J. Indones. Math. Soc.
Vol. 19, No. 1 (2013), pp. 61–66.

AN OTHER PROOF OF THE INSOLUBILITY OF FERMAT'S CUBIC EQUATION IN EISENSTEIN'S RING

Elias Lampakis

Kiparissia, T.K: 24500, Greece
eliaslampakis@yahoo.gr

Abstract. We present an other proof of the well known insolubility of Fermat's equation $x^3 + y^3 = z^3$ in Eisenstein's ring $\mathbb{Z}[\omega]$ when $\omega^3 = 1$, $\omega \neq 1$, $x\,y\,z \neq 0$. Assuming the existence of a nontrivial solution $(a_1 + b_1\,\omega,\ a_2 + b_2\,\omega,\ a_3 + b_3\,\omega)$ the proof exploits the algebraic properties, (degree, kind of roots, coefficients' relations), of the polynomial $f(x) = (a_1 + b_1\,x)^3 + (a_2 + b_2\,x)^3 - (a_3 + b_3\,x)^3$. In the course of action, the well known algebraic structure of the group of rational points of the elliptic curve $y^2 = x^3 + 16$ provides the final result.

Key words: Fermat's cubic equation, Eisenstein's ring, elliptic curves.

Abstrak. Kami menyajikan sebuah bukti lain dari insolubilitas terkenal dari persamaan Fermat $x^3+y^3 = z^3$ pada ring Eisenstein $\mathbb{Z}[\omega]$ dengan $\omega^3 = 1$, $\omega \neq 1$, $x\,y\,z \neq 0$. Akibat pengasumsian keberadaan solusi nontrivial $(a_1+b_1\,\omega,\ a_2+b_2\,\omega,\ a_3+b_3\,\omega)$, diberikan bukti dengan memanfaatkan sifat-sifat aljabar (derajat, jenis akar, dan relasi koefisien) dari polinom $f(x) = (a_1+b_1\,x)^3+(a_2+b_2\,x)^3-(a_3+b_3\,x)^3$. Dalam hal penerapan lebih lanjut, struktur aljabar terkenal dari grup titik-titik rasional kurva eliptik $y^2 = x^3 + 16$ memberikan hasil akhir.

Kata kunci: Persamaan kubik Fermat, ring Eisenstein, kurva-kurva eliptik.

1. Introduction

When $\omega^3 = 1, \omega \neq 1$ it is well known Ireland and Rosen [2, p. 248], Ribenboim [5, p. 43] that the Fermat type cubic equation

$$x^3 + y^3 = z^3, \tag{1}$$

2000 Mathematics Subject Classification: 11D41, 11D25, 11G05.
Received: 16-03-2013, revised: 19-03-2013, accepted: 20-03-2013.

has only trivial ($x\,y\,z = 0$) solutions in $\mathbb{Z}[\omega]$. The proof is based on the algebraic properties of $\mathbb{Z}[\omega]$ as a unique factorization domain. It is a classical approach within the frame of Algebraic Number Theory.

In this note we present an other method for proving the insolubility of (1) in $\mathbb{Z}[\omega]$ when $x\,y\,z \neq 0$. Our approach exploits the algebraic properties, (degree, kind of roots, coefficients' relations), of the polynomial

$$\begin{aligned} f(x) &= (a_1 + b_1\,x)^3 + (a_2 + b_2\,x)^3 - (a_3 + b_3\,x)^3 = \\ &= [p_1(x)]^3 + [p_2(x)]^3 - [p_3(x)]^3 \in \mathbb{Z}[x], \end{aligned} \tag{2}$$

when

$$(x_0, y_0, z_0) = (a_1 + b_1\,\omega,\ a_2 + b_2\,\omega,\ a_3 + b_3\,\omega), \quad (x_0\,y_0\,z_0 \neq 0), \tag{3}$$

is a hypothetical nontrivial solution of (1) in $\mathbb{Z}[\omega]$. In the course of action, we show that the existence of (3), through the properties of (2), implies the existence of a rational point (X_0, Y_0), $(X_0\,Y_0 \neq 0)$, on the elliptic curve

$$y^2 = x^3 + 16. \tag{4}$$

The structure of the group of rational points on (4) is well known Husmöler [1], Cremona's Elliptic Curves software package Mwrank [3], `Pari/GP` software package [4], Cremona's Elliptic Curves tables [6]. Equation (4) has rank 0 and torsion subgroup of order 3. Apart from the point at infinity, $(x, y) = (0, \pm 4)$ are the only rational points on (4). The latter contradicts the constraint $X_0\,Y_0 \neq 0$ thus rejecting (3) as a solution of (1) in $\mathbb{Z}[\omega]$.

2. Algebraic Properties of $f(x)$

Assuming the existence of a nontrivial solution $(x_0, y_0, z_0) = (a_1 + b_1\,\omega,\ a_2 + b_2\,\omega,\ a_3 + b_3\,\omega)$ of (1) in $\mathbb{Z}[\omega]$, some necessary constraints upon the a_m's, b_m's, $m \in I = \{1, 2, 3\}$ follow. The condition of $x_0\,y_0\,z_0 \neq 0$ implies

$$|a_m| + |b_m| \neq 0,\ \forall\, m \in I. \tag{5}$$

If $a_m = 0$ or $b_m = 0$ for all $m \in I$, then a substitution of (x_0, y_0, z_0) into (1) implies either $b_1^3 + b_2^3 = b_3^3$ or $a_1^3 + a_2^3 = a_3^3$ respectively. Since the a_m's, b_m's are in $\mathbb{Z}$ the latter holds only when at least one of the b_m's or the a_m's respectively is zero. Then at least one of the $a_m + b_m\,\omega$ is zero contradicting (5). Hence,

$$|a_1| + |a_2| + |a_3| \neq 0 \text{ and } |b_1| + |b_2| + |b_3| \neq 0. \tag{6}$$

A substitution of (x_0, y_0, z_0) into (1) clearly implies $f(\omega) = 0$. Since $f(x) \in \mathbb{Z}[x]$, $f(\overline{\omega}) = \overline{f(\omega)} = 0$. It follows that when (1) has a nontrivial solution in $\mathbb{Z}[\omega]$, $f(x)$ has two complex roots $\omega, \overline{\omega}$. The existence of a third root depends on the coefficient $t_3 = b_1^3 + b_2^3 - b_3^3$ of the leading term of $f(x)$. If $t_3 = 0$, then $f(x)$ has only two roots. The next result answers the questions concerning the degree of $f(x)$ and the kind of roots $f(x)$ possesses.

Proposition 2.1. *If (1) has a nontrivial solution* (x_0, y_0, z_0) *in* $\mathbb{Z}[\omega]$*, then*

i). $f(x)$ *has degree 3.*

ii). $f(x)$ *has nonzero constant term.*

iii). *The roots of* $f(x)$ *are* $-c/d \in \mathbb{Q} - \{0\}$, ω, $\overline{\omega} = \omega^2$.

PROOF. i). We have already shown that $f(x)$ has at least degree 2. Let the coefficient $t_3 = b_1^3 + b_2^3 - b_3^3$ of its leading term be zero. Since $b_m \in \mathbb{Z}$ for all $m \in I$, there exists $b \in \mathbb{Z}$ such that $(b_1, b_2, b_3) = (0, b, b)$ or $(b, 0, b)$ or $(-b, b, 0)$ or $(b, -b, 0)$. All four cases follow along similar lines. We treat in detail only the first one,

$$(b_1, b_2, b_3) = (0, b, b). \tag{7}$$

Then a substitution of $(x_0, y_0, z_0) = (a_1, a_2 + b\,\omega, a_3 + b\,\omega)$ into (1) along with the facts that $\omega^3 = 1$, $\omega^2 + \omega + 1 = 0$ imply,

$$\left[a_1^3 + a_2^3 - a_3^3 - 3\,b^2\,(a_2 - a_3)\right] + \left[3\,b\,(a_2 - a_3)\,((a_2 + a_3) - b)\right]\omega = 0. \tag{8}$$

The coefficient of ω in (8) has to be zero. Namely, $b = 0$ or $a_2 = a_3$ or $b = a_2 + a_3$. If $b = 0$, then (7) contradicts (6). Hence, $b \neq 0$. Notice that, (5), (7) imply $a_1 \neq 0$. If $a_2 = a_3$, then (8) implies $a_1 = 0$, a contradiction. Hence, $a_2 \neq a_3$. If $b = a_2 + a_3$, then $a_2 + a_3 \neq 0$ (since $b \neq 0$). Additionally, a rational point (X_0, Y_0) with

$$X_0 = 4\,\frac{a_1}{a_2 - a_3} \in \mathbb{Q} - \{0\} \;\;,\;\; Y_0 = 12\,\frac{a_2 + a_3}{a_2 - a_3} \in \mathbb{Q} - \{0\}, \tag{9}$$

exists such that

$$\begin{aligned}\frac{(a_2 - a_3)^3}{64}\left[X_0^3 + 16 - Y_0^2\right] &= a_1^3 - 2\,a_2^3 + 2\,a_3^3 + 3\,a_2\,a_3^2 - 3\,a_2^2\,a_3 = \\ &= a_1^3 + a_2^3 - a_3^3 - 3\,(a_2 + a_3)^2\,(a_2 - a_3) \overset{(8)}{=} 0.\end{aligned}$$

Since $a_2 \neq a_3$, the latter provides the existence of a rational point (X_0, Y_0) on the elliptic curve $y^2 = x^3 + 16$ with $X_0\,Y_0 \neq 0$, a contradiction. As we have already mentioned in the introduction, (4) has no such rational points. Overall, (8) fails to hold and $t_3 \neq 0$. As a result $f(x)$ has degree 3.

ii). The constant term of $f(x)$ is $t_0 = a_1^3 + a_2^3 - a_3^3$. We can show that $t_0 \neq 0$ by following exactly the same reasoning as in i).

iii). We already know that ω, $\overline{\omega}$ are roots of $f(x)$. The polynomial $x^2 + x + 1 = (x - \omega)\,(x - \overline{\omega})$ divides $f(x)$ exactly. Namely,

$$f(x) = (d\,x + c)\,(x^2 + x + 1),$$

with $c, d \in \mathbb{Z} - \{0\}$ since $f(x) \in \mathbb{Z}[x]$, $d = t_3 \neq 0$, $c = t_0 \neq 0$. $\square$

The most important consequence of Proposition 2.1 is a certain relation between the coefficients of $f(x)$ implied by the existence of the nonzero rational root $-c/d$. Let

$$k_m = \begin{cases} -1 & , \quad m = 1, 2, \\ 1 & , \quad m = 3. \end{cases}$$

Proposition 2.2. *If (1) has a nontrivial solution (x_0, y_0, z_0) in $\mathbb{Z}[\omega]$, then $\lambda \in \mathbb{Q} - \{0\}$ and exactly one value of m in $I = \{1, 2, 3\}$ exist such that, for $m \neq \ell \neq j$, $m, \ell, j \in I$*

$$a_m = \lambda\,(a_\ell + k_m\,a_j) \ \ , \ \ b_m = \lambda\,(b_\ell + k_m\,b_j). \tag{10}$$

Proof. Recalling the notation in (2) and the fact that $f(-c/d) = 0$ we distinguish the following cases:

a). $p_m(-c/d) \neq 0$, $\forall\, m \in I$. Then $a_m\,d - b_m\,c \neq 0$, $\forall\, m \in I$ and $f(-c/d) = 0$ implies $(a_1\,d - b_1\,c)^3 + (a_2\,d - b_2\,c)^3 = (a_3\,d - b_3\,c)^3$, a contradiction.

b). $p_m(-c/d) = 0$, $\forall\, m \in I$. Then $a_m\,d = b_m\,c$, $\forall\, m \in I$. The latter along with (5) and $c, d \in \mathbb{Z} - \{0\}$ imply $a_m \neq 0$, $b_m \neq 0$, $\forall\, m \in I$. Since $c + d\,\omega \neq 0$ and $a_m = (c/d)\,b_m$, $x_0^3 + y_0^3 = z_0^3$ implies $b_1^3 + b_2^3 = b_3^3$, a contradiction.

c). $p_m(-c/d) = 0$ for exactly two values of $m \in I$. Then $f(-c/d) = 0$ implies that $p_m(-c/d) = 0$ for the third value of $m \in I$ contradicting (b).

d). $p_m(-c/d) = 0$ for exactly one value of $m \in I$. Then $a_m\,d = b_m\,c$. The latter along with (5) and $c, d \in \mathbb{Z} - \{0\}$ imply $a_m \neq 0$, $b_m \neq 0$. Let ℓ, j be the other two elements of I. Then $f(-c/d) = 0$ implies,

$$(a_\ell\,d - b_\ell\,c)^3 + k_m\,(a_j\,d - b_j\,c)^3 = 0 \Rightarrow (a_\ell\,d - b_\ell\,c) = -k_m\,(a_j\,d - b_j\,c),$$

or, $(a_\ell + k_m\,a_j)\,d = (b_\ell + k_m\,b_j)\,c$. The substitution $d = (b_m/a_m)\,c$ into the latter implies

$$\frac{a_\ell + k_m\,a_j}{a_m} = \frac{b_\ell + k_m\,b_j}{b_m} = g \in \mathbb{Q}. \tag{11}$$

If $g = 0$, then for the various values of $m \in I$, $x_0^3 + y_0^3 = z_0^3$ along with (11) imply either $x_0 = 0$ or $y_0 = 0$ or $z_0 = 0$ contradicting (5). Finally $g \in \mathbb{Q} - \{0\}$. Set $\lambda = 1/g \in \mathbb{Q} - \{0\}$ in (11) and the result follows. □

We close the investigation of the algebraic properties of $f(x)$ by noting that, without loss of generality, the exact value of m in (10) of Proposition 2.2 may assumed to be 1. If $m = 2$ or 3, then we transform (1) to the equivalent equations $y^3 + x^3 = z^3$ or $(-z)^3 + y^3 = (-x)^3$ and denote by (y_0, x_0, z_0) or $(-z_0, y_0, -x_0)$ the nontrivial solution $(a_1 + b_1\,\omega,\ a_2 + b_2\,\omega,\ a_3 + b_3\,\omega)$ of each one in $\mathbb{Z}[\omega]$ respectively. Now we can go further ahead and, again without loss of generality, specify the values of $\ell, j \in \{2, 3\}$, $\ell \neq j$ in (10). Since $a_1 = \lambda\,(a_\ell - a_j) = -\lambda\,(a_j - a_\ell)$, $b_1 = \lambda\,(b_\ell - b_j) = -\lambda\,(b_j - b_\ell)$, we may assume $\ell = 2$, $j = 3$.

Under the previous developments, (10) provides the following relation between x_0, y_0, z_0.

Proposition 2.3. *If (1) has a nontrivial solution* (x_0, y_0, z_0) *in* $\mathbb{Z}[\omega]$*, then a* $\lambda \in \mathbb{Q} - \{0\}$ *exists such that*

$$x_0 = \lambda\,(y_0 - z_0). \tag{12}$$

3. Insolubility of $x^3 + y^3 = z^3$ in $\mathbb{Z}[\omega]$ when $x\,y\,z \neq 0$

Now we are ready to proceed with the final steps of the proof of the insolubility of (1) in $\mathbb{Z}[\omega]$ when $x\,y\,z \neq 0$. Note that, when $a, b \in \mathbb{Z}$, $|a| + |b| \neq 0$,

$$\frac{1}{a + b\,\omega} = \frac{a + b\,\omega^2}{(a + b\,\omega)\,(a + b\,\omega^2)} = \frac{(a - b) - b\,\omega}{a^2 + b^2 - a\,b}. \tag{13}$$

Proposition 3.1. *If (1) has a nontrivial solution* (x_0, y_0, z_0) *in* $\mathbb{Z}[\omega]$*, then the elliptic curve (4) has a rational point* (X_0, Y_0) *with* $X_0\,Y_0 \neq 0$.

Proof. Let $w_0 = y_0/z_0 \overset{(13)}{\in} \mathbb{Q}(\omega) = \left\{p + q\,\frac{-1+\sqrt{-3}}{2}\,,\ p, q \in \mathbb{Q}\right\} = \mathbb{Q}(\sqrt{-3})$. (5) implies $w_0 \neq 0$. (1) and (5) imply $w_0 \neq 1$.

$$\begin{aligned} x_0^3 + y_0^3 = z_0^3 \quad &\overset{(12)}{\Rightarrow} \quad \lambda^3\,(w_0 - 1)^3 + w_0^3 - 1 = 0 \\ &\Rightarrow \quad (\lambda^3 + 1)\,w_0^2 + (-2\,\lambda^3 + 1)\,w_0 + (\lambda^3 + 1) = 0. \end{aligned} \tag{14}$$

$\lambda = -1$ in (14) implies $w_0 = 0$, a contradiction. Hence, $\lambda \neq -1$. The discriminant of (14) is $D = -12\,\lambda^3 - 3$. $D = 0$ implies $\lambda = -1/\sqrt[3]{4}$, a contradiction since λ is a rational. Hence, $D \neq 0$. The roots of (14) are

$$w_0 = \frac{2\,\lambda^3 - 1}{2\,(\lambda^3 + 1)} \pm \frac{\sqrt{D}}{2\,(\lambda^3 + 1)} = \frac{2\,\lambda^3 - 1}{2\,(\lambda^3 + 1)} \pm \frac{\sqrt{4\,\lambda^3 + 1}}{2\,(\lambda^3 + 1)}\,\sqrt{-3}. \tag{15}$$

Since $w_0 \in \mathbb{Q}(\sqrt{-3}) - \{0\}$, a $\mu \in \mathbb{Q}$ should exist such that, $\mu = \sqrt{4\,\lambda^3 + 1}$. We have $\mu \in \mathbb{Q} - \{0\}$ since $\lambda \neq -1/\sqrt[3]{4}$. Additionally,

$$\mu = \sqrt{4\,\lambda^3 + 1} \Rightarrow (4\,\mu)^2 = (4\,\lambda)^3 + 16.$$

Hence, the elliptic curve (4) has the rational point $(X_0, Y_0) = (4\,\lambda, 4\,\mu)$. $\lambda, \mu \in \mathbb{Q} - \{0\}$ imply that $X_0\,Y_0 \neq 0$. □

The algebraic structure of the group of rational points on (4) as stated in the introduction along with Proposition 3.1 lead to the final conclusion.

Theorem 3.2. $x^3 + y^3 = z^3$ *is insoluble in* $\mathbb{Z}[\omega]$ *when* $x\,y\,z \neq 0$.

Proof. Let (1) have a nontrivial ($x_0\,y_0\,z_0 \neq 0$) solution in $\mathbb{Z}[\omega]$. According to Proposition 3.1, the elliptic curve (4) has a rational point (X_0, Y_0) with $X_0\,Y_0 \neq 0$. The latter contradicts the algebraic structure of the group of rational points on (4) as stated in the introduction namely, the only rational points of (4) are $(x, y) = (0, \pm 4)$ with $x\,y = 0$. $\square$

References

[1] Husmöler, D., *Elliptic Curves*, Springer, New York, 2004.
[2] Ireland, K. and Rosen, M., *A Classical Introduction to Modern Number Theory*, Springer Verlag, 1990.
[3] Mwrank, in http://www.sagemath.org.
[4] PARI/GP, in http://pari.math.u-bordeaux.fr/.
[5] Ribenboim, P., *Fermat's Last Theorem For Amateurs*, Springer Verlag, New York, 1999.
[6] http://www.warwick.ac.uk/~masgaj/ftp/data/.