



Lifting The Exponent (LTE)

Entrenamiento extra

Fecha

Por: Argel

Resumen

En esta ocasión les presentaremos una herramienta muy interesante y fuerte que sirve para tratar con situaciones en las que nos interesa el mayor exponente de un primo que divide a una cierta expresión, a esta herramienta la conocemos como Lifting The Exponent o LTE.

1. La introducción

El lemma de Lifting The Exponent que normalmente por conveniencia se refiere a él como LTE, es un método muy poderoso con el cual se pueden resolver ecuaciones diofantinas exponenciales. LTE nos sirve para obtener el mayor exponente de un primo tal que divide a un $a^n \pm b^n$.

1.1. La notación y algunas definiciones

Para empezar vamos a definir $v_p(x)$ como el exponente más grande tal que el primo p divide a x . En lo particular, si $v_p(x) = \alpha$ entonces $p^\alpha | x$, pero $p^{\alpha+1} \nmid x$. A su vez se escribe $p^\alpha || x$, si y solo si $v_p(x) = \alpha$. Entonces se tiene $v_p(xy) = v_p(x) + v_p(y)$ y $v_p(x+y) \geq \min\{v_p(x), v_p(y)\}$.

1.2. Dos lemas útiles

Lema 1 Sean x, y dos enteros (no necesariamente positivos) y sea n un entero positivo. Dado un primo arbitrario p (en particular, se puede tener $p = 2$), tal que $\text{mcd}(n, p) = 1$, $p | x - y$ y x ni y divisibles entre p . Se tiene

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

Para este lemma es buena idea aprovechar la factorización de $x^n - y^n$ y el hecho de que $p | x - y$.

Lema 2 Sean x, y dos enteros (no necesariamente positivos) y sea n un entero positivo impar. Dado un primo arbitrario p (en particular, se puede tener $p = 2$), tal que $\text{mcd}(n, p) = 1$, $p | x + y$, x ni y divisibles entre p . Se tiene

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

Es importante recordar que x, y pueden ser negativos y n es impar.

2. Ahora sí, LTE

2.1. Dos formas de LTE

Primera forma de LTE Sean x, y dos enteros (no necesariamente positivos), sea n un entero positivo y sea p un primo impar tal que $p | x - y$, x, y no divisibles por p . Se tiene

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

Segunda forma de LTE Sean x, y dos enteros (no necesariamente positivos), sea n un entero positivo impar y sea p un primo impar tal que $p | x + y$, x, y no divisibles por p . Se tiene

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

2.2. El caso de $p = 2$

Si se pudieron dar cuenta de las dos formas de LTE vistas previamente, ambas implicaban que p fuera distinto a 2, el caso de $p = 2$ es bastante curioso. **LTE para $p = 2$** Sean x, y dos enteros impares tales que $4|x - y$. Entonces

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

n un entero par Sea x, y dos enteros impares y sea n un entero positivo par. Entonces

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

3. Algunos Ejemplos

3.1. Ejemplo 1: A beginning

Use el lema de LTE para encontrar el exponente más grande de 3 que divide a $5^{18} - 2^{18}$. Entonces usando LTE se obtiene

$$V_p(5^{18} - 2^{18}) = V_p(5 - 2) + V_p(18)$$

Ahora como $18 = 2 \cdot 3^2$

$$V_p(5^{18} - 2^{18}) = 1 + 2 = 3$$

Por lo tanto 3^3 divide a nuestra expresión.

3.2. Ejemplo 2: Free as a bird

Sea n un entero libre de cuadrados. Muestre que no hay un par de enteros positivos coprimos x, y tales que

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

Primero consideremos n par. Si hay un primo impar $p|(x + y)$, entonces $x^n + y^n \equiv x^n + (-x)^n \equiv 2x^n \pmod{p}$ ya que n par, entonces $p|x, p|y$ pero recordando que $\text{mcd}(x, y) = 1$ se ha llegado a una contradicción. Como x, y son positivos, la única manera posible en la que no hay un primo impar p que divide a $x + y$ es si $x + y$ es una potencia de 2. En dado caso x, y ambos tienen que ser impares considerando que son coprimos. Entonces con n par x^n y y^n son ambos 1 (mód 8), entonces $v_2(x^n + y^n) = 1$, pero $v_2((x + y)^3) \geq 3$, pero de nuevo tenemos una contradicción.

Ahora supongamos que n es impar. Si hay un primo impar $p|(x + y)$, entonces $3v_p(x + y) \leq v_p(x^n + y^n)$. Entonces por LTE

$$3v_p(x + y) \leq v_p(x + y) + v_p(n) \leq v_p(x + y) + 1$$

ya que n es libre de cuadrados.

$$2v_p(x + y) \leq 1$$

Simplificando se tiene $v_p(x + y) \leq \frac{1}{2}$, lo que es imposible debido a $p|(x + y)$.

El caso que nos hace falta considerar es con $x + y$ una potencia de 2. Pero en este caso $v_2(x^n + y^n) = v_2(x + y)$. Ahora recordemos que con n impar

$$\frac{x^n + y^n}{x + y} = x^{n-1} - x^{n-2}y + \dots - xy^{n-2} + y^{n-1}$$

x, y son impares $yx^{n-1} - x^{n-2}y + \dots - xy^{n-2} + y^{n-1}$ tiene una cantidad impar de términos, entonces toda la suma es impar. Con lo anterior se concluye que es imposible que $(x + y)^3$ divida a $x^n + y^n$, esto ya que la potencia de 2 de un lado de la ecuación excede al otro.

4. Agregados culturales

1. Do you even lift? The exponent
2. Existe otro lema en el cual LTE se encuentra inspirado, este es el Lemma de Hensel.
3. Finalmente, como si Hensel no fuera suficiente, existe otro lema similar pero mucho menos conocido que LTE, pero eso no lo escucharon de mi.

5. Resumen de LTE

Bueno, esas fueron varias cosas las que se han visto, por lo tanto, a continuación un resumen.

Sea p un número primo y sean x, y dos enteros (no necesariamente enteros tales que no son divisibles por p)

1. Para un entero positivo n

a) Si $p \neq 2$ y $p|x - y$, entonces

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

b) Si $p = 2$ y $4|x - y$, entonces

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

c) Si $p = 2$, n es par, y $2|x - y$, entonces

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

2. Para un entero positivo entero n , si $p|x + y$, entonces

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

3. Para un entero positivo n con $\text{mcd}(p, n) = 1$, y $p|x - y$, se tiene

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

Si n es impar, $\text{mcd}(p, n) = 1$, y $p|x + y$, entonces se tiene

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

Una cosa importante al usar LTE es siempre revisar la condición $p|x \pm y$, de lo contrario se puede obtener una respuesta errónea.

6. Problemas

1. Demuestre que para cada natural $n > 1$ se tiene $(n - 1)^2 | n^{n-1} - 1$.
2. Sea k un entero positivo. Encuentre todos los enteros positivos n tales que $3^k | 2^n - 1$.
3. Sean a, n dos enteros positivos y sea p un número primo impar tal que

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

Demuestre que

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

4. Muestra que el único valor positivo entero de a para el cual $4(a^n + 1)$ es un cubo perfecto para todos los enteros positivos n , es 1.
5. Sea p un número primo, a y n enteros positivos. Pruebe que si

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

entonces $n = 1$.

6. Sean x, y, p, n, k enteros positivos tales que n es impar y p es un primo impar. Demuestre que si $x^n + y^n = p^k$, entonces n es una potencia de p .
7. Encuentre la suma de todos los divisores d de $N = 19^{88} - 1$ que son de la forma $d = 2^a 3^b$ con $a, b \in \mathbb{N}$.
8. Sea p un número primo. Resuelva la ecuación $a^p - 1 = p^k$ en el conjunto de los enteros positivos.
9. Encuentre todos los primos p, q tales que $\frac{(5^p - 2^p)(5^q - 2^q)}{pq}$ es un entero.
10. Encuentre todos los enteros positivos a tales que $\frac{5^a + 1}{3^a}$ es un entero positivo.
- 11.
12. Sean m, n, b tres enteros positivos con $m \neq n$ y $b > 1$. Muestra que si los divisores primos de los números $b^n - 1$ y $b^m - 1$ son los mismo, entonces $b + 1$ es una potencia perfecta de 2.
13. Encuentre el mayor grado k de 1991 para el cual 1991^k divide al número

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

14. Encuentre todos los enteros positivos x, y tales que $p^x - y^p = 1$, donde p es primo.
15. Encuentre todos los enteros positivos n tales que $3^n - 1$ sea divisible por 2^n .
16. Sea p un número primo tal que $p \neq 3$ y enteros a, b tales que $p|a + b$ y $p^2|a^3 + b^3$. Demuestra que $p^2|a + b$ o $p^3|a^3 + b^3$.
17. Sean x y y dos números positivos racionales tales que para infinitamente tantos enteros positivos n , el número $x^n - y^n$ es un entero positivo. Demuestre que x y y son ambos enteros positivos.
18. Sean a, b números reales distintos tales que los números

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

son todos enteros. Demuestre que a, b son ambos enteros.

19. Encuentre todas las soluciones enteras positivas de la ecuación $x^{2009} + y^{2009} = 7^z$
20. Para un número n , sea a el número natural más grande para el cual $5^n - 3^n$ es divisible por 2^a . Además sea b el número natural más grande para el cual $2^b \leq n$. Demuestre que $a \leq b + 3$
21. Determine todos los enteros $n > 1$ tales que

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

Sea un entero.

22. Sea n un entero positivo impar. Demuestre que $((n - 1)^n + 1)^2$ divide a $n(n - 1)^{(n-1)^n + 1} + n$.

23. Sean $a > b > 1$ enteros positivos y b un número impar, sea n un entero positivo. Si $b^n | a^n - 1$, entonces muestre que $a^b > \frac{3^n}{n}$.
24. Sean $a, n \geq 2$ dos enteros, que tienen la siguiente propiedad: existe un entero $k \geq 2$, tal que n divide $(a - 1)^k$. Demuestre que n también divide a $a^{n-1} + a^{n-2} + \dots + a + 1$.
25. Encuentre funciones suprayectivas $f : \mathbb{N} \rightarrow \mathbb{N}$ tales que para cada $m, n \in \mathbb{N}$ y cada primo p , el número $f(m + n)$ es divisible por p si y sólo si $f(m) + f(n)$ es divisible por p .