Euler’s proof of Fermat’s Last Theorem

for \( n = 3 \) is incorrect

Nguyen Van Quang
Hue - Vietnam, 05 - 2016

Abstract

We have spotted an error of Euler’s proof, so that the used infinite descent is impossible in his proof (case A).

1 Euler’s proof for \( n = 3 \)

First, we rewrite a proof for \( n = 3 \), which was proven by Euler in 1770 as follows:

As Fermat did for the case \( n = 4 \), Euler used the technique of infinite descent. The proof assumes a solution \((x,y,z)\) to the equation \( x^3 + y^3 + z^3 = 0 \), where the three non-zero integers \( x, y, z \) are pairwise coprime and not all positive. One of three must be even, whereas the other two are odd. Without loss of generality, \( z \) may be assumed to be even.

Since \( x \) and \( y \) are both odd, their sum and difference are both even numbers.

\[
2u = x + y \\
2v = x - y
\]

Where the non-zero integers \( u \) and \( v \) are coprime and have different parity (one is even, the other odd). Since \( x = u + v \) and \( y = u - v \), it follows that

\[-z^3 = (u + v)^3 + (u - v)^3 = 2u(u^2 + 3v^2)\]

Since \( u \) and \( v \) have opposite parity, \( u^2 + 3v^2 \) is always an odd number. Therefore, since \( z \) even, \( u \) is even and \( v \) is odd. Since \( u \) and \( v \) are coprime, the greatest common divisor of \( 2u \) and \( u^2 + 3v^2 \) is either 1 (case A) or 3 (case B).

Proof for Case A

In this case, the two factors of \(-z^3\) are coprime. This implies that 3 does not divide \( u \) and the two factors are cubes of two smaller numbers, \( r \) and \( s \).

\[
2u = r^3 \\
u^2 + 3v^2 = s^3
\]

Since \( u^2 + 3v^2 \) is odd, so is \( s \). Then Euler claimed that it is possible to write:

\[s = e^2 + 3f^2\]

which \( e \) and \( f \) integers, so that

\[u = e(e^2 - 9f^2)\]
\[ v = 3f(e^2 - f^2) \]

Since \( u \) is even and \( v \) is odd, then \( e \) is even and \( f \) is odd. Since

\[ r^3 = 2u = 2e(e - 3f)(e + 3f) \]

The factors \( 2e, (e - 3f), (e + 3f) \) are coprime, since 3 can not divide \( e \): if \( e \) were divisible by 3, then 3 would divide \( u \), violating the designation of \( u \) and \( v \) as coprime. Since the three factors on the right-hand side are coprime, they must individually equal cubes of smaller integers

\[-2e = k^3\]
\[ e - 3f = l^3\]
\[ e + 3f = m^3\]

Which yields a smaller solution \( k^3 + l^3 + m^3 = 0 \). Therefore, by the argument of infinite descent, the original solution \((x, y, z)\) was impossible.

**Proof for Case B**

In this case, the greatest common divisor of \( 2u \) and \( u^2 + 3v^2 \) is 3. That implies that 3 divides \( u \), and one may express \( u = 3w \) in terms of a smaller integer \( w \). Since \( u \) is divisible by 4, so is \( w \), hence, \( w \) is also even. since \( u \) and \( v \) are coprime, so are \( v \) and \( w \). Therefore, neither 3 nor 4 divide \( v \).

Substituting \( u \) by \( w \) in the equation for \( z^3 \) yields

\[-z^3 = 6w(9w^2 + 3v^2) = 18w(3w^2 + v^2)\]

Because \( v \) and \( w \) are coprime, and because 3 does not divide \( v \), then 18w and \( 3w^2 + v^2 \) are also coprime. Therefore, since their product is a cube, they are each the cube of smaller integers, \( r \) and \( s \)

\[ 18w = r^3\]
\[ 3w^2 + v^2 = s^3\]

By the step as in case A, it is possible to write:

\[ s = e^2 + 3f^2\]

which \( e \) and \( f \) integer, so that

\[ v = e(e^2 - 9f^2)\]
\[ w = 3f(e^2 - f^2)\]

Thus, \( e \) is odd and \( f \) is even, because \( v \) is odd. The expression for 18w then becomes

\[ r^3 = 18w = 54f(e^2 - f^2) = 54f(e + f)(e - f)\]

Since \( 3^3 \) divides \( r^3 \) we have that 3 divides \( r \), so \((r/3)^3\) is an integer that equals \( 2f(e + f)(e - f)\). Since \( e \) and \( f \) are coprime, so are the three factors \( 2e, e + f, \) and \( e - f \), therefore, they are each the cube of smaller integers \( k, l, \) and \( m \).

\[-2f = k^3\]
\[ e + f = l^3\]
\[ e - f = m^3\]

which yields a smaller solution \( k^3 + l^3 + m^3 = 0 \). Therefore, by the argument of infinite descent, the original solution \((x, y, z)\) was impossible.
2 Arguments

**Lemma.** if the equation $x^3 + y^3 + z^3 = 0$ is satisfied in integers, then one of the numbers $x$, $y$, and $z$ must be divisible by 3

**proof.** From the equation $x^3 + y^3 + z^3 = 0$, we obtain:

$$(x + y + z)^3 = 3(z + x)(z + y)(x + y)$$

Then, $x + y + z$ is divisible by 3, $(x + y + z)^3$ is divisible by $3^3$

So $(z + x)(z + y)(x + y)$ must be divisible by 3:

If $z + x$ is divisible by 3, then $y$ is divisible by 3

If $z + y$ is divisible by 3, then $x$ is divisible by 3

If $x + y$ is divisible by 3, then $z$ is divisible by 3

Hence, one of $x$, $y$, and $z$ must be divisible by 3.

**Mistake in Euler’s proof**

For the case A

Since step,

$$u = e(e^2 - 9f^2)$$

$$v = 3f(e^2 - f^2)$$

Euler already considered only $u$, and passed over $v$, and it was a gap of proof as follows:

Since $v = 3f(e^2 - f^2)$, then $v$ is divisible by 3.

Since

$$2v = x - y$$

Then, $x - y$ is divisible by 3, hence, both of them are divisible by 3, or both not divisible by 3. Since $x$ and $y$ are coprime, then $x$ and $y$ have not common divisor, so both $x$ and $y$ are not divisible by 3. By lemma above, $z$ must be divisible by 3, which implies that $2u$ and $u^2 + 3v^2$ have common divisor 3, a contradiction. Case A is impossible!

Or by other argument as follows:

$2u = r^3$ then $u = 2^2r^{33}$, since in the case A, $u$ is not divisible by 3, then $r'$ is not divisible by 3

It gives:

$$2^2r^{33} = e(e^2 - 9f^2)$$

$$9ef^2 = e^3 - 2^2r^{33}$$

$$9ef^2 = e^3 - r^{33} - 3r^{33}$$

The term: $e^3 - r^{33} = (e - r')((e - r')^2 + 3er')$ is not divisible by 3, or is divisible by $3^2$

Hence, Left hand side of equation: $9ef^2 = e^3 - r^{33} - 3r^{33}$ is divisible by $3^2$, right hand side is not. Case A is impossible!

These above arguments is the correct proof for case A if

$$u = e(e^2 - 9f^2)$$

$$v = 3f(e^2 - f^2)$$

is the only way for $u^2 + 3v^2$ to be expressed as a cube. However, Euler only showed that is the possible way.
References
1. Proof of Fermat’s Last Theorem for specific exponents- Wikipedia.
2. Quang N V, A proof of the four color theorem by induction. Vixra:1601.0247(CO)
Email:
nguyenvquang67@gmail.com
quangnlu67@yahoo.com.vn