Gulf Journal of Mathematics
Vol 13, Issue 2 (2022) 12-18

ISSN: 2309-4966
https://doi.org/10.56947/gjom.v13i2.868

SPECIAL CASE OF FERMAT'S THEOREM

LUIS H. GALLARDO[1*]

Abstract. We prove under a mild condition that the only rationals x, y with $x \geq 0, y \geq 0$ and $x + y = \mathrm{N}(k)$, for some $k \in \mathbb{Q}^*$, and $x^p + y^p = 1$ are $x = 0, y = 1$ and $x = 1, y = 0$. Here, we let N denote the norm from $\mathbb{Q}(\omega_p)$ to $\mathbb{Q}$ for p an odd prime number.

1. Introduction

Let p be an odd prime number. Let ω_p (or just ω for fixed p) denote a zero of the cyclotomic polynomial $\Phi_p(x) = x^{p-1} + \cdots + 1 \in \mathbb{Q}[x]$. Likewise, let Tr denote, as usual, the trace function from $\mathbb{Q}(\omega)$ onto $\mathbb{Q}$, and N the norm function from $\mathbb{Q}(\omega)$ into $\mathbb{Q}$.

We are interested in describing, by elementary methods, the intersection of a line $X + Y = \ell$ with the curve $X^p + Y^p = 1$, with X, Y restricted to non-negative values, in a special case (for more general results in two directions see [1, 2]). Of course, our result is not new, since Wiles [5], and Taylor and Wiles [4] proved, unconditionally, and by deep methods, that the intersection (when non empty) contains exactly the points $(1, 0)$ and $(0, 1)$. These two *solutions* share (trivially) the following property. The sum $s = x + y$ equals the norm of some rational number $\ell = k$. Namely, $k = 1$. We ask then for solutions $(x, y) \in \mathbb{Q}^2$, such that $x \geq 0, y \geq 0$, with the same property, namely that $s = \mathrm{N}(k) = k^{p-1}$ for some rational number k. When k is chosen appropriately, i.e., when the two curves intersect on some real points, with non-negative coordinates, it is not trivial to decide if these solutions are rational or not.

We can now write the condition $x^p + y^p = 1$ in the form

$$\mathrm{N}(k(x + y\omega)) = 1, \tag{1.1}$$

since the norm N is multiplicative and

$$\frac{x^p + y^p}{x + y} = (x + y\omega) \cdots (x + y\omega^{p-1}) = \mathrm{N}(x + y\omega). \tag{1.2}$$

By Hilbert's 90's theorem (see Lemma 2.2) there exists a nonzero $z \in \mathbb{Q}(\omega)$ such that

$$k(x + y\omega) = \frac{\sigma(z)}{z}, \tag{1.3}$$

Date: Received: Apr 29, 2022; Accepted: Aug 30, 2022.

* Corresponding author.

2010 *Mathematics Subject Classification.* Primary 11R18, 11D41; Secondary 11T06, 11R32.
Key words and phrases. Cyclotomic extension, traces, norms, Hilbert's 90 theorem.

where σ is a generator of the Galois group of the extension $\mathbb{Q}(\omega)$ over $\mathbb{Q}$.

It turns out that, under a mild condition, we can reduce the problem to the case in which $\mathrm{Tr}(z) \neq 0$ in (1.3). Thus, we are able to solve it in two special cases. Otherwise, the problem seems out of reach by elementary methods.

Remark 1.1. The main difference between our approach and the approach in [4, 5] is that they proved the full theorem. This was done by a proof of a special case of the Shimura-Taniyama-Weil conjecture involving deep and sophisticated properties of appropriate elliptic curves associated to the problem. While our approach proves only a very special case of the theorem and uses no more than elementary tools of algebraic number fields, namely the norm and the trace. In other words, our approach is more direct but far less deep.

The object of the present paper is to prove the following results, in which we use the notation above.

Our first result improves on Hilbert's 90 theorem in a special case.

Theorem 1.2. *We can chose a conjugate $a_1 = \tau(a)$, for some $\tau \in G$, of a in Lemma 2.2 such that $b_1 = \tau(b)$ satisfies*

$$\langle\, 1, b_1 \,\rangle \neq 0.$$

provided that b is such that $\langle\, m_j,\, 1\rangle$ is a linear combination of the $\langle\, \tau(b),\, 1\rangle$ for $\tau \in G$. Here, the minimal polynomial of b over $\mathbb{Q}$ is $A(x) = m_0 + m_1 x + \cdots + m_{p-2}x^{p-2}$. Thus,

$$\mathrm{Tr}(b) \neq 0.$$

Our second result solves Fermat's equation on a special case using only elementary facts.

Theorem 1.3. *Let p be an odd prime number. Assume that $x, y \in \mathbb{Q}$, with $x \geq 0, y \geq 0$, satisfies $x + y = k^{p-1}$ for some positive $k \in \mathbb{Q}$, and $x^p + y^p = 1$. Then for some $z \in \mathbb{Q}(\omega)$ that satisfies (1.3) and the condition on b in Theorem 1.2 we have $\mathrm{Tr}(z) \neq 0$. Moreover, we have $x = 0$ and $y = 1$, or $x = 1$ and $y = 0$, provided that $\mathrm{Tr}(z\omega) = 0$, or $\mathrm{Tr}(z) = \mathrm{Tr}(z\omega)$.*

The following notation is useful. Let

$$\langle\, , \,\rangle \colon \mathbb{Q}(\omega) \times \mathbb{Q}(\omega) \mapsto \mathbb{Q}$$

denote the bilinear map

$$(x, y) \mapsto \mathrm{Tr}(xy).$$

2. Tools

For convenience of the reader, we recall here some useful facts.

Lemma 2.1. *The cyclotomic polynomial $\Phi_p(x) = x^{p-1} + \cdots + 1$ is the minimal polynomial of ω for a prime number p.*

Hilbert's 90 theorem [3, Theorem 6.1] applied to the cyclic extension $\mathbb{Q}(\omega)$ over $\mathbb{Q}$ gives the following:

Lemma 2.2. *If $a \in \mathbb{Q}(\omega)$ satisfies $\mathrm{N}(a) = 1$ then there exists a nonzero $b \in \mathbb{Q}(\omega)$ such that*

$$a = \sigma(b)/b,$$

where σ is a generator of the Galois group G of the extension $\mathbb{Q}(\omega)/\mathbb{Q}$.

The following technical result is useful.

Lemma 2.3. *Let p be an odd prime number. Write $z = \sum_{j=0}^{p-2} z_j \omega^j \in \mathbb{Q}(\omega)$. Then*

$$\mathrm{Tr}(\omega z) = \mathrm{Tr}(z) - p z_0. \tag{2.1}$$

Proof. We have

$$\omega z = \sum_{j=0}^{p-3} z_j \omega^{j+1} + z_{p-2}\omega^{p-1}. \tag{2.2}$$

Rewrite (2.2), using Lemma 2.1, and putting $k = j + 1$, as

$$\omega z = \sum_{k=1}^{p-2} z_{k-1}\omega^k - \sum_{k=0}^{p-2} z_{p-2}\omega^k. \tag{2.3}$$

In other words, (2.3) means

$$\omega z = \sum_{k=1}^{p-2} (z_{k-1} - z_{p-2})\omega^k - z_{p-2}. \tag{2.4}$$

Take the trace Tr in both sides of (2.4) to get the following:

$$\mathrm{Tr}(\omega z) = (1-p) z_{p-2} - \sum_{k=1}^{p-2} (z_{k-1} - z_{p-2}), \tag{2.5}$$

since $\mathrm{Tr}(1) = p - 1$, and $\mathrm{Tr}(\omega^k) = -1$ for $1 \leq k \leq p-2$. Rewrite (2.5) as

$$\mathrm{Tr}(\omega z) = (-p+2) z_{p-2} - (z_{p-2} + \sum_{k=1}^{p-2} z_{k-1}) + (p-2) z_{p-2}. \tag{2.6}$$

In other words, (2.6) says that

$$\mathrm{Tr}(\omega z) = \sum_{\ell=0}^{p-2} z_\ell. \tag{2.7}$$

On the other hand, similarly, we have

$$\mathrm{Tr}(z) = p z_0 - \sum_{\ell=0}^{p-2} z_\ell. \tag{2.8}$$

The result follows from (2.7) and (2.8). □

3. Proof of Theorem 1.2

Proof. Assume, contrary to what we want to prove, that

$$\langle\, 1, \tau(b)\,\rangle = 0 \tag{3.1}$$

for all $\tau \in G$. We claim that the minimal polynomial of b, namely

$$A(x) = \prod_{\tau \in G} (x - \tau(b)), \tag{3.2}$$

when written as

$$A(x) = x^{p-2} + \sum_{j=0}^{p-3} a_j x^j \in \mathbb{Q}[x], \tag{3.3}$$

satisfies

$$A(x) = x^{p-2}. \tag{3.4}$$

In order to prove the claim, observe (comparing equations (3.2) and (3.3)) that Newton's relations implies that each a_j is a homogeneous polynomial in the $\tau(b)$ for $b \in G$. Thus, $\langle\, 1, a_{p-3}\,\rangle = 0$. For the remaining coefficients, we use our condition on b to get $\langle\, 1, a_j\,\rangle = 0$.

Thus, for each j, equation (3.1) implies that one has

$$0 = \langle\, 1, a_j\,\rangle. \tag{3.5}$$

Hence, for each j, one has $a_j \in \mathbb{Q}$, and

$$0 = \langle\, 1, a_j\,\rangle = a_j \langle\, 1, 1\,\rangle = (p-1)a_j. \tag{3.6}$$

Clearly, (3.6) implies that for all j we have

$$a_j = 0. \tag{3.7}$$

This proves the claim.

But (3.4) implies that

$$A(0) = 0^{p-2} = 0. \tag{3.8}$$

Moreover, equation (3.2) implies that

$$A(0) = \mathrm{N}(b). \tag{3.9}$$

Comparing equations (3.8) and (3.9), it follows that

$$\mathrm{N}(b) = 0. \tag{3.10}$$

Clearly, (3.10) contradicts the fact that $b \neq 0$.

Thus, we proved that

$$0 \neq \langle\, 1, \tau(b)\,\rangle. \tag{3.11}$$

Therefore, (3.11) implies that

$$\mathrm{Tr}(b) \neq 0, \tag{3.12}$$

since

$$\mathrm{Tr}(b) = \langle\, 1, b\,\rangle = \langle\, 1, \tau(b)\rangle. \tag{3.13}$$

This proves the theorem. □

4. Proof of Theorem 1.3

Since k is rational, $k^{p-1} = \mathrm{N}(k)$, the norm is multiplicative, and (1.2) holds, we can write the equation

$$x^p + y^p = 1 \tag{4.1}$$

as

$$\mathrm{N}(k(x + y\omega)) = 1. \tag{4.2}$$

By Lemma 2.2 and Theorem 1.2 we obtain

$$k(x + y\omega) = \frac{\sigma(z)}{z} \tag{4.3}$$

for some nonzero $z \in \mathbb{Q}(\omega)$, such that

$$\mathrm{Tr}(z) \neq 0, \tag{4.4}$$

where σ generates the Galois group of the extension $\mathbb{Q}(\omega)/\mathbb{Q}$.

Put

$$z = z_0 + z_1\omega + \cdots + z_{p-2}\omega^{p-2} \in \mathbb{Q}(\omega). \tag{4.5}$$

Rewrite (4.3) as

$$kx \cdot z + ky \cdot (z\omega) = \sigma(z). \tag{4.6}$$

Taking the trace Tr in both sides of (4.6) we obtain

$$kx\mathrm{Tr}(z) + ky\mathrm{Tr}(z\omega) = \mathrm{Tr}(z), \tag{4.7}$$

since $\mathrm{Tr}(\sigma(z)) = \mathrm{Tr}(z)$.

Moreover, by Lemma 2.3 and (4.7) one has

$$\mathrm{Tr}(z)(k(x + y) - 1) = kypz_0. \tag{4.8}$$

Assume first that

$$\mathrm{Tr}(\omega z) = \mathrm{Tr}(z). \tag{4.9}$$

By Lemma 2.3 we obtain $z_0 = 0$. Thus, from (4.4) and (4.8) we obtain that

$$k(x + y) = 1. \tag{4.10}$$

Since $x + y = k^{p-1}$ (4.11) implies that

$$k^p = 1. \tag{4.11}$$

Hence, $k = 1$, i.e.,

$$x + y = 1. \tag{4.12}$$

Thus, if $(x, y) \notin \{(1, 0), (0, 1)\}$ we have the contradiction

$$1 = x + y > x^p + y^p = 1. \tag{4.13}$$

It remains to consider the case when

$$\mathrm{Tr}(\omega z) = 0. \tag{4.14}$$

By Lemma 2.3 we deduce from (4.14) that

$$\mathrm{Tr}(z) = pz_0. \tag{4.15}$$

Thus, from (4.4) and (4.8) we obtain

$$kx = 1. \tag{4.16}$$

From (4.1), (4.16), and

$$kx + ky = k^p, \tag{4.17}$$

we obtain

$$ky = k^p - 1. \tag{4.18}$$

From (4.1) multiplied by k^p together with (4.16), we obtain

$$k^p y^p = k^p - 1. \tag{4.19}$$

In other words, (4.18) and (4.19) says that

$$t^p = t, \tag{4.20}$$

with

$$t = k^p - 1. \tag{4.21}$$

If $t = 1$ we obtain from (4.21) the contradiction

$$2 = k^p. \tag{4.22}$$

If $t = 0$, then we get $k^p = 1$ from (4.21). Thus, (4.17) says that

$$ky = 0. \tag{4.23}$$

Thus, (4.23) implies that $y = 0$. From (4.16) we get then $k = 1$ and $x = 1$.

This finishes the proof of the theorem.

Remark 4.1. Observe that equation (4.2), can be rewritten as (4.3), namely

$$kx \cdot z + ky \cdot (z\omega) = \sigma(z). \tag{4.24}$$

Taking the trace Tr in both sides of (4.24) we obtain

$$kx\mathrm{Tr}(z) + ky\mathrm{Tr}(z\omega) = \mathrm{Tr}(z). \tag{4.25}$$

Equation (4.25) holds when $\mathrm{Tr}(z) = 0$ and when $\mathrm{Tr}(z) \neq 0$. However, (4.25) cannot help to prove that the equation

$$x^p + y^p = 1$$

has the trivial solutions when

$$\mathrm{Tr}(z) = \mathrm{Tr}(z\omega) = 0,$$

since (4.25) becomes the trivial identity $0 = 0$.

In other words, Theorem 1.2, greatly simplifies the study of equation (4.25).

Acknowledgement. We thank the referee and the editor for useful comments and suggestions.

References

[1] E. Ballico. Existence of embeddings of varieties in projective spaces whose points are spanned by low degree smoothable zero-dimensional subschemes *Gulf J. Math.*, 8(1), 1–5, 2020. https://doi.org/10.56947/gjom.v8i1.281

[2] G. Kientega, T. Tapsoba, C. Tougma. Kummer extensions and Pólya fields *Gulf J. Math.*, 6(3), 12–24, 2018. https://doi.org/10.1016/S0262-1762(19)30185-3

[3] S. Lang. *Algebra.* Revised third ed., Graduate Texts in Mathematics, 211, Springer-Verlag, New York, 2002.

[4] R. Taylor, A. Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. Math.*, (2) 141(3), 553–572, 1995.

[5] A. Wiles. Modular elliptic curves and Fermat's Last Theorem. *Ann. Math.*, (2) 141(3), 4433–551, 1995. https://doi.org/10.2307/2118559

[1] Univ. Brest, UMR CNRS 6205, Laboratoire de Mathématiques de Bretagne Atlantique, F-29238 Brest, France.

Email address: Luis.Gallardo@univ-brest.fr