THE GENERALIZED FERMAT CONJECTURE

ADALBERTO GARCÍA-MÁYNEZ, MARGARITA GARY,
AND ADOLFO PIMIENTA ACOSTA

In memory of Adalberto García-Máynez 1941-2016.

Abstract. If a, b, c are non-zero integers, we considerer the following problem: for which values of n the line $ax + by + cz = 0$ may be tangent to the curve $x^n + y^n = z^n$?

We give a partial solution: if $n = 5$ or if $n - 1$ is a prime a number, then the answer is the line cannot be tangent to the curve. This problem is strongly related to Fermat' s Last Theorem.

1. Introduction

The classical Fermat Conjecture (was proved to be true [6]) states the impossibility of finding three integers $\neq 0$ α, β, γ such that $\alpha^n + \beta^n = \gamma^n$, where n is an integers≥ 3. In geometrical terms, the theorem is equivalent to say that the Fermat curve $x^n+y^n = z^n$, where $n \geq 3$, contains no points whose coordinates in the proyective plane over $\mathbb{C}$ can be expressed in the form $[\lambda : \mu : \nu]$, where λ, μ, ν are non-zero rational numbers. If $\mathbb{F}$ is a field extension of $\mathbb{Q}$, we shall say that a point P in the proyective plane over $\mathbb{C}$ is an $\mathbb{F}-$point if there exist elements $\lambda, \mu, \nu \in \mathbb{F}$ not all zero, such that $P = [\lambda : \mu : \nu]$. Thus Fermat's Theorem states that the curve $x^n+y^n = z^n$ contains no $\mathbb{Q}-$points for $n \geq 3$. It is well know that the Fermat curves do not have singular points and hence every point $[x_0 : y_0 : z_0]$ of the curve yields a unique tangent line $x_0^{n-1}x + y_0^{n-1}y = z_0^{n-1}z$. We shall say that a line L is an $\mathbb{F}-$tangent to the Fermat curve $x^n + y^n = z^n$ if the equation of L can be expressed in the form $\lambda x + \mu y = \nu z$, where $\lambda, \mu, \nu \in \mathbb{F}$ not all zero and L is the tangent at some point of the curve. It is obvious that the tangent at an $\mathbb{F}-$point of the curve is an $\mathbb{F}-$tangent but the converse is not

2010 *Mathematics Subject Classification.* Primary 11R04, 11R09, 11R11, 11R58; Secondary 41A50.

Key words and phrases. Tangent, Fermat curve, Chebyshev polynomials.

The first and third author thank to Dr. Francisco González Acuña for several fruitful conversations about the solution of the conjecture in the title.

The second author was supported by Grupo de Investigación e Innovación en Ciencias Básicas, GICNEX..

true: the line $x+y=z$ is a $\mathbb{Q}-$tangent of the Fermat curve $x^7+y^7=z^7$ but the points of tangency are not $\mathbb{Q}-$points: in fact the line, $x+y=z$ is tangent to the curve at the points $(\cos\frac{\pi}{3}+i\sin\frac{\pi}{3}, \cos\frac{\pi}{3}-i\sin\frac{\pi}{3}, 1)$, $(\cos\frac{\pi}{3}-i\sin\frac{\pi}{3}, \cos\frac{\pi}{3}+i\sin\frac{\pi}{3}, 1)$ and there is no further intersection of the line with the curve. We can state now the generalized Fermat Conjecture.

Fermat's Last Theorem (FLT), formulated in 1637, states that no three distinct positive integers α, β and γ can satisfy the equation

$$\alpha^n+\beta^n=\gamma^n$$

if n is an integer greater than 2.

Generalized Fermat Conjecture (GFC). Let n be a natural number ≥ 3 which is not congruent to $1 \pmod 6$; then the Fermat curve $x^n+y^n=z^n$ has no $\mathbb{Q}-$tangents.

The main relation between GFC and FLT lies in the imposibility that Fermat curve $x^n+y^n=z^n$ has no $\mathbb{Q}-$tangents.

In this paper we shall prove the Generalized Fermat Conjecture for $n=5$ and for every integer $n\geq 3$ such that $n-1$ is a prime number.

2. Preliminary

The terminology of [2], [3], [4] and [5], is used throughout.

Let p be a prime number ≥ 3. We know $\Big[\mathbb{Q}(\zeta_p{}^1) : \mathbb{Q}\Big] = p-1$: in fact, $x^{p-1}-x^{p-2}+x^{p-3}-\cdots+1$ is the minimal polynomial of ζ_p over $\mathbb{Q}$. Using this fact, we can prove the following result:

Proposition 2.1. *Let p be a prime number ≥ 3. Then* $\Big[\mathbb{Q}\Big(\cos\frac{\pi}{p}\Big) : \mathbb{Q}\Big] = \frac{p-1}{2}$.

Proof. It is easy to prove that $\mathbb{Q}\Big(\zeta_p\Big) = \mathbb{Q}\Big(\cos\frac{\pi}{p}, i\sin\frac{\pi}{p}\Big)$. So:

$$\begin{aligned} p-1 &= \Big[\mathbb{Q}\Big(\zeta_p\Big) : \mathbb{Q}\Big] \\ &= \Big[\mathbb{Q}\Big(\cos\frac{\pi}{p}, i\sin\frac{\pi}{p}\Big) : \mathbb{Q}\Big] \\ &= \Big[\mathbb{Q}\Big(\cos\frac{\pi}{p}, i\sin\frac{\pi}{p}\Big) : \mathbb{Q}\Big(\cos\frac{\pi}{p}\Big)\Big]\Big[\mathbb{Q}\Big(\cos\frac{\pi}{p}\Big) : \mathbb{Q}\Big]. \end{aligned}$$

The second degree polynomial $x^2+1-\cos^2\frac{\pi}{p} \in \mathbb{Q}\Big(\cos\frac{\pi}{p}\Big)[x]$ has the number $i\sin\frac{\pi}{p}$ as a root. Since $i\sin\frac{\pi}{p} \notin \mathbb{Q}\Big(\cos\frac{\pi}{p}\Big)$, this polynomial is

[1]Let us denote by ζ_p the primitive pth root of unity given by $e^{\frac{i\pi}{p}}$.

irreducible in $\mathbb{Q}\Big(\cos\frac{\pi}{p}\Big)[x]$ and, therefore it is precisely the minimal polynomial of $i\sin\frac{\pi}{p}$ over $\mathbb{Q}\Big(\cos\frac{\pi}{p}\Big)$. Therefore:

$$\Big[\mathbb{Q}\Big(\cos\frac{\pi}{p}, i\sin\frac{\pi}{p}\Big) : \mathbb{Q}\Big(\cos\frac{\pi}{p}\Big)\Big] = 2$$

and, by the tower law, we have

$$\Big[\mathbb{Q}\Big(\cos\frac{\pi}{p}\Big) : \mathbb{Q}\Big] = \frac{p-1}{2},$$

as wanted. □

Remark 2.2. Since $\mathbb{Q}\Big(\cos\frac{\pi}{p} + i\sin\frac{\pi}{p}\Big) = \mathbb{Q}\Big(\cos\frac{n\pi}{p} + i\sin\frac{n\pi}{p}\Big)$ for every $n \in \{1, 2, \ldots, p-1\}$, we have $\Big[\mathbb{Q}\Big(\cos\frac{n\pi}{p}\Big) : \mathbb{Q}\Big] = \frac{p-1}{2}$ if $n \not\equiv 0 \pmod{p}$.

The Chebyshev polynomials $S_m(x)$ $(m = 0, 1, 2, \ldots)$ (see [1]) are defined recursively as follows:

$$\begin{aligned} S_0(x) &= 0 \\ S_1(x) &= 1 \\ S_m(x) &= xS_{m-1}(x) - S_{m-2}(x) \qquad \text{for } m \geq 2. \end{aligned}$$

Lemma 2.3. *$deg(S_m) = m-1$ $(m = 1, 2, \ldots)$ and for every $m \geq 1$ and $\theta \in (0, \pi)$, $S_m(2\cos\theta) = \dfrac{\sin m\theta}{\sin\theta}$.*

Proof. The sentence about the degrees is clear from the definition. For the second part, observe that $S_1(2\cos\theta) = \dfrac{\sin\theta}{\sin\theta} = 1$. Inductively, suppose

$S_r(2\cos\theta) = \dfrac{\sin r\theta}{\sin\theta}$ for each r with $1 \leq r \leq m$. Then:

$$\begin{aligned}
S_{m+1}(x) &= \frac{\sin(m+1)\theta}{\sin\theta} \\
&= \frac{\sin m\theta\cos\theta + \sin\theta\cos m\theta}{\sin\theta} \\
&= \frac{2\sin m\theta\cos\theta - [\sin m\theta\cos\theta - \sin\theta\cos m\theta]}{\sin\theta} \\
&= \frac{2\sin m\theta\cos\theta - \sin(m-1)\theta}{\sin\theta} \\
&= 2\cos\theta\cdot\frac{\sin m\theta}{\sin\theta} - \frac{\sin(m-1)\theta}{\sin\theta} \\
&= 2\cos\theta S_m(2\cos\theta) - S_{m-1}(2\cos\theta)
\end{aligned}$$

□

Lemma 2.4. *Let p be a prime number ≥ 3 and let j, k be non-zero integers which are not divisible by p. Then the number $\dfrac{\sin\frac{kj\pi}{p}}{\sin\frac{j\pi}{p}}$ is rational if only if $k \equiv \pm 1 \pmod p$.*

Proof. Suppose $k \not\equiv \pm 1 \pmod p$. Let $k_0 \in \{2, 3, \ldots, p-2\}$ be such that $k_0 \equiv k \pmod p$. Then

$$\frac{\sin\frac{k_0 j\pi}{p}}{\sin\frac{j\pi}{p}} = \pm\frac{\sin\frac{kj\pi}{p}}{\sin\frac{j\pi}{p}}.$$

If $\lambda = \dfrac{\sin\frac{k_0 j\pi}{p}}{\sin\frac{j\pi}{p}}$, then by Lemma 2.3, $2\cos\frac{j\pi}{p}$ is a root of the polynomial $S_{k_0}(x) - \lambda$. Since $\sin\frac{k_0 j\pi}{p} = \sin\frac{(p-k_0)j\pi}{p}$, the polynomial $S_{p-k_0}(x) - \lambda$ has also the number $2\cos\frac{j\pi}{p}$ as a root. If λ where rational, (Proposition 2.1) would imply.:

$$k_0 - 1 \quad = \quad deg(S_{k_0}(x) - \lambda) \geq \frac{p-1}{2}$$

and

$$p - k_0 - 1 \quad = \quad deg(S_{p-k_0}(x) - \lambda) \geq \frac{p-1}{2}$$

Adding these two equations, we would obtain $p-2 \geq p-1$, a contradiction. Hence the number λ has to be irrational. □

3. Main result

We prove the generalized Fermat conjecture for the special case $n = 5$ and for every integer $n \geq 3$ such that $n-1$ is a prime number.

Theorem 3.1 (Generalized Fermat Conjecture)**.** *Let λ, μ be non-zero rational numbers and let n be a natural number such that $n-1$ is prime or $n = 5$. Then the line $L\colon \lambda x + \mu y = z$ is not tangent to the Fermat curve of degree n.*

Proof. Suppose, on the contrary, that L is tangent to $C\colon x^n + y^n = z^n$ and let $[x_0 : y_0 : 1]$ be a point of tangency. We shall prove this point is rational, contradicting Fermat's theorem. We have then $x_0^{n-1} = \lambda$ and $y_0^{n-1} = \mu$. If we set $w = \cos\frac{\pi}{n-1} + i\sin\frac{\pi}{n-1}$. It is easy to prove that $w^0 = 1, w^2, \ldots, w^{2n-4}$ is the complete list roots of unity of order $n-1$ and $w^1, w^3, \ldots, w^{2n-3}$ is the complete list of roots of -1 of order $n-1$. Therefore, there exists two integers $j, k \in \{0, 1, \ldots, 2n-3\}$ such that $x_0 = w^j|\lambda|^{\frac{1}{n-1}}$ and $y_0 = w^k|\mu|^{\frac{1}{n-1}}$. Observe that if x_0 and y_0 are not real numbers, then we should have $j \neq k$. Since $\lambda x_0 + \mu y_0 = 1$, we have then the following equation:

$$w^j(\lambda|\lambda|^{\frac{1}{n-1}}) + w^k(\mu|\mu|^{\frac{1}{n-1}}) = 1. \tag{3.1}$$

With no loss of generality, we may suppose that $j \leq k$. We prove first that the numbers x_0, y_0 are both real numbers, that is, the only possible values of j, k are 0 or $n-1$. Indeed, if $k \neq 0, n-1$, then also $j \neq 0, n-1$ and we would have a second equation taking conjugates:

$$w^{-j}(\lambda|\lambda|^{\frac{1}{n-1}}) + w^{-k}(\mu|\mu|^{\frac{1}{n-1}}) = 1. \tag{3.2}$$

Adding and subtracting (3.1) and (3.2), we would have

$$\cos\frac{\pi j}{n-1}\lambda|\lambda|^{\frac{1}{n-1}} + \cos\frac{\pi k}{n-1}\mu|\mu|^{\frac{1}{n-1}} = 1.$$

$$\sin\frac{\pi j}{n-1}\lambda|\lambda|^{\frac{1}{n-1}} + \sin\frac{\pi k}{n-1}\mu|\mu|^{\frac{1}{n-1}} = 0.$$

The determinant of this system is:

$$\sin\frac{\pi k}{n-1}\cos\frac{\pi j}{n-1} - \sin\frac{\pi j}{n-1}\cos\frac{\pi k}{n-1} = \sin\frac{\pi(k-j)}{n-1}$$

and it is equal to zero only if $k = j$ or $k = j + (n-1)$. But then $w^j = \pm w^k$ and equation (3.1) could be written as follows:

$$w^k(\pm\lambda|\lambda|^{\frac{1}{n-1}} + \mu|\mu|^{\frac{1}{n-1}}) = 1$$

and w^k would be a real number, which a contradiction. Therefore, $\sin\frac{\pi(k-j)}{n-1} \neq 0$. Applying Cramer's rule, we obtain:

$$\lambda|\lambda|^{\frac{1}{n-1}} = \frac{\sin\frac{\pi k}{n-1}}{\sin\frac{\pi(k-j)}{n-1}} \qquad \mu|\mu|^{\frac{1}{n-1}} = -\frac{\sin\frac{\pi j}{n-1}}{\sin\frac{\pi(k-j)}{n-1}}.$$

If $n-1$ is a prime number $p \geq 3$, then:

$$\lambda|\lambda|^{\frac{1}{p}} = \frac{\sin\frac{\pi k}{p}}{\sin\frac{\pi(k-j)}{p}}; \quad \mu|\mu|^{\frac{1}{p}} = -\frac{\sin\frac{\pi j}{p}}{\sin\frac{\pi(k-j)}{p}}. \tag{3.3}$$

We know $[\mathbb{Q}(w):\mathbb{Q}] = p-1$. It is obvious that $w^k + w^{p-k} = 2i\sin\frac{k\pi}{p}$ for each integer k. Therefore, both numbers $\lambda|\lambda|^{\frac{1}{p}}$ and $\mu|\mu|^{\frac{1}{p}}$ belong to $\mathbb{Q}(w)$ and, for this reason, the degrees $[\mathbb{Q}(|\lambda|^{\frac{1}{p}}):\mathbb{Q}]$ and $[\mathbb{Q}(|\mu|^{\frac{1}{p}}):\mathbb{Q}]$ are both $\leq p-1$. Since the only possible values of $[\mathbb{Q}(t^{\frac{1}{p}}):\mathbb{Q}]$, for t a positive rational, are 1 or p, we conclude that $|\lambda|^{\frac{1}{p}}$ and $|\mu|^{\frac{1}{p}}$ are both rational numbers. The trigonometric quotients in (3.3) are then rational numbers.

Since p is a prime number, there exist integers s_1 and s_2 such that:

$$\begin{aligned} s_1(k-j) &\equiv k \pmod p \\ s_2(k-j) &\equiv j \pmod p \end{aligned}$$

By Lemma 2.4, we deduce $s_1, s_2 \equiv \pm 1 \pmod p$. But then $\sin\frac{\pi k}{p} = \sin\frac{\pi j}{p}$, which, as $j \neq k$ should imply $k-j = mp$ for some positive integer m: however as $k, j \leq 2n-3$, the only posibility is to have $k-j = p$ which a contradiction.

If $n = 5$, then $w = \cos\frac{\pi}{4} + i\sin\frac{\pi}{4} = \frac{\sqrt{2}}{2}(1+i)$ and

$$\lambda|\lambda|^{\frac{1}{4}} = \frac{\sin\frac{\pi k}{4}}{\sin\frac{\pi(k-j)}{4}}; \quad \mu|\mu|^{\frac{1}{4}} = -\frac{\sin\frac{\pi j}{4}}{\sin\frac{\pi(k-j)}{4}}.$$

The only possible values of $\sin\frac{\pi k}{4}$ with $1 \leq k \leq 7$ are $0, \pm 1, \pm\frac{\sqrt{2}}{2}$. For example if $k = 6$ and $j = 1$, give $\lambda|\lambda|^{\frac{1}{4}} = \frac{\sin\frac{3\pi}{2}}{\sin\frac{5\pi}{4}} = \sqrt{2}$ and $\mu|\mu|^{\frac{1}{4}} = -\frac{\sin\frac{\pi}{4}}{\sin\frac{5\pi}{4}} = 1$. If $\lambda > 0$ and $\mu > 0$, necessarly j is odd, k is even, $k-j > 4$, $j < 4$, $j \neq 3$ and $k > 4$. If $\lambda < 0$ and $\mu < 0$, then j, k are odd numbers, $k-j < 4$, $j < 4$ and $k > 4$. The only possibility is $k = 5$ and $j = 3$. But then $|\lambda|^{\frac{5}{4}} = \frac{\sqrt{2}}{2} = |\mu|^{\frac{5}{4}}$ and $\lambda = -\sqrt[5]{\frac{1}{4}} = \mu$ contradicting the rationality of λ and μ. If $\lambda < 0$ and $\mu > 0$, then j is odd, k is even, $k-j < 4$, $k > 4$ and $j > 4$. The only possibility is $j = 5$ and $k = 6$. Then $|\lambda|^{\frac{5}{4}} = \sqrt{2}$ and $\lambda = -\sqrt[5]{4}$, contradicting again the rationality of λ. Finally, if $\lambda > 0$

and $\mu < 0$, then j is even, k is odd, $k - j < 4, j < 4, k < 4$. The only possibility is $j = 2$ and $|\mu|^{\frac{5}{4}} = \sqrt{2}$ and $\mu = -\sqrt[5]{4}$, contradicting again the rationality of μ.

We have proved then that the only possible values of j, k are $0, n-1$. Hence, $x_0 = \pm|\lambda|^{\frac{1}{n-1}}$ and $y_0 = \pm|\mu|^{\frac{1}{n-1}}$.

The equation (3.1) may therefore be written as

$$\pm\lambda|\lambda|^{\frac{1}{n-1}} \pm \mu|\mu|^{\frac{1}{n-1}} = 1.$$

Let us say, to fix ideas, that

$$\lambda|\lambda|^{\frac{1}{n-1}} + \mu|\mu|^{\frac{1}{n-1}} = 1.$$

Setting $\alpha = \mu|\mu|^{\frac{1}{n-1}}$, we deduce α is a common root of the rational polynomials $\varphi(x) = x^{n-1} - \mu^{n-1}|\mu|$ and $\psi(x) = (1-x)^{n-1} - \lambda^{n-1}|\lambda|$. If $n-1$ is an odd prime number, α will be the only common root of $\varphi(x)$ and $\psi(x)$, because if we had another common root, this would be of the form $w^{2k}\mu|\mu|^{\frac{1}{n-1}}$, with $k = 1, \ldots, n-2$ and we would have on substituting in $\psi(x)$, an equation of the form:

$$w^j\lambda|\lambda|^{\frac{1}{n-1}} + w^k\mu|\mu|^{\frac{1}{n-1}} = 1$$

with $j, k \neq 0, n-1$, which we have already proved is impossible. If $n - 1 = 2$, the polynomials $\varphi(x)$ and $\psi(x)$ have degree 2 and therefore they could not have another common root. If $n - 1 = 4$, then $-\alpha$ cannot be a root of $\psi(x)$, because in that case $(1-\alpha)^4 = (1+\alpha)^4$ and this would imply that $\alpha = 0$. Reasoning as before, we deduce that $w^k\alpha$, with $k \neq 0, 4$, cannot be a root of $\psi(x)$. Therefore, in any situation, $x - \alpha$ must be the greatest common divisor of $\varphi(x)$ and $\psi(x)$. But $\varphi(x)$ and $\psi(x)$ are both rational polynomials and so its greatest common divisor must also be a rational polynomial. We conclude then that α is a rational number, so also $|\mu|^{\frac{1}{n-1}}$ must be rational. In similar way, we can prove that $|\lambda|^{\frac{1}{n-1}}$ is rational. But then $[x_0 : y_0 : 1]$ is a rational solution of $x^n + y^n = z^n$, contradicting Fermat's Theorem.

□

4. Acknowledgment

The authors would like to thank the referee for his useful comments, which have helped improve the exposition, particularly of Section 3.

References

[1] B. Fine and G. Rosenberger. *Classification of all generating pairs of two generator Fuchsian groups.* London Math. Soc. Lecture Note Ser. 211, (1995) 205-232.

[2] D. J. H. Garling. *A Course in Galois Theory.* Cambridge University Press, 1986.

[3] S. Lang. *Cyclotomic Fields I and II.* Graduate Texts in Mathematics, 121, Springer-Verlag, New York, 1990.

[4] J. H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves.* Graduate Texts in Mathematics, 151, Springer-Verlag, New York, 1994.

[5] L. Washington. *Introduction to Cyclotomic Fields.* Graduate Texts in Mathematics, Springer-Verlag, New York, 1996.

[6] A. Wiles. *Modular elliptic curves and Fermat's Last Theorem.* Ann. Math. 141 (1995), 443-551.

Instituto de Matemáticas; Universidad Nacional Autónoma de México; Area de la Investigación Científica Circuito Exterior, Ciudad Universitaria Coyoacán, 04510. México, D. F.

Email address: agmaynez@matem.unam,mx

Departamento de Ciencias Naturales y Exactas, Universidad de la Costa-CUC, calle 58 # 55-66, Barranquilla, Colombia

Email address: mgary@cuc.edu.co

Facultad de Ciencias Básicas y Biomédicas, Universidad Simón Bolivar, calle 58 # 55-132, Barranquilla, Colombia

Email address: adolfo.pimienta@unisimonbolivar.edu.co