Eisenstein's Criterion, Fermat's Last Theorem, and a Conjecture on Powerful Numbers

Pietro Paparella
Division of Engineering & Mathematics
University of Washington Bothell
18115 Campus Way NE
Bothell, WA 98011
USA
pietrop@uw.edu

Abstract

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

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 [8], with the assistance of Taylor [7], gave the first complete proof of FLT.

Given integers $\ell > m > 0$, we define monic polynomials X_n, Y_n, and Z_n (that depend on ℓ and m) with the property that μ is a zero of X_n if and only if $(\mu, \mu + m, \mu + \ell)$ 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. Although the results fall far short of constituting 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). A conjecture on powerful numbers is also offered.

2 The Auxiliary Polynomials

Given $\ell > m > 0$, 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

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

where

$$Q_k(\ell, m) := \frac{\ell^k - m^k}{\ell - m} = \sum_{i=0}^{k-1} \ell^{k-1-i} m^i, \; k = 1, \ldots, n. \tag{4}$$

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

Proof. Following the binomial theorem, notice that

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

If $\nu := \mu + m$, then

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

If $\xi := \mu + \ell$, then

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

and the result is established. □

It can be shown 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 $\gcd(\ell, m) = 1$ ([6, p 2]). Herein it is assumed 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. *The polynomials X_n, Y_n, and Z_n are simultaneously irreducible or reducible.*

Proof. Following Proposition 1, notice that

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

Thus,

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

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 a monic polynomial

$$f(t) = t^n - \sum_{i=1}^{n} a_i t^{n-i} \in \mathbb{C}[t], \tag{5}$$

let

$$f_k(t) := t^k - \sum_{i=1}^{k} a_i t^{k-i},\ 0 \le k \le n, \tag{6}$$

where the sum on the right is defined to be zero whenever it is empty. Notice that $f = f_n$ and $f(t) = t f_{n-1}(t) - a_n$.

Lemma 3. *If f is the polynomial defined in (5), f_k is the polynomial defined in (6), 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

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

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

Remark 4. 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 3,

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

i.e., f is reducible.

Corollary 5. *If $(x, x+m, x+\ell) \in \mathbb{N}^3$ satisfies (1), then the polynomials X_n, Y_n, and Z_n are reducible.*

3 Main Results

The following result is fundamental (see, e.g., [5, Theorem 2.1.3]) and follows from a result due to Schönemann (see, e.g., [1]).

Theorem 6 (Eisenstein's criterion)**.** *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:*

1. $p \nmid a_0$;
2. $p \mid a_k$, $k = 1, \ldots, n$; *and*
3. $p^2 \nmid a_n$,

then f *is irreducible over* $\mathbb{Z}$.

With f and p as in Theorem 6, let

$$\mathrm{Eis}(f,p) := \begin{cases} 1, & \text{(i), (ii), and (iii) are satisfied;} \\ 0, & \text{otherwise.} \end{cases}$$

The following result is well-known in the literature on FLT (see [6, (3B)(5), p. 81] and references therein). For definiteness, we include a proof that depends only on the definition of the polynomial Q in (4).

Lemma 7. *Let* $n > 1$ *and* p *be a prime. If* $\gcd(\ell, m) = 1$, $p \nmid n$, *and* $p \mid (\ell - m)$, *then* $p \nmid Q_n(\ell, m)$.

Proof. If $p \mid \ell - m$, then there is an integer j such that $\ell = m + pj$. Thus,

$$\begin{aligned} Q_n(\ell, m) &= \frac{(m+pj)^n - m^n}{pj} \\ &= \left(\sum_{k=0}^{n} \binom{n}{k} m^{n-k} p^k j^k - m^n \right) / pj \\ &= \sum_{k=1}^{n} \binom{n}{k} m^{n-k} p^{k-1} j^{k-1} \\ &= nm^{n-1} + \sum_{k=2}^{n} \binom{n}{k} m^{n-k} p^{k-1} j^{k-1} \\ &= nm^{n-1} + \sum_{k=1}^{n} \binom{n}{k+1} m^{n-k-1} p^k j^k, \end{aligned}$$

and $Q_n(\ell, m) \equiv (nm^{n-1}) \not\equiv 0 \pmod{p}$. ☐

Theorem 8. *If* X_n *is defined as in* (2) *and there is a prime* p *such that* $p \mid \ell - m$, $p^2 \nmid \ell - m$, *and* $p \nmid n$, *then* X_n *is irreducible.*

Proof. Immediate in view of (2), Theorem 6, and Lemma 7. ☐

Remark 9. The import of Theorem 8 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 (sequence A001694 in the On-Line Encyclopedia of Integer Sequences (OEIS) [4]). Otherwise, it is called *non-powerful*.

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

$$ct^{1/2} - 3t^{1/3} \leq \kappa(t) \leq ct^{1/2}, \tag{7}$$

where $c := \zeta(3/2)/\zeta(3) \approx 2.1733$ and ζ denotes the Riemann zeta function (an improvement of (7) can be found in [3]). Consequently, $\kappa(t)/t \longrightarrow 0$ as $t \longrightarrow \infty$.

If

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

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 10. *If there is a prime p such that $p \mid \ell$, $p^2 \nmid \ell$, and $p \nmid n$, then Y_n irreducible.*

Proof. Immediate in view of (3), Theorem 6, and Lemma 7. □

Theorem 11. *If $2\ell - m$ is singly even, then Z_n is irreducible.*

Proof. If $2\ell - m$ is singly even, then ℓ 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 ℓ and $\ell - m$ are odd, notice that

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

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., $\mathrm{Eis}(Z_n, 2) = 1$. □

Example 12. If $(\ell, m) = (9, 4)$, $n \geq 2$, $n \not\equiv 0 \pmod 5$, then $\mathrm{Eis}(X_n, 5) = 1$; and if $n \equiv 0 \pmod 5$, then $\mathrm{Eis}(Z_n, 2) = 1$ since $2(9) - 4 = 14$ is singly even.

Example 13. 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 13 and is related to sequence A133364 of the OEIS [4], would not only establish this, but seems to be more important in its own right.

Conjecture 14. If $a > 1$ is powerful, then there is a prime p and a powerful number b such that a=b+p.

4 Acknowledgements

I would like to thank Ioana Dumitriu, Jennifer McLoud-Mann, Casey Mann, and Steven J. Miller for their generosity.

References

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

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

[3] G. Mincu and L. Panaitopol, More about powerful numbers, *Bull. Math. Soc. Sci. Math. Roumanie (N.S.)* **52(100)**(4) (2009), 451–460.

[4] The OEIS Foundation Inc., *The On-Line Encyclopedia of Integer Sequences*, http://oeis.org.

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

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

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

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

2010 *Mathematics Subject Classification*: Primary 11D41; Secondary 11A05, 11C08, 11P32.
Keywords: Fermat's last theorem, Eisenstein's criterion, powerful number

---

(Concerned with sequences A001694, A133364.)

Return to Journal of Integer Sequences home page.