Journal of Analysis & Number Theory
An International Journal

http://dx.doi.org/10.18576/jant/080101

Euler's Double Equations Equivalent to Fermat's Last Theorem

Andrea Ossicini

Via delle Azzorre 352-D2, 00121 Roma, Italy

Received: 24 Feb. 2020, Revised: 13 Apr. 2020, Accepted: 12 May 2020
Published online: 1 Jul. 2020

Abstract: In this work we illustrate that a possible proof of Fermat's Last Theorem derives from an appropriate use of the concordant forms of Euler and from an equivalent ternary quadratic homogeneous Diophantine equation able to accommodate a solution of Fermat's equation. The impossibility of solving the second degree Diophantine equation thus obtained is certainly possible also through methods known and discovered by Fermat.

Keywords: Fermat's Last Theorem, Arithmetic algebraic geometry, Diophantine geometry.

1 Introduction

It is well known that around the middle of the seventeenth century Pierre Fermat stated what is now called the Fermat's Last Theorem.

In modern language, Fermat's statement means: "The equation $X^n + Y^n = Z^n$, when n is a natural number larger than 2, has no solution in integer all positive".

The search for a successful proof of this theorem was, indeed, very hard and long and only in 1995 an accepted solution was published by A. Wiles ([1] and [2]).

Nevertheless, in his proof, A. Wiles used new concepts and new theories in modern methods of algebraic theories, concepts and theories not available to P. Fermat in his time.

In this paper we have try to prove Fermat's Last Theorem making use of elementary techniques, certainly known to P. Fermat.

We show that making use of the concordant forms of Euler and a ternary quadratic homogeneous Diophantine equation, it is possible to derive a proof of the Fermat's Last Theorem without recurring to modern techniques, but exploiting the important criterion of Legendre for determining the solutions of ternary quadratic homogeneous equation ([3],Chap. IV,§6,pp. 326-328).

2 From the concordant forms of Euler to Fermat's Last Theorem

Let $m,n \in \mathbf{Z} / \{0\}$ be integers with $m \neq n$. Following Euler (see [4]), the quadratic forms X^2+mY^2 and X^2+nY^2 (or the numbers m and n themselves) are called *concordant* if there are integers (X,Y,Z,T) with $Y \neq 0$ such that:

$$X^2+mY^2 = Z^2 \quad ; \quad X^2+nY^2 = T^2. \tag{0}$$

In 1780 Euler seeks criteria for the treatment of the double equations (0) and his interest and our own turns to proofs of impossibility for the cases m=1, n=3 or 4 and others equivalent to these two ([3], Chap. III, §XVI, pp. 253-254).

In practice, Euler called X^2+mY^2 and X^2+nY^2 *concordant* forms if they can both be made squares by choice of integers X,Y each not zero; otherwise, *discordant* forms.

At this stage, let us introduce the following Euler double equations:

$$P^2+Y_1^nQ^2 = V^2,\ P^2-X_1^nQ^2 = T^2 \tag{1}$$

with $X_1^n+Y_1^n = Z_1^n$ and $n \geq 3$.

By multiplying the first two equations (1) together, and multiplying by $\frac{P^2}{Q^6}$, we get([5]):

$$\frac{P^2V^2T^2}{Q^6} = \frac{P^6}{Q^6} + (Y_1^n - X_1^n)\frac{P^4}{Q^4} - X_1^nY_1^n\frac{P^2}{Q^2}. \tag{2}$$

* Corresponding author e-mail: andrea.ossicini@yahoo.it

If we then replace $\frac{P^2}{Q^2}$ by X and also $\frac{PVT}{Q^3}$ by Y we find that

$$Y^2 = X\left(X - X_1^n\right)\left(X + Y_1^n\right).$$

This is known as Frey Elliptic curve ([6], p. 156).

In mathematics, a Frey curve or Frey–Hellegouarch curve is the elliptic curve:

$$Y^2 = X\left(X - X_1^n\right)\left(X + Y_1^n\right) \tag{3}$$

or, equivalently :

$$Y^2 = X\left[X^2 + X\left(Y_1^n - X_1^n\right) - X_1^n Y_1^n\right] \tag{4}$$

associated with a (hypothetical) solution of Fermat's equation : $X_1^n + Y_1^n = Z_1^n$.

In fact, the discriminant

$$\Delta = \sqrt{\left(Y_1^n - X_1^n\right)^2 + 4X_1^n Y_1^n} = X_1^n + Y_1^n = Z_1^n,$$

that determines the existence of the polynomial

$$\left(X - X_1^n\right)\left(X + Y_1^n\right) = X^2 + X\left(Y_1^n - X_1^n\right) - X_1^n Y_1^n,$$

is a perfect power of order n.

Thanks to the spectacular work of A. Wiles, today we know that Frey's elliptic curve not exist ([6], pp. 154–156) and from this derives indirectly, as an absurd, the Fermat Last Theorem.

Now, multiplying the first two equations (1) respectively by X_1^n and by Y_1^n and at end adding together we get the following homogeneous ternary quadratic equation (see Section 3 [7]):

$$X_1^n V^2 + Y_1^n T^2 = Z_1^n P^2 \tag{5}$$

with the identity $X_1^n + Y_1^n = Z_1^n$ and $n \geq 3$.

So, we can also enunciate the following theorem:

Fundamental Theorem: *Fermat's Last Theorem is true only if the homogeneous ternary quadratic Diophantine equation (5) does not exist.*

Proof.

Nobody prevents us from assuming the evident solution $V = T = P = 1$ in the equazion (5) and with this we obtain the solution of Fermat equation: $X_1^n + Y_1^n = Z_1^n$.

Now from the Euler double equations (1) by subtracting , we have:

$$V^2 - T^2 = Z_1^n Q^2 = 0.$$

By definition, in Euler's *concordant* forms, Q is absolutely non-zero integer.

It follows that $Z_1^n = 0$, the homogeneous ternary quadratic Diophantine equation (5) it does not exist and Fermat's Last Theorem is proved.

We observe that the same result can be achieved immediately if we assume $V = T = P = 1$ already in Eqs.(1), in fact with Q non-zero integer we even have $X_1^n = Y_1^n = 0$ and therefore still $Z_1^n = 0$.

Theorem 1.1: *Fermat's Last Theorem is true if and only if is not possible a solution in integers of Eqs.(1) with Q non-zero integer, that is these are discordant forms.*

In practice, this means that if the system of quadratic Eqs.(1) admits only the trivial solutions $(m, 0, \pm m, \pm m)$, that include also (1,0,1,1), then the quadratic forms $P^2 + Y_1^n Q^2 = V^2$ and $P^2 - X_1^n Q^2 = T^2$ are a fortiori called *discordant* (see a proof in Section 4).

The proof ends here, as we have verified the close connection between the nature of Euler's double equations and Fermat's Last Theorem.

3 On Homogeneous Ternary Quadratic Diophantine Equation $aX^2 + bY^2 = cZ^2$

Theorem 2.1: *Let $x^n + y^n = z^n$, with g.c.d.$(x,y) = 1$ and $n \geq 3$ have a solution, then there exists an equation $ax^2 + by^2 = cz^2$ were a,b,c are relatively prime, square-free whose a solution could be reduced to a solution of Fermat's equation.*

Proof.

Let the equation $x^n + y^n = z^n$ where x, y, z are relatively prime and $n \geq 3$ is an odd integer have a solution $x = \alpha, y = \beta, z = \gamma$ where α, β, γ are pairwise relatively prime.

Using the "fundamental theorem of arithmetic" we can represent $\alpha = X_1 U_1^2$, $\beta = Y_1 U_2^2$, $\gamma = Z_1 U_3^2$, where X_1, Y_1, Z_1 are pairwise relatively prime and square-free natural numbers.

The equation

$$X_1 x^2 + Y_1 y^2 = Z_1 z^2$$

with $x = X_1^k U_1^n, y = Y_1^k U_2^n, z = Z_1^k U_3^n$ where $k = \frac{n-1}{2}$ and $n > 1$ odd number is the equation with the desired solution.

In this case we have:

$$X_1^n((U_1)^n)^2 + Y_1^n((U_2)^n)^2 = Z_1^n((U_3)^n)^2 \tag{6}$$

and with $V = (U_1)^n, T = (U_2)^n$ and $P = (U_3)^n$ we have:

$$X_1^n V^2 + Y_1^n T^2 = Z_1^n P^2$$

that is the Diophantine equation (5).

Theorem 2.2: *There is no homogeneous ternary quadratic Diophantine equation able to accommodate a solution of Fermat's equation* $x^n + y^n = z^n$ *when* $n > 2$.

Proof.
This Theorem is obviously true if Fermat's Last Theorem is true.

In conclusion we observe that with the following evident solutions: $U_1 = 1$, $U_2 = 1$ and $U_3 = 1$ and also $U_1 = U_2 = U_3$ in Eq.(6) we obtain the fundamental Hypothesis (Reductio ad Absurdum) of Fermat's Last Theorem:

$$X_1{}^n + Y_1{}^n = Z_1{}^n.$$

Now by the evident solutions, indicated above, we can derive an infinite number of solutions of Eq.(6).

Let's remember indeed that for Legendre's Theorem if a ternary quadratic homogeneous Diophantine equation (assuming a, b and c are fixed) has an integral solution, then the number of possible solutions is infinite, but this is not possible only by using the Euler double equations (1) in this particolar context.

4 Indeterminate Analysis of second degree.

Our goal is to take care of the resolution, into *integers*, of quadratic equation with *integer coefficients*, depending on n unknowns ([8], Cap. I, pp. 60-69).

We will develop our considerations on the equation in three unknowns:

$$F(X,Y,Z) = aX^2 + bY^2 + cZ^2 +$$

$$dXY + eXZ + fYZ = 0 \qquad (7)$$

warning that, all what we will say, extends immediately to the case of n unknowns.

Since the (7) is an equation homogeneous, if (A,B,C) are the solutions also (*mA, mB, mC*) are solutions.

Therefore we deem identical two solutions such as (A,B,C) and (*mA, mB, mC*).

Such assumption, will narrow the search to the only primitive solutions of Eq.(7), that is, to those in which X, Y and Z are pairwise relatively prime.

Let (x,y,z) be a solution in integers of the Eq.(7) and then $F(x,y,z) = 0$ and we put:

$$X = \rho \cdot x + \xi, Y = \rho \cdot y + \eta, Z = \rho \cdot z + \zeta \qquad (8)$$

where ξ, η, ζ are arbitrary integer constants and ρ an unknown to be determined, so that Eqs.(8) provide an integer solution for Eq.(7).

It must be:

$$F(X,Y,Z) = \rho^2 \left[ax^2 + by^2 + cz^2 + dxy + exz + fyz\right] +$$

$$+\rho \cdot [2a\xi \cdot x + 2b\eta \cdot y + 2c\zeta \cdot z] +$$

$$+\rho \cdot [d(\xi \cdot y + \eta \cdot x) + e(\xi \cdot z + \zeta \cdot x) + f(\eta \cdot z + \zeta \cdot y)] +$$

$$+ [a\xi\xi + b\eta\eta + c\zeta\zeta + d\xi\eta + e\xi\zeta + f\eta\zeta] = 0.$$

But the coefficient of ρ^2, equal to $F(x,y,z)$, is null and the known term is $F(\xi,\eta,\zeta)$, so, set equal to M (with $M \neq 0$ due to the arbitrary of ξ, η, ζ), the coefficient ρ of the above equation is equal to $\rho = -\frac{F(\xi,\eta,\zeta)}{M}$.

Consequently, if it is known an integer solution of Eq.(7), we have infinite other, by putting in Eqs.(8), in place of ρ, the value now found; then, unless the divisor M, we have:

$$X = \xi \cdot M - xF(\xi,\eta,\zeta); Y = \eta \cdot M - yF(\xi,\eta,\zeta);$$

$$Z = \zeta \cdot M - zF(\xi,\eta,\zeta). \qquad (9)$$

These are the general solutions of Eq.(7).

To prove it, we will show, by appropriately selecting ξ, η, ζ, the previous solutions provide a solution of Eq.(7), given arbitrarily.

Let this (A,B,C) , it is meanwhile F(A,B,C)=0; if now, in Eqs.(9) we write $\xi = A$, $\eta = B$, $\zeta = C$, we have the solution: *X=AM ; Y=BM ; Z=CM* , that, unless the factor M, it is identified with the one already provided.

In conclusion:

Theorem 3.1: *Let (x, y, z) be an integer solution of Eq.(7). All its integer solutions are given by Eqs.(9), unless the integer divider M.*

Now we solve the Pythagorean equation $F(X,Y,Z) = X^2 + Y^2 - Z^2 = 0$ in integer numbers.

Keeping in mind that this equation is homogeneous we know that we can consider identical the two solutions, as (1,0,1) and $(m,0,m)$.

Let's consider, at this point, the trivial solution (1,0,1) and we will have:

$M = 2(\xi - \zeta)$; $F(\xi,\eta,\zeta) = \xi^2 + \eta^2 - \zeta^2$ for which all the solutions, keeping in mind the Eqs.(9), are given by the relations:

$$X = 2\xi(\xi - \zeta) - \xi^2 - \eta^2 + \zeta^2 = (\xi - \zeta)^2 - \eta^2;$$

$$Y = 2\eta(\xi - \zeta);$$

$$Z = 2\zeta(\xi - \zeta) - \xi^2 - \eta^2 + \zeta^2 = -(\xi - \zeta)^2 - \eta^2.$$

Therefore assumed $(\xi-\zeta)=\theta$ and observed that from a solution (x,y,z) we get others changing sign to one, or two, or all (x,y,z), we have:

$$X=\theta^2-\eta^2 \quad ; \quad Y=2\theta\eta \quad ; \quad Z=\theta^2+\eta^2$$

which provide us with all the primitive integer solutions of Pythagorean equation.

In fact, since this equation is the Pythagorean triangle, in general, it accepts the following integer solutions, where θ,η are natural numbers and k a rational proportionality factor (the values of $X$and Y are interchangeable if necessary):

$$X=k\left(\theta^2-\eta^2\right); \quad Y=k(2\theta\eta); \quad Z=k\left(\theta^2+\eta^2\right).$$

Similar considerations for the equation $X^2+aY^2=Z^2$, of which one solution is (1,0,1).

In this case we have the following integer solutions, where θ,η are natural numbers and k a rational proportionality factor (see also [9], kap. V, §29, pp. 39-44):

$$X=k\left(\theta^2-a\eta^2\right);Y=k(2\theta\eta);Z=k\left(\theta^2+a\eta^2\right). \qquad (10)$$

At this stage, let us introduce the following Euler double equations:

$$P'^2+Y_1^nQ^2=V^2,\ P''^2-X_1^nQ^2=T''^2 \qquad (11)$$

with $X_1^n+Y_1^n=Z_1^n$ and $n\geq 3$ or

$$P'^2+Y_1^nQ^2=V^2,\ P'''^2-X_1^nQ'^2=T'''^2 \qquad (12)$$

with $X_1^n+Y_1^n=Z_1^n$ and $n\geq 3$.

From Eqs.(10) we have the following solutions of first Euler equation of Eqs.(11):

$$P'=k\left(\theta^2-Y_1^n\eta^2\right),Q=k(2\theta\eta),$$

$$V=k\left(\theta^2+Y_1^n\eta^2\right) \qquad (13)$$

and the following solutions of second Euler equation of Eqs.(11):

$$P''=k\left(\theta^2+X_1^n\eta^2\right),Q=k(2\theta\eta),$$

$$T''=k\left(\theta^2-X_1^n\eta^2\right) \qquad (14)$$

or the following solutions of second Euler equation of Eqs.(12):

$$P'''=k'\left(\theta'^2+X_1^n\eta'^2\right),Q'=k'\left(2\theta'\eta'\right),$$

$$T'''=k'\left(\theta'^2-X_1^n\eta'^2\right). \qquad (15)$$

Now assuming $V=T=P$ in the equations (1) with Q non-zero integer we have the following result due to Eqs.(13) and Eqs.(14):

$$P=P'=P''\Rightarrow -Y_1^n=X_1^n\Rightarrow Z_1^n=0$$

and

$$V=T''\Rightarrow Y_1^n=-X_1^n\Rightarrow Z_1^n=0.$$

While, with Eqs.(13) and Eqs.(15), we have:

$$P=P'=V\Rightarrow -Y_1^n=Y_1^n\Rightarrow Y_1^n=0$$

and

$$P=P'''=T'''\Rightarrow X_1^n=-X_1^n\Rightarrow X_1^n=0$$

and therefore still $Z_1^n=0$.

Euler's double equations (1) are *discordant* forms and Fermat's Last Theorem is true.

Additional Remarks

REMARK 1. The proof, here presented, is valid in the case of all odd exponents greater than one (see the proof of the Theorem 2.1).

Let's remember that a proof for an exponent natural $n>2$ implies that Fermat's Last Theorem is true for all multiples of n.

We observe however that the case $n=4$ and multiples of 4 was solved by Fermat ([10] ,Chap. II, pp. 50–56).

REMARK 2. In this work we have not used the proof of non-existence of the Frey elliptic curve, but we have limited ourselves to proof of non-existence of the single homogeneous ternary quadratic equation Eq.(6), defined with the Theorem 2.1, but whose origin [see Eq.(5)] is implicit in the nature of Euler's double equations.

REMARK 3. The double equations of Euler gave rise in different ways to the elliptic curve of Frey and to a particular homogeneous ternary quadratic equation: both characterized by the presence of ${X_1}^n$, ${Y_1}^n$ and ${Z_1}^n$ in their coefficients.

For this it was possible to use a similar strategy to build a proof of Fermat's Last Theorem.

References

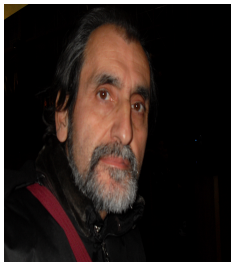
[1] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Ann. of Math. **141** (1995), pp. 443–551.

[2] R. Taylor, A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. **141** (1995), pp. 553–557.

[3] A. Weil, *Number Theory: an Approach Through History from Hammurapi to Legendre,* reprint of 1984 Edition , Birkhäuser, Boston, 2007.

[4] L. Euler, *De binis formulis speciei xx+myy et xx+nyy inter se concordibus et discordibus*, Mem. Acad. Sci. St.-Petersbourg, Opera Omnia: Ser. **1**, Vol. **5**, pp. 406–413 (1780).

[5] K. Ono, *Euler's concordant forms*, Acta Arithmetica **LXXVIII.2** (1996), no. 2,pp. 101–123.
[6] H. Davenport, *The Higher Arithmetic - an introduction to the theory of number*, 8th ed., Cambridge University Press, New York, 2008.
[7] F. Sidokhine, *Fermat's Last Theorem: Algebra, Geometry, and Number Theory*, https://arxiv.org/pdf/1607.06118v1.pdf, (2016).
[8] U. Bini, *Lezioni di Analisi Matematica*, vol. I, (coll. dir. da Francesco Severi), ed. Vallecchi, Firenze, 1931.
[9] L. E. Dickson, E. Bodewig, *Einfuehrung in die Zahlentheorie*, ed. B. G. Teubner, Leipzig/Berlin, 1931.
[10] W. Sierpinski, *Elementary Theory of Numbers,* Elsevier Science Publish'ers B.V., Amsterdam, Vol. **31,** 2^a English ed. 1988.



Andrea Ossicini graduated with a Degree in Mathematics with "110 cum laude", at the Institute of High Mathematics, "Guido Castelnuovo ", of University of Rome, "La Sapienza". After graduating, he began a brilliant career in Computer Science and worked as a Manager in several companies, dealing with Electronic Information Systems. Besides, for about 10 years he was a member of the Computer Measurement Group (CMG) - Italy, giving valuable contributions to professionals, in the field of Computer Performance Evaluation and Management. Alongside these work activities, he has always cultivated a profound interest in the History of Mathematics: his preferred Mathematician is Leonhard Euler, whom he obstinately studied for many years. Now he has a researcher and published some interesting works, in the field of Number Theory. In particular, he mentions two latest papers (I and II) concerning an Alternative Form of the Functional Equation for Riemann's Zeta Function, at Acts. Semin. Mat. Fis. Univ. Modena Reggio Emilia 56 (2008-2009), 95-111 and Acta Univ. Palacki. Olomuc., Fac. Rerum Nat., Math. 53, No. 2, 115-138 (2014).