Lifting The Exponent Lemma LTE

Robert Sparkes

August 19, 2016

Contents

1 Introduction

LTE is used for solving problems involving exponential Diophantine equations, occasionally giving very simple solutions.
Define $||x||_p$ to be the greatest power of p that divides x.
$||x||_p = \alpha \leftrightarrow p^\alpha||x$
Some quick examples to show the structures present in this fuction:

$$ \tag{1.1}$$

$$||xy||_p = ||x||_p \cdot ||y||_p \tag{1.2}$$

$$||x + y||_p \geq min||x||_p, ||y||_p \tag{1.3}$$

Since we are looking at a function I will let $||x||_p = v_p(x)$

2 Foundation

[Lemma 1].
For $x, y \in \mathbb{Z}, n \in \mathbb{N}, p \in \mathbb{P}$ s.t. $(n, p) = 1, p|(x - y) and p \nmid x, y$

$$v_p(x^n - y^n) = v_p(x - y) \tag{2.1}$$

Proof:
$(x^n - y^n) = (x - y)(x^{n-1} + x^{n-2} \cdot y + \cdots + y^{n-1})$
clearly we want to show that $p \nmid (x^{n-1} + \cdots + y^{n-1})$
since $p|(x - y), x \equiv y \pmod p$
so $(x^{n-1} + \ldots y^{n-1}) \equiv nx^{n-1} \not\equiv 0 \pmod p$

[Lemma 2]
For $x, y \in \mathbb{Z}, n \in \mathbb{N}, 2 \nmid n, p \in \mathbb{P}$ s.t. $(n, p) = 1, p|(x + y), p \nmid x, y$

$$v_p(x^n + y^n) = v_p(x + y) \tag{2.2}$$

Since n is odd and y can be negative, we can write;
$v_p(x^n - (-y)^n) = v_p(x - (-y)) = v_p(x + y)$ (By Lemma 1)

3 LTE Lemma

3.1 $p \neq 2$

[Theorem 1]
For $x, y \in \mathbb{Z}, n \in \mathbb{N}, p \in \mathbb{P} \setminus 2$ s.t. $p|(x-y), p \nmid x,, y$

$$v_p(x^n - y^n) = v_p(x-y) + v_p(n) \tag{3.1}$$

Proof:
First we will show that $v_p(x^p - y^p) = v_p(x-y) + 1$, which is equivalent to;
$p|(x^{p-1} + \cdots + y^{p-1})$
$p^2 \nmid (x^{p-1} + \cdots + y^{p-1})$

$x^{p-1} + \cdots + y^{p-1} \equiv px^{p-1} \equiv 0$ (mod p)

Now, let $y = x + kp$, where $k \in \mathbb{Z}$
For $t \in \mathbb{Z}, 1 \leq t < p$

$$\begin{align} \tag{3.2} \\ y^t x^{p-1-t} &\equiv (x+kp)^t (x^{p-1-t}) \tag{3.3} \\ &\equiv (x^{p-1-t})(x^t + t(kp)(x^{t-1}) + (\frac{t(t-1)}{2})(kp)^2(x^{t-2}) + \dots) \tag{3.4} \\ &\equiv x^{p-1-t}(x^t + tkpx^t - 1) \tag{3.5} \\ &\equiv x^{p-1} + tkpx^{p-2} \ (mod\ p^2) \tag{3.6} \end{align}$$

$\rightarrow y^t x^{p-1-t} \equiv x^{p-1} + tkpx^{p-2}$ (mod p), $t = 1, 2 \dots, (p-1)$

Using this we have;

$$\begin{align} \tag{3.7} \\ x^{p-1} + \cdots + y^{p-1} &\equiv x^{p-1} + (x^{p-1} + kpx^{p-2}) + (x^{p-1} + 2kpx^{p-2}) + \cdots + (x^{p-1} + (p-1)kpx^{p-2}) \tag{3.8} \\ &\equiv px^{p-1} + (1 + 2 + \cdots + (p-1))kpx^{p-2} \tag{3.9} \\ &\equiv px^{p-1} + (\frac{p(p-1)}{2})kpx^{p-2}) \tag{3.10} \\ &\equiv px^{p-1} + \frac{p-1}{2}kp^2x^{p-2} \tag{3.11} \\ &\equiv px^{p-1} \not\equiv 0 \ (mod\ p) \tag{3.12} \end{align}$$

Returning to the problem, suppose $n = p^\alpha b, (p, b) = 1$

$$\begin{align} \tag{3.13} \\ ||x^n - y^n||_p &= ||(x^{p^\alpha})^b - (y^{p^\alpha})^b||_p \tag{3.14} \\ &= ||x^{p^\alpha} - y^{p^\alpha}||_p \tag{3.15} \\ &= ||(x^{p^\alpha})^p + (y^{p^\alpha})^p||_p \tag{3.16} \\ &= ||x^{p^{\alpha-1}} - y^{p^{\alpha-1}}||_p + 1 \tag{3.17} \\ &\vdots \tag{3.18} \\ &\equiv ||x-y||_p + \alpha \tag{3.19} \\ &\equiv ||x-y||_p + ||n||_p \tag{3.20} \end{align}$$

[Theorem 2]
For $x, y \in \mathbb{Z}, n \in \mathbb{N}, 2 \nmid n, p \in \mathbb{P} \setminus 2$ s.t. $p|(x+y), p \nmid x, y$

(3.21)

$$v_p(x^n + y^n) = v_p(x+y) + v_p(n) \tag{3.22}$$

Proof;
Follows from Theorem 1 in the same way that Lemma 2 followed from Lemma 1

3.2 $p = 2$

Theorem 3
For $x, y \in \mathbb{Z}, 2 \nmid x, y$ s.t $4|(x-y)$. Then

(3.23)

$$v_2(x^n - y^n) = v_2(x-y) + v_2(n) \tag{3.24}$$

Proof;
We have already shown that for any $p \in \mathbb{P}$ with $(p, n) = 1, p|(x-y), p \nmid x, y$, we have

(3.25)

$$v_p(x^n - y^n) = v_p(x-y) \tag{3.26}$$

so we only need to show that

(3.27)

$$v_2(x^{2^n} - y^{2^n}) = v_2(x-y) + n \tag{3.28}$$

Notice that this is a difference of squares and so we can write

(3.29)

$$(x^{2^{n-1}} - y^{2^{n-1}})(x^{2^{n-2}} - y^{2^{n-2}}) \ldots (x^2 - y^2)(x-y)(x+y) \tag{3.30}$$

we are given that $x \equiv y \equiv \pm 1 \pmod 4$ and so $x^{2^k} \equiv y^{2^k} \equiv 1$ (mod4) $\forall\, k \in \mathbb{N}$ and thus $x^{2^k} + y^{2^k} \equiv 2 \pmod 4$.
From this we see that the powers of 2 in all of the above factors is 1 except for $(x-y)$ and so we are done.

[Theorem 4]
For $x, y \in \mathbb{Z}, 2 \nmid x, y$ and $n \in \mathbb{N}, 2|n$.

(3.31)

$$v_2(x^n + y^n) = v_2(x-y) + v_2(x+y) + v_2(n) - 1 \tag{3.32}$$

Proof;
First it is important to note that $(2n+1)^2 \equiv 1 \pmod 4$, which yeilds; $4|(x^2 - y^2)$.
Let $n = m \cdot 2^k$ for $m \in \mathbb{Z}, 2 \nmid m$ and $k \in \mathbb{N}$

(3.33)

$$\begin{aligned}
v_2(x^n - y^n) &= v_2(x^{m \cdot 2^k} - y^{m \cdot 2^k}) && (3.34)\\
&= v_2((x^2)^{2^{k-1}} - (y^2)^{2^{k-1}}) && (3.35)\\
&\vdots && (3.36)\\
&= v_2(x^2 - y^2) + k - 1 && (3.37)\\
&= v_2(x-y) + v_2(x+y) + v_2(n) - 1 && (3.38)
\end{aligned}$$

4 Recap

For a prime p and $x, y \in \mathbb{Z}$ which are not divisible by p We have;

1. For $n \in \mathbb{N}$
   - $p \neq 2$ and $p|(x-y)$
   $$v_p(x^n - y^n) = v_p(x-y) + v_p(n) \tag{4.1}$$
   - $p = 2$ and $4|(x-y)$
   $$v_2(x^n - y^n) = v_2(x-y) + v_2(n) \tag{4.2}$$
   - $p = 2$ and $2|(x-y)$
   $$v_2(x^n - y^n) = v_2(x-y) + v_2(x+y) + v_2(n) - 1 \tag{4.3}$$
2. For $n \in \mathbb{N}, 2 \nmid n$ and $p|(x+y)$
   $$v_p(x^n + y^n) = v_p(x+y) + v_p(n) \tag{4.4}$$
3. For $n \in \mathbb{N}, (p, n) = 1$
   $$v_p(x^n - y^n) = v_p(x-y) \tag{4.5}$$

   and if $2 \nmid n, (p, n) = 1$
   $$v_p(x^n + y^n) = v_p(x+y) \tag{4.6}$$

5 Problems

1. Let a, n be two positive integers and let p be an odd prime number such that
   $$\tag{5.1}$$
   $$a^p \equiv 1 \ (mod\ p^n) \tag{5.2}$$
   Prove that
   $$\tag{5.3}$$
   $$a \equiv 1 \ (mod\ p^{n-1}) \tag{5.4}$$
2. Prove that the number $a^{a-1} - 1$ is never square-free for all integers $a > 2$ [Definition; A square-free number has no repeated prime factors. $p^1||N \ \forall \ p$]
3. (Ireland 1996) Let p be a prime number and a, n positive integers. Prove that if
   $$2^p + 3^p = a^n \tag{5.5}$$
   Then $n = 1$
4. Let k be a positive integer. Find all positive integers n s.t.
   $$\tag{5.6}$$
   $$3^k | 2^{n-1} \tag{5.7}$$
5. Find the sum off all divisors d of $N = 19^{88} - 1$ which are of the form $2^a 3^b$ with $a, b \in \mathbb{N}$
6. (IMO 1990 Q3) Determine all integers greater than 1 s.t.
   $$\tag{5.8}$$
   $$\frac{2^n + 1}{n^2} \tag{5.9}$$
   is an integer.