n$th 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 $\alpha, \beta$ are positive real numbers for which

$$\alpha + \beta = 1,$$

then $\alpha$ and $\beta$ 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 $\alpha^n$ implies that the algebraic number $\alpha$ 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, $\alpha$ 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
When other $n$th roots than positive real ones are allowed in the inverse Fermat equation, then there are a few special solutions. Namely, consider the identities

\[
1 + 1^\frac{1}{4} = 16^\frac{1}{4},
\]
\[
1 + 1^\frac{1}{5} = 1^\frac{1}{5},
\]
\[
1 + 9^\frac{1}{3} = 64^\frac{1}{3},
\]
\[
1 + 1^\frac{1}{6} = 729^\frac{1}{6},
\]

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 $\delta$ with the property that $\delta^n$ 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 $\alpha$, $\beta$, and $\gamma$ 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 $\alpha$, $\beta$, $\gamma$ 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 $\alpha$ is real, then the same proof as above shows that the solution is trivial. Suppose that $\alpha$ is not real. Then the same reasoning leads to two circles that intersect in two nonreal points, so $\alpha$ is imaginary quadratic. From $|\alpha| \leq 1$, $|1 - \alpha| = |\beta| \leq 1$ one sees that the real part of $\alpha$ 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 $\pm 1$. Further, $\zeta$ belongs to the quadratic field generated by $\alpha$. 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 $\pm 1$ 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 $\alpha$ generates the Gaussian field, then $\zeta$ has order 4, and the same is true for $\eta$, 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 $\alpha$ generates the Eisenstein field, then $\zeta$ has order 3 or 6, and the same is true for $\eta$. If both $\zeta$ and $\eta$ 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 $\zeta$ and $\eta$ 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

[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