AN ELEMENTARY PROOF OF FERMAT LAST THEOREM

THEOPHILUS AGAMA

Abstract. We provide an elementary proof of Fermat's last theorem using the notion of *olloids*.

1. Introduction

Fermat's Last Theorem (FLT), one of the most famous and long-standing conjectures in number theory, asserts that no three positive integers x, y, z can satisfy the equation $x^n + y^n = z^n$ for $n \geq 3$. The conjecture, first proposed by Pierre de Fermat in 1637, was famously noted in the margin of his copy of an ancient Greek text, where he claimed to have discovered a "marvelous proof" but lamented the narrow margin that prevented him from recording it. Despite Fermat's assertion, no proof was found during his lifetime, and the conjecture remained unproven for over 350 years (Fermat, 1637).

For much of this time, FLT was considered one of the most elusive conjectures in mathematics. Over the centuries, progress has been made by proving the theorem for specific values of the indices n. For example, Fermat himself proved the case for $n = 4$, and Euler demonstrated the result for $n = 3$ in the eighteenth century. Dirichlet and Legendre later proved the case for $n = 5$ in the 19th century (Fermat, 1637). Despite these partial results, the general case of FLT remained unsolved.

A crucial breakthrough occurred in the 1990s with the work of Sir Andrew Wiles. After years of solitary work, Wiles presented his proof of FLT in 1994, utilizing advanced techniques from algebraic geometry, modular forms, and elliptic curves (Wiles, 1995). Central to Wiles' approach was the Taniyama-Shimura-Weil conjecture (now a theorem), which posits a deep connection between elliptic curves and modular forms. Wiles' proof hinged on showing that a particular type of elliptic curve could not exist, which in turn implied the truth of FLT. Although Wiles' initial proof contained a gap, it was later corrected in 1995, solidifying the result and ending centuries of speculation on the validity of the theorem [1].

The work of several mathematicians played a critical role in the eventual proof. Ribets theorem in the 1980s was pivotal, showing that the truth of FLT was equivalent to a special case of the Taniyama-Shimura-Weil conjecture [2]. Ribet's insight linked modular forms to the problem of Fermat's Last Theorem, providing a crucial step toward the proof. The contributions of Frey, Nron, and others in the study of elliptic curves also formed the mathematical backdrop against which Wiles worked [4].

Moreover, the work of Pierre Deligne, whose proof of the Weil conjectures in the 1970s revolutionized algebraic geometry, laid the groundwork for understanding the

Date: December 22, 2024.
2000 *Mathematics Subject Classification.* Primary 54C40, 14E20; Secondary 46E25, 20C20.
Key words and phrases. olloids.

deep structure of modular forms and elliptic curves. These results were essential for Wiles' later work on FLT, showing that the connection between elliptic curves and modular forms could be used to prove the theorem [3].

Wiles' proof is regarded as a milestone in modern mathematics, combining multiple areas of study that had not previously been linked in such a direct manner. Despite the highly technical nature of the proof, which draws upon structures such as elliptic curves, modular forms, and algebraic geometry, its resolution of FLT has had profound implications for number theory and related fields. The rigorous and highly non-elementary nature of the proof means that it is far removed from Fermat's original, elementary conjecture, but it provides a deep insight into the structures underlying number theory.

In this paper, we revisit Fermat's Last Theorem from an elementary perspective. Although Wiles proof remains definitive, we provide an elementary proof in this paper that uses the notion of the olloid.

2. The notion of the olloid

In this section we launch the notion of the **olloid** and prove a fundamental lemma, which will be relevant for our studies in the sequel.

Definition 2.1. Let $\mathbb{F}_s^k := \left\{(u_1, u_2, \ldots, u_s) \in \mathbb{R}^s \mid \sum_{i=1}^{s} u_i^k = 1,\ k > 1\right\}$. Then we call $\mathbb{F}_s^k$ an s-dimensional **olloid** of degree $k > 1$. We say $g : \mathbb{N} \longrightarrow \mathbb{R}$ is a generator of the s-dimensional olloid of degree k if there exists some vector $(v_1, v_2, \ldots, v_s) \in \mathbb{F}_s^k$ such that $v_i = g(i)$ for each $1 \leq i \leq s$.

Question 2.2. Does there exists a fixed generator $g : \mathbb{N} \longrightarrow \mathbb{R}$ with infinitely many olloids?

Remark 2.3. Although it may be difficult to provide a general answer to question 2.2, we can, in fact, provide an answer by imposing certain conditions for which the generator of the **olloid** must satisfy. In particular, we launch a basic and a fundamental principle relevant for our studies in the sequel.

Lemma 2.4 (Expansion principle)**.** *Let $\mathbb{F}_s^k$ be an s-dimensional **olloid** of degree $k > 1$ for a fixed $k \in \mathbb{N}$. If $g : \mathbb{N} \longrightarrow \mathbb{R}^+$ is a generator with continuous derivative on $[1, s]$ and decreasing on $\mathbb{R}^+$ such that*

$$1 - \frac{1}{g(s)^r} > \int_1^s \frac{g'(t)}{g(t)^2}dt + \frac{1}{g(s)}\int_1^s \frac{g'(t)}{g(t)^2}dt + \cdots + \frac{1}{g(s)^{r-1}}\int_1^s \frac{g'(t)}{g(t)^2}dt$$

*for $r \in \mathbb{N}$ then $g : \mathbb{N} \longrightarrow \mathbb{R}^+$ is also a generator of the **olloid** $\mathbb{F}_s^{k+r}$ of degree $k + r$.*

Proof. Suppose $g : \mathbb{N} \longrightarrow \mathbb{R}^+$ is a generator of the **olloid** $\mathbb{F}_s^k$ with continuous derivative on $[1, s]$. Then there exists a vector $(v_1, v_2, \ldots, v_s) \in \mathbb{F}_s^k$ such that $v_i = g(i)$ for each $1 \leq i \leq s$, so that we can write

$$\sum_{i=1}^{s} \frac{g(i)^{k+1}}{g(i)} := \sum_{i=1}^{s} g(i)^k = 1.$$

Let us assume to the contrary that there exists no $r \in \mathbb{N}$ such that $g : \mathbb{N} \longrightarrow \mathbb{R}^+$ is a generator of the **olloid** $\mathbb{F}_s^{k+r}$. By applying the summation by parts, we obtain

the inequality

$$\frac{1}{g(s)}\sum_{i=1}^{s} g(i)^{k+1} \geq 1 - \int_{1}^{s} \frac{g'(t)}{g(t)^2}dt \tag{2.1}$$

by using the inequality

$$\sum_{i=1}^{s} g(i)^{k+1} < \sum_{i=1}^{s} g(i)^{k} = 1.$$

By applying summation by parts on the left side of (2.1) and using the contrary assumption, we obtain further the inequality

$$\frac{1}{g(s)^2}\sum_{i=1}^{s} g(i)^{k+2} \geq 1 - \int_{1}^{s} \frac{g'(t)}{g(t)^2}dt - \frac{1}{g(s)}\int_{1}^{s} \frac{g'(t)}{g(t)^2}dt. \tag{2.2}$$

By induction we can write the inequality as

$$\frac{1}{g(s)^r}\sum_{i=1}^{s} g(i)^{k+r} \geq 1 - \int_{1}^{s} \frac{g'(t)}{g(t)^2}dt - \frac{1}{g(s)}\int_{1}^{s} \frac{g'(t)}{g(t)^2}dt - \cdots - \frac{1}{g(s)^{r-1}}\int_{1}^{s} \frac{g'(t)}{g(t)^2}dt$$

for any $r \geq 2$ with $r \in \mathbb{N}$. Since $g : \mathbb{N} \longrightarrow \mathbb{R}^+$ is decreasing, it follows that

$$1 - \int_{1}^{s} \frac{g'(t)}{g(t)^2}dt - \frac{1}{g(s)}\int_{1}^{s} \frac{g'(t)}{g(t)^2}dt - \cdots - \frac{1}{g(s)^{r-1}}\int_{1}^{s} \frac{g'(t)}{g(t)^2}dt > 1$$

and using the requirement

$$1 - \frac{1}{g(s)^r} > \int_{1}^{s} \frac{g'(t)}{g(t)^2}dt + \frac{1}{g(s)}\int_{1}^{s} \frac{g'(t)}{g(t)^2}dt + \cdots + \frac{1}{g(s)^{r-1}}\int_{1}^{s} \frac{g'(t)}{g(t)^2}dt$$

for $r \in \mathbb{N}$, we have the inequality

$$1 = \sum_{i=1}^{s} g(i)^{k} \geq \sum_{i=1}^{s} g(i)^{k+r} > 1$$

which is absurd. This completes the proof of the Lemma. □

Remark 2.5. It is worth noting that the extra condition in Lemma 2.4 can be rewritten in the form

$$\frac{1}{g(s)^r} - 1 < \sum_{i=0}^{r-1} \frac{1}{g(s)^i}\left(\frac{1}{g(s)} - \frac{1}{g(1)}\right)$$

3. **The elementary proof**

In this section, we provide an elementary proof of Fermat last theorem by applying Lemma 2.4.

Theorem 3.1. *The equation $x^n + y^n = z^n$ for $n \geq 3$ has no solution in the positive integers.*

3.1. **Proof.**

3.2. **Step 1.** We rewrite Fermat's equation $x^n + y^n = z^n$ $(n \geq 2)$ fixed in the form

$$\left(\frac{1}{z/x}\right)^n + \left(\frac{1}{z/y}\right)^n = 1.$$

This is therefore a 2-dimensional *olloid* of degree $n \geq 2$. Since the equation has a solution for $n = 2$ there exists a generator $g(t)$ of the 2-dimensional *olloid* $\mathbb{F}_2^2$ of degree 2. The generator $g(t) := \frac{1}{t}$ of this *olloid* is unique. In fact, with $t_{x,z} = \frac{z}{x}$ and $t_{y,z} = \frac{z}{y}$, we see that $g(t_{x,z})^n + g(t_{y,z})^n = 1$. Hence $g(t) := \frac{1}{t}$ is indeed the unique generator of this 2-dimensional *olloid* $\mathbb{F}_2^n$ of degree $n = 2$.

3.3. **Step 2.** It is easy to check that the generator $g(t) := \frac{1}{t}$ of the 2-dimensional *olloid* $\mathbb{F}_2^2$ is decreasing on $(0, \infty)$ and continuously differentiable on $[1, s]$.

3.4. **Step 3.** We now verify the validity of the inequality to be satisfied by the generator $g(t) = \frac{1}{t}$. This is the most crucial part of the argument. This requirement, if satisfied by the unique generator $g(t) = \frac{1}{t}$, will extend the status of g as a generator of the *olloid* $\mathbb{F}_2^2$ to an arbitrary degree. Suppose that for $r \in \mathbb{N}$ with $r \geq 1$, we have

$$\frac{1}{g(2)^r} - 1 < \sum_{i=0}^{r-1} \frac{1}{g(2)^i}\left(\frac{1}{g(2)} - \frac{1}{g(1)}\right).$$

Given that $g(t) := \frac{1}{t}$, this inequality reduces to $2^r - 1 < \sum\limits_{i=0}^{r-1} 2^i = 2^r - 1$, which is absurd. Thus, the unique generator $g(t) := \frac{1}{t}$ of the 2-dimensional *olloid* $\mathbb{F}_2^2$ cannot be extended to any degree $n + r \geq 3$.

3.5. **Step 4.** Since the unique generator $g(t) := \frac{1}{t}$ of the 2-dimensional *olloid* satisfies the condition in the Lemma but cannot be extended to 2-dimensional *olloids* $\mathbb{F}_2^{n+r}$ of degree $n + r \geq 3$, it follows that the 2-dimensional olloid $\mathbb{F}_2^n$ of degree of $n \geq 3$ has no generator. This implies the equation $x^n + y^n = z^n$ for $n \geq 3$ does not have a non-trivial solution over positive integers.
[1]

References

1. Wiles, Andrew, *Modular elliptic curves and Fermat's last theorem*, Annals of mathematics, vol. 141(3), JSTOR, 1995, 443–551.
2. Ribet, Kenneth A, *On modular representations of Gal (Q/Q) arising from modular forms*, Invent. math, vol. 100:2, 1990, 431–476.
3. Deligne, Pierre, *Théorie de hodge: Iii*, Publications Mathématiques de l'IHÉS, vol. 44, 1974, 5–77.
4. Frey, Gerhard, *On ternary equations of Fermat type and relations with elliptic curves*, Springer, 1997, 527–548.

Department of Mathematics, African Institute for Mathematical Sciences, Ghana
E-mail address: theophilus@aims.edu.gh/emperordagama@yahoo.com

[1]