J. of Ramanujan Society of Mathematics and Mathematical Sciences
Vol. 11, No. 1 (2023), pp. 43-54
DOI: 10.56827/JRSMMS.2023.1101.3 **ISSN (Online): 2582-5461**
ISSN (Print): 2319-1023

SOME DIOPHANTUS-FERMAT DOUBLE EQUATIONS EQUIVALENT TO FREY'S ELLIPTIC CURVE

Andrea Ossicini
Via delle Azzorre 352-D2, 00121 Roma, ITALY
E-mail : andrea.ossicini@gmail.com

(**Received:** *Oct. 10, 2023* **Accepted:** *Dec. 06, 2023* **Published:** *Dec. 30, 2023)*

Abstract: In this work I demonstrate that a possible origin of the Frey elliptic curve derives from an appropriate use of the double equations of Diophantus-Fermat and from an isomorphism: a birational application between the double equations and an elliptic curve.
From this origin I deduce a Fundamental Theorem which allows an exact reformulation of Fermat's Last Theorem.
A complete proof of this Theorem, consisting of a system of homogeneous ternary quadratic Diophantine equations, is certainly possible also through methods known and discovered by Fermat,in order to solve his extraordinary equation.

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

2020 Mathematics Subject Classification: 11D41 (primary), 11G05 (secondary).

1. The double equations of Diophantus-Fermat and the Frey elliptic curve

A careful reading of the existing documentation about the Diophantine problems, reveals that Fermat, and especially Euler, often used the so-called "double equations" of Diophantus, that is $ax^2 + bx + c = z^2$; $a'x^2 + b'x + c' = t^2$ with the conditions that a and a', or c and c' are squares.
These conditions ensure the existence of rational solutions of the double equations.

These equations can be written in a more general form as:

$$ax^2 + 2bxy + cy^2 = z^2 \qquad a'x^2 + 2b'xy + c'y^2 = t^2. \tag{1}$$

Indeed usually both Fermat and Euler considered only the curves of those forms which have, in the projective space, at least one "visible" rational point.
Fermat and Euler derive from few evident solutions an infinite number of solutions. Under this last hypothesis ([5], Chap. II, Appendix III, pp. 135–139) the curve determined by the equations (1) results isomorphic to the one given by

$$Y^2 = X\left[(b'X - b)^2 - (a'X - a)(c'X - c)\right] \tag{2}$$

i.e. an elliptic curve (see also Appendix A).
In fact, an elliptic curve, which has at least one rational point, can be written as a cubic $y^2 = f(x)$, where f is a polynomial of degree 3.
Given this, we consider the following system, consisting of a pair of ≪double equations ≫

$$\begin{cases} (3)_1 & X_1^n V^2 + Y_1^n T^2 = U'^2 \qquad V^2 - T^2 = W^2 \\ (3)_2 & X_1^n W^2 + Z_1^n T^2 = U'^2 \qquad W^2 + T^2 = V^2 \end{cases} \tag{3}$$

where X_1, Y_1, Z_1 are integer numbers (positive or negative), pairwise relatively primes, $n > 2$ is a natural number and U', V, W, T are integer variables.
Applying the isomorphism described by Eq. (2) we obtain, from the first two equations of the system (3), i.e. the $(3)_1$, the elliptic curve

$$Y^2 = X(X - X_1^n)(X + Y_1^n), \tag{4}$$

and from the other two equations, the $(3)_2$, the further elliptic curve

$$Y^2 = -X(X - X_1^n)(X - Z_1^n). \tag{5}$$

Combining Eq. (4) and Eq. (5) and using the relation $X = X_1^n/2$ one obtains the following identity:

$$X_1^n + Y_1^n = Z_1^n. \tag{6}$$

Now the elliptic curve (4), together with the identity (6), is nothing but the Frey elliptic curve ([1], pp.154–156).
In Mathematics, a Frey curve, or Frey–Hellegouarch curve, is the elliptic curve:

$$Y^2 = X(X - X_1^n)(X + Y_1^n) \tag{7}$$

or, equivalently :

$$Y^2 = X\left[X^2 + X\left(Y_1^n - X_1^n\right) - X_1^n Y_1^n\right] \tag{8}$$

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.
Frey suggested, in 1985, that the existence of a non-trivial solution to $X^n + Y^n = Z^n$ would imply the existence of a non-modular elliptic curve,viz.

$$Y^2 = X(X - X^n)(X + Y^n).$$

This suggestion was proved by Ribet in 1986.
This curve is semi-stable and in 1993 Wiles announced a proof (subsequently found to need another key ingredient, furnished by Wiles and Taylor) that every semi-stable elliptic curve is modular, the semi-stable case of the Taniyama-Shimura-Weil conjecture ([6] and [4]).
Hence no non-trivial $X^n + Y^n = Z^n$ can exist.
Moreover, as Euler found out, treating similar problems, regarding algebraic curves of genus 1, the two problems, connected to curves (4) and (5), are completely equivalent.
In our case it is simple to verify that the elliptic curve (5) can be reduced to (4) by the transformation $X \Rightarrow -X + X_1^n$ and the identity (6).

2. The Diophantine System

One can reduce the system (3) to the following Diophantine system

$$\begin{cases} X_1^n V^2 + Y_1^n T^2 = U'^2 \\ X_1^n W^2 + Z_1^n T^2 = U'^2 \\ W^2 + T^2 = V^2. \end{cases} \tag{9}$$

Our proof of Fermat's Last Theorem consists in the demonstration that it is not possible a resolution in whole numbers, all different from zero, of a system derived from system (9), but analogous, [see section 4 and system (19)], with integer coefficients and using integer variables U, W', T', V'.
From the first two equations of the system (9) one obtains

$$X_1^n V^2 + Y_1^n T^2 = X_1^n W^2 + Z_1^n T^2. \tag{10}$$

Now from Eq.(10) is

$$X_1^n \left(V^2 - W^2\right) = \left(Z_1^n - Y_1^n\right)\ T^2. \tag{11}$$

Eq. (11) results in identity (6) if the third equation in the systems (9), $W^2 + T^2 = V^2$, is satisfied.
In fact, since this equation is the Pythagorean triangle, in general, it accepts the following integer solutions, where p, q are natural numbers and k a proportionality factor (the values of W and T are interchangeable if necessary):

$$W = k\,(2pq)\,; \quad T = k\left(p^2 - q^2\right); \quad V = k\left(p^2 + q^2\right).$$

We can therefore consider also the primitive integer solutions with $p, q \in$ N

$$W = 2pq\,; \qquad T = p^2 - q^2; \qquad V = p^2 + q^2. \tag{12}$$

Thus Eq. (11), with p and q relatively prime, of opposite parity and $p > q > 0$ now is reduced to the identity (6).

3. On Homogeneous Ternary Quadratic Diophantine Equations

$$aX^2 + bY^2 - cZ^2 = 0.$$

Theorem 3.1. *Let $x^n + y^n = z^n$, with $(x, y) = 1$ and $n \geq 3$ has a solution, then there exists an equation $ax^2 + by^2 = cz^2$, where a, b, c are relatively prime and reduced to the minimum terms, whose a solution could be reduced to a solution of Fermat's equation.*

Proof. Let X_1, Y_1, Z_1 be three whole numbers pairwise relatively prime such as to satisfy the Fermat equation $x^n + y^n = z^n$.
Then the following homogeneous ternary quadratic Diophantine equation, with $(V, T, P) = 1$ exists:

$$X_1^n V^2 + Y_1^n T^2 = Z_1^n P^2. \tag{13}$$

We observe that with the following particular nontrivial solutions:
$V = 1, T = 1$ and $P = 1$ or $V = T = P$ in Eq.(13) we obtain the fundamental Hypothesis (Reductio ad Absurdum) of the F.L.T.:

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

Now by the evident solutions, indicated above, we can derive an infinite number of solutions of Eq.(13).

Let's remember 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.
Having said this, it is possible to transform the previous Diophantine equation (13) into the following equivalent equation,with $(V', T', P') = 1$:

$$X_1 V'^2 + Y_1 T'^2 = Z_1 P'^2. \tag{14}$$

It is sufficient to assume $V' = X_1^k V, T' = Y_1^k T, P' = Z_1^k P$ where $k = \frac{n-1}{2}$ and $n > 1$ odd number.
Using the "fundamental theorem of Arithmetic" we can represent ([3], Theorem 19, p. 31): $X_1 = X_2 U_1^2,\ Y_1 = Y_2 U_2^2,\ Z_1 = Z_2 U_3^2$.
In this case is possible to transform the previous Diophantine equation (14) into the following equivalent Diophantine equation with the relative coefficients reduced to the minimum terms:

$$X_2 V''^2 + Y_2 T''^2 = Z_2 P''^2.$$

In fact just assume $V'' = U_1 V', T'' = U_2 T', P'' = U_3 P'$.
We observe that X_2, Y_2, Z_2 are pairwise relatively prime and square-free numbers.
The proof ends here by properly verifying also the nature of exponent n.

Theorem 3.2. *Let's suppose that $x^n + y^n = z^n$, with $n \geq 3$ has a solution, in this case we will have an equation $ax^2 + by^2 = cz^2$, where c is a square, whose solution could be reduced to a solution of Fermat's equation.*

Proof. From Theorem 3.1 [see Eq.(13)] we have the following equation $X_1^n V^2 + Y_1^n T^2 = Z_1^n U^2$ that could be reduced to a solution of Fermat's equation with $n \geq 3$ odd integer.
Now multiplying the coefficient X_1^n, Y_1^n, Z_1^n by factor Z_1^n we have

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

and with $X_0 = X_1 Z_1,\ Y_0 = Y_1 Z_1,\ Z_0 = Z_1^2$ we get

$$X_0^n V^2 + Y_0^n T^2 = Z_0^n U^2 \tag{15}$$

and $Z_0^n = (Z_1^n)^2$, that is a square.
In this case we have also, with g.c.d.$(X_0, Y_0) = Z_1$, the equation of Fermat

$$X_0^n + Y_0^n = Z_0^n. \tag{16}$$

The proof ends here.

4. The Lost Proof

At this point, multiplying the Eq.(15) by factoring quadratic Z_0^n we have

$$X_0^n Z_0^n V^2 + Y_0^n Z_0^n T^2 = Z_0^n Z_0^n U^2$$

and finally with $V' = Z_0^{\frac{n}{2}} V$, $T' = Z_0^{\frac{n}{2}} T$ we obtain $X_0^n V'^2 + Y_0^n T'^2 = (Z_0^n)^2 U^2$.
That said, let's consider the following double equations of Diophantus-Fermat, necessary to give rise to the well known Frey's elliptic curve

$$X_0^n V'^2 + Y_0^n T'^2 = (Z_0^n)^2 U^2 = U''^2 \ ; \ V'^2 - T'^2 = W'^2 : \tag{17}$$

$$Y^2 = X\,(X - X_0^n)\,(X + Y_0^n)\,.$$

that together with the identity (16) can be rewritten in

$$Z_0^{2n} U^2 = X_0^n V'^2 + Y_0^n T'^2 = X_0^n W'^2 + Z_0^n T'^2. \tag{18}$$

In practice we have rewritten the system (9) in the following Diophantine system:

$$\begin{cases} X_0^n V'^2 + Y_0^n T'^2 = Z_0^{2n} U^2 \\ X_0^n W'^2 + Z_0^n T'^2 = Z_0^{2n} U^2 \\ W'^2 + T'^2 = V'^2. \end{cases} \tag{19}$$

Eqs.(18) give us:

$$U^2 \left[Z_0^n\right]^2 - V'^2 \left[Z_0^n\right] + W'^2 Y_0^n = 0 \tag{20}$$

or equivalently

$$U^2 \left[Z_0^n\right]^2 - T'^2 \left[Z_0^n\right] - W'^2 X_0^n = 0. \tag{21}$$

Z_0^n is a square, so the product of the two roots in Eq. (20), through the Viete-Girard formulas, is

$$\left[Z_0^n\right]_1 \cdot \left[Z_0^n\right]_2 = \tfrac{W'^2 Y_0^n}{U^2} \Rightarrow Y_0^n, \text{ which is a square,}$$

and in Eq.(21) is

$$\left[Z_0^n\right]_1 \cdot \left[Z_0^n\right]_2 = \tfrac{-W'^2 X_0^n}{U^2} \Rightarrow -X_0^n, \text{ which is a square.}$$

These latest results are certainly true only with the assumption that W'^2 is non-zero.
From Theorem 3.1 we have that X_1, Y_1, Z_1 are pairwise relatively prime and with $Y_0^n = \square^1 = Y_1^n Z_1^n$ and $X_0^n = -\square = X_1^n Z_1^n$ we obtain:

$$Z_1^n = \square \ ; \ Y_1^n = \square \ ; \ X_1^n = -\square \ .$$

[1]The symbol $\square$ represents an indeterminate square.

With this last result, obtained also thanks to the use of a Pythagorean equation [see Eqs.(17)], one finds also:

$$[Z_0^n]_1 \cdot [Z_0^n]_2 = \frac{W'^2 Y_0^n}{U^2} = \frac{-W'^2 X_0^n}{U^2}.$$

This gives finally the special solution:

$$Y_1^n = -X_1^n \Rightarrow Z_1^n = 0.$$

Consequently the Diophantine system (19) does not admit integer solutions.
A further confirmation of these conclusions comes from what is reported below.
Keeping in mind that Eq. (20) and Eq. (21) have arisen from rewriting the original System (9) into System (19), we have to consider the various substitutions we have subsequently applied and in particular by $V' = Z_0^{\frac{n}{2}} V$, $T' = Z_0^{\frac{n}{2}} T$ e $W' = Z_0^{\frac{n}{2}} W$ (because of the Pythagorean identity $V^2 = T^2 + W^2$) we can rewrite Eq. (20) and Eq. (21) as follows:

$$[Z_1^n]^3 \left[Z_1^n \left(U^2 - V^2 \right) + W^2 Y_1^n \right] = 0 \tag{22}$$

or equivalently

$$[Z_1^n]^3 \left[Z_1^n \left(U^2 - T^2 \right) - W^2 X_1^n \right] = 0. \tag{23}$$

At this point, canceling the second factors of the two products (22) and (23) we have:

$$[Z_1^n (V^2 - U^2)] = W^2 Y_1^n \qquad \text{and} \qquad [Z_1^n (U^2 - T^2)] = W^2 X_1^n.$$

By dividing them among themselves, with Z_1^n e W^2 different from zero, and simplifying we get back the Diophantine equation original:

$$X_1^n V^2 + Y_1^n T^2 = Z_1^n U^2. \tag{24}$$

Therefore this equation can exist only on condition that Z_1^n e W^2 are both non-zero. In addition, the quantities $(V^2 - U^2)$ and $(U^2 - T^2)$ cannot be null, because the Pythagorean identity would imply $W^2 = V^2 - T^2 = 0$.
Now from Eqs. (20) and (21), considering the sum of the roots, through the Viete-Girard formulas, we have:

$$[Z_0^n]_1 + [Z_0^n]_2 = \tfrac{V'^2}{U^2}$$

and

$$[Z_0^n]_1 + [Z_0^n]_2 = \tfrac{T'^2}{U^2}.$$

The two sums must be equal, therefore from $V'^2 = Z_0^n V^2$ and $T'^2 = Z_0^n T^2$ we get that if Z_0^n is different from zero:

$$V'^2 = T'^2 \Rightarrow V^2 = T^2 \Rightarrow W^2 = 0. \tag{25}$$

In summary, I would like to state that Eqs (20) and (21) through their roots (see products and relative sums) they only provide the following result:

$$Z_1^n = 0 \quad or \quad W^2 = 0.$$

which prove, in an absolute way, on the one hand the non existence of the original Diophantine equation Eq (24) (as it is not can build) on the other hand the "power" of the Diophantus System original (9),which includes among its three homogeneous ternary equations of second degree also a Pythagorean equation (PT).
The need for such a soluble Pythagorean equation (PT) in integers, it is fully justified by a proposition stated and proved by A. Weil, who established the existence of an isomorifism between some appropriate double equations of Diophantus-Fermat and a certain elliptic curve, or the existence of a birational application between the double equations and an elliptic curve.

5. Analytical digressions

There is no doubt that the system (19), inspired by system (9), represents a true "lockpick" of the Fermat Last Theorem.
Through the former system, keeping in mind always the possibility of exchanging the role of X_0 and Y_0 into identity (16), we are able to establish the following Fundamental Theorem:

The Fermat Last Theorem is true if and only if a solution in integers, all different from zero, of the following Diophantine system, made of three homogeneous equations of second degree, with integer coefficients X_0^n,Y_0^n,Z_0^n, where n is a natural number > 2 and with U, T', V', W' integer indeterminates is not possible.

$$\begin{cases} X_0^n V'^2 + Y_0^n T'^2 = Z_0^{2n} U^2 \\ X_0^n W'^2 + Z_0^n T'^2 = Z_0^{2n} U^2 \\ W'^2 + T'^2 = V'^2. \end{cases} \tag{26}$$

The presence of a Pythagorean equation in this system has been proved to be essential, not only to connect the most general Fermat's equation to the supposed Frey's elliptic curve, but to demonstrate the above indicated Fundamental Theorem (see Section 4) and at the end to provide also a proof of Fermat's Last Theorem, using a method of Reductio ad Absurdum.

6. Conclusions

In this paper I demonstrate that a possible origin of Frey's elliptic curve derives from an appropriate use of the so-called "double equations" of Diophantus-Fermat

and from an isomorphism: a birational application between the double equations and an elliptic curve.
This Frey elliptic curve does not exist ([1], pp. 154–156) and from this derives indirectly, as an absurd, the Fermat Last Theorem.
In this work we wanted to emphasize that a proof of the Fermat Last Theorem can not be separated by the strong links with the supposed Frey elliptic curve, although this does not mean that Fermat, in another way, was unable to produce our own proof.

Appendix A. Elliptic Curves from Frey to Diophantus

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

$$Y^2 = X\left(X - X_1^n\right)\left(X + Y_1^n\right) \tag{27}$$

or, equivalently:

$$Y^2 = X\left[X^2 + X\left(Y_1^n - X_1^n\right) - X_1^n Y_1^n\right] \tag{28}$$

associated with a (hypothetical) solution of Fermat's equation : $X_1^n + Y_1^n = Z_1^n$.
In the language of Diophantus and of Fermat, we consider the following "double equation":

$$ax^2 + 2bxy + cy^2 = z^2 \qquad a'x^2 + 2b'xy + c'y^2 = t^2. \tag{29}$$

In Weil's Appendix III ([5], Ch. II, pp.135-139) he established (modulo the existence of a rational point) an isomorphism between the curve defined by the equations (29) and a certain elliptic curve defined by:

$$Y^2 = X\left[\left(b'X - b\right)^2 - \left(a'X - a\right)\left(c'X - c\right)\right] =$$

$$X\left[\left(b'^2 - a'c'\right)X^2 + \left(ca' + ac' - 2bb'\right)X - ac + b^2\right]. \tag{30}$$

Let's suppose that the first double equation is $ax^2 + Y_1^n y^2 = z^2$.
In this case we have considered the following assumptions in Eq.(30): $b = 0$ and $c = Y_1^n$.
Now the coefficient of X^2 in Eq.(28) is equal to coefficient of X^2 in Eq.(30): $(b'^2 - a'c') = 1$ and the coefficient of X and the known term in Eq.(28) are equal to the ones in Eq.(30):

$$(ca' + ac' - 2bb') = Y_1^n - X_1^n; \;\; -ac + b^2 = -X_1^n Y_1^n, \tag{31}$$

but with $b = 0$ and $c = Y_1^n$ we have

$$-ac = -X_1^n Y_1^n \Rightarrow -aY_1^n = -X_1^n Y_1^n \Rightarrow a = X_1^n.$$

From the first of Eq.(31) we have $Y_1^n a' + X_1^n c' = Y_1^n - X_1^n \Rightarrow\ a' = 1$,
$c' = -1\ \Rightarrow b' = 0$.
With these results we have the following double equation of Diophantus:
$X_1^n x^2 + Y_1^n y^2 = z^2$ and $x^2 - y^2 = t^2$ equivalently to $X_1^n V^2 + Y_1^n T^2 = U'^2$ and $V^2 - T^2 = W^2$ [see the equations of the system (3), i.e. the $(3)_1$].

Additional Remarks

Remark 1. Fermat's idea, in my opinion, to prove his Last Theorem, could take place through the following logical steps:

1- Define a quadratic and homogeneous ternary equation, in the normal form of Lagrange, able to accommodate a solution, with n greater than or equal to 3, of its extraordinary equation (6) [see Theorem 3.2].

2- Connect this appropriate Diophantine equation of 2nd degree to the classic Pythagorean equation [see Eqs.(17)] to build a complete Diophantine system capable of determining its possible whole solution [see system (19)] .

3- Establish that this Diophantine system does not admit congruent integer solutions and therefore as a consequence of this, there are no three integers that satisfy Fermat's equation (6).

Remark 2. The truth is that the impossibility to solve single equations can be proved as deduction from the impossibility of solving a system of equations.
The Fundamental Theorem is a reformulation of the Fermat Last Theorem: his following statements are equivalent:
(A) Fermat's Last Theorem is true $\Leftrightarrow$ (A') The Diophantine System does not allow integer solutions different from zero.
Let $n > 2$; there is a bijection between the following sets:
(S) the set of solutions (x, y, z) of Fermat's Equation, where x, y, z are nonzero natural numbers; and
(S') the set of solutions (u, t', v', w') of the Diophantine System, where u, t', v', w' are nonzero natural numbers.
The set of solutions of (S) and (S') are the same, that gives rise to an empty set, as shown in the Fundamental Theorem.
In the literature there are other Diophantine equations, that were compared to Fermat's equation, i.e. a first result, due to Lebesgue in 1840, is the following Theorem:

If Fermat's Last Theorem is true for the exponent $n \geq 3$ then the equation $X^{2n} + Y^{2n} = Z^2$ has only trivial solutions.

The proof of this theorem is extremely simple and is found in [2].
In this case, however, it cannot be said that Lebesgue's theorem is equivalent to

Fermat's Last Theorem, while on the contrary, the Fundamental Theorem is just equivalent to Fermat's last theorem.

Remark 3. I conclude this work with the following observation by A. Weil ([5], Chap. IV, § VI, pp. 335–336): " Infinite descent a' la Fermat depends ordinarily upon no more than the following simple observation: if the product $\alpha \cdot \beta$ of two ordinary integers (resp. two integers in an algebraic number-field) is equal to an m-th power, and if the g.c.d. of α and β can take its values only in a given finite set of integers (resp. of ideals), then both α and β are m-th powers, up to factors which can take their values only in some assignable finite set." (See the section 4: The Lost Proof.)

References

[1] Davenport H., The Higher Arithmetic - an introduction to the theory of number, 8th ed., Cambridge University Press, New York, 2008.

[2] Lebesgue V. A., Sur un thèoréme de Fermat, J. Math. Pures Appl., 5 (1840), 184-185.

[3] Sierpinski W., Elementary Theory of Numbers, Elsevier Science Publish'ers B. V., Amsterdam, Vol. 31, 2^a English ed. 1988.

[4] Taylor R., Wiles A., Ring-theoretic properties of certain Hecke algebras, Ann. of Math., 141 (1995), 553-57.

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

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