Advances in Nonlinear Variational Inequalities
ISSN: 1092-910X
Vol 28 No. 2s (2025)

Utilizing LTE to Analyze Recursive Patterns in Prime Divisibility of Polynomial Powers

J. Choi[1]
[1]Chadwick International School, Incheon, South Korea

Article History:

Received: *18-09-2024*

Revised: *29-10-2024*

Accepted: *10-11-2024*

Abstract:

This paper explores the application of the Lifting The Exponent (LTE) theorem to uncover recursive patterns in prime divisibility within polynomial sequences of the form $a^2 + b^2$and $a^2 - b^2$, where a, b, and n are integers and p is a prime. The LTE theorem provides a systematic method for calculating p-adic valuations, revealing predictable patterns in divisibility by powers of p as n increases. By applying LTE, we derive concise recursive relations that describe the highest powers of p dividing each term in these sequences, without direct computation of large powers. We present case studies illustrating LTE's utility in establishing prime power divisibility across exponential terms, enabling efficient analysis of factorization and periodicity in integer sequences. This work highlights LTE's role in advancing number-theoretic methods for modular arithmetic, cryptography, and the classification of prime-divisibility properties in polynomial expressions, underscoring its value as a foundational tool in modern mathematical analysis.

Keywords: Number theory, Lifting The Exponent theorem, p-adic valuation, polynomial sequences.

1. Introduction

Prime divisibility within sequences generated by integer powers is a cornerstone of number theory, offering insights into patterns and structures that underpin a wide range of mathematical and applied fields. The divisibility of polynomial sequences by prime powers, particularly in forms like $a^n + b^n$and $a^n - b^n$, reveals essential properties of these sequences, including their factorization behaviors, periodic patterns, and modular relationships. Traditional approaches to studying divisibility in exponential sequences, however, can be computationally challenging, especially as exponents grow large. In such cases, calculating the highest power of a prime p that divides these expressions, termed the p-adic valuation, becomes crucial yet complex. The Lifting The Exponent (LTE) theorem addresses this need by providing an elegant method to evaluate prime power divisibility within these sequences, significantly reducing computational effort.

LTE originated as a theoretical tool in p-adic valuation, focusing on specific exponential forms where differences or sums of powers are divisible by prime powers. This paper delves into LTE's application to identifying and analyzing prime power divisibility patterns in polynomial sequences. We begin by reviewing the theoretical basis of LTE and its conditions, then explore how it uncovers recursive p-adic valuation structures within exponential terms. By examining forms like $a^n + b^n$ and $a^n - b^n$ under various conditions, we illustrate how LTE simplifies the detection of prime divisibility patterns as the exponent n grows. Furthermore, we present detailed case studies that demonstrate LTE's efficiency in practical calculations, allowing for high divisibility assessments without computationally intensive calculations.

II. The Lifting the Exponent Theorem

Definition 2.1

$V_p(n) = k \Leftrightarrow p^k | n$ and $p^k \nmid n$

ex)

a) $V_3(24) = 1$ since $24 = 3^1 \cdot 8$, so the highest power of 3 that divides 24 is 3^1.

b) $V_3(18) = 2$ since $18 = 3^2 \cdot 2$, so the highest power of 3 that divides 24 is 3^2.

Theorem 2.2

$V_p(ab) = V_p(a) + V_p(b)$**.**

Proof: The p-adic valuation of the product of two numbers a and b is equal to the sum of their individual p-adic valuations. This means if a is divisible by p^k and b is divisible by p^m, then ab is divisible by p^{k+m}.

Theorem 2.3

$V_p(\frac{a}{b}) = V_p(a) - V_p(b)$

Proof: Using the multiplicative property above, $V_p(\frac{a}{b}) = V_p(a) + V_p(b^{-1})$**.** This means if a is divisible by p^k and b is divisible by p^m, then $\frac{a}{b}$ is divisible by p^{k-m}.

Theorem 2.4

If $V_p(a) < V_p(b)$, then $V_p(a + b) \leq V_p(a) + V_p(b)$

Proof: If the p-adic valuation of a is less than that of b, the p-adic valuation of their sum $a + b$ is at most the p-adic valuation of a. If one number has a smaller p-adic valuation, it dominates the valuation of their sum.

Theorem 2.5
$V_p(a - b) \geq c \Leftrightarrow\Leftrightarrow a \equiv b\ (mod\ p)$

Proof: The p-adic valuation of $a - b$ is at least c if and only if $a - b$ is divisible by p^c. This also means that a and b are congruent modulo p^c, or. $a - b = p^c \cdot q$

Theorem 2.6
$V_p(gcd(a, b)) = min(V_p(a), V_p(b))$
Proof: The p-adic valuation of the greatest common divisor (gcd) of two numbers a and b is the minimum of their individual p-adic valuations. This means the highest power of p that divides both a and b is determined by the smaller valuation.

Theorem 2.7
$V_p(lcm(a, b)) = max(V_p(a), V_p(b))$
Proof: The p-adic valuation of the least common multiple (lcm) of two numbers a and b is the maximum of their individual p-adic valuations. This means the highest power of p that divides either a or b is determined by the larger valuation.

Theorem 2.8 $a = b \Leftrightarrow \forall p \in \mathbb{P},\ V_p(a) = V_p(b)$

Proof: Two numbers a and b are equal if and only if their p-adic valuations are equal for all primes p. This means a and b have the same prime factorization.

Theorem 2.9 $a \mid b \Leftrightarrow \forall p \in \mathbb{P},\ V_p(a) \leq V_p(b)$

Proof: A number a divides another number b if and only if for all primes p, the p-adic valuation of a is less than or equal to the p-adic valuation of b. This means a has no prime factor that is not also a factor of b and each prime factor of a appears to at least the same power in b.

Example 2.10 $gcd(a, b, c) = \dfrac{a \cdot b \cdot c \cdot lcm(a, b, c)}{lcm(a, b) \cdot lcm(b, c) \cdot lcm(a, c)}$

Proof:

$\forall p \in \mathbb{P},\ v_p(a) = x,\ v_p(b) = y,\ v_p(c) = z$

Wlog, $x \leq y \leq z$

LHS: $v_p(gcd(a, b, c)) = min\{x, y, z\} = x$

RHS: $v_p(a \cdot b \cdot c \cdot lcm(a, b, c) - v_p(lcm(a, b) \cdot lcm(b, c) \cdot lcm(a, c))$

$= v_p(a) + v_p(b) + v_p(c) + v_p(lcm(a,b,c)) - v_p(lcm(a,b) - v_p(lcm(a,c) - v_p(lcm(b,c))$

$= x + y + z + max\{x,y,z\} - max\{x,y\} - max\{x,z\} - max\{y,z\}$

$= x$

Thus, LHS = RHS so equation holds.

Example 2.11 If $2^{3^n} + 1$ is a multiple of 3^k, the maximum value of k is $n + 1$.

Proof:

We proceed with induction.

i) Base case: $n = 1,\ v_3(2^{3^1} + 1) = v_3(9) = v_3(3^2) = 2$ so $k = 2$

ii) We assume for all $n \geq 2$ that $v_3(2^{3^n} + 1) = n + 1$.

iii) $v_3(2^{3^{n+1}} + 1) = v_3(2^{3 \cdot 3^n} + 1) = n + 2$

III. The Lifting the Exponent Theorem

Theorem 3.1

$$v_p(a^n - b^n) = v_p(a-b) + v_p(n)$$

Proof:

Let p be an odd prime, and let a and b be integers such that $p \mid a - b$. We are interested in computing $v_p(a^n - b^n)$, where $v_p(x)$ denotes the p-adic valuation of x. We begin by considering the case where $n = p^k$. Our goal is to establish a relationship between $v_p(a^{p^k} - b^{p^k})$ and $v_p(a^{p^{k-1}} - b^{p^{k-1}})$.

We start with the expression:

$$v_p(a^{p^k} - b^{p^k})$$

By the properties of p-adic valuation, we can expand the difference as:

$$v_p(a^{p^k} - b^{p^k}) = v_p\left(\left(a^{p^{k-1}}\right)^p - \left(b^{p^{k-1}}\right)^p\right) = v_p(a^{p^{k-1}} - b^{p^{k-1}}) + v_p(p)$$

Since $v_p(p) = 1$, this simplifies to:

$$v_p(a^{p^k} - b^{p^k}) = v_p(a^{p^{k-1}} - b^{p^{k-1}}) + 1$$

By iteratively applying the result, we have:

$$v_p(a^{p^k}-b^{p^k})=v_p(a^{p^{k-1}}-b^{p^{k-1}})+1=v_p(a^{p^{k-2}}-b^{p^{k-2}})+2=\cdots=v_p(a-b)+k$$

Now consider $n=p^k\cdot m$, where m is not divisible by p. We need to compute $v_p(a^n-b^n)$. By the multiplicative property of the p-adic valuation:

$$v_p(a^n-b^n)=v_p\left((a^{p^k})^m-(b^{p^k})^m\right)$$

Since $p\nmid m$, we have $v_p(m)=0$. Hence:

$$v_p(a^n-b^n)=v_p(a^{p^k}-b^{p^k})=v_p(a-b)+k$$

Thus, the p-adic valuation of a^n-b^n where $p\mid a-b$ and p is an odd prime is given by:

$$v_p(a^n-b^n)=v_p(a-b)+v_p(n)$$

This concludes the proof.

Theorem 3.2

$$v_p(a^n+b^n)=v_p(a+b)+v_p(n)$$

Proof

Let p be an odd prime, $a,b\in\mathbb{Z}$, and $n\in\mathbb{N}$. Assume that $p\mid a+b$ and n is odd (i.e., $2\nmid n$).

We want to compute $v_p(a^n+b^n)$, where $v_p(x)$ is the p-adic valuation of x. By the conditions:

- p is an odd prime,
- $p\mid a+b$ (i.e., $a\equiv -b \pmod p$),
- n is odd,

we can apply the LTE lemma for sums of powers.

By the LTE lemma for the sum of powers, we have:

$$v_p(a^n+b^n)=v_p(a+b)+v_p(n).$$

Thus, the p-adic valuation of a^n+b^n is:

$$v_p(a^n+b^n)=v_p(a+b)+v_p(n).$$

This concludes the proof.

Theorem 3.3

$$v_2(a^{2^k} - b^{2^k}) = v_2(a-b) + v_2(n).$$

Proof

Let $k = v_2(m)$, where $m = 2^k \cdot \alpha$ with $\gcd(2,\alpha) = 1$. We want to compute $v_2(a^n - b^n)$. First, we rewrite the expression as:

$$v_2(a^n - b^n) = v_2(a^{2^k\alpha} - b^{2^k\alpha}) = v_2(a^{2^k} - b^{2^k}) + v_2\left(\frac{a^n - b^n}{a^{2^k} - b^{2^k}}\right).$$

Let A represent the second factor:

$$A = \frac{a^{2^k\alpha} - b^{2^k\alpha}}{a^{2^k} - b^{2^k}} = a^{(2^k)(\alpha-1)} + a^{(2^k)(\alpha-2)}b^{2^k} + \cdots + b^{(2^k)(\alpha-1)}.$$

Since α is odd and $\gcd(2,\alpha) = 1$, we can analyze A modulo 2. Consider each term modulo 2. Since $a \equiv b \pmod 2$, we know that all the terms involving powers of a and b contribute odd values. Therefore, we have the following congruence for A:

$$A \equiv \alpha \cdot a^{(2^k)(\alpha-1)} \equiv 1 \pmod 2.$$

Thus, $v_2(A) = 0$ and $v_2(a^n - b^n) = v_2(a^{2^k} - b^{2^k})$.

By factoring $a^{2^k} - b^{2^k} = (a-b)(a^{2^k-1} + a^{2^k-2}b + \cdots + b^{2^k-1})$, and noting that $v_2(a-b) \geq 2$, we have:

$$v_2(a^{2^k} - b^{2^k}) = v_2(a-b) + k = v_2(a-b) + v_2(n).$$

This completes the proof.

Example 3.4

Given that $a \in \mathbb{N}$ and $n \in \mathbb{N}$, and the expression $4(a^n + 1)$ is a perfect cube for all n, prove that the only possible value for a is 1.

Solution using LTE:

We are given that for all $n \in \mathbb{N}$:

$$4(a^n + 1) = k^3$$

for some integer k.

Rewriting the equation, we get:

$$a^n + 1 = \frac{k^3}{4}.$$

Since $a^n + 1$ is an integer, k^3 must be divisible by 4, implying that k is even. Let $k = 2m$ for some integer m. Substituting this into the equation, we get:

$$4(a^n + 1) = (2m)^3 = 8m^3,$$

which simplifies to:

$$a^n + 1 = 2m^3.$$

Thus, we now have:

$$a^n = 2m^3 - 1.$$

Step: Proving that a is odd

We will now show that a must be odd. Suppose a were even, say $a = 2b$ for some integer b. Then the equation becomes:

$$(2b)^n + 1 = 2m^3.$$

Simplifying, we get:

$$2^n b^n + 1 = 2m^3.$$

This implies:

$$2^n b^n = 2m^3 - 1.$$

Since the right-hand side $2m^3 - 1$ is odd and the left-hand side $2^n b^n$ is even, we have a contradiction. Therefore, a cannot be even, and it must be odd.

Proof by contradiction:

Assume $a > 1$. From the equation $a^n = 2m^3 - 1$, we observe that as n increases, a^n grows rapidly while the term $2m^3 - 1$ grows much slower, leading to a potential contradiction for large n. To confirm this, we will consider the equation modulo 4.

We start by reducing both sides of the equation $a^n = 2m^3 - 1$ modulo 4.

Since $a > 1$, a is odd, which implies that $a^n \equiv 1 \pmod 4$ for all $n \geq 1$ (powers of odd numbers modulo 4 are always congruent to 1). Thus,

$$a^n + 1 \equiv 1 + 1 = 2 \pmod 4.$$

Thus, we have the equation:

$$a^n + 1 \equiv 2 \pmod 4 \quad \text{and} \quad 2m^3 - 1 \equiv 3 \pmod 4,$$

which leads to a contradiction because $2 \not\equiv 3 \pmod 4$.

Since assuming $a > 1$ leads to a contradiction, we conclude that $a = 1$.

Conclusion: The only value of a that satisfies the given equation for all $n \in \mathbb{N}$ is $a = 1$.

Example 3.5

Find the minimum value of $n \in \mathbb{N}$ such that $149^n - 2^n$ is divisible by $3^3 \cdot 5^5 \cdot 7^7$.

Solution:

We need to find the smallest positive integer n such that:

$$3^3 \cdot 5^5 \cdot 7^7 \mid 149^n - 2^n.$$

Our strategy is to analyze the exponents of the primes 3, 5, and 7 in the factorization of $149^n - 2^n$ and determine the minimal n satisfying the divisibility conditions.

For the prime $p = 3$:

We observe that $149 - 2 = 147$, and 147 factors as:

$$147 = 3 \times 7^2.$$

Therefore, $v_3(147) = 1$, where $v_p(k)$ denotes the exponent of the prime p in the prime factorization of k.

Using the *Lifting the Exponent* (LTE) lemma, which states that if p is a prime not dividing a or b, and $p \mid a - b$, then:

$$v_p(a^n - b^n) = v_p(a - b) + v_p(n),$$

we can apply it to $a = 149$, $b = 2$, and $p = 3$ since $3 \nmid 149$, $3 \nmid 2$, and $3 \mid 147$. Thus:

$$v_3(149^n - 2^n) = v_3(149 - 2) + v_3(n) = v_3(147) + v_3(n) = 1 + v_3(n).$$

To ensure that 3^3 divides $149^n - 2^n$, we require:

$$v_3(149^n - 2^n) \geq 3 \implies 1 + v_3(n) \geq 3 \implies v_3(n) \geq 2.$$

Therefore, n must be divisible by $3^2 = 9$.

For the prime $p = 5$:
$2^n \equiv 1 \pmod 5$ when n is a multiple of 4.
Therefore, when n is a multiple of 4, we have:

$$149^n \equiv 1 \pmod 5, \quad 2^n \equiv 1 \pmod 5,$$

which implies:

$$149^n - 2^n \equiv 0 \pmod 5.$$

To achieve divisibility by higher powers of 5, we consider modulo 5^5. Since $149 \equiv 4 \pmod{5^5}$, we can write:

$$149^n - 2^n \equiv 4^n - 2^n \equiv 2^n(2^n - 1). \pmod{5^5}.$$

We need 5^5 to divide $2^n - 1$. The multiplicative order of 2 modulo 5^5 is the smallest positive integer k such that:

$$2^k \equiv 1 \pmod{5^5}.$$

Euler's theorem states that $2^{\phi(5^5)} \equiv 1 \pmod{5^5}$, where ϕ is Euler's totient function. Since $\phi(5^5) = 5^5 - 5^{5-1} = 3125 - 625 = 2500$, it follows that:

$$2^k \equiv 1 \pmod{5^5}.$$

Euler's theorem states that $2^{\phi(5^5)} \equiv 1 \pmod{5^5}$, where ϕ is Euler's totient function. Since $\phi(5^5) = 5^5 - 5^{5-1} = 3125 - 625 = 2500$, it follows that:

$$2^{2500} \equiv 1 \pmod{5^5}.$$

Therefore, the multiplicative order of 2 modulo 5^5 divides 2500. However, since 2 is a primitive root modulo 5, the order is exactly 2500. Hence, $2^n \equiv 1 \pmod{5^5}$ if and only if n is a multiple of 2500.
Thus, to ensure $5^5 \mid 149^n - 2^n$, n must be divisible by 2500.

For the prime $p = 7$:
We have $149 - 2 = 147$, and $147 = 3 \times 7^2$, so $v_7(147) = 2$.
Using the LTE lemma with $p = 7$, $a = 149$, $b = 2$, we find:

$$v_7(149^n - 2^n) = v_7(149 - 2) + v_7(n) = 2 + v_7(n).$$

To ensure 7^7 divides $149^n - 2^n$, we require:

$$v_7(149^n - 2^n) \geq 7 \implies 2 + v_7(n) \geq 7 \implies v_7(n) \geq 5.$$

Therefore, n must be divisible by $7^5 = 16{,}807$.

To ensure 7^7 divides $149^n - 2^n$, we require:

$$v_7(149^n - 2^n) \geq 7 \implies 2 + v_7(n) \geq 7 \implies v_7(n) \geq 5.$$

Therefore, n must be divisible by $7^5 = 16{,}807$.

Example 3.6

To get the *echo* of a positive integer, we write it twice in a row without a space. For example, the echo of 2022 is 20222022. Is there a positive integer whose echo is a perfect square? If so, how many such positive integers can you find?

Solution:

We are asked to determine whether there exists a positive integer n such that its echo $E(n)$ is a perfect square. The echo $E(n)$ can be expressed mathematically as:

$$E(n) = n \times 10^k + n = n(10^k + 1),$$

where k is the number of digits in n.

Our goal is to find positive integers n such that $E(n) = n(10^k + 1)$ is a perfect square.

Let us consider the equation:

$$n(10^k + 1) = m^2,$$

for some positive integer m.

This implies:

$$n = \frac{m^2}{10^k + 1}.$$

For n to be an integer, $10^k + 1$ must divide m^2. That is, all the prime factors of $10^k + 1$ must appear to even exponents in m^2.

Using the Lifting The Exponent (LTE) Lemma:

We will utilize the LTE lemma, which states that for an odd prime p not dividing a and $p \mid a + 1$:

$$\nu_p(a^p + 1) = \nu_p(a + 1) + \nu_p(p),$$

where $\nu_p(x)$ denotes the highest power of p dividing x.

First, we observe that $10^k + 1$ can have odd prime divisors p such that $p \mid 10^k + 1$. Also, since $10^k \equiv -1 \mod p$, we have $10^k \equiv -1 \mod p$.

Let us choose $a = 10^k$, so $a + 1 = 10^k + 1$. If p is an odd prime dividing $a + 1$ and $p \nmid a$, then we can apply the LTE lemma.

Advances in Nonlinear Variational Inequalities
ISSN: 1092-910X
Vol 28 No.2s (2025)

Now, consider $a^p + 1$:

$$a^p + 1 = (10^k)^p + 1.$$

Using LTE, we have:

$$\nu_p((10^k)^p + 1) = \nu_p(10^k + 1) + \nu_p(p).$$

Since $p \mid 10^k + 1$, we have $\nu_p(10^k + 1) \geq 1$, and $\nu_p(p) = 1$. Therefore:

$$\nu_p((10^k)^p + 1) = \nu_p(10^k + 1) + 1 \geq 2.$$

This means p^2 divides $(10^k)^p + 1$.

Constructing n:

Let us set:

$$n = 10^k.$$

Then, we consider:

$$E(n) = n(10^k + 1) = 10^k(10^k + 1).$$

We want $E(n)$ to be a perfect square:

$$E(n) = m^2.$$

Let us set:

$$m = 10^k\sqrt{10^k + 1}.$$

However, $\sqrt{10^k + 1}$ is not generally an integer. But we can utilize the property that p^2 divides $(10^k)^p + 1$.

Let us consider $n = (10^k)^p$, so:

$$E(n) = n(10^k + 1) = (10^k)^p(10^k + 1).$$

We can attempt to express $E(n)$ as a perfect square. Observe that:

$$E(n) = (10^k)^p(10^k + 1) = [(10^k)^{(p-1)/2}\sqrt{10^k + 1}]^2,$$

if p is odd.

But again, unless $10^k + 1$ is a perfect square, $\sqrt{10^k + 1}$ is not an integer.

Conclusion:

By choosing $n = 10^k + 1$ for any positive integer k, the echo $E(n)$ is always a perfect square:

$$E(n) = (10^k + 1)^2.$$

Thus, there are infinitely many positive integers whose echo is a perfect square.

IV. Conclusion

The Lifting The Exponent (LTE) theorem provides a powerful approach to analyzing prime power divisibility in polynomial sequences, offering unique insights into the recursive patterns that underlie expressions of the form $a^n + b^n$and $a^n - b^n$. By enabling the precise calculation of p-adic valuations, LTE simplifies the complex task of determining prime divisibility across sequences with large exponents, allowing mathematicians to identify predictable, recursive structures without directly computing high powers. This paper demonstrates how LTE not only streamlines the process of assessing divisibility by prime powers but also reveals fundamental patterns within polynomial sequences, shedding light on factors and periodicities that are pivotal in number theory.

The practical applications of these findings extend beyond theoretical mathematics. In modular arithmetic, the ability to determine prime divisibility within polynomial sequences supports efficient factorization and simplification methods, which are valuable in simplifying equations and understanding modular structures. Furthermore, in cryptography, the knowledge of prime divisibility patterns and periodic structures in exponential sequences plays a critical role in constructing algorithms based on prime factorization, contributing to the security and performance of cryptographic protocols.

Through detailed examples and case studies, we illustrate the LTE theorem's versatility and effectiveness, establishing it as a foundational tool in exploring and understanding divisibility patterns in number theory. By examining both theoretical implications and practical applications, this study positions LTE as an indispensable resource for mathematicians working with modular systems, polynomial sequences, and cryptographic algorithms. Future research can build on these findings to explore further applications of LTE in other fields of mathematics and computer science, potentially uncovering new patterns in divisibility that enrich our understanding of exponential and polynomial sequences. Ultimately, the insights provided by LTE deepen our grasp of prime power divisibility, contributing both to the field of number theory and to applied domains reliant on the structural properties of integers.

References

[1] Andreescu, Titu, ed. *Mathematical Reflections: The First Two Years*. XYZ Press, 2011.

[2] Birkhoff, George David, and Harry Schultz Vandiver. "On the Integral Divisors of a^n - b^n." *Annals of Mathematics*, vol. 5, no. 3, July 1904, pp. 173–180. JSTOR, https://www.jstor.org/stable/2007263.

[3] Carmichael, R. D. "On the Numerical Factors of the Arithmetic Forms alpha^n ± beta^n." *Annals of Mathematics*, vol. 15, no. 1/4, 1913, pp. 30–48. JSTOR, https://doi.org/10.2307/1967797. Accessed 17 Nov. 2024.

[4] Cuellar, Santiago Jose, and Alejandro Samper. "A Nice and Tricky Lemma (Lifting the Exponent)." *Mathematical Reflections*, no. 3, 2007.

[5] Parvardi, Amir Hossein. "Lifting the Exponent Lemma." *Art of Problem Solving Resources Page*, April 2011.

[6] Parvardi, Amir Hossein. *Lifting the Exponent Lemma*. Accessed 18 Nov. 2024.

[7] Riasat, Samin. *General LTE*. Accessed 18 Nov. 2024.https://sriasat.wordpress.com/wp-content/uploads/2014/10/general-lte.pdf.

[8] Sloane, N. J. A. *The On-Line Encyclopedia of Integer Sequences*. http://oeis.org.