ON FERMAT'S LAST THEOREM FOR N = 3 AND N = 4

R. ANDREW OHANA

Abstract. A solution to Fermat's equation, $x^n + y^n = z^n$, is called trivial if $xyz = 0$. In this paper we will prove Fermat's Last Theorem, which states all rational solutions are trivial for $n > 2$, when $3 \mid n$ or $4 \mid n$. For $n = 3$ we will show all solutions in the Eisenstein Field, $\mathbb{Q}(\sqrt{-3})$, are trivial. Our proof is in the same vain as Gauss' proof, but argued towards a different contradiction. For $n = 4$ we will show all solutions in the Gaussian Field, $\mathbb{Q}(i)$, are trivial. We will follow Hilbert's proof given in [3] which has the flavor of argument made by Gauss with the Eisenstein Field.

Contents

1. Introduction

Let $n > 0$ be an integer, then

$$x^n + y^n = z^n$$

is called Fermat's equation. While we can consider equation can be considered over any ring, we will focus on solutions which lie in the integers while exploring other rings as the need arises. When starting to study a diophantine equation, we first ask whether a solution exists, here we can see that for any n there are infinitely many solutions, specifically we can let $x = 0$ and $y = z \in \mathbb{Z}$. Our next question, is this all of our solutions?

The answer is a bit muddled, clearly it isn't all our solutions, we can let $y = 0$ and $x = z \in \mathbb{Z}$ or for n odd let $z = 0$ and $x = -y \in \mathbb{Z}$, so we will restate this question: Do all solutions to Fermat's equation have at least one of $x, y, z = 0$? Since the integers form an integral domain, we can state this condition as $xyz = 0$, for further discussion we will refer to these solutions of Fermat's equation as *trivial solutions*.

We also can see that if there is a solution (a, b, c), then $(a/d, b/d, c/d)$ is a solution where $d = \gcd(a, b, c)$, hence existence of a non-trivial solution can be reduced to existence of a non-trivial coprime solution, we call coprime solutions *primitive*. We will now start our investigation with $n = 1$.

Date: March 12, 2010.

Proposition 1.1. *There are an infinite number of non-trivial primitive solutions to Fermat's equation for $n = 1$.*

Proof. Let k be any non-zero non-unit integer, and let $x = k$, $y = k + 1$ and $z = 2k + 1$, then $x + y = z$ is a primitive solution to Fermat's equation when $n = 1$. □

With $n = 2$ Fermat's equation is simply the Pythagorean Theorem, the integer solutions to the Pythagorean Theorem are called *Pythagorean triples*. Euclid in [2] gave a complete characterization of primitive Pythagorean triples, which as a corollary shows there are an infinite number of non-trivial primitive solutions to Fermat's equation for $n = 2$. We present a more modern proof of Euclid's characterization.

Proposition 1.2. *Let $P = (a, b, c) \in \mathbb{Z}^3_{>0}$, then P is a non-trivial primitive Pythagorean triple if and only if there exist unique coprime $m, n \in \mathbb{Z}_{>0}$ with $n < m$ and different parity such that*

$$\begin{aligned} a &= m^2 - n^2 \\ b &= 2mn \\ c &= m^2 + n^2, \end{aligned}$$

up to symmetry in a and b.

Proof. Our parameterization is clearly a primitive Pythagorean triple, so we simply need to show every Pythagorean triple is represented uniquely in our parameterization. Let (a, b, c) be a non-trivial primitive Pythagorean triple, then $(a/c, b/c)$ is a rational solution on the first quadrant of the unit circle,

$$u^2 + v^2 = 1. \tag{1}$$

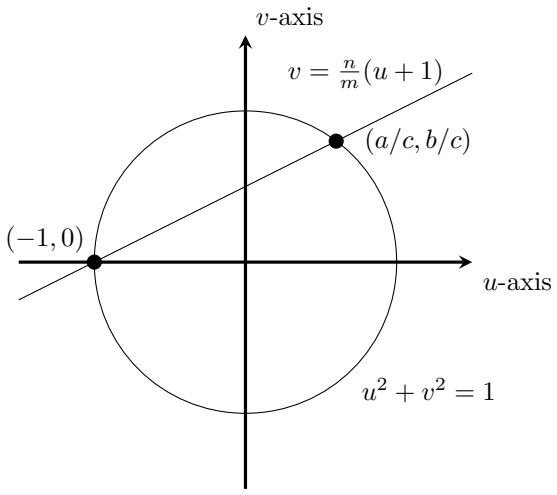

FIGURE 1. Parameterizing Pythagorean triples with the unit circle.

Hence there exists a unique line with rational slope $n/m < 1$ reduced with $m, n > 0$ through $(-1, 0)$,

$$v = \frac{n}{m}(u + 1).$$

Since this line intersects the unit circle at $(-1, 0)$ and $(a/c, b/c)$ solving for the second we get

$$\frac{a}{c} = \frac{m^2 - n^2}{m^2 + n^2}$$
$$\frac{b}{c} = \frac{2mn}{m^2 + n^2}.$$

If m, n have different parity, we can easily verify the right hand sides are reduced, so we are done. If m, n are both odd, then let $p = \frac{m+n}{2}$ and $q = \frac{m-n}{2}$, then we can see

$$\frac{a}{c} = \frac{2pq}{p^2 + q^2}$$
$$\frac{b}{c} = \frac{p^2 - q^2}{p^2 + q^2},$$

and that p, q are coprime and have different parity, hence this is now a reduced expression. Hence we have obtained our parameterization. □

Corollary 1.3. *There are an infinite number of non-trivial primitive solutions to Fermat's equation for $n = 2$.*

Proof. For each $n \in \mathbb{Z}_{>0}$ there exists a distinct solution of Fermat's equation for $n = 2$ by Proposition 1.2 by using the parameterization with $m = n + 1$. □

So far for every case we have looked at, we have found an infinite number of non-trivial primitive solutions to Fermat's equation, so we might start thinking there are an infinite number of non-trivial solutions for Fermat's equation equation in general. This conclusion, however, is false, in fact it turns out that there doesn't exist a single non-trivial solution for Fermat's equation when $n > 2$.

Theorem 1 (Fermat's Last Theorem)**.** *All solutions to Fermat's equation are trivial for $n > 2$.*

This theorem was conjectured nearly 400 years, by Pierre de Fermat who proved a single case, specifically there are only trivial solutions to Fermat's equation for $n = 4$. Progress made towards this theorem proved slow over the centuries, where progress was made a single case at a time. This first substantial work towards a general theorem was made in the 1800s, by Sophie Germain. Her technique was ultimately abandoned as work in algebraic number theory developed and appeared more promising. The theorem was finally proved in 1995, when Andrew Wiles proved enough of the modularity theorem to prove Fermat's Last Theorem.

Our presentation of Fermat's Last Theorem for cases $n = 3$ and $n = 4$ will follow the special cases that were studied in 1800s, relying on the development algebra. Most of these proofs rely on the minimality principle, and as such constructing from a solution a smaller solution is key. Specifically, our proof for both the $n = 3$ and $n = 4$ case relies on the following lemma.

Lemma 1.4. *Let R be a UFD, if $x, y \in R$ are coprime with*

$$xy = z^n,$$

for some $z \in R$ and $n \in \mathbb{Z}_{>0}$, then there exist $u, v \in R$ and $a \in R^\times$ such that

$$x = au^n$$
$$y = a^{-1}v^n.$$

Proof. For $xy \in R^\times \cup \{0\}$ this is trivial, so suppose x is a non-unit. Let coprime $x, y \in R$ be values for which the lemma fails to hold such that the length of the irreducible decomposition of x, which we will denote as $l(x)$, is minimal. Let $w \in R$ be an irreducible divisor of x, then since $w \mid z^n$ and since R is a UFD, we must have $w \mid z$. But thus $w^n \mid z^n = xy$ and since $w \mid x$ and x, y are coprime, we must have $w^n \mid x$. Hence the lemma fails to hold for $x/w^n, y$, but this contradicts the minimality of $l(x)$ since $l(x/w^n) = l(x) - n < l(x)$. □

2. For $n = 3$

Our proof of Fermat's Last Theorem for $n = 3$ will follow [1], however we will assume a greater mathematical background, and thus simply the proof where possible. We will show Fermat's Last Theorem for $n = 3$ by considering solutions in the Eisenstein integers. The Eisenstein integers, denoted $\mathbb{Z}[\zeta_3]$, is the integral span over $\left\{1, e^{2\pi i/3}\right\}$, this set forms a Euclidean Domain with units $\pm 1, \pm\zeta_3, \pm\zeta_3^{-1}$. Fermat's equation is particularly interesting in this ring, since we can factor in various ways, for example

$$x^3 + y^3 = (x + y)(x + \zeta_3 y)(x + \zeta_3^{-1} y).$$

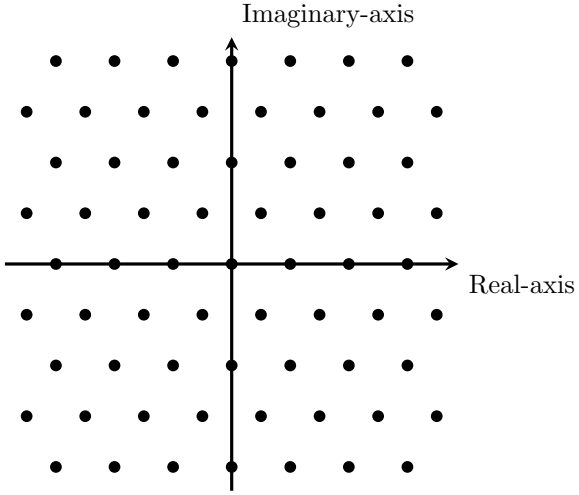

Figure 2. The Eisenstein integers on the complex plane

Specifically, we will show that there must exist a smaller solution by looking at the quotient rings for various powers of the irreducible element $1 - \zeta_3$. The highest power necessary for our proof is $(1 - \zeta_3)^4$, so we will start with a lemma describing the group structure of the units in this ring.

Lemma 2.1. $(\mathbb{Z}[\zeta_3]/((1-\zeta_3)^4))^\times \cong C_2 \times C_3^3$

Proof. Since $C_2 \times C_3^3$ is the only cyclic decomposition of abelian groups of order 54 for which all elements have order dividing 6, it is sufficient to show $\alpha^6 \equiv 1 \pmod{(1-\zeta_3)^4}$ for $\alpha \in \mathbb{Z}[\zeta_3]$ coprime to $1-\zeta_3$. Note that $(\mathbb{Z}[\zeta_3]/((1-\zeta_3)^2))^\times \cong \mathbb{Z}[\zeta_3]^\times$, hence for α coprime to $1-\zeta_3$, we conclude $\alpha^2 = (1-\zeta_3)^2\beta + \zeta_3^k$ for some $k \in \mathbb{Z}/(3)$ and $\beta \in \mathbb{Z}[\zeta_3]$. But thus $\alpha^6 = (1-\zeta_3)^4((1-\zeta_3)^2\beta^3 + 3\beta^2 - \zeta_3^{-1}\beta) + 1$, hence $\alpha^6 \equiv 1 \pmod{(1-\zeta_3)^4}$. □

We next need to see how $1-\zeta_3$ divides the left side of Fermat's equation, the surprising result is that we can 'bootstrap' the divisibility, i.e. if we have can divide by a certain power of $1-\zeta_3$, then we can divide by a larger power of $1-\zeta_3$. This is very difficult to prove in more generality, but for our proof we require only one case.

Lemma 2.2. *If* $1-\zeta_3 \nmid \alpha, \beta$ *and* $(1-\zeta)^3 \mid \alpha^3 + \zeta_3^r\beta^3$ *for some* $r \in \mathbb{Z}/(3)$*, then* $r = 0$ *and* $(1-\zeta_3)^4 \mid \alpha^3 + \beta^3$*.*

Proof. From Lemma 2.1 we know there are two elements of order no more than 2, namely 1 and -1. Since $1-\zeta_3 \nmid \alpha, \beta$, we know that there then must exist $a, b \in \mathbb{Z}/(2)$ such that

$$\begin{aligned} \alpha^3 &\equiv (-1)^a \pmod{(1-\zeta_3)^4} \\ \beta^3 &\equiv (-1)^b \pmod{(1-\zeta_3)^4}, \end{aligned} \tag{2}$$

hence

$$0 \equiv \alpha^3 + \zeta_3^r\beta^3 \equiv (-1)^a + \zeta_3^r(-1)^b \pmod{(1-\zeta_3)^3}.$$

But since

$$\left|(-1)^a + \zeta_3(-1)^b\right| \leq 2 < 3\sqrt{3} = \left|1-\zeta_3\right|^3,$$

we in fact know

$$(-1)^a + \zeta_3^r(-1)^b = 0.$$

Rearranging we find $\zeta_3^r = (-1)^{a+b+1}$, from which we know $r = 0$ and $a + b = 1$. But thus $(-1)^a + (-1)^b = 0$, hence from (2) we conclude $(1-\zeta_3)^4 \mid \alpha^3 + \beta^3$. □

The next thing to notice is that we can rewrite Fermat's equation as $x^3 + y^3 + (-z)^3 = 0$, so if we can show there are no non-trivial solutions to $x^3 + y^3 + z^3 = 0$, then Fermat's Last Theorem holds for $n = 3$. Using this with our last lemma we can conclude that a fair amount on the divisibility of a solution with respect to $1-\zeta_3$.

Lemma 2.3. *If* $\alpha, \beta, \gamma \in \mathbb{Z}[\zeta_3]$ *are pairwise coprime with*

$$(1-\zeta_3)^4 \mid \alpha^3 + \beta^3 + \gamma^3,$$

then up to symmetry

$$\begin{aligned} (1-\zeta_3)^2 &\mid \gamma \\ 1-\zeta_3 &\mid \alpha + \beta. \end{aligned}$$

Proof. Since $\delta^3 \equiv \delta \pmod{1-\zeta_3}$, we have

$$\alpha + \beta + \gamma \equiv \alpha^3 + \beta^3 + \gamma^3 \equiv 0 \pmod{1-\zeta_3}. \tag{3}$$

If $1-\zeta_3 \nmid \alpha, \beta, \gamma$, then since their sum is divisible by $1-\zeta_3$, there exists $k \in \mathbb{Z}/(2)$ and $\lambda, \mu, \nu \in \mathbb{Z}[\zeta_3]$ such that

$$\begin{aligned}\alpha &= (1-\zeta_3)\lambda + (-1)^k \\ \beta &= (1-\zeta_3)\mu + (-1)^k \\ \gamma &= (1-\zeta_3)\nu + (-1)^k.\end{aligned}$$

Let $\xi_k = \lambda^k + \mu^k + \nu^k$, then notice

$$\delta = \frac{\alpha^3+\beta^3+\gamma^3}{3} = (1-\zeta_3)((\xi_1 + (-1)^k\xi_2) - (\xi_3 + (-1)^k\xi_2)\zeta_3) + (-1)^k,$$

hence $1-\zeta_3 \nmid \delta$. But since $3(-\zeta_3)(1-\zeta_3) = (1-\zeta_3)^3 \mid 3\delta$, we have $1-\zeta_3 \mid \delta$, a contradiction, thus we conclude $1-\zeta_3 \mid \gamma$ up to symmetry. From (3) and Lemma 2.2 we conclude $(1-\zeta_3)^4 \mid \alpha^3+\beta^3$, hence $(1-\zeta_3)^4 \mid \gamma^3$, and thus $(1-\zeta_3)^2 \mid \gamma$. Finally, from (3) we get $1-\zeta_3 \mid \alpha+\beta$. □

We finally have the necessary lemmas to derive a contradiction from the existence of a non-trivial solution.

Theorem 2. *All solutions to $x^3+y^3=z^3$ are trivial.*

Proof. Let $(\alpha, \beta, \gamma) \in \mathbb{Z}[\zeta_3]^3$ be a non-trivial solution to

$$\alpha^3+\beta^3+\gamma^3 = 0 \tag{4}$$

with $|\alpha\beta\gamma|$ minimized. Notice that α, β, γ are pairwise coprime, since if ε was a irreducible common factor of any pair, then from (4) we see that it would divide the third, hence $(\alpha/\varepsilon, \beta/\varepsilon, \gamma/\varepsilon)$ would be a solution to (4) and

$$\left|\frac{\alpha}{\varepsilon}\frac{\beta}{\varepsilon}\frac{\gamma}{\varepsilon}\right| < |\alpha\beta\gamma|.$$

Now notice from Lemma 2.3 we have $(1-\zeta_3)^2 \mid \gamma$ and $1-\zeta_3 \mid \alpha+\beta$, since $\zeta_3 \equiv \zeta_3^{-1} \equiv 1 \pmod{1-\zeta_3}$ we additionally have $1-\zeta_3 \mid \alpha+\zeta_3\beta$ and $1-\zeta_3 \mid \alpha+\zeta_3^{-1}\beta$. Hence let

$$\begin{aligned}\lambda &= \frac{\alpha+\beta}{1-\zeta_3} \\ \mu &= \frac{\alpha+\zeta_3\beta}{1-\zeta_3} \\ \nu &= \frac{\alpha+\zeta_3^{-1}\beta}{1-\zeta_3}\end{aligned}$$

and first notice

$$\lambda + \zeta_3\mu + \zeta_3^{-1}\nu = 0, \tag{5}$$

thus if σ is a common divisor of any pair in λ, μ, ν, it must divide the third. But note now that

$$\begin{aligned}\sigma \mid \alpha &= \lambda - \zeta_3\nu \\ \sigma \mid \beta &= \lambda - \mu,\end{aligned}$$

therefore since α and β are coprime, λ, μ, ν must be pairwise coprime.

Now let

$$\xi = -\frac{\gamma}{1-\zeta_3}$$

then from (4) we have

$$\lambda\mu\nu = \xi^3, \tag{6}$$

therefore since λ, μ, ν are pairwise coprime and since -1 is a cube, by Lemma 1.4, we know there exist $\varphi, \chi, \psi \in \mathbb{Z}[\zeta_3]$ and $m, n \in \mathbb{Z}/(3)$ such that

$$\begin{aligned}\lambda &= \zeta_3^{-m-n}\varphi^3\\ \mu &= \zeta_3^m\chi^3\\ \nu &= \zeta_3^n\psi^3.\end{aligned}$$

Note that φ, χ, ψ are pairwise coprime, since otherwise λ, μ, ν would not be, additionally since $1-\zeta_3 \mid \xi$ (since $(1-\zeta_3)^2 \mid \gamma$), we conlude, up to symmetry, $1-\zeta_3 \mid \varphi$. From (5), we have

$$\varphi^3 + \zeta_3^r\chi^3 + \zeta_3^{-r}\psi^3 = 0,$$

where $r = 1 + n - m$, but thus, since $(1-\zeta_3)^3 \mid \chi^3 + \zeta_3^r\psi^3$, from Lemma 2.2 must have $r = 0$. Hence (φ, χ, ψ) is a non-trivial solution to (4), but from (6) we obtain

$$|\varphi\chi\psi| = |\xi| = \frac{|\gamma|}{\sqrt{3}} < |\gamma| \leq |\alpha\beta\gamma|,$$

contradicting the minimality of $|\alpha\beta\gamma|$, hence all solutions to (4) are trivial. Thus we conclude all solutions to $x^3 + y^3 = z^3$ are trivial since for any solution $(x, y, -z)$ is a solution to (4). □

3. For $n = 4$

Our proof of Fermat's Last Theorem for $n = 4$ will follow Ribenboim's exposition of Hilbert's proof given in [4]. We will show Fermat's Last Theorem by considering solutions to $x^4 + y^4 = z^2$ in the Gaussian integers. The Gaussian integers, denoted $\mathbb{Z}[i]$, is the integral span over $\{1, i\}$, this set forms a Euclidean Domain with units $\pm 1, \pm i$.

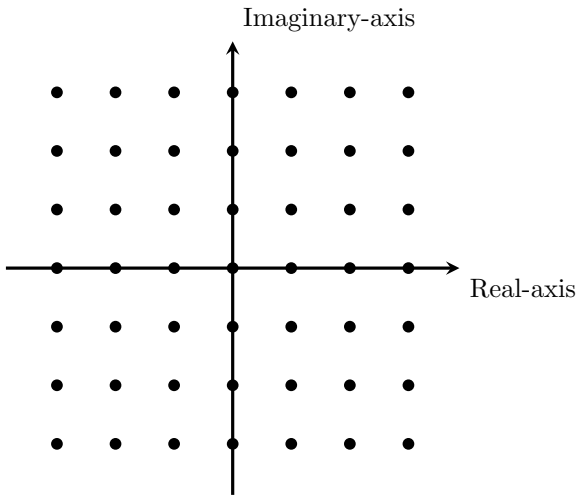

Figure 3. The Gaussian integers on the complex plane

Unlike the $n = 3$ case with the Eisenstein integers, it is not possible to completely factor the left side of Fermat's equation in the Gaussian integers, this is the main reason why we consider solutions to $x^4 + y^4 = z^2$ instead.

Similarly to the Eisenstein integers, we study quotient groups of powers of the irreducible element $1 + i$, unlike $1 - \zeta_3$ though, the group structure of the units for a particular power isn't enough. Hence, we give the following lemma.

Lemma 3.1. *For all $\alpha \in \mathbb{Z}[i]$ coprime to $1 + i$,*

$$\alpha^2 \equiv \pm 1 \pmod{(1+i)^5}$$
$$\alpha^4 \equiv 1 \pmod{(1+i)^7}.$$

Proof. Since $(\mathbb{Z}[i]/((1+i)^3))^\times \cong \mathbb{Z}[i]^\times$, there exists a $\beta \in \mathbb{Z}[i]$ and $a \in \mathbb{Z}/(4)$ such that $\alpha = (1+i)^3\beta + i^a$, hence $\alpha^2 = (1+i)^5((1+i)\beta^2 + i^{a-1}\beta) + i^{2a}$. Similarly we have $\alpha^4 = (1+i)^7((1+i)^5\beta^4 + 4i^a(1+i)^2\beta^3 + 3i^{2a-1}(1+i)\beta^2 + i^{2-a}\beta) + 1$, hence we have our desired equivalences. □

Again, we rewrite the equation we are studying, in this case $x^4 + y^4 = z^2$, with zero on the right side, thus $x^4 + y^4 - z^2 = 0$, so using this along with the previous lemma we can conclude a bit on the divisibility of a solution by $1 + i$.

Lemma 3.2. *If $\alpha, \beta, \gamma \in \mathbb{Z}[i]$ are coprime with*

$$(1+i)^5 \mid \alpha^4 + \beta^4 - \gamma^2,$$

then $(1+i)^2 \mid \alpha$ up to symmetry.

Proof. Since $\delta^n \equiv \delta \pmod{1+i}$, we have

$$\alpha + \beta + \gamma \equiv \alpha^4 + \beta^4 - \gamma^2 \equiv 0 \pmod{1+i},$$

hence $1 + i$ must divide one of α, β, γ. If it divides one of the first two, we are done up to symmetry, so suppose that $1 + i \mid \gamma$, then there exist λ, μ, ν such that

$$\alpha = (1+i)\lambda + 1$$
$$\beta = (1+i)\mu + 1$$
$$\gamma = (1+i)\nu.$$

Let $\xi_k = \lambda^k + \mu^k$, then notice

$$\delta = \frac{\alpha^4 + \beta^4 - \gamma^2}{2} = 2(-\xi_4 + (1+i)^3\xi_3 + 2i\xi_2 + (1+i)\xi_1) + i\nu^2 + 1,$$

hence since $(1+i)^2 \mid \delta$, we must have $\nu^2 \equiv i \pmod{(1+i)^2}$, an impossibility. Therefore, up to symmetry $1 + i \mid \alpha$. Now since $1 + i \nmid \beta$, we know from Lemma 3.1 that $\beta^4 \equiv 1 \pmod{(1+i)^4}$, hence $\gamma^2 \equiv 1 \pmod{(1+i)^4}$. But thus $\gamma \equiv 1 \pmod{(1+i)^2}$ since otherwise $\gamma \equiv i \pmod{(1+i)^2}$ which would imply for some $\psi \in \mathbb{Z}[i]$, $\gamma^2 = (1+i)^4\psi^2 + 2i(1+i)^2\psi - 1 \equiv -1 \pmod{(1+i)^4}$ which is an impossibility. So let

$$\psi = \frac{\gamma - 1}{(1+i)^2},$$

then note that

$$\gamma^2 - 1 = (\gamma - 1)(\gamma + 1) = (1+i)^2\psi((1+i)^2\psi + 2) = (1+i)^4\psi(\psi + i^{-1}),$$

hence since either ψ or $\psi + i^{-1}$ is divisible by $1 + i$, we conclude $(1+i)^5 \mid \gamma^2 - 1$. Since from Lemma 3.1 we know $(1+i)^5 \mid \beta^4 - 1$, we can conclude $(1+i)^5 \mid \alpha^4$, hence $(1+i)^2 \mid \alpha$. □

We now have enough to argue towards a contradiction with the existence of a non-trivial solution to Fermat's equation for $n = 4$. Our argument now contradicts the minimality of the multiplicity of $1 + i$ in our factors of our non-trivial solution, rather than the magnitude of the product of our non-trivial solution as we did with the Eisenstein integers.

Theorem 3. *All solutions to $x^4 + y^4 = z^4$ are trivial.*

Proof. Let $(\alpha, \beta, \gamma, k) \in \mathbb{Z}[i]^3 \times \mathbb{Z}$ be a non-trivial solution to

$$((1+i)^k\alpha)^4 + \beta^4 = \gamma^2, \tag{7}$$

such that $1 + i, \alpha, \beta, \gamma$ are coprime and k is minimal. Rearranging we find

$$(1+i)^{4k}\alpha^4 = (\gamma + \beta^2)(\gamma - \beta^2),$$

and since from Lemma 3.2 we know $k > 0$, thus $(1+i)^4 \mid (\gamma + \beta^2)(\gamma - \beta^2)$. In fact we can conclude $\gcd_{\mathbb{Z}[i]}(\gamma + \beta^2, \gamma - \beta^2) = (1+i)^2$:

(1) $(1+i)^2 \mid \gamma + \beta^2, \gamma - \beta^2$, because $\gamma - \beta^2 \equiv \gamma + \beta^2 \pmod{(1+i)^2}$.
(2) if δ is a common divisor, then

$$\delta \mid 2\gamma \ = (\gamma + \beta^2) + (\gamma - \beta^2)$$
$$\delta \mid 2\beta^2 = (\gamma + \beta^2) - (\gamma - \beta^2). \tag{8}$$

We can thus conclude $(1+i)^{4k-2} \mid \gamma + \beta^2$ and $(1+i)^2 \mid \gamma - \beta^2$ without loss of generality since $(i\beta)^2 = -\beta^2$. Hence let

$$\lambda = \frac{\gamma + \beta^2}{(1+i)^{4k-2}}$$
$$\mu = \frac{\gamma - \beta^2}{(1+i)^2},$$

then we can conclude from (7) that

$$\alpha^4 = \lambda\mu,$$

thus since λ, μ are coprime, from Lemma 1.4 there exist $\varphi, \chi \in \mathbb{Z}[i]$ and $a \in \mathbb{Z}/(4)$ such that

$$\lambda = i^{-a}\varphi^4$$
$$\mu = i^a\chi^4.$$

From (8) we get

$$i^{1-a}((1+i)^{k-1}\varphi)^4 + i^{a-1}\chi^4 = \beta^2 \tag{9}$$

hence since $k > 1$ from Lemma 3.2 we know $(1+i)^4 \mid \beta^2 + i^{a+1}\chi^4$ and from Lemma 3.1 we know $(1+i)^4 \mid i^{2b} + i^{a+1}$ for some $b \in \mathbb{Z}/(4)$. But since $\left|i^{2b} + i^{a+1}\right| \leq 2 < 4 = |1+i|^4$ we know $i^{2b} + i^{a+1} = 0$, hence $a = 2b + 1$. Substituting in b and rearranging (9) we obtain

$$((1+i)^{k-1}\varphi)^4 + \chi^4 = (i^b\beta)^2,$$

indicating $(\varphi, \chi, i^b\beta, k-1)$ is a non-trivial solution to (7). Since $1 + i, \varphi, \chi, \beta$ must be coprime from how φ, χ are defined, we have contradicted the minimality of k, hence there are no non-trivial coprime solutions to (7).

If (α, β, γ) is a solution to

$$\alpha^4 + \beta^4 = \gamma^2, \tag{10}$$

then $(\lambda, \mu, \nu) = (\alpha/\varepsilon, \beta/\varepsilon, \gamma/\varepsilon^2)$ is a solution, where $\varepsilon = \gcd_{\mathbb{Z}[i]}(\alpha, \beta)$. Notice λ, μ, ν are coprime since λ^2, μ^2, ν are coprime and any common divisor of λ and ν would then necessarily divide λ^2, μ^2. Now from Lemma 3.2 we know that $1 + i$ divides λ up to symmetry hence there exists $\varphi \in \mathbb{Z}[i]$ and $k \in \mathbb{Z}_{>0}$ such that $\lambda = (1 + i)^k \varphi$ and $1 + i \nmid \varphi$. But now (φ, μ, ν, k) is a coprime solution to (7), hence it must be trivial, thus (α, β, γ) is a trivial solution to (10). But thus we conclude that all solutions to $x^4 + y^4 = z^4$ are trivial, since (x, y, z^2) is a solution to (10). □

4. Conclusion

With our proofs we have accomplished three things. We have given evidence for Fermat's Last Theorem, while Fermat's Last Theorem is true, this is not proof. What is more significant is our reduction of the problem, that is to show Fermat's Last Theorem, we need only consider Fermat's equation when n is prime:

Consider Fermat's equation with n composite, then either there is an odd prime $p \mid n$ or n is a power of 2. In the first case, if (a, b, c) is a solution to $x^n + y^n = z^n$ then $(a^{n/p}, b^{n/p}, c^{n/p})$ is a solution to $x^p + y^p = z^p$, hence we only need to show all solutions to Fermat's equation for p an odd prime are trivial. In the second case, then since $n > 2$, we have $4 \mid n$, hence if (a, b, c) is a solution to $x^n + y^n = z^n$ then $(a^{n/4}, b^{n/4}, c^{n/4})$ is a solution to $x^4 + y^4 = z^4$, hence it must be (a, b, c) must be trivial.

Finally, Fermat's Last Theorem is true not just over the integers, but also over the rationals, since we can multiply through by the denominators and get a solution to the integers. With our proofs, we have also shown that over the Gaussian field, Fermat's Last Theorem is true for $4 \mid n$, and over the Eisenstein field, Fermat's Last Theorem is true for $3 \mid n$. So we might ask the question, given a number field K, for what n does Fermat's Last Theorem hold?

As far as the author of this paper is aware, the question goes unstudied. What is clear though, is the study of Fermat's equation, one so simple that Fermat's Last Theorem can be understood by the general populace, is incredibly intricate and even the simplest of cases require a substantial amount of machinery to prove.

References

[1] Dörrie, H. *100 Great Problems of Elementary Mathematics*. Dover Publications, Inc., 1965.
[2] Euclid. *Euclid's Elements*. Green Lion Press, 2003. English translation: translated by Heath, T. L.
[3] Hilbert, D. *The Theory of Algebraic Number Fields*. Springer-Verlag, Inc., 1998. English translation: translated by Adamson, I. T.
[4] Ribenboim, P. *Fermat's Last Theorem for Amateurs*. Springer-Verlag, Inc., 1991.