**Notes on Number Theory and Discrete Mathematics**
**Print ISSN 1310–5132, Online ISSN 2367–8275**
**Vol. 25, 2019, No. 2, 22–29**
**DOI: 10.7546/nntdm.2019.25.2.22-29**

# Eisenstein's criterion, Fermat's last theorem, and a conjecture on powerful numbers

**Pietro Paparella**

Division of Engineering and Mathematics, University of Washington Bothell
18115 Campus Way NE, Bothell, WA 98011-8246, United States
e-mail: pietrop@uw.edu

**Received:** 2 January 2019 **Accepted:** 18 March 2019

**Abstract:** Given integers $\ell > m > 0$, monic polynomials $X_n$, $Y_n$, and $Z_n$ are given with the property that the complex number $\rho$ is a zero of $X_n$ if and only if the triple $(\rho, \rho + m, \rho + \ell)$ satisfies $x^n + y^n = z^n$. It is shown that the irreducibility of these polynomials implies Fermat's last theorem. It is also demonstrated, in a precise asymptotic sense, that for a majority of cases, these polynomials are irreducible via application of Eisenstein's criterion. We conclude by offering a conjecture on powerful numbers.

**Keywords:** Eisenstein's criterion, Fermat's last theorem, Fermat equation, Irreducible polynomial, Powerful numbers.
**2010 Mathematics Subject Classification:** 11A99, 11C08, 11D41.

## 1 Introduction

In its original form, *Fermat's last theorem* (FLT) asserts that there are no positive solutions to the Diophantine equation

$$x^n + y^n = z^n \tag{1}$$

if $n > 2$. As is well-known, Wiles [7], with the assistance of Taylor [6], gave the first complete proof of FLT.

Given integers $\ell > m > 0$, we consider monic polynomials $X_n$, $Y_n$, and $Z_n$ with the property that $\rho$ is a zero of $X_n$ if and only if $(\rho, \rho + m, \rho + \ell)$ satisfies (1). It is shown, in a precise asymptotic sense, that for a vast majority of cases, these polynomials are irreducible via direct

application of Eisenstein's criterion (the irreducibility of these polynomials is equivalent to FLT). Although the results fall far short of a full proof of FLT – in fact, the possibility is left open that there are infinitely-many cases to consider – they are nevertheless appealing given that: (i) they are elementary in nature; (ii) they apply to all values of $n$ (including $n = 2$); and (iii) they apply to the well-known *first-case* and *second-case* of (1). We conclude by offering a Goldbach-type conjecture on powerful numbers.

# 2 The auxiliary polynomials

For fixed integers $\ell > m > 0$, let

$$X_n(t) = X_n(t,(\ell,m)) := t^n - \sum_{k=1}^{n} \binom{n}{k} t^{n-k}(\ell - m)Q_k(\ell,m), \tag{2}$$

$$Y_n(t) = Y_n(t,(\ell,m)) := t^n + \sum_{k=1}^{n} (-1)^k \binom{n}{k} t^{n-k}\ell Q_k(m,m-\ell), \tag{3}$$

and

$$Z_n(t) = Z_n(t,(\ell,m)) := t^n + \sum_{k=1}^{n} (-1)^k \binom{n}{k} t^{n-k}\left(\ell^k + (\ell - m)^k\right), \tag{4}$$

where

$$Q_k(\ell,m) := \frac{\ell^k - m^k}{\ell - m} = \sum_{i=0}^{k-1} \ell^{k-1-i}m^i,\ k = 1,\ldots,n. \tag{5}$$

**Proposition 2.1.** *If $\rho \in \mathbb{C}$, then $(\rho, \rho+m, \rho+\ell) \in \mathbb{C}^3$ satisfies* (1) *if and only if $X_n(\rho) = Y_n(\rho+m) = Z_n(\rho+\ell) = 0$.*

*Proof.* Following the binomial theorem, notice that

$$\begin{aligned}
&\rho^n + (\rho+m)^n = (\rho+\ell)^n \\
\Longleftrightarrow &\rho^n - \sum_{k=1}^{n} \binom{n}{k} \rho^{n-k}(\ell^k - m^k) = 0 \\
\Longleftrightarrow &\rho^n - \sum_{k=1}^{n} \binom{n}{k} \rho^{n-k}(\ell - m)Q_k(\ell,m) = 0 \\
\Longleftrightarrow &X_n(\rho) = 0.
\end{aligned}$$

If $\sigma := \rho + m$, then

$$\begin{aligned}
&(\sigma - m)^n + \sigma^n = (\sigma + (\ell - m))^n \\
\Longleftrightarrow &\sigma^n + \sum_{k=1}^{n} \binom{n}{k} \sigma^{n-k}\left((-m)^k - (\ell - m)^k\right) = 0 \\
\Longleftrightarrow &\sigma^n + \sum_{k=1}^{n} (-1)^k \binom{n}{k} \sigma^{n-k}\left(m^k - (-1)^k(\ell - m)^k\right) = 0
\end{aligned}$$

$$\begin{aligned}
&\iff \sigma^n + \sum_{k=1}^{n} (-1)^k \binom{n}{k} \sigma^{n-k} \left(m^k - (m-\ell)^k\right) = 0 \\
&\iff \sigma^n + \sum_{k=1}^{n} (-1)^k \binom{n}{k} \sigma^{n-k} \ell Q_k(m, m-\ell) \\
&\iff Y_n(\sigma) = Y_n(\rho + m) = 0.
\end{aligned}$$

If $\tau := \rho + \ell$, then

$$\begin{aligned}
&(\tau - \ell)^n + (\tau + (m-\ell))^n = \tau^n \\
&\iff \tau^n + \sum_{k=1}^{n} \binom{n}{k} \tau^{n-k} \left((-\ell)^k + (m-\ell)^k\right) = 0 \\
&\iff \tau^n + \sum_{k=1}^{n} (-1)^k \binom{n}{k} \tau^{n-k} \left(\ell^k + (-1)^k (m-\ell)^k\right) = 0 \\
&\iff \tau^n + \sum_{k=1}^{n} (-1)^k \binom{n}{k} \tau^{n-k} \left(\ell^k + (\ell - m)^k\right) = 0 \\
&\iff Z_n(\tau) = Z_n(\rho + \ell) = 0,
\end{aligned}$$

and the result is established. □

It is well-known that if $(x, y, z) \in \mathbb{N}^3$ satisfies (1), with $x < y < z$, $\gcd(x, y, z) = 1$, and $(\ell, m) := (z - x, y - x)$, then $\gcd(\ell, m) = 1$ [5, p 2]. Thus, there is no loss in generality in assuming that $\gcd(\ell, m) = 1$. Unless otherwise stated, it is assumed herein that $\gcd(\ell, m) = 1$.

Recall that a polynomial $f$ with coefficients from $\mathbb{Z}$ is called *reducible (over $\mathbb{Z}$)* if $f = gh$, where $g$ and $h$ are polynomials of positive degree with coefficients from $\mathbb{Z}$. If $f$ is not reducible, then $f$ is called *irreducible (over $\mathbb{Z}$)*.

**Proposition 2.2.** *The polynomials $X_n$, $Y_n$, and $Z_n$ are simultaneously irreducible or reducible.*

*Proof.* Following Proposition 2.1, notice that

$$\begin{aligned}
X_n(\rho - m) = 0 &\iff (\rho - m)^n + \rho^n = (\rho - m + \ell)^n \\
&\iff (\rho - m)^n + \rho^n = (\rho + \ell - m)^n \\
&\iff Y_n(\rho) = 0.
\end{aligned}$$

Thus,

$$X_n(t - m) = \prod_{\{\rho \in \mathbb{C} | Y_n(\rho) = 0\}} (t - \rho) = Y_n(t).$$

A similar argument demonstrates that $X_n(t - \ell) = Z_n(t)$. Thus, the polynomials $X_n$, $Y_n$, and $Z_n$ are simultaneously irreducible or reducible. □

Given

$$f(t) = t^n - \sum_{i=1}^{n} a_i t^{n-i} \in \mathbb{C}[t], \tag{6}$$

let

$$f_k(t) := t^k - \sum_{i=1}^{k} a_i t^{k-i},\ 0 \leq k \leq n, \tag{7}$$

where the sum on the right is defined to be zero whenever it is empty. Notice that $f = f_n$, $f(t) = tf_{n-1}(t) - a_n$, and $(f_j)_k = f_k$, $0 \leq k \leq j$.

**Lemma 2.3** (Remainder theorem)**.** *If $f$ is the polynomial defined in* (6)*, $f_k$ is the polynomial defined in* (7)*, and $r \in \mathbb{C}$, then*

$$f(t) = (t-r)\sum_{k=0}^{n-1} f_k(r)t^{n-1-k} + f(r).$$

*Proof.* Proceed by induction on $n$. If $n = 1$, then

$$f(t) = t - a_1 = t - r + r - a_1 = (t-r) + f(r),$$

and the base-case is established.

Assume that the result holds for every polynomial of degree $j$, where $j \geq 1$. If $f(t) = t^{j+1} - \sum_{i=1}^{j+1} a_i t^{j+1-i}$, and $r \in \mathbb{C}$, then

$$\begin{aligned}
f(t) &= tf_j(t) - a_{j+1} \\
&= t\left((t-r)\sum_{k=0}^{j-1}(f_j)_k(r)t^{j-1-k} + f_j(r)\right) - a_{j+1} \\
&= (t-r)\sum_{k=0}^{j-1} f_k(r)t^{j-k} + tf_j(r) - a_{j+1} \\
&= (t-r)\sum_{k=0}^{j-1} f_k(r)t^{j-k} + (t-r)f_j(r) + rf_j(r) - a_{j+1} \\
&= (t-r)\sum_{k=0}^{j} f_k(r)t^{j-k} + f(r),
\end{aligned}$$

establishing the result when $n = j + 1$. The entire result now follows by the principle of mathematical induction. □

If $f(t) = t^n - \sum_{i=1}^{n} a_i t^{n-i} \in \mathbb{Z}[t]$ and $r \in \mathbb{Z}$ is a zero, then, following Lemma 2.3,

$$f(t) = (t-r)\sum_{k=0}^{n-1} f_k(r)t^{n-1-k},$$

i.e., $f$ is reducible over $\mathbb{Z}$. The connection to FLT is now apparent.

**Corollary 2.3.1.** *If $(x, x+m, x+\ell) \in \mathbb{N}^3$ satisfies* (1)*, then $X_n$, $Y_n$, and $Z_n$ are reducible.*

# 3 Main results

Corollary 2.3.1 provides a direct method of proving FLT; indeed, if it can be shown that any of the polynomials $X_n$, $Y_n$, or $Z_n$ is irreducible, then there is no solution to (1) of the form $(x, x+m, x+\ell) \in \mathbb{N}^3$. The following result is a well-known irreducibility test (see, e.g., Prasolov [4, Theorem 2.1.3]) and follows from a result due to Schönemann (Cox [1]).

**Theorem 3.1** (Eisenstein's criterion [EC])**.** *Let $f(t) = \sum_{k=0}^{n} a_k t^{n-k} \in \mathbb{Z}[t]$. If there is a prime number $p$ such that: $p \nmid a_0$; $p \mid a_k$, $k = 1, \ldots, n$; and $p^2 \nmid a_n$, then $f$ is irreducible over $\mathbb{Z}$.*

The following result is well-known in the literature on FLT (see Ribenboim [5, (3B)(5), p. 81] and references therein).

**Lemma 3.2.** *Let $n > 1$ and $p$ be a prime. If $\gcd(\ell, m) = 1$, $p \nmid n$, and $p \mid (\ell - m)$, then $p \nmid Q_n(\ell, m)$.*

If $k$ is an integer and $p$ is a prime, then we say that $k$ is *singly divisible by* $p$, denoted by $p \,||\, k$, whenever $p \mid k$, but $p^2 \nmid k$. An integer that is singly divisible by two is called *singly even*.

**Theorem 3.3.** *Let $X_n$ be defined as in* (2)*. If there is a prime $p$ such that $p \,||\, \ell - m$ and $p \nmid n$, then $X_n$ is irreducible.*

*Proof.* Immediate in view of (2), Theorem 3.1, and Lemma 3.2. □

*Remark* 3.4. The import of Theorem 3.3 is amplified by the following observation: a positive integer $a$ is called *powerful* if $p^2$ divides $a$ for every prime $p$ that divides $a$; otherwise, it is called *nonpowerful*.

Golomb [2] proved that if $\kappa(t)$ denotes the number of powerful numbers in the interval $[1, t]$, then

$$ct^{1/2} - 3t^{1/3} \leq \kappa(t) \leq ct^{1/2}, \tag{8}$$

where $c := \zeta(3/2)/\zeta(3) \approx 2.1733$ and $\zeta$ denotes the Riemann zeta function. Consequently, the set of powerful numbers has *natural density* zero, i.e., $\kappa(n)/n \longrightarrow 0$ as $n \longrightarrow \infty$.

If

$$\Delta(t) := \{\delta = \ell - m \in \mathbb{N} \mid 1 \leq m < \ell \leq t,\ \delta \text{ powerful},\ \gcd(\ell, m) = 1\},$$

then $|\Delta(t)| = \kappa(t)$. Thus, $|\Delta(t)|/t \longrightarrow 0$ as $t \longrightarrow \infty$.

In case $\ell - m$ is powerful, we offer the following results.

**Theorem 3.5.** *Let $Y_n$ be defined as in* (3)*. If there is a prime $p$ such that $p \,||\, \ell$ and $p \nmid n$, then $Y_n$ is irreducible.*

*Proof.* Immediate in view of (3), Theorem 3.1, and Lemma 3.2. □

**Theorem 3.6.** *Let $Z_n$ be defined as in* (4)*. If $2\ell - m$ is singly even, then $Z_n$ is irreducible.*

*Proof.* If $2\ell - m$ is singly even, then $\ell$ is odd, $m$ is even, and there is an odd integer $q$ such that $2\ell - m = 2q$. As a consequence, $m = 2(\ell - q) \equiv 0 \pmod 4$. As $\ell$ and $\ell - m$ are odd, notice that

$$\left(\ell^k + (\ell - m)^k\right) \equiv 0 \pmod 2,\ k = 1, \ldots, n.$$

Moreover, since

$$\ell^n + (\ell - m)^n = 2\ell^n + \sum_{k=1}^{n} (-1)^k \binom{n}{k} \ell^{n-k} m^k$$

it follows that $(\ell^n + (\ell - m)^n) \equiv 2\ell^n \not\equiv 0 \pmod 4$, i.e., $Z_n$ is irreducible via EC with $p = 2$. □

**Example 3.7.** If $(\ell, m) = (9, 4)$, $n \geq 2$, $n \not\equiv 0 \pmod 5$, then $X_n$ is irreducible via EC with $p = 5$; otherwise, if $n \equiv 0 \pmod 5$, then $Z_n$ is irreducible via EC with $p = 2$ since $2(9) - 4 = 14$ is singly even.

**Example 3.8.** For a positive integer $n$, let $P(n) := \{(\ell, m) \in \mathbb{R}^2 \mid 0 \leq m < \ell \leq n,\ \gcd(\ell, m) = 1\}$. Figure 1 depicts the set $P(500)$.

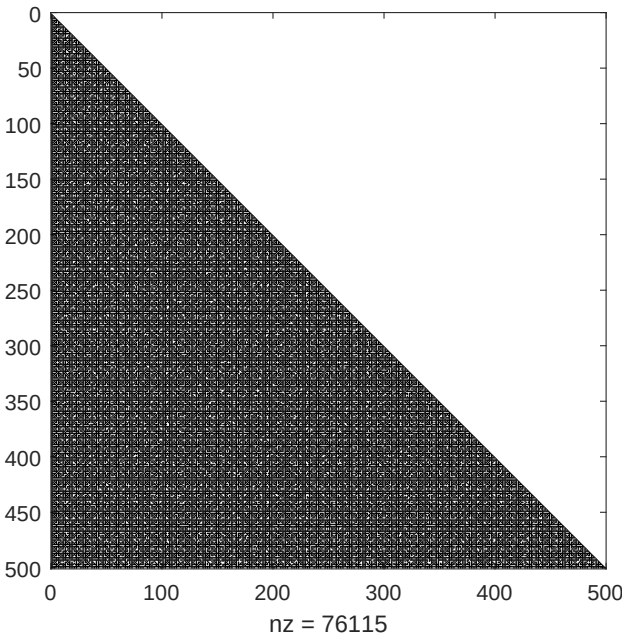


Figure 1. The set $P(500)$. Note that 'nz' stands for 'nonzero'.

Let $p$ be a prime less than 500. If $p \mid\mid \ell - m$, then $X_n$ is irreducible for every positive integer $n$ satisfying $n \geq 500$, i.e., there is no solution to $x^n + y^n = z^n$ of the form $(x, x + m, x + \ell) \in \mathbb{N}^3$. Figure 2 contains the remaining elements of $P(500)$ that can not be eliminated in this manner (i.e., following Theorem 3.3). Figure 3 contains all pairs that can not be eliminated from Theorems 3.3 and 3.5. Finally, Figure 4 contains all elements that can not be eliminated from Theorems 3.3, 3.5, and 3.6.

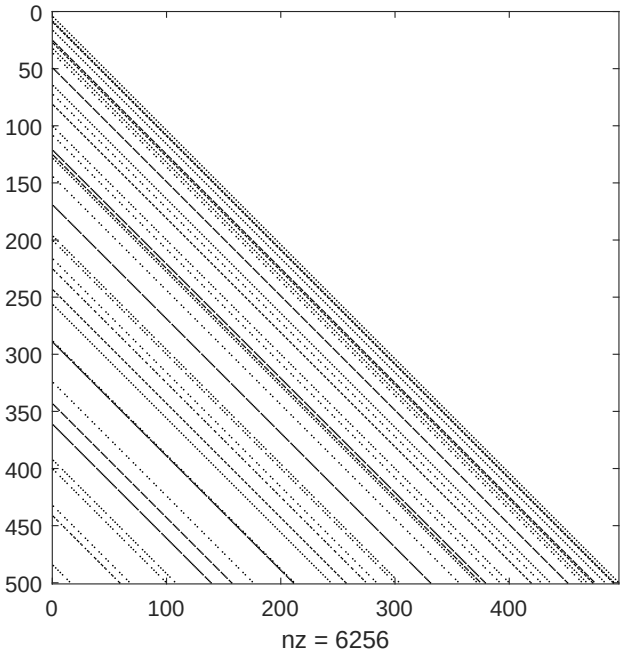


Figure 2. Remaining pairs after Theorem 3.3 applied.

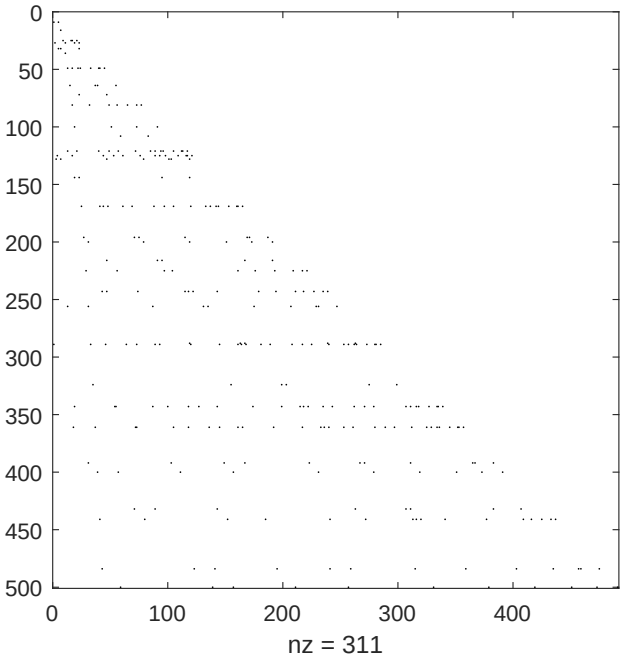


Figure 3. Remaining pairs after Theorems 3.3 and 3.5 are applied.

**Example 3.9.** If $(\ell, m) = (9, 5)$, then the irreducibility of the auxiliary polynomials cannot be asserted from the previous results.

As mentioned in the introduction, the above results leave the possibility that there are infinitely-many cases to resolve. The following conjecture, which generalizes Example 3.9, would not only establish this, but is seemingly of great import in and of itself [3].

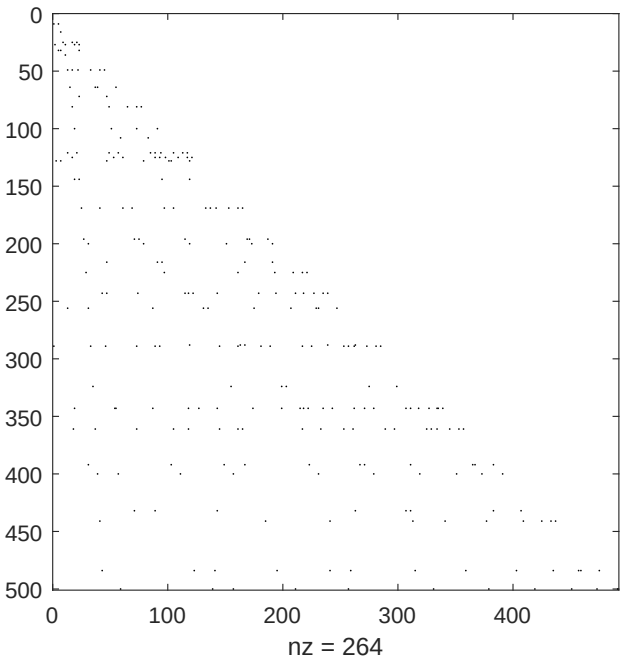


Figure 4. Remaining pairs after Theorems 3.3, 3.5, and 3.6 are applied.

**Conjecture 3.10.** If $a > 1$ is powerful, then there is a prime $p$ and a powerful number $b$ such that $a = b + p$.

# References

[1] Cox, D. A. (2011). Why Eisenstein proved the Eisenstein criterion and why Schönemann discovered it first [reprint of mr2572615]. *Amer. Math. Monthly*, 118(1), 3–21.

[2] Golomb, S. W. (1970). Powerful numbers. *Amer. Math. Monthly*, 77, 848–855.

[3] Paparella, P. Is every powerful number the sum of a powerful number and a prime? MathOverflow. Available online: `https://mathoverflow.net/q/269080` (version: 2017-05-07).

[4] Prasolov, V. V. (2010). *Polynomials Algorithms and Computation in Mathematics*, 11, Springer-Verlag, Berlin. Translated from the 2001 Russian second edition by Dimitry Leites, Paperback edition [of MR2082772].

[5] Ribenboim, P. (1999). *Fermat's last theorem for amateurs*. Springer-Verlag, New York.

[6] Taylor, R. & Wiles, A. (1995). Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, 141(3), 553–572.

[7] Wiles, A. (1995). Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3), 443–551.