The Diophantine equation \( x^4 \pm y^4 = iz^2 \) in Gaussian integers

Filip Najman

1 Introduction

The Diophantine equation \( x^4 \pm y^4 = z^2 \), where \( x, y \) and \( z \) are integers was studied by Fermat, who proved that there exist no nontrivial solutions. Fermat proved this using the infinite descent method, proving that if a solution can be found, then there exists a smaller solution (see for example [1], Proposition 6.5.3). This was the first particular case proven of Fermat’s Last Theorem (which was completely proven by Wiles in [8]).

The same Diophantine equation, but now with \( x, y \) and \( z \) being Gaussian integers, i.e. elements of \( \mathbb{Z}[i] \), was later examined by Hilbert (see [3], Theorem 169). Once again, it was proven that there exist no nontrivial solutions. Other authors also examined similar problems. In [6] equations of the form \( ax^4 + by^4 = cz^2 \) in Gaussian integers with only trivial solutions were studied. In [2] a different proof than Hilbert’s, using descent, that \( x^4 + y^4 = z^4 \) has only trivial solutions in Gaussian integers.

In this short note, we will examine the Diophantine equation

\[
x^4 \pm y^4 = iz^2
\]

in Gaussian integers and find all the solutions of this equation. Also, we will give a new proof of Hilbert’s results. Our strategy will differ from the one used by Hilbert and will be based on elliptic curves.

For an elliptic curve \( E \) over a number field \( K \), it is well known, by the Mordell-Weil theorem, that the set \( E(K) \) of \( K \)-rational points on \( E \) is a finitely generated abelian group. The group \( E(K) \) is isomorphic to \( T \oplus \mathbb{Z}^r \), where \( r \) is a non-negative integer and \( T \) is the torsion subgroup. We will be interested in the case when \( K = \mathbb{Q}(i) \). We will work only with elliptic curves with rational coefficients and by a recent result of the author (see [4]), if an elliptic curve has rational coefficients, then the torsion of the elliptic curve over \( \mathbb{Q}(i) \) is either cyclic of order \( m \), where \( 1 \leq m \leq 10 \) or \( m = 12 \), of the form \( \mathbb{Z}_2 \oplus \mathbb{Z}_{2m} \), where \( 1 \leq m \leq 4 \), or \( \mathbb{Z}_4 \oplus \mathbb{Z}_4 \).

\*Mathematics subject classification (2000) 11D25, 11D41
Throughout this note, the following extension of the Lutz-Nagell Theorem is used to compute torsion groups of elliptic curves.

**Theorem (Extended Lutz-Nagell Theorem).** Let $E : y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}[i]$. If a point $(x, y) \in E(\mathbb{Q}(i))$ has finite order, then

1. $x, y \in \mathbb{Z}[i]$. \\
2. Either $y = 0$ or $y^2|4A^3 + 27B^2$.

The proof of the Lutz-Nagell Theorem can easily be extended to elliptic curves over $\mathbb{Q}(i)$. Details of the proof can be found in [7], Chapter 3. An implementation in Maple can be found in [7], Appendix A.

## 2 New results

We are now ready to prove our main result.

**Theorem 1.** We call a solution $(x, y, z)$ trivial if $xyz = 0$.

(i) The equation $x^4 - y^4 = iz^2$ has only trivial solutions in Gaussian integers.

(ii) The only nontrivial solutions satisfying $\gcd(x, y, z) = 1$ in Gaussian integers of the equation $x^4 + y^4 = iz^2$ are $(x, y, z)$, where $x, y \in \{\pm i, \pm 1\}$, $z = \pm i(1 + i)$.

**Proof:**

(i) Suppose $(x, y, z)$ is a nontrivial solution. Dividing the equation by $y^4$ and by a variable change $s = \frac{x}{y}$, $t = \frac{z}{y^2}$, we obtain the equation $s^4 - 1 = it^2$, where $s, t \in \mathbb{Q}(i)$. We can rewrite this equation as

$$r = s^2,$$  \hfill (1)

$$r^2 - 1 = it^2.$$  \hfill (2)

Multiplying these equations we obtain $i(st)^2 = r^3 - r$. Again, with a variable change $a = st$, $b = -ir$ and dividing by $i$, we obtain the equation defining an elliptic curve

$$E : a^2 = b^3 + b.$$ 

Using the program [5], written in PARI, we compute that the rank of this curve is 0. It is easy to compute, using the Extended Lutz-Nagell Theorem, that $E(\mathbb{Q}(i))_{\text{tors}} = \mathbb{Z}_2 \oplus \mathbb{Z}_2$ and that $b \in \{0, \pm i\}$. It is obvious that all the possibilities lead to trivial solutions.

(ii) Suppose $(x, y, z)$ is a nontrivial solution satisfying $\gcd(x, y, z) = 1$. Dividing the equation by $y^4$ and by a variable change $s = \frac{x}{y}$, $t = \frac{z}{y^2}$, we obtain
the equation $s^4 + 1 = it^2$, where $s, t \in \mathbb{Q}(i)$. We can rewrite this equation as

$$r = s^2,$$

$$r^2 + 1 = it^2.$$  \hfill (3)

Multiplying these equations we obtain $i(st)^2 = r^3 + r$. Again, with a variable change $a = st$, $b = -ir$ and dividing by $i$, we obtain the equation defining an elliptic curve

$$E : a^2 = b^3 - b.$$  \hfill (4)

Using the program [5], we compute that the rank of this curve is 0. Using the Extended Lutz-Nagell Theorem we compute that $E(\mathbb{Q}(i))_{\text{tors}} = \mathbb{Z}_2 \oplus \mathbb{Z}_4$ and that $b \in \{0, \pm i, \pm 1\}$. Obviously $b = 0$ leads to a trivial solution. It is easy to see that $b = \pm 1$ leads to $r = \pm i$ and this is impossible, since $r$ has to be a square by (3). This leaves us the possibility $b = \pm i$. Since we can suppose that $x$ and $y$ are coprime, this case leads us to the solutions stated in the theorem.

\begin{proof}

3 A new proof of Hilbert’s results

We now give a new proof of Hilbert’s result, which is very similar to Theorem 1.

**Theorem 2.** The equation $x^4 \pm y^4 = z^2$ has only trivial solutions in Gaussian integers.

**Proof:**

(i) Suppose $(x, y, z)$ is a nontrivial solution. Dividing the equation by $y^4$ and by a variable change $s = \frac{x}{y}$, $t = \frac{z}{y^2}$, we obtain the equation $s^4 \pm 1 = t^2$, where $s, t \in \mathbb{Q}(i)$. We can rewrite this equation as

$$r = s^2,$$

$$r^2 \pm 1 = t^2;$$  \hfill (5)

and by multiplying these two equations, together with a variable change $a = st$, we get the two elliptic curves

$$a^2 = r^3 \pm r.$$  \hfill (6)

As in the proof of Theorem 1, both elliptic curves have rank 0 and it is easy to check that all the torsion points on both curves lead to trivial solutions. \hfill \square

**Remark**

Note that from the proofs of Theorems 1 and 2 it follows that the mentioned solutions are actually solutions the only solutions over $\mathbb{Q}(i)$, not just $\mathbb{Z}[i]$.  

\begin{proof}

\end{proof}
References

[1] H. Cohen, *Number Theory, Volume I: Tools and Diophantine Equations*, Springer, 2007.

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

[3] D. Hilbert, *Jahresbericht d. Deutschen Math.-Vereinigung*, 4, 1894/1895, 517–525.

[4] F. Najman, *Torsion of elliptic curves over quadratic cyclotomic fields*, Math J. Okayama Univ., to appear.

[5] D. Simon, *Le fichier gp*, http://www.math.unicaen.fr/~simon/ell.gp.

[6] S. Szabo, *Some Fourth Degree Diophantine Equations in Gaussian integers*, Integers 4 (2004), A16.

[7] T. Thongjunthug, *Elliptic curves over $\mathbb{Q}(i)$*, Honours thesis (2006)

[8] A. Wiles, *Modular Elliptic Curves and Fermat’s Last Theorem*, Ann. Math. 141 (1995), 443–541.

FILIP NAJMAN
DEPARTMENT OF MATHEMATICS,
UNIVERSITY OF ZAGREB,
BIJENIČKA CESTA 30, 10000 ZAGREB,
CROATIA
E-mail address: fnajman@math.hr