Lifting the Exponent Lemma (LTE)

Remy Lee

May 3, 2011

1 What is LTE?

Lifting the Exponent Lemma is a powerful tool used in the olympiad level that trivializes number theory problems to basic arithmetic calculations. This lecture will deal with LTE in the context of AIME/ARML level problems.

2 First Things First

We will use the conventional notation for divisibility: for integers a and b, $a \mid b$ signifies that a evenly divides b.

We will define $v_p(n)$ to be the greatest power of p that divides n. For example, since $144 = 2^4 \cdot 3^2$, we have $v_2(144) = 4$, $v_3(144) = 2$, and $v_5(144) = 0$. Note that if $v_p(x) = a$, $p^a \mid x$, but $p^{a+1} \nmid x$.

Finally, for those of you who are not familiar with modular arithmetic, $a \equiv b \pmod{m}$ denotes that a and b have the same remainder upon dividing by m. For example, $1337 \equiv 42 \pmod{259}$ because both $1337 \div 259$ and $42 \div 259$ have a remainder of 42.

3 The Lemma(s)

Theorem 1: Let x and y be (not neccessarily positive) integers, let n be a positive integer, and let p be an *odd prime* such that $p \mid x - y$ and neither of x and y are divisible by p. Then

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

Proof Outline 1: First we must show that when $v_p(n) = 0$, $v_p(x^n - y^n) = v_p(x - y)$. Clearly, since $x \equiv y \pmod{p}$,

$$\frac{x^n - y^n}{x - y} \equiv \sum_{k=0}^{n-1} x^k y^{n-1-k} \equiv \sum_{k=0}^{n-1} x^{n-1} \not\equiv 0 \pmod{p}.$$

Now we use induction on $v_p(n)$. The base case is not hard to prove: When $v_p(n) = 1$,

$$v_p(x^p - y^p) = v_p(x - y) + 1$$

This is true because

$$p \mid x^{p-1} + x^{p-2}y + x^{p-3}y^2 + \cdots xy^{p-2} + y^{p-1}$$

and

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

Now we proceed to the inductive step. Let $n = p^a b$ where p does not divide b. We use this fact to prove that

$$\begin{aligned} v_p(x^n - y^n) &= v_p((x^{p^a})^b - (y^{p^a})^b) && (1) \\ &= v_p(x^{p^a} - y^{p^a}) && (2) \\ &= v_p(x^{p^{a-1}} - y^{p^{a-1}}) + 1 && (3) \\ &= v_p(x - y) + v_p(n). && (4) \end{aligned}$$

Theorem 2: 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 Outline 2: We know that $4 \mid x^2 - y^2$. Let $n = m \cdot 2^k$ where $2 \nmid m$. Then

$$\begin{aligned} v_2(x^n - y^n) &= v_2(x^{m \cdot 2^k} - y^{m \cdot 2^k}) && (5) \\ &= v_2(x^2 - y^2) + k - 1 && (6) \\ &= v_2(x - y) + v_2(x + y) + v_2(n) - 1. && (7) \end{aligned}$$

4 Problems

Remember that when dealing with number theory problems that involve exponents, Fermat's Little Theorem (FLT) is also quite helpful.

1. Find the largest integer k such that $1991^k \mid (1990^{1991^{1992}} + 1992^{1991^{1990}})$

   Hint: How can we rewrite the first term so it has the same exponent as the second term?

2. Find the sum of all positive integers a such that $a^{a-1} - 1$ is not divisible by a perfect square greater than 1.

3. Find the sum of all divisors d of $(19^{88} - 1)$ such that $d = 2^a 3^b$.

   Hint: Find the maximum value of d.

4. Find a positive integer n such that n has exactly 2000 distinct prime factors and $n \mid (2^n + 1)$. What is the minimum prime factor that can divide n that is greater than 3?

   Hint: Consider $n = 3^k$ then consider $n = p(3^k)$ such that $p > 3$ divides $2^{3^k} + 1$.

5. Find the sum of all positive integers a such that $3^a \mid (5^a + 1)$.

6. Determine the product of all integers $n > 1$ such that $n^2 \mid (2^n + 1)$.

   Hint: Consider the minimal prime p that divides n and apply FLT.

7. If n divides $2^{n-1} + 1$ then n must be divisble by a positive integer m. Determine m.

8. How many distinct ordered pairs of prime numbers (p, q) exist such that pq divides $(5^p - 2^p)(5^q - 2^q)$?