FLT Generalized to Gaussian Primes

Silas Richelson

February 8, 2005

1 Abstract

This paper examines Fermat's Last Theorem, $x^n + y^n = z^n$, for $n \geq 3$, when x, y and z are Gausian primes, and n is an odd integer, and proves that FLT holds in such cases.

2 Introduction

A Gaussian number is defined as a number that can be written as $a + bi$ where $a, b \in \mathbb{R}$, and also, $i = \sqrt{-1}$. A Gaussian integer is a Gaussian number where a and b are rational integers. In any integer field a unit is an element of the field, I, with the following property

$$|a| = |I \cdot a|$$

where a is an arbitrary element in the field. In the rational number field, the units are ± 1. In the Gaussian field the units are ± 1 and $\pm i$. A Gaussian prime is defined as a Gaussian integer that cannot be written as the product of two non-units.

Every complex number has a conjugate. The conjugate of the Gaussian number $\alpha = a+bi$ is $\alpha' = a-bi$. Notice that both $\alpha+\alpha' = 2a$ and $\alpha \cdot \alpha' = a^2+b^2$ are real. The norm of α, written as $N(\alpha) = \alpha \cdot \alpha'$. At this point we introduce two lemmas concerning $N(\alpha)$ when α is a Gaussian prime.

Lemma 1 *If ρ is a Gaussian prime, then $\rho \cdot \rho' = p$ where p is an integer prime.*

Proof Suppose p is a composite integer. Then $p = p_1 \cdot p_2$ where $p_1, p_2 \in \mathbb{Z}, p_1, p_2 \neq 1$. However, then $\rho \cdot \rho' = p_1 \cdot p_2$. This means that one of the four conditions must occur:

(1) $p_1 | \rho$
(2) $p_1 | \rho'$
(3) $p_2 | \rho$
(4) $p_2 | \rho'$

However, this is impossible as both ρ and ρ' are prime, and are therefore cannot be divisible by either p_1 or p_2 as $p_1, p_2 \neq 1$. □

Lemma 2 *If ρ is a Gaussian prime then $\rho \cdot \rho' \equiv 1 (\mathrm{mod}\, 4)$*

Proof Since ρ is a Gaussian prime, ρ can be written as $\rho = a + bi$, where $a, b \in \mathbb{Z}$. Also, notice that a and b must be of opposite parity, because if they are of the same parity then

$$(1+i)|a+bi$$

which cannot be the case since $a + bi = \rho$ which is prime. Therefore

$$\rho \cdot \rho' = (a+bi)(a-bi) = a^2 + b^2.$$

However, if t is even then $t^2 \equiv 0 (\mathrm{mod}\, 4)$, if t is odd, $t^2 \equiv 1 (\mathrm{mod}\, 4)$. Since a and b are of opposite parity, $a^2 + b^2 \equiv 1 \pmod 4$. □

Now we are able to prove the main theorem.

3 Fermat's Last Theorem for Gaussian Primes

Theorem 1 *The equation*

$$\alpha^n + \beta^n = \sigma^n (3.1)$$

has no solutions when α, β, σ are Gaussian primes and n is odd.

Proof We begin by multiplying each side of (**??**.1) by its conjugate

$$[\alpha^n + \beta^n][(\alpha')^n + (\beta')^n] = \alpha^n(\alpha')^n + \beta^n(\beta')^n + \alpha^n(\beta')^n + \beta^n(\alpha')^n = [\sigma^n][(\sigma')^n].$$

By lemma 3, $\alpha \cdot \alpha', \beta \cdot \beta', \sigma \cdot \sigma'$ are all equal to integer primes. Let

$$\alpha \cdot \alpha' = a, \beta \cdot \beta' = b, \sigma \cdot \sigma' = c$$

where a, b and c are integer primes. Also, $\alpha \cdot \beta'$ and $\alpha' \cdot \beta$ are complex conjugates. Therefore $(\alpha \cdot \beta')^n$ and $(\alpha' \cdot \beta)^n$ are also conjugates, which means that $(\alpha \cdot \beta')^n + (\alpha' \cdot \beta)^n = 2r$ where r some integer (more specifically, the real part of both $(\alpha \cdot \beta')^n$ and $(\alpha' \cdot \beta)^n$). Substitution in (3.2) yields

$$a^n + b^n + 2r = c^n.$$

This means that one of a, b and c must be even. However, all are prime, which means that exactly one of a, b and c must equal 2. Assume without loss of generality that $c = 2$. Observe that since $c = \sigma \cdot \sigma'$, and $2 = (1+i)(1-i)$, either $\sigma = 1 + i, \sigma' = 1 - i$ or visa versa. Substitution in (3.1) yields

$$\alpha^n + (1 \pm i)^n = \beta^n.$$

In this equation we can assume without loss of generality that $|\alpha| < |\beta|$, because if $|\alpha| > |\beta|$, then the equation can be rewritten as follows

$$\alpha^n = \beta^n - (1 \pm i)^n.$$

Also, since n is odd, $(-1)^n = -1$, which means that

$$\alpha^n = \beta^n + (-1)^n(1 \pm i)^n = \beta^n + (-1 \mp i)^n.$$

Therefore, any such equation where the isolated prime (i.e. the prime that is alone on its side of the equation) has greater magnitude than the nonisolated prime (i.e. the prime that is on the same side of the equation as $(1 \pm i)^n$), can be transposed so that in the new equation, the isolated prime has less magnitude than the nonisolated prime. Therefore, we may assume without loss of generality that α is the nonisolated prime and that $|\alpha| < |\beta|$.

Continuing, we recall that (3.1) yields

$$\alpha^n + (1 \pm i)^n = \beta^n.$$

Multiplication of each side by its conjugate yields

$$a^n + 2^n + [(1+i)^n \cdot (\alpha')^n + (1-i)^n \cdot \alpha^n] = b^n.$$

Also, recall that we let n be odd. Therefore we can let $n = 2N + 1$ where N is an arbitrary integer. Substitution yields

$$a^{2N+1} + 2^{2N+1} + [(1+i)^{2N+1} \cdot (\alpha')^{2N+1} + (1-i)^{2N+1} \cdot (\alpha)^{2N+1}] = b^{2N+1}.$$

Now examining the term $[(1+i)^{2N+1} \cdot (\alpha')^{2N+1} + (1-i)^{2N+1} \cdot (\alpha)^{2N+1}]$ more closely, we notice that

$$\begin{aligned}
&(1+i)^{2N+1}(\alpha')^{2N+1} + (1-i)^{2N+1}(\alpha)^{2N+1} \\
&= (1+i)(1+i)^{2N}(\alpha')^{2N+1} + (1-i)(1-i)^{2N}(\alpha)^{2N+1} \\
&= (1+i)(2i)^N(\alpha')^{2N+1} + (1-i)(-2i)^N(\alpha)^{2N+1} \\
&= (1+i) \cdot 2^N \cdot i^N \cdot (\alpha')^{2N+1} + (1-i) \cdot 2^N \cdot (-i)^N \cdot (\alpha)^{2N+1} \\
&= 2^N[(1+i) \cdot i^N \cdot (\alpha')^{2N+1} + (1-i) \cdot (-i)^N \cdot (\alpha)^{2N+1}]
\end{aligned}$$

Substitution yields

$$a^{2N+1} + 2^{2N+1} + 2^N[(1+i) \cdot i^N \cdot (\alpha')^{2N+1} + (1-i) \cdot (-1)^N \cdot (\alpha)^{2N+1}] = b^{2N+1}$$

Transposition yields

$$2^{2N+1} + 2^N[(1+i) \cdot i^N \cdot (\alpha')^{2N+1} + (1-i) \cdot (-i)^N \cdot (\alpha)^{2N+1}] = b^{2N+1} - a^{2N+1}$$

$$2^N[2^{N+1} + (1+i) \cdot i^N \cdot (\alpha')^{2N+1} + (1-i) \cdot (-i)^N \cdot (\alpha)^{2N+1}] = (b-a)(b^{2N} + b^{2N-1}a + \cdots + a^{2N}).$$

Notice that $(b^{2N} + \cdots + a^{2N})$ is an odd integer as, since both a and b are odd, which means that each term is an odd integer. Moreover, there are $2N + 1$, an odd number, of terms. Therefore $(b^{2N} + \cdots + a^{2N})$ is a polynomial with an odd number of odd terms, making it an odd number. Therefore, 2 does not divide $(b^{2N} + \cdots + a^{2N})$. However, by the previous equation,

$$2^N | (b-a)(b^{2N} + \cdots + a^{2N}).$$

It follows that $2^N|(b-a)$. Also, recall that $|\alpha| < |\beta|$, which means that $a < b$. Therefore, $2^N \leq (b-a)$. However, this implies that

$$(b^{2N} + \cdots + a^{2N}) \leq 2^{N+1} + (1+i) \cdot i^N \cdot (\alpha')^{2N+1} + (1-i) \cdot (-i)^N \cdot (\alpha)^{2N+1}$$

The goal of the remainder of the proof is to find a quantity that the right side of the previous inequality is less than, and to show that the left side must be greater than it, thereby yielding a contradiction. Notice that

$$\begin{aligned}
&2^{N+1} + (1+i) \cdot i^N \cdot (\alpha')^{2N+1} + (1-i) \cdot (-1)^N \cdot (\alpha)^{2N+1} \\
&\leq |2^{N+1} + (1+i) \cdot i^N \cdot (\alpha')^{2N+1} + (1-i) \cdot (-1)^N \cdot (\alpha)^{2N+1}| \\
&\leq 2^{N+1} + |1+i| \cdot |i^N| \cdot |(\alpha')^{2N+1}| + |1-i| \cdot |(-i)^N| \cdot |(\alpha)^{2N+1}| \\
&= 2^{N+1} + \sqrt{2} \cdot |(\alpha')^{2N+1}| + \sqrt{2} \cdot |(\alpha)^{2N+1}| \\
&= 2^{N+1} + 2\sqrt{2} \cdot |\alpha^{2N+1}| \\
&= 2^{N+1} + 2\sqrt{2} \cdot \sqrt{a^{2N+1}} \\
&\leq 2^{N+1} + 2\sqrt{2} \cdot \sqrt{a^{2N+2}} \\
&= 2^{N+1} + 2\sqrt{2} \cdot a^{N+1}
\end{aligned}$$

Therefore,

$$b^{2N} + \cdots + a^{2N} \leq 2^{N+1} + 2\sqrt{2} \cdot a^{N+1}.$$

Notice that as N increases, $b^{2N} + \cdots + a^{2N}$ increases faster than $2^{N+1} + 2\sqrt{2} \cdot a^{N+1}$ does, as the power of N in $b^{2N} + \cdots + a^{2N}$ is greater, and $a > 1$. Therefore, if the above inequality holds when $N = 1$, which results from $n = 3$, the minimum value of n, then the inequality will always hold.

$$b^2 + ab + a^2 \leq 2^2 + 2\sqrt{2} \cdot a^2 = 4 + 2\sqrt{2} \cdot a^2$$

Recall $a < b$, which means that

$$\begin{aligned}
b^2 + \text{ab} + a^2 < a^2 + a^2 + a^2 = 3a^2 \leq 4 + 2\sqrt{2} \cdot a^2 \\
\implies 3a^2 - 2\sqrt{2} \cdot a^2 = a^2(3 - 2\sqrt{2}) \leq 4 \\
\implies a^2 \leq \frac{4}{3 - 2\sqrt{2}} = \frac{4}{\sqrt{9} - \sqrt{8}} = 4\sqrt{9} + 4\sqrt{8} \leq 4 \cdot 3 + 4 \cdot 3 = 24 < 25 \\
\implies a < 5.
\end{aligned}$$

However, this is impossible as by lemmas 3 and 4, a must be an integer prime congruent to 1 mod 4. The smallest such prime is 5. Therefore, $a \geq 5$. A contradiction has been reached. Therefore the equation $\alpha^n + \beta^n = \sigma^n$ has no solutions when α, β, and σ are Gaussian primes and n is an integer greater than or equal to 3. $\square$