Lifting The Exponent Lemma (LTE)

Version 3 - Amir Hossein Parvardi

February 28, 2011

Lifting The Exponent Lemma is a new topic in number theory and is a method for solving some exponential Diophantine equations. In this article we analyze this method and present some of its applications.

We can use the Lifting The Exponent Lemma (this is a long name, let's call it **LTE**!) in lots of problems involving exponential equations, especially when we have some prime numbers (and actually in some cases it "explodes" the problems). This lemma shows how to find the greatest power of a prime p – which is often ≥ 3 – that divides $a^n \pm b^n$ for some positive integers a and b. The proofs of theorems and lemmas in this article have nothing difficult and all of them use elementary mathematics. Understanding the theorems usage and its meaning is more important to you than remembering its detailed proof.

I would like to thank makar and ZetaX(Daniel) for their notations about the article. And I specially appreciate JBL(Joel) helps about TeX issues.

1 Descriptions and Signs

For two integers a and b we say a is divisible by b and write $b \mid a$ if and only if there exits some integer q such that $a = qb$.

We define $\|x\|_p$ to be the greatest power of a prime p that divides x; i.e. if $\|x\|_p = \alpha$ then $p^\alpha \mid x$ but $p^{\alpha+1} \nmid x$. We also write $p^\alpha \| x$, if and only if $\|x\|_p = \alpha$. So obviously we have $\|xy\|_p = \|x\|_p \|y\|_p$ and $\|x + y\|_p \leq \|x\|_p + \|y\|_p$.

In lots of articles about this subject, we see the $v_p(x)$ sign. To be coherent with these subjects, we can define v_p in terms of $\|x\|_p$, So that $\|x\|_p = p^{-v_p(x)}$.

Example. The greatest power of 3 that divides 63 is 3^2. because $3^2 = 9 \mid 63$ but $3^3 = 27 \nmid 63$. i.e. $3^2 \| 63$ or $\|63\|_3 = 2$, and we write $v_3(63) = 2$.

Example. Clearly we see that if p and q be two different prime numbers, then $\|p^\alpha q^\beta\|_p = \alpha$, or $p^\alpha \| p^\alpha q^\beta$, and we write $v_p(p^\alpha q^\beta) = \alpha$.

2 Two Important and Useful Lemmas

Lemma 1. *Let x and y be (not necessary positive) integers and let n be a positive integer. Given an arbitrary prime p (i.e. we can have $p = 2$) such that*

$\gcd(n,p)=1$, $p \mid x-y$ *and neither* x *nor* y *is divisible by* p *(i.e.* $p \nmid x$ *and* $p \nmid y$*). We have*

$$v_p(x^n-y^n)=v_p(x-y).$$

Proof. We use the fact that

$$x^n-y^n=(x-y)(x^{n-1}+x^{n-2}y+x^{n-3}y^2+\cdots+y^{n-1}).$$

Now if we show that $p \nmid x^{n-1}+x^{n-2}y+x^{n-3}y^2+\cdots+y^{n-1}$, then we are done. In order to show this, we use the assumption $p \mid x-y$. So we have $x-y \equiv 0 \pmod{p}$, or $x \equiv y \pmod{p}$. Thus

$$\begin{aligned} x^{n-1}+x^{n-2}y+x^{n-3}y^2+\cdots+y^{n-1} & \\ &\equiv x^{n-1}+x^{n-2}\cdot x+x^{n-3}\cdot x^2+\cdots+x\cdot x^{n-2}+x^{n-1} \\ &\equiv nx^{n-1} \\ &\not\equiv 0 \pmod{p}. \end{aligned}$$

This completes the proof. □

Lemma 2. *Let* x *and* y *be (not necessary positive) integers and let* n *be an odd positive integer. Given an arbitrary prime* p *(i.e. we can have* $p=2$*) such that* $\gcd(n,p)=1$, $p \mid x+y$ *and neither* x *nor* y *is divisible by* p*, we have*

$$v_p(x^n+y^n)=v_p(x+y).$$

Proof. This is almost like the proof of **Lemma 1**, and we give it here only for the sake of completeness. We have $p \mid x+y$ or $x \equiv -y \pmod{p}$. Thus

$$\begin{aligned} x^{n-1}-x^{n-2}y+x^{n-3}y^2-\cdots+y^{n-1} & \\ &\equiv x^{n-1}-x^{n-2}\cdot(-x)+x^{n-3}\cdot(-x)^2+\cdots-(-x)\cdot x^{n-2}+x^{n-1} \\ &\equiv nx^{n-1} \\ &\not\equiv 0 \pmod{p}. \end{aligned}$$

Since $x^n+y^n=(x+y)(x^{n-1}-x^{n-2}y+x^{n-3}y^2-\cdots+y^{n-1})$, this completes the proof. □

3 Lifting The Exponent Lemma (LTE)

Theorem 1 (First Form of LTE)**.** *Let* x *and* y *be (not necessary positive) integers and let* n *be a positive integer and* p *be an odd prime such that* $p \mid x-y$ *and none of* x *and* y *are divisible by* p *(i.e.* $p \nmid x$ *and* $p \nmid y$*). We have*

$$v_p(x^n-y^n)=v_p(x-y)+v_p(n).$$

Proof. We may use induction on number of prime divisors of n. First, let us prove the following statement:

$$v_p(x^p - y^p) = v_p(x - y) + 1. \tag{1}$$

In order to prove this, we will show that

$$p \mid x^{p-1} + x^{p-2}y + \cdots + xy^{p-2} + y^{p-1} \tag{2}$$

and

$$p^2 \nmid x^{p-1} + x^{p-2}y + \cdots + xy^{p-2} + y^{p-1}. \tag{3}$$

For **(2)**, we note that

$$x^{p-1} + x^{p-2}y + \cdots + xy^{p-2} + y^{p-1} \equiv px^{p-1} \equiv 0 \pmod{p}.$$

Now, let $y = x + kp$, where k is an integer. For an integer $1 < t < p$ we have

$$\begin{aligned} y^t x^{p-1-t} &\equiv (x + kp)^t x^{p-1-t} \\ &\equiv x^{p-1-t}\left(x^t + t(kp)(x^{t-1}) + \frac{t(t-1)}{2}(kp)^2(x^{t-2}) + \cdots\right) \\ &\equiv x^{p-1-t}\left(x^t + t(kp)(x^{t-1})\right) \\ &\equiv x^{p-1} + tkpx^{p-2} \pmod{p^2}. \end{aligned}$$

This means

$$y^t x^{p-1-t} \equiv x^{p-1} + tkpx^{p-2} \pmod{p^2}, \quad t = 2, 3, 4, \ldots, p-1.$$

Using this fact, we have

$$\begin{aligned} &x^{p-1} + x^{p-2}y + \cdots + xy^{p-2} + y^{p-1} \\ &\quad\equiv x^{p-1} + (x^{p-1} + kpx^{p-2}) + (x^{p-1} + 2kpx^{p-2}) + \cdots + (x^{p-1} + (p-1)kpx^{p-2}) \\ &\quad\equiv px^{p-1} + (1 + 2 + \cdots + p - 1)kpx^{p-2} \\ &\quad\equiv px^{p-1} + \left(\frac{p(p-1)}{2}\right)kpx^{p-2} \\ &\quad\equiv px^{p-1} + \left(\frac{p-1}{2}\right)kp^2x^{p-1} \\ &\quad\equiv px^{p-1} \not\equiv 0 \pmod{p^2}. \end{aligned}$$

So we proved **(3)** and the proof of **(1)** is complete. Now let us return to our problem. We want to show that

$$v_p(x^n - y^n) = v_p(x - y) + v_p(n).$$

Suppose that $n = p^\alpha b$ where $\gcd(p, b) = 1$. So

$$\begin{aligned}
\|x^n - y^n\|_p &= \|(x^{p^\alpha})^b - (y^{p^\alpha})^b\|_p \\
&= \|x^{p^\alpha} - y^{p^\alpha}\|_p = \|(x^{p^{\alpha-1}})^p - (y^{p^{\alpha-1}})^p\|_p \\
&= \|x^{p^{\alpha-1}} - y^{p^{\alpha-1}}\|_p + 1 = \|(x^{p^{\alpha-2}})^p - (y^{p^{\alpha-2}})^p\|_p + 1 \\
&= \|x^{p^{\alpha-2}} - y^{p^{\alpha-2}}\|_p + 2 \\
&\vdots \\
&= \|(x^{p^1})^1 - (y^{p^1})^1\|_p + \alpha - 1 = \|x - y\|_p + \alpha \\
&= \|x - y\|_p + \|n\|_p.
\end{aligned}$$

Note that we used the fact that if $p \mid x - y$, then we have $p \mid x^k - y^k$, because we have $x - y \mid x^k - y^k$ for all positive integers k. The proof is complete. □

Theorem 2 (Second Form of LTE)**.** *Let x, y be two integers, n be an odd positive integer, and p be an odd prime such that $p \mid x + y$ and none of x and y are divisible by p. We have*

$$v_p(x^n + y^n) = v_p(x + y) + v_p(n).$$

Proof. This is almost the same as the proof of the **First Form**. We use induction again. First, we show that

$$v_p(x^p - y^p) = v_p(x - y) + 1 \tag{4}$$

In order to prove this, we will show that

$$p | x^{p-1} - x^{p-2}y + x^{p-3}y^2 - \cdots - xy^{p-2} + y^{p-1} \tag{5}$$

and

$$p^2 \nmid x^{p-1} - x^{p-2}y + x^{p-3}y^2 - \cdots - xy^{p-2} + y^{p-1}. \tag{6}$$

For **(5)**, use the fact that $p \mid x + y \implies x \equiv -y \pmod p$. So

$$x^{p-1} - x^{p-2}y + x^{p-3}y^2 - \cdots - xy^{p-2} + y^{p-1} \equiv px^{p-1} \equiv 0 \pmod p.$$

For **(6)** we can assume that $y = kx + p$, where k is an integer. For an integer $1 < t < p$ we have

$$\begin{aligned}
y^t x^{p-1-t} &\equiv (-x + kp)^t x^{p-1-t} \\
&\equiv x^{p-1-t}\left((-x)^t + t(kp)((-x)^{t-1}) + \frac{t(t-1)}{2}(kp)^2((-x)^{t-2}) + \cdots\right) \\
&\equiv x^{p-1-t}\left((-x)^t + t(kp)((-x)^{t-1})\right) \\
&\equiv (-1)^t x^{p-1} + (-1)^t tkpx^{p-2} \pmod{p^2}.
\end{aligned}$$

This means

$$y^t x^{p-1-t} \equiv (-1)^t x^{p-1} + (-1)^t tkpx^{p-2} \pmod{p^2}, \quad t = 2, 3, 4, \ldots, p-1.$$

Using this fact, we have

$$\begin{aligned}
&x^{p-1} - x^{p-2}y + x^{p-3}y^2 - \cdots - xy^{p-2} + y^{p-1} \\
&\quad \equiv x^{p-1} - (-x^{p-1} + kpx^{p-2}) + (x^{p-1} - 2kpx^{p-2}) - \cdots + (x^{p-1} - (p-1)kpx^{p-2}) \\
&\quad \equiv px^{p-1} - (1 + 2 + \cdots + p - 1)kpx^{p-2} \\
&\quad \equiv px^{p-1} - \left(\frac{p(p-1)}{2}\right) kpx^{p-2} \\
&\quad \equiv px^{p-1} - \left(\frac{p-1}{2}\right) kp^2 x^{p-1} \\
&\quad \equiv px^{p-1} \not\equiv 0 \pmod{p^2}.
\end{aligned}$$

and so **(4)** is proven. Return to our problem, recall that we want to show that

$$v_p(x^n - y^n) = v_p(x - y) + v_p(n).$$

Suppose that $n = p^\alpha b$ where $\gcd(p, b) = 1$. Thus

$$\begin{aligned}
v_p(x^n + y^n) &= v_p((x^{p^\alpha})^b + (y^{p^\alpha})^b) \\
&= v_p(x^{p^\alpha} + y^{p^\alpha}) = v_p((x^{p^{\alpha-1}})^p + (y^{p^{\alpha-1}})^p) \\
&= v_p(x^{p^{\alpha-1}} + y^{p^{\alpha-1}}) + 1 = v_p((x^{p^{\alpha-2}})^p + (y^{p^{\alpha-2}})^p) + 1 \\
&= v_p(x^{p^{\alpha-2}} + y^{p^{\alpha-2}}) + 2 \\
&\;\;\vdots \\
&= v_p((x^{p^1})^1 + (y^{p^1})^1) + \alpha - 1 = v_p(x + y) + \alpha \\
&= v_p(x + y) + v_p(n).
\end{aligned}$$

Note that we used the fact that if $p \mid x + y$, then we have $p \mid x^k + y^k$, because we have $x + y \mid x^k + y^k$ for all odd positive integers k. The proof is complete. □

4 What about $p = 2$?

Question. Why did we assume that p is an odd prime, i.e., $p \neq 2$? Why can't we assume that $p = 2$ in our proofs?

Hint. Note that $\frac{p-1}{2}$ is an integer just for $p > 2$.

Theorem 3 (LTE for the case $p = 2$)**.** *Let x and y be two odd integers such that $4 \mid x - y$. Show that*

$$v_2(x^n - y^n) = v_2(x - y) + v_2(n).$$

Proof. We showed that for any prime p such that $\gcd(p, n) = 1, p \mid x - y$ and none of x and y are divisible by p, we have

$$v_p(x^n - y^n) = v_p(x - y)$$

So it suffices to show that

$$v_2(x^{2^n} - y^{2^n}) = v_2(x - y) + n.$$

Factorization gives

$$x^{2^n} - y^{2^n} = (x^{2^{n-1}} + y^{2^{n-1}})(x^{2^{n-2}} + y^{2^{n-2}}) \cdots (x^2 + y^2)(x + y)(x - y)$$

Now since $x \equiv y \equiv \pm 1 \pmod 4$ then we have $x^{2^k} \equiv y^{2^n} \equiv 1 \pmod 4$ for all positive integers k and so $x^{2^k} + y^{2^k} \equiv 2 \pmod 4, k = 1, 2, 3, \ldots$. This means the power of 2 in all of the factors in the above production (except $x - y$) is one. We are done. □

Theorem. *Let x and y be two odd integers and let n be an even positive integer. Then*

$$v_2(x^n - y^n) = v_2(x - y) + v_2(x + y) + v_2(n) - 1.$$

Proof. We know that square of an odd integer is of the form $4k + 1$. So for odd x and y we have $4 \mid x^2 - y^2$. Now let m be an odd integer and k be a positive integer such that $n = m \cdot 2^k$. So

$$\begin{aligned} v_2(x^n - y^n) &= v_2(x^{m \cdot 2^k} - y^{m \cdot 2^k}) \\ &= v_2((x^2)^{2^k} - (y^2)^{2^k}) \\ &\vdots \\ &= v_2(x^2 - y^2) + k - 1 \\ &= v_2(x - y) + v_2(x + y) + v_2(n) - 1. \end{aligned}$$

□

5 Abstract

Let p be a prime number and let x and y be two (not necessary positive) integers which are not divisible by p. Then:

a) For a positive integer n if

- $p \neq 2$ and $p \mid x - y$, then

$$v_p(x^n - y^n) = v_p(x - y) + v_p(n).$$

- $p = 2$ and $4 \mid x - y$, then

$$v_2(x^n - y^n) = v_2(x - y) + v_2(n).$$

- $p = 2$ and $2 \mid x - y$, then

$$v_2(x^n - y^n) = v_2(x - y) + v_2(x + y) + v_2(n) - 1.$$

b) For an odd positive integer n, if $p \mid x + y$, then

$$v_p(x^n + y^n) = v_p(x + y) + v_p(n).$$

c) For a positive integer n with $\gcd(p, n) = 1$, we have

$$v_p(x^n - y^n) = v_p(x - y).$$

and if n be odd with $\gcd(p, n) = 1$, then we have

$$v_p(x^n + y^n) = v_p(x + y).$$

6 Some Problems to solve with LTE

Problem 1. Let k be a positive integer. Find all positive integers n such that $3^k \mid 2^n - 1$.

Problem 2 (UNESCO Competition 1995)**.** Let a, n be two positive integers and let p be an odd prime number such that

$$a^p \equiv 1 \pmod{p^n}.$$

Prove that

$$a \equiv 1 \pmod{p^{n-1}}.$$

Problem 3 (Iran Second Round 2008)**.** Show that the only positive integer value of a for which $4(a^n + 1)$ is a perfect cube for all positive integers n, is 1.

Problem 4. Let $k > 1$ be an integer. Show that there exists infinitely many positive integers n such that

$$n | 1^n + 2^n + 3^n + \cdots + k^n.$$

Problem 5. Show that $a^n - b^n$ has a prime divisor which isn't a divisor of $a - b$.

Problem 6 (Ireland 1996)**.** Let p be a prime number, and a and n positive integers. Prove that if

$$2^p + 3^p = a^n$$

then $n = 1$.

Problem 7 (Russia 1996)**.** Find all positive integers n for which there exist positive integers x, y and k such that $\gcd(x, y) = 1, k > 1$ and $3^n = x^k + y^k$.

Problem 8 (Russia 1996)**.** Let x, y, p, n, k be positive integers such that n is odd and p is an odd prime. Prove that if $x^n + y^n = p^k$, then n is a power of p.

Problem 9. Let p be a prime number. Solve the equation $a^p - 1 = p^k$ in the set of positive integers.

Problem 10. Find all solutions of the equation

$$(n-1)! + 1 = n^m$$

in positive integers.

Problem 11 (Bulgaria 1997)**.** For some positive integer n, the number $3^n - 2^n$ is a perfect power of a prime. Prove that n is a prime.

Problem 12. Let m, n, b be three positive integers with $m \neq n$ and $b > 1$. Show that if prime divisors of the numbers $b^n - 1$ and $b^m - 1$ be the same, then $b + 1$ is a perfect power of 2.

Problem 13 (IMO ShortList 1991)**.** Find the highest degree k of 1991 for which 1991^k divides the number

$$1990^{1991^{1992}} + 1992^{1991^{1990}}.$$

Problem 14 (Balkan 1993)**.** Let p be a prime number and $m > 1$ be a positive integer. Show that if for some positive integers $x > 1, y > 1$ we have

$$\frac{x^p + y^p}{2} = \left(\frac{x+y}{2}\right)^m,$$

then $m = p$.

Problem 15 (Czech Slovakia 1996)**.** Find all positive integers x, y such that $p^x - y^p = 1$, where p is a prime.

Problem 16 (Romania TST 1993)**.** Let n be a square-free number. Show that there does not exist positive integers x and y such that

$$(x+y)^3 | x^n + y^n.$$

Problem 17. Let x and y be two positive real numbers such that for each positive integer n, the number $x^n - y^n$ is a positive integer. Show that x and y are both positive integers.

Problem 18. Let x and y be two positive rational numbers such that for infinitely many positive integers n, the number $x^n - y^n$ is a positive integer. Show that x and y are both positive integers.

Problem 19 (IMO 2000)**.** Does there exist a positive integer n such that n has exactly 2000 prime divisors and n divides $2^n + 1$?

Problem 20 (China Western Mathematical Olympiad 2010)**.** Suppose that m and k are non-negative integers, and $p = 2^{2^m} + 1$ is a prime number. Prove that

- $2^{2^{m+1}p^k} \equiv 1 \pmod{p^{k+1}}$;
- $2^{m+1}p^k$ is the smallest positive integer n satisfying the congruence equation $2^n \equiv 1 \pmod{p^{k+1}}$.

Problem 21. Let $p \geq 5$ be a prime. Find the maximum value of positive integer k such that

$$p^k | (p-2)^{2(p-1)} - (p-4)^{p-1}.$$

Problem 22. Find all positive integers a, b which are greater than 1 and

$$b^a | a^b - 1.$$

Problem 23. Let a, b be distinct real numbers such that the numbers

$$a - b,\ a^2 - b^2,\ a^3 - b^3, \ldots$$

Are all integers. Prove that a, b are both integers.

Problem 24 (MOSP 2001)**.** Find all quadruples of positive integers (x, r, p, n) such that p is a prime number, $n, r > 1$ and $x^r - 1 = p^n$.

Problem 25 (China TST 2009)**.** Let $a > b > 1$ be positive integers and b be an odd number, let n be a positive integer. If $b^n \mid a^n - 1$, then show that $a^b > \frac{3^n}{n}$.

Problem 26 (Romanian Junior Balkan TST 2008)**.** Let p be a prime number, $p \neq 3$, and integers a, b such that $p \mid a + b$ and $p^2 \mid a^3 + b^3$. Prove that $p^2 \mid a + b$ or $p^3 \mid a^3 + b^3$.

Problem 27. Let m and n be positive integers. Prove that for each odd positive integer b there are infinitely many primes p such that $p^n \equiv 1 \pmod{b^m}$ implies $b^{m-1} \mid n$.

Problem 28 (IMO 1990)**.** Determine all integers $n > 1$ such that

$$\frac{2^n + 1}{n^2}$$

is an integer.

Problem 29. Find all positive integers n such that

$$\frac{2^{n-1}+1}{n}.$$

is an integer.

Problem 30. Find all primes p, q such that $\frac{(5^p-2^p)(5^q-2^q)}{pq}$ is an integer.

Problem 31. For some natural number n let a be the greatest natural nubmer for which $5^n - 3^n$ is divisible by 2^a. Also let b be the greatest natural number such that $2^b \leq n$. Prove that $a \leq b + 3$.

Problem 32 (IMO ShortList 2007)**.** Find all surjective functions $f : \mathbb{N} \to \mathbb{N}$ such that for every $m, n \in \mathbb{N}$ and every prime p, the number $f(m+n)$ is divisible by p if and only if $f(m) + f(n)$ is divisible by p.

Problem 33. Determine all sets of non-negative integers x, y and z which satisfy the equation

$$2^x + 3^y = z^2.$$

Problem 34. Find all positive integer solutions of equation $x^{2009} + y^{2009} = 7^z$

Problem 35 (Romania TST 1994)**.** Let n be an odd positive integer. Prove that $((n-1)^n + 1)^2$ divides $n(n-1)^{(n-1)^n+1} + n$.

Problem 36. Find all positive integers n such that $3^n - 1$ is divisible by 2^n.

Problem 37. Let p be a prime and a, b be positive integers such that $a \equiv b \pmod{p}$. Prove that if $p^x \| a - b$ and $p^y \| n$, then $p^{x+y} \| a^n - b^n$.

Problem 38 (Romania TST 2009)**.** Let $a, n \geq 2$ be two integers, which have the following property: there exists an integer $k \geq 2$, such that n divides $(a-1)^k$. Prove that n also divides $a^{n-1} + a^{n-2} + \cdots + a + 1$.

Problem 39. Find all the positive integers a such that $\frac{5^a+1}{3^a}$ is a positive integer.

Problem 40. Let a, b, n be positive integers such that $2^\alpha \| \frac{a^2-b^2}{2}$ and $2^\beta \| n$. Prove that $2^{\alpha+\beta} \| a^n - b^n$.

References

[1] Sepehr Ghazi Nezami, *Leme Do Khat* (in English: Lifting The Exponent Lemma) published on October 2009. http://imo09.blogfa.com/page/2khat.aspx

[2] Santiago Cuellar, Jose Alejandro Samper, *A nice and tricky lemma (lifting the exponent)*, Mathematical Reflections **3** 2007.

[3] AoPS topic #324597, *Lifting The Exponent Lemma (LTE)*, posted by amparvardi: http://www.artofproblemsolving.com/Forum/viewtopic.php?t=324597

[4] AoPS topic #374822, *CWMO 2010, Day 1, Problem 1*, posted by chaotic iak: http://www.artofproblemsolving.com/Forum/viewtopic.php?t=374822

[5] AoPS topic #268964, *China TST, Quiz 6, Problem 1*, posted by Fang-jh: http://www.artofproblemsolving.com/Forum/viewtopic.php?t=268964

[6] AoPS topic #57607, *exactly 2000 prime divisors*, posted by Valentin Vornicu: http://www.artofproblemsolving.com/Forum/viewtopic.php?t=57607

[7] AoPS topic #220915, *Highest degree for 3-layer power tower*, posted by orl: http://www.artofproblemsolving.com/Forum/viewtopic.php?t=220915

[8] AoPS topic #368210, *Iran NMO 2008 (Second Round) - Problem4*, posted by sororak: http://www.artofproblemsolving.com/Forum/viewtopic.php?t=368210