LTE and FLT

Jay Y.J

April 2025

1 Abstract

We present a generalization of the well-known Lemma of Lifting the Exponent (LTE), introducing a novel valuation function. Using this framework, we outline a new approach to Fermat's Last Theorem that relies solely on elementary number theory techniques.

2 Introduction

Consider the function $\nu_k(x)$**[1]** where $\nu_k(x)$ is the p-adic valuation function that shows how many ks can be divided into x. In other words, if $x = k^a b$ where kx, then $\nu_k(x) = \nu_k(k^a b) = a$. Let us examine this function by entering the expression $(a+b)^n - b^n$ inside $\nu_p(x)$ where p is a prime number greater than 2 and $p|a$, pb, and n is a natural number. We will prove the following theorem;

LTE(Lifting the Exponent Lemma) [2]

$$\nu_p((a+b)^n - b^n) = \nu_p(an)$$

Proof of LTE Using the binomial theorem, we can say that the ith term of $(a+b)^n$ is $\frac{n!}{(n-i)!i!} \cdot a^i b^{n-i}$.
We have to prove that $\nu_p(an) < \nu_p(\frac{n!}{(n-i)!i!} \cdot a^i b^{n-i})$ for all i such that $2 \leq i \leq n-1$ as $\nu_p(nab^{n-1}) = \nu_p(na)$ and nab^{n-1} is the first term of $(a+b)^n - b^n$.
Because pb, it can be rewritten as $\nu_p(an) < \nu_p(\frac{n!}{(n-i)!i!} \cdot a^i)$, which can be rewritten as $\nu_p((n-i)!i!) < \nu_p((n-1)! \cdot a^{i-1})$, which is equivalent to $\nu_p((n-i)!) + \nu_p(i!) < \nu_p((n-1)!) + \nu_p(a^{i-1})$ as $\nu_p(\alpha\beta) = \nu_p(\alpha) + \nu_p(\beta)$.
Because $2 \leq i \leq n-1$, $\nu_p((n-i)!) \leq \nu_p((n-1)!)$. Also, $\nu_p(i!) \leq \nu_p(a^{i-1})$ because of Legendre's Formula**[3]** and $\nu_p(a^{n-1}) = (n-1)\nu_p(a) \geq n-1$,

$$\nu_p(i!) = \lfloor \frac{i}{p} \rfloor + \lfloor \frac{i}{p^2} \rfloor + \lfloor \frac{i}{p^3} \rfloor + ... < \lfloor \frac{i}{2} \rfloor + \lfloor \frac{i}{2^2} \rfloor + \lfloor \frac{i}{2^3} \rfloor ... \leq i-1 \leq \nu_p(a^{i-1})$$

where $\lfloor x \rfloor$ is the *floor function*, showing the integer part of x(this logic works for every i except 3, when $\lfloor \frac{i}{p} \rfloor + \lfloor \frac{i}{p^2} \rfloor + \lfloor \frac{i}{p^3} \rfloor + ... = \lfloor \frac{i}{2} \rfloor + \lfloor \frac{i}{2^2} \rfloor + \lfloor \frac{i}{2^3} \rfloor ....$

Inequality $\nu_p((n-i)!) + \nu_p(i!) < \nu_p((n-1)!) + \nu_p(a^{i-1})$ still works because $\nu_p((n-i)!) < \nu_p((n-1)!)$.
Thus, we have proven Theorem 0.1. The same can be proved when $p = 2$ and $4|a$ because the proof is same except the part

$$\nu_p(i!) = \lfloor \frac{i}{2} \rfloor + \lfloor \frac{i}{2^2} \rfloor + \lfloor \frac{i}{2^3} \rfloor ... < 2i - 2 \leq \nu_p(a^{i-1})$$

Generalization Also, we can improve our Theorem 0.1 by removing the condition $p \nmid b$ by solving $\nu_p(k^n((a+b)^n - b^n)) = \nu_p((ak+bk)^n - b^n k^n))$, which is $\nu_p((a+b)^n - b^n) + \nu_p(k^n) = \nu_p(k \cdot an) + (n-1)\nu_p(k)$ where k may or may not be divisible by p. Because of this, ka and kb can be any number under condition $\nu_p(a) > \nu_p(b)$. Restating Theorem 0.1 by this, we know that the following statement is true;

Theorem 1.0

$$\nu_p((a+b)^n - b^n) = \nu_p(a) + (n-1)\nu_p(b) + \nu_p(n) = \nu_p(nab^{n-1})$$

where $\nu_p(a) > \nu_p(b)$ when p is a prime above 2, and $\nu_p(a) > \nu_p(b) + 1$ when p=2.

3 Application and examples

Theorem 2.0 $a^n + b^n = c^n$ The theorem is that there are no natural numbers a, b, c such that $a^n + b^n = c^n$ where n is a natural number greater than two.

Proof of Theorem 2.0 Assume that there is a a, b, c, n such that $a^n + b^n = c^n$. Then we can also assume that there is a a, b, c, n such that $\gcd(a, b, c) = 1$, which has the simplest form. We can say that $\gcd(a, b) = \gcd(b, c) = \gcd(c, a) = 1$ because if two of the three had a common divisor k such that $a = a'k, b = b'k, k > 1$, then $a^n + b^n = a'^n k^n + b'^n k^n = k^n(a'^n + b'^n) = c^n$, and thus c also having k as a factor, contradicting the statement that $\gcd(a, b, c) = 1$. Therefore, a, b, c are all co-prime to each other. Also, we only have to prove that n is 4 or a prime number because equations with greater ns can be expressed with lower ns with the original factors of n's. Since Theorem 2.0 is trivial when $n = 4$[**4**](proving by contradiction using Pythagorean triples), we can assume that n is a prime number. To use LTE, we must transform $a^n + b^n = c^n$ to fit it into the expression of Theorem 1.0. We can do that by saying $c = b + d$ as $c > b$ where d is a natural number.

Remark Note that b and d are also relatively prime.
Restating $a^n + b^n = c^n$, we get $a^n = (d+b)^n - b^n$. Let p be a prime factor of d. Since b and d are relatively prime, we can use LTE. By using Theorem 0.1, the following is true;

$$\nu_p((d+b)^n - b^n) = \nu_p(n) + \nu_p(d) = \nu_p(a^n)$$

Assume that $p \neq n$(we will observe when $n = p$ later). Since n is prime and hence not divisible by p,

$$\nu_p(d) = \nu_p(a^n)$$

This process can be applied to all of the prime factors of d except 2 when $\nu_2(d) = 1$. If so, then a is also an even number because d and b are relatively prime as b and a are also relatively prime, which makes a even in the equation $a^n + b^n = (b+d)^n$. So, a^n can be expressed by d as $a^n = de$ where d and e are relatively prime because for every p, $\nu_p(d) = \nu_p(a^n)$ is satisfied. And as d and e are relatively prime, they are both the nth power of some number. Therefore, a^n can be expressed as $a^n = \alpha^n\beta^n$ where $d = \alpha^n$ and $e = \beta^n$.
So, $\alpha^n\beta^n + b^n = (b+\alpha^n)^n$. Since the process applied to a can be applied to b, the following is true;

$$\alpha^n\beta^n + \gamma^n\delta^n = (\gamma\delta + \alpha^n)^n = (\alpha\beta + \gamma^n)^n$$

where $b = \gamma^n\delta^n$, $c = a + \gamma^n$, and $\alpha, \beta, \gamma, \delta$ are relatively prime to each other as $gcd(a,b) = gcd(\alpha,\beta) = gcd(\gamma,\delta) = 1$.
$c = \gamma\delta + \alpha^n = \alpha\beta + \gamma^n$, $\gamma\delta - \gamma^n = \alpha\beta - \alpha^n$, $\gamma(\gamma^{n-1} - \delta) = \alpha(\alpha^{n-1} - \beta)$. Since $\alpha \nmid \gamma$, $\alpha | \gamma^{n-1} - \delta$ and so $\delta = \gamma^{n-1} - m\alpha$. Also, $\beta = \alpha^{n-1} - k\gamma$.
Substituting these values into δ, β, we get $c = \alpha^n + \gamma^n - m\alpha\gamma = \alpha^n + \gamma^n - k\alpha\gamma$ and so $m = k$.

$$\alpha^n(\alpha^{n-1} - k\gamma)^n + \gamma^n(\gamma^{n-1} - k\alpha)^n = (\alpha^n + \gamma^n - k\alpha\gamma)^,$$

and so

$$(\alpha^n - k\alpha\gamma)^n + (\gamma^n - k\alpha\gamma)^n = (\alpha^n + \gamma^n - k\alpha\gamma)^n$$

But, $(\alpha^n - k\alpha\gamma)^n + (\gamma^n - k\alpha\gamma)^n < (\alpha^n - k\alpha\gamma)^n + (\gamma^n)^n < (\alpha^n + \gamma^n - k\alpha\gamma)^n$, so it contradicts. When $n = p$, $a^n = nde$ where nd and e are co-prime. Because $gcd(a,b) = 1$, n cannot divide b, and so in the same way, $a^n = \alpha^n\beta^n, b^n = \gamma^n\delta^n$ where $nd = \alpha^n, c - a = \gamma^n$ and $\alpha, \beta, \gamma, \delta$ are all relatively prime to each other. So, $\alpha^n\beta^n + \gamma^n\delta^n = (\frac{\alpha^n}{n} + \gamma\delta)^n = (\gamma^n + \alpha\beta)^n$. In the same way, $\delta = \gamma^{n-1} - m\alpha, \beta = \frac{\alpha^{n-1}}{n} - k\gamma$, $m = k$, $(\frac{\alpha^n}{n} - k\alpha\gamma)^n + (\gamma^n - k\alpha\gamma)^n = (\frac{\alpha^n}{n} + \gamma^n - k\alpha\gamma)^n$. The rest is the same as above. Therefore, we have proved Theorem 2.0

4 References

[1] Hardy, G.H. & Wright, E.M, *Introduction to the Theory of Numbers*

[2] V. J. Brandon. *"Lifting The Exponent Lemma (LTE)," Art of Problem Solving Wiki*

[3] Legendre, A-M., *Essai sur la théorie des nombres*, de Polignac, A., *Recherches nouvelles sur les nombres premiers.*

[4]https://crypto.stanford.edu/pbc/notes/numberfield/fermatn4.html