INTEGERS: ELECTRONIC JOURNAL OF COMBINATORIAL NUMBER THEORY 8 (2008), #A32

IN GAUSSIAN INTEGERS $\mathbf{X^3 + Y^3 = Z^3}$ HAS ONLY TRIVIAL SOLUTIONS – A NEW APPROACH

Elias Lampakis
Lampropoulou (Terma), Kiparissia, T.K: 24500, GREECE
labakis@otenet.gr

Received: 2/10/08, Revised: 7/7/08, Accepted: 7/13/08, Published: 7/18/08

Abstract

It will be shown via a new method that in the Ring of Gaussian Integers $\mathbb{Z}[i]$ the solutions of the Diophantine equation $x^3 + y^3 = z^3$ are trivial, namely, $x\,y\,z = 0$. The result is achieved by showing that the existence of nontrivial Gaussian Integer solutions implies the existence of rational points on the elliptic curve $y^2 = x^3 + 432$, which is already known to have none.

1. Introduction

In this paper we present a new method that addresses the question of the existence of nontrivial solutions to the Fermat type Diophantine equation

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

with x, y, z in the ring of Gaussian integers $\mathbb{Z}[i]$. By nontrivial we mean solutions x, y, z in $\mathbb{Z}[i]$ for which $x\,y\,z \neq 0$.

In L.E. Dickson's History of the Theory of Numbers [1, p. 550], one can find that this question has already been answered by R. Feuter [2] within the frame of algebraic number theory. Namely, he has proven that if $\xi^3+\eta^3+\zeta^3 = 0$ is solvable by numbers $\neq 0$ of an imaginary quadratic domain $k(\sqrt{m})$, where $m < 0$, $m \equiv 2 \pmod 3$, then the class number of k is divisible by 3. Now $k = \mathbb{Z}$, $m = -1$ and $\mathbb{Z}$ is a Principal Ideal Domain having class number 1 not divisible by 3.

Our method is new since it transfers, via elementary polynomial theory, the question of the existence of a nontrivial solution of (1) in $\mathbb{Z}[i]$, to the question of the existence of a rational point on the elliptic curve

$$y^2 = x^3 + 432, \tag{2}$$

which is already known [1] to have none. Equation (2) is curve $432A3$ in Cremona's tables with rank 0 and order of torsion subgroup 1; namely, its torsion subgroup contains only the point at infinity. Thus (2) has no rational points of infinite or finite order.

So far various extensions of Fermat's Last Theorem (FLT) have been treated in a vast number of publications. Many references may be found in [5]. Some concern the nature of the exponents, others, the nature of the solution's underlying ring. We mention, for example, [3] for rational exponents and [4] for exponents in $\mathbb{Z}[i]$. On the other hand, in [5, 6] one can find the solution of the cubic exponent case of FLT in $\mathbb{Z}[\omega]$, $\omega^3 = 1$, $\omega \neq 1$; in [5, 7, 8] the solution of the fourth exponent case in $\mathbb{Z}[i]$; and in [9] the solution of the n^{th} exponent case in the ring of polynomials of an algebraically closed field with characteristic 0. There are also mixed cases as in [10] where the exponents are not necessarily equal, the equation may have coefficients other than 1 but the solutions are in $\mathbb{Z}$, or in [11] with two exponents equal to 4, one exponent equal to 2, not all coefficients equal to 1, and underlying ring of solutions $\mathbb{Z}[i]$. The latter is a generalization of the fourth exponent case in [5, 7, 8].

2. The Equation $\mathbf{x^3 + y^3 = z^3}$ in $\mathbb{Z}[\mathbf{i}]$

In order for us to demonstrate the above-mentioned connection between the nontrivial solutions of (1) in $\mathbb{Z}[i]$ and the rational points on (2), we introduce the following notations and assumptions. Let $(x_0, y_0, z_0) = (a_1 + b_1\, i\,,\ a_2 + b_2\, i\,,\ a_3 + b_3\, i)$ be a nontrivial solution of (1) in $\mathbb{Z}[i]$. Also let $I = \{1, 2, 3\}$. If $a_m = 0$ or $b_m = 0$ for all m in I, (1) implies either $b_1^3 + b_2^3 = b_3^3$ or $a_1^3 + a_2^3 = a_3^3$, respectively. Since a_m, b_m are in $\mathbb{Z}$, the latter holds only when at least one of the b_m's or the a_m's, respectively, is 0. Then at least one of the $a_m + b_m\, i$ is 0, a contradiction. Thus $|a_1| + |a_2| + |a_3| \neq 0$ and $|b_1| + |b_2| + |b_3| \neq 0$. Additionally, let $p_m(x) = a_m + b_m\, x$, $f(x) = p_1^3(x) + p_2^3(x) - p_3^3(x)$ be polynomials in $\mathbb{Z}[x]$. Finally, set

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

Our first partial result about (1), Theorem 1, is based upon the kind of roots that $f(x)$ possesses. For this piece of information we need the following lemma that determines the degree of $f(x)$ and its behavior at 0. Notice the catalytic appearance of (2) in the proof.

Lemma 1 *If* (1) *has a nontrivial solution* (x_0, y_0, z_0) *in* $\mathbb{Z}[i]$*, then* $f(x)$ *has degree 3 and* $f(0) \neq 0$.

Proof. The coefficient of x^3 in $f(x)$ is $t_3 = b_1^3 + b_2^3 - b_3^3$, whereas the constant term is $t_0 = a_1^3 + a_2^3 - a_3^3$. Assume $t_3 = 0$. Then $(b_1, b_2, b_3) = (0, b, b)$ or $(b, 0, b)$ or $(b, -b, 0)$ or

$(-b, b, 0)$ for some b, and (1) implies, respectively,

$$\left[a_1^3 + a_2^3 - a_3^3 + 3\,b^2\,(a_3 - a_2)\right] - \left[3\,b\,\left(a_3^2 - a_2^2\right)\right]\,i = 0 \tag{3}$$
$$\left[a_1^3 + a_2^3 - a_3^3 + 3\,b^2\,(a_3 - a_1)\right] - \left[3\,b\,\left(a_3^2 - a_1^2\right)\right]\,i = 0 \tag{4}$$
$$\left[a_1^3 + a_2^3 - a_3^3 - 3\,b^2\,(a_2 + a_1)\right] - \left[3\,b\,\left(a_2^2 - a_1^2\right)\right]\,i = 0 \tag{5}$$
$$\left[a_1^3 + a_2^3 - a_3^3 - 3\,b^2\,(a_2 + a_1)\right] + \left[3\,b\,\left(a_2^2 - a_1^2\right)\right]\,i = 0. \tag{6}$$

The imaginary part in all four cases is 0. If $b = 0$, then $b_1 = b_2 = b_3 = 0$ in (x_0, y_0, z_0), which contradicts $|b_1| + |b_2| + |b_3| \neq 0$. Thus $b \neq 0$ and $a_m = \pm a_j$, $m \neq j$, m, j in I. Now we treat case (3) in detail. All other cases follow along the same reasoning. If $a_2 = a_3$, then $a_1 = 0$ and $a_1 + b_1\,i = 0$, a contradiction. If $a_2 = -a_3$, then

$$\begin{aligned} 6\,b^2\,a_3 = (-a_1)^3 + 2\,a_3^3 \;&\Rightarrow\; 3\,(2\,b)^2\,(2\,a_3) = 4\,(-a_1)^3 + (2\,a_3)^3 \\ &\Rightarrow\; 4^2\,3^4\,(2\,b)^2\,(2\,a_3) = 4^3\,3^3\,(-a_1)^3 + 4^2\,3^3\,(2\,a_3)^3 \\ &\Rightarrow\; (72\,b)^2\,(2\,a_3) = (-12\,a_1)^3 + 432\,(2\,a_3)^3. \end{aligned} \tag{7}$$

If $a_3 = 0$, then $a_1 = 0$ and $a_1 + b_1\,i = 0$, a contradiction. Thus $a_3 \neq 0$ and dividing both sides of (7) by $(2\,a_3)^3$ we conclude that $(x, y) = (-6\,a_1/a_3\,,\, 36\,b/a_3)$ is a rational point on (2), a contradiction. Finally, $t_3 \neq 0$ and $f(x)$ has degree 3. The case when $t_0 = 0$ can be discarded using the same reasoning as above. Thus $f(0) \neq 0$. □

The following theorem establishes the relation that must be satisfied by the real and imaginary parts of the nonzero Gaussian integers that solve (1).

Theorem 1 *If* (1) *has a nontrivial solution* (x_0, y_0, z_0) *in* $\mathbb{Z}[i]$ *then* λ *in* $\mathbb{Q} - \{0\}$ *and exactly one value of* m *in* I *exist such that for* $m \neq \ell \neq j$, ℓ, j *in* I,

$$a_m = \lambda\,(a_\ell + k_m\,a_j)\;\;,\;\; b_m = \lambda\,(b_\ell + k_m\,b_j)$$

Proof. (1) implies that $f(i) = 0$ and $\overline{f(i)} = f(-i) = 0$. Thus $f(x) = (c + d\,x)\,(x^2 + 1)$, c, d in $\mathbb{Z} - \{0\}$ since the degree of $f(x)$ is 3 and $f(0) \neq 0$. We have the following cases,

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

b. $p_m(-c/d) = 0$ for all m in I. Then $a_m\,d = b_m\,c$ for all m in I. Note that $b_m = 0$ implies that $a_m = 0$ and vice versa. In that case, $a_m + b_m\,i = 0$, a contradiction. Thus $a_m \neq 0$, $b_m \neq 0$ for all m in I. Now $a_m = (c/d)\,b_m$, $c + d\,i \neq 0$ and (1) 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 $p_m(-c/d) = 0$ for the third value of m in I, contradicting case (**b**).

d. $p_m(-c/d) = 0$ for exactly one value of m in I. Let ℓ, j be the other two elements of I. $a_m\,d = b_m\,c$ and $a_m \neq 0$, $b_m \neq 0$, since c, d in $\mathbb{Z} - \{0\}$. And $f(-c/d) = 0$ 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

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

Since $d = (b_m/a_m)\, c$, we take

$$(a_\ell + k_m\, a_j)\, b_m - (b_\ell + k_m\, b_j)\, a_m = 0 \Rightarrow \left| \begin{array}{cc} a_\ell + k_m\, a_j & a_m \\ b_\ell + k_m\, b_j & b_m \end{array} \right| = 0.$$

The vectors $(a_\ell + k_m\, a_j\, ,\, b_\ell + k_m\, b_j)$ and $(a_m\, ,\, b_m)$ are linearly dependent in $\mathbb{Q}$. For the unique value of $m \in I$, there exist $\lambda \in \mathbb{Q} - \{0\}$ such that $a_m = \lambda\, (a_\ell + k_m\, a_j)$, $b_m = \lambda\, (b_\ell + k_m\, b_j)$. □

Remark 1 *If* (1) *has nontrivial solutions in* $\mathbb{Z}[i]$ *so do the equations*

$$y^3 + x^3 = z^3 \tag{8}$$
$$(-z)^3 + y^3 = (-x)^3 \tag{9}$$

and vice versa. Thus, without loss of generality, we may assume in Theorem 1 that the exact value of $m \in I$ *is 1. If* m *is 2 or 3 we substitute* (8) *or* (9) *in* (1) *, denoting by* (y_0, x_0, z_0) *or* $(-z_0, y_0, -x_0)$ *the nontrivial solution* $(a_1 + b_1\, i\, ,\, a_2 + b_2\, i\, ,\, a_3 + b_3\, i)$ *of each one in* $\mathbb{Z}[i]$*, respectively.*

Our next result establishes the connection between the existence of nontrivial solutions of a type (1) equation in $\mathbb{Z}[i]$ and the existence of rational points on (2).

Theorem 2 *If* (1) *has a nontrivial solution* (x_0, y_0, z_0) *in* $\mathbb{Z}[i]$ *then* (2) *has a rational point.*

Proof. Theorem 1 and Remark 1 imply $a_1 = \lambda\, (a_\ell - a_j)$, $b_1 = \lambda\, (b_\ell - b_j)$, $\ell \neq j$ in $\{2, 3\}$, λ in $\mathbb{Q} - \{0\}$. Since we can write $a_1 = -\lambda\, (a_j - a_\ell)$, $b_1 = -\lambda\, (b_j - b_\ell)$, it is obvious that, without loss of generality, we may assume $\ell = 2$, $j = 3$. Set $w = (a_2 + b_2\, i)/(a_3 + b_3\, i)$ in $\mathbb{Q}(i) - \{0\}$. We have $w \neq 1$, else (1) implies $a_1 + b_1\, i = 0$, a contradiction. On the other hand, dividing both sides of (1) by $(a_3 + b_3\, i)^3$, we take

$$\left[\frac{a_1 + b_1\, i}{a_3 + b_3\, i}\right]^3 + \left[\frac{a_2 + b_2\, i}{a_3 + b_3\, i}\right]^3 = 1 \;\Rightarrow\; \lambda^3\, (w - 1)^3 + w^3 = 1$$
$$\Rightarrow\; \left[(\lambda^3 + 1)\, w^2 + (-2\, \lambda^3 + 1)\, w + (\lambda^3 + 1)\right] = 0.$$

We have $\lambda \neq -1$, else the latter would imply $w = 0$, $a_2 + b_2\, i = 0$, a contradiction. The discriminant of the latter is $-12\, \lambda^3 - 3$, and

$$w = \frac{2\, \lambda^3 - 1}{2\, (\lambda^3 + 1)} \pm \frac{\sqrt{12\, \lambda^3 + 3}}{2\, (\lambda^3 + 1)}\, \sqrt{-1} = \frac{2\, \lambda^3 - 1}{2\, (\lambda^3 + 1)} \pm \frac{\sqrt{12\, \lambda^3 + 3}}{2\, (\lambda^3 + 1)}\, i.$$

Since w is in $\mathbb{Q}(i) - \{0\}$, there exists $\mu \in \mathbb{Q}$ such that

$$\mu = \sqrt{12\,\lambda^3 + 3} \;\Leftrightarrow\; 9\left(\frac{\mu}{3}\right)^2 = 12\,\lambda^3 + 3 \Leftrightarrow 3\left(\frac{\mu}{3}\right)^2 = 4\,\lambda^3 + 1$$
$$\Leftrightarrow\; 4^2\,3^4\left(\frac{\mu}{3}\right)^2 = 4^3\,3^3\,\lambda^3 + 4^2\,3^3 \Leftrightarrow (12\,\mu)^2 = (12\,\lambda)^3 + 432,$$

implying that (2) has the rational solution $(x, y) = (12\,\lambda\,,\ 12\,\mu)$. □

Now we state our main result about the solutions of (1) in $\mathbb{Z}[i]$.

Theorem 3 *If (x, y, z) is a solution of (1) in $\mathbb{Z}[i]$, then $x\,y\,z = 0$.*

Proof. Let (x, y, z) be a solution of (1) in $\mathbb{Z}[i]$ with $x\,y\,z \neq 0$. Theorem 2 implies that (2) has a rational point. We have already mentioned that (2) has no rational points [1]. Thus $x\,y\,z = 0$. □

Acknowledgments

We are thankful to professor J. Silverman of Brown University for communicating to us the conductor of $y^2 = x^3 + 432$, something that simplified the investigation in Cremona's tables. We would also like to thank the anonymous referee for valuable suggestions concerning the historical status of the problem.

References

1. Cremona's Tables, http://modular.fas.harvard.edu/cremona/allcurves.00000-09999.gz

2. R. Feuter, Sitzungsber. Akad. Wiss. Heidelberg (Math.), **4**, A, 1913 No. 25.

3. C. Bennett, A. M. W. Glass and G. Székely, *Fermat's Last Theorem for Rational Exponents*, American Mathematical Monthly **111** (2004) 322–329.

4. J. Zuehlke, *Fermat's Last Theorem for Gaussian Integer Exponents*, American Mathematical Monthly **106** (1999) 49.

5. P. Ribenboim, *Fermat's Last Theorem For Amateurs*, Springer–Verlag, New York, 1999.

6. K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer Verlag, New York, 1990.

7. D. Hilbert, Jahresbericht d. Deutschen Math.–Vereinigung, **4** (1894–1895) 517–525.

8. J. T. Cross, *In the Gaussian Integers $\alpha^4 + \beta^4 \neq \gamma^4$*, Math. Magazine **66** (1993) 105–108.

9. S. Lang, *Old and new conjectured Diophantine Inequalities*, Bulletin (New Series) of the AMS **23** (1990) 36–75.

10. M. Bennett and C. M. Skinner, *Ternary Diophantine Equations via Galois Representations and Modular Forms*, CanadianMJ **56** (2004) 23–54.

11. S. Szabó, *Some Fourth Degree Diophantine Equations in Gaussian Integers*, Integers: Electronic Journal of Combinatorial Number Theory **4** (2004) A16, 17 pages.