

# Using a Proof Assistant for Non-Trivial Theorems.

By A. E. Mahrouss

July 19, 2026

## Contents

|                                     |          |
|-------------------------------------|----------|
| <b>1 Abstract:</b>                  | <b>2</b> |
| <b>2 Synopsis:</b>                  | <b>2</b> |
| 2.1 Theorems and Proofs: . . . . .  | 2        |
| 2.2 Notes on Theorem 1.1: . . . . . | 2        |
| <b>3 Remarks:</b>                   | <b>2</b> |
| <b>4 Going Forward:</b>             | <b>2</b> |
| 4.1 Conclusion: . . . . .           | 2        |

## 1 Abstract:

PER previous documents, our duty is now to write proof statements in Lean. Lean is a formidable proof assistant. We could use it to prove smaller theorems to then prove bigger theorems. Or, practice using it (Lean) to learn our craft.

## 2 Synopsis:

### 2.1 Theorems and Proofs:

LET the following theorem for  $x, y, z \in \mathbb{Z}$ . The following theorem per FLT (Fermat's Last Theorem) admits an identity for the following:

**Theorem 2.1.** *There exists no solutions for  $p^n$  in  $\mathbb{Z}$ . If and only If:*

$$x^n + y^n + z^n = p^n, \quad \forall n, c, x, y, z, p \neq 0, n \geq 2.$$

For all variables of  $n, x, y, z, p \in \mathbb{Z}$ . We could go by induction per Fermat Last Theorem that  $x^n + y^n + z^n$  equals to:

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

For  $\forall x^n + y^n + z^n \in \mathbb{Z}$ :

$$x^n + y^n + z^n = a^n + b^n.$$

If and only If for  $\forall x^n + y^n + z^n \in \mathbb{Z}$ :

$$x^n + y^n + z^n \neq 0, \quad x^n + y^n + z^n \geq 2, \quad \forall x^n + y^n + z^n \in \mathbb{Z}.$$

Thus we can induce the following for  $\forall x^n + y^n + z^n \in \mathbb{Z}$ :

$$x^n + y^n + z^n - a^n = b^n, \quad x^n + y^n + z^n - b^n = a^n.$$

If and only If for  $\forall x^n + y^n + z^n \in \mathbb{Z}$ :

$$x^n + y^n + z^n - a^n - b^n = 0, \quad x^n + y^n + z^n \neq 0.$$

*Remark 2.2.* There is a possibility that  $x^n + y^n + z^n \geq 2$ , may be replaced under some circumstances with  $x^n + y^n + z^n \geq \mathbb{P}_0$ . Where  $\mathbb{P}$  is a sequence of pair numbers greater than one.

### 2.2 Notes on Theorem 1.1:

*Remark 2.3.* One method for proving Theorem 1.1 is using proofs by direct and/or induction of the FLT by Wiles.

## 3 Remarks:

PROOF sources have been distributed with the repository, one exercise would be for the reader to implement such non-trivial proof in Lean.

However usage of Lean may not be warranted for every proof writing.

## 4 Going Forward:

### 4.1 Conclusion:

WHILE a short note, the purpose is for the development of methodology on using proof assistants for non-trivial conjectures and theorems of Pure Mathematics.

---

## References

- [1] AVIGAD, J., DE MOURA, L., AND KONG, S. Theorem proving in lean.
- [2] HARDY, G. *A Course of Pure Mathematics*. Cambridge Mathematical Library. Cambridge University Press, 2002.
- [3] WEIL, A., AND WEIL, A. *Basic number theory*, vol. 1974. Springer, 1967.
- [4] WILES, A. Modular elliptic curves and fermat’s last theorem. *Annals of mathematics* 141, 3 (1995), 443–551.