Valuación p-ádica y lema del exponente.

Héctor Raúl Fernández Morales
10001noesprimo@gmail.com

abril, 2021

En este documento introducimos el concepto de valuación p-ádica y desarrollamos los resultados más relevantes relacionados con este. Finalmente presentamos el **Lema del Exponente(lifting the exponent lemma, LTE)** que tan de moda está en el presente.

Background: Se asume que el lector está familiarizado con los conceptos esenciales de divisibilidad: algoritmo de euclides, teorema de Bezout, teorema fundamental de la aritmética, congruencias. Además es altamente recomendable estudiar previamente el reporte de Aritmética Modular.

Contents

1 Definición y principales resultados

Definition 1. *Sea p primo, se define la **valuación $p-$ádica** de m como el exponente de la mayor potencia de p que divide a m. La notación es $\nu_p(m)$.*

Theorem 1. *Sean $a, b \in \mathbb{Z}$ y p un número primo:*

- $a|b \quad \Leftrightarrow \nu_p(a) \leq \nu_p(b)$ *para todos los primos p.*
- $\nu_p(ab) = \nu_p(a) + \nu_p(b)$.
- $\nu_p(a^n) = n\nu_p(a)$.
- *Si $b|a$ entonces $\nu_p(\frac{a}{b}) = \nu_p(a) - \nu_p(b)$.*
- $\nu_p(a+b) \geq \min\{\nu_p(a), \nu_p(b)\}$ *y la igualdad se cumple si $\nu_p(a) \neq \nu_p(b)$. En otras palabras, si $\nu_p(a) > \nu_p(b)$ entonces $\nu_p(a+b) = \nu_p(b)$.*

Problem 1 (IMO Shortlist 2007)**.** *Sean $b, n > 1$ enteros. Para todo $k > 1$ existe un entero a_k tal que $k|b - a_k^n$. Prueba que $b = m^n$ para algun entero m.*

Solution. Supongamos que existe un primo p tal que $p|b$ y $n \nmid \nu_p(b)$. Entonces tenemos que

$$b = p^{cn+d}b_1, \qquad 1 \leq d \leq n-1$$

donde $\gcd(b_1, p) = 1$. Sea ahora $k = p^{(c+1)n}$, sabemos que

$$(c+1)n = \nu_p(k) \leq \nu_p(b - a_k^n),$$

Analicemos dos casos,
Primer caso $\boxed{\nu_p(a_k) \leq c}$. Entonces tenemos que

$$\nu_p(b) > \nu_p(a_k^n) \Rightarrow (c+1)n \leq \nu_p(b - a_k^n) = \nu_p(a_k^n) \leq c^n$$

Contradicción.
Segundo caso $\boxed{\nu_p(a_k) \geq c+1}$. Entonces tenemos que

$$\nu_p(b) < \nu_p(a_k^n) \Rightarrow (c+1)n \leq \nu_p(b - a_k^n) = \nu_p(b) = cn + d$$

Contradicción.
De donde d tiene que ser cero y el problema está resuelto. □

2 Valuación p-ádica de factoriales

La valuación p-ádica suele aparecer con mucha frecuencia en problemas que involucran factoriales y esto es debido a los siguientes teoremas atribuidos a Legendre.

Theorem 2 (Legendre)**.** *Para todos $n, p \geq 1$, con p primo, tenemos que*

$$\nu_p(n!) = \sum_{i=1}^{\infty} \lfloor \frac{n}{p^i} \rfloor.$$

Theorem 3 (Legendre)**.** *Para todos $n, p \geq 1$, con p primo, tenemos que*

$$\nu_p(n!) = \frac{n - s_p(n)}{p-1}$$

donde $s_p(n)$ denota la suma de los dígitos de n en base p.

Problem 2 (Canadá 1985)**.** *Encuentra todos los enteros positivos n tales que*

$$2^{n-1} | n!$$

Solution. Del teorema de Legendre tenemos que

$$\nu_2(n!) = n - s_2(n) \geq n - 1 \Rightarrow 1 \geq s_2(n),$$

y esto solo sucede cuando n es potencia de 2. □

3 Máximo común divisor y mínimo común múltiplo

Hay una relación bastante directa entre la valuación p-ádica, el máximo común divisor y el mínimo común múltiplo.

Lemma 1. *Sean m, n enteros. Entonces para todo primo p tenemos que*

$$\nu_p(\gcd(n,m)) = \min\{\nu_p(m), \nu_p(n)\}$$
$$\nu_p(\operatorname{lcm}(n,m)) = \max\{\nu_p(m), \nu_p(n)\}.$$

Problem 3 (IMO 2018)**.** *Sea a_1, a_2, ... una sucesión de enteros positivos. Supongamos que existe un entero positivo $N > 1$ tal que para todo $n \geq N$ el número*

$$\frac{a_1}{a_2} + \frac{a_2}{a_3} + \cdots + \frac{a_{n-1}}{a_n} + \frac{a_n}{a_1}$$

es un entero. Prueba que existe un entero positivo M tal que $a_m = a_{m+1}$ para todo $m \geq M$.

Solution. Primeramente veamos que la diferencia $\frac{a_{n+1}}{a_1} - \frac{a_n}{a_1} + \frac{a_n}{a_{n+1}}$ es también entera para $n \geq N$, de donde

$$a_1 a_{n+1} \mid a_{n+1}^2 - a_n a_{n+1} + a_1 a_n \equiv (a_{n+1} - a_1)(a_{n+1} - a_n).$$

Supongamos que $\nu_p(a_1) > \nu_p(a_{n+1})$ y $\nu_p(a_n) > \nu_p(a_{n+1})$, esto implica que

$$\nu_p(a_{n+1} - a_1) = \nu_p(a_{n+1})$$
$$\nu_p(a_{n+1} - a_n) = \nu_p(a_{n+1})$$

de donde $2\nu_p(a_{n+1}) \geq \nu_p(a_1) + \nu_p(a_{n+1}) \Rightarrow \nu_p(a_{n+1}) \geq \nu_p(a_1)$, contradicción. Hemos probado que $\nu_p(a_{n+1}) \geq \min\{\nu_p(a_1), \nu_p(a_n)\}$. Análogamente podemos completar la demostración de

$$\min\{\nu_p(a_1), \nu_p(a_n)\} \leq \nu_p(a_{n+1}) \leq \max\{\nu_p(a_1), \nu_p(a_n)\}.$$

Como consecuencia de esto tenemos que

- $\gcd(a_1, a_n) \mid a_{n+1} \mid \operatorname{lcm}(a_1, a_n)$ para todo $n \geq N$.
- $\gcd(a_1, a_n) \mid \gcd(a_1, a_{n+1})$ y $\operatorname{lcm}(a_1, a_{n+1}) \mid \operatorname{lcm}(a_1, a_n)$ para todo $n \geq N$.

Ahora $\{\gcd(a_1, a_n)\}_{n \geq N}$ y $\{\operatorname{lcm}(a_1, a_n)\}_{n \geq N}$ son creciente y decreciente respectivamente y están acotadas por a_1, entonces dichas sucesiones son eventualmente constante. Sea $\gcd(a_1, a_m) = u$ y $lcm(a_1, a_m) = v$ para todo $m \geq M$, entonces

$$a_m = \frac{\gcd(a_1, a_m) \cdot \operatorname{lcm}(a_1, a_m)}{a_1} = \frac{uv}{a_1}$$

para todo $m \geq M$ y hemos concluido el problema. □

4 Lema del exponente

Esta es la sección principal de este reporte. En los últimos años el lema del exponente ha ganado mucha popularidad, no sabría decir específicamente en qué año comenzó a usarse por el nombre de **Lifting the Exponent** pero sospecho que en el pasado simplemente para cada problema relacionado se hacía una demostración ad hoc de la variante necesaria de dicho lema. El siguiente resultado colapsa todas las variantes del lema, la demostración no la incluimos y el lector que se sienta con confianza puede intentar probarlo, no es extremadamente complicado, eso sí, en las referencias se puede encontrar dicha demostración.

Theorem 4. *Sea p un número primo y sean x, y dos números enteros que no son divisibles por p. Entonces:*

[a] Para un entero positivo n si

- $p \neq 2$ *y* $p|x-y$ *entonces*

$$\nu_p(x^n - y^n) = \nu_p(x-y) + \nu_p(n)$$

- $p = 2$ *y* $4|x-y$ *entonces*

$$\nu_2(x^n - y^n) = \nu_2(x-y) + \nu_2(n)$$

- $p = 2$, n *es par y* $2|x-y$ *entonces*

$$\nu_2(x^n - y^n) = \nu_2(x-y) + \nu_2(x+y) + \nu_2(n) - 1$$

[b] Para un entero positivo impar n, si $p|x+y$ entonces

$$\nu_p(x^n + y^n) = \nu_p(x+y) + \nu_p(n).$$

[c] Para un entero positivo n, si $p \nmid n$ y $p|x-y$ entonces

$$\nu_p(x^n - y^n) = \nu_p(x-y).$$

si n es impar, $p \nmid n$ y $p|x+y$ entonces

$$\nu_p(x^n + y^n) = \nu_p(x+y).$$

Problem 4 (IMO 1990)**.** *Encuentra todos los enteros positivos n tales que $\frac{2^n+1}{n^2}$ es entero.*

Solution. Trivialmente $\boxed{n=1}$ es solución. Asumamos que $n \neq 1$, sea $p > 2$ el menor primo que divide a n, tenemos entonces que

$$p|2^n + 1|2^{2n} - 1$$

y por FLT, $p|2^{p-1} - 1$, usando el truco del exponente obtenemos que

$$p|2^{\gcd(2n, p-1)} - 1.$$

lo que implica que $\gcd(2n, p-1) > 1$. Veamos que la minimalidad de p implica que $\gcd(n, p-1) = 1$, de donde concluimos que $\gcd(2n, p-1) = 2$ y entonces $p = 3$.
Veamos que usando LTE

$$2\nu_3(n) \leq \nu_3(2^n + 1) = v_3(2 + 1) + \nu_3(n)$$

y obtenemos que $\nu_3(n) = 1$.
Veamos que $\boxed{n = 3}$ es solución. Sea ahora $n = 3k$ con $k > 1$ y $\gcd(k, 6) = 1$. Usando el mismo procedimiento, sea q el menor primo que divide a k, entonces se cumple que

$$q|2^{\gcd(6k, q-1)} - 1.$$

Nuevamente por la minimalidad de q tenemos que $\gcd(k, q-1) = 1$ de donde $\gcd(6k, q-1) \in \{1, 2, 3, 6\}$, analizando todos los casos llegamos a que $q = 7$, pero los posibles restos de las potencias de 2 en la división por 7 son $\{1, 2, 4\}$ de donde $7 \nmid 2^n + 1$, lo que implica que $k = 1$ y no existen más soluciones. □

Problem 5 (IMO 1999)**.** *Encuentra todos los pares de enteros positivos* (x, p) *tal que* p *es primo,* $x \leq 2p$ *y* $x^{p-1}|(p-1)^x + 1$.

Solution. Veamos que si $x = 1$ cualquier primo p es solución y si $x = 2$ tenemos que

$$2^{p-1}|(p-1)^2 + 1$$

de donde $p \leq 5$ y analizando los casos tenemos la solución $(x, p) = (2, 2)$. Obivamente el caso $p = 2$ no proporciona nuevas soluciones así que en lo adelante $x \geq 3$ y $p \geq 3$.
Trivialmente x es impar, sea ahora q el menor primo que divide a x, con la misma estrategia del problema anterior tenemos que

$$q|(p-1)^{\gcd(2x, q-1)} - 1.$$

Por la minimalidad de q tenemos que $\gcd(2x, q-1) = 2$ y obtenemos que $q|p(p-2)$. Veamos que

$$q|(p-1)^x + 1 = ((p-2) + 1)^x + 1.$$

de donde si $q|p-2$ entonces $q|2$ contradicción, de donde $q|p$ o lo que es lo mismo $q = p$.
Como $x \leq 2p$ tenemos que $\nu_p(x) = 1$, usando LTE

$$p - 1 \leq \nu_p((p-1)^x + 1) = 1 + \nu_p(x) = 2,$$

de donde $p \leq 3$ y para $p = 3$ tenemos que $x \leq 6$, analizando los casos obtenemos la solución $(x, p) = (3, 3)$. Concluyendo, todas las soluciones son $\boxed{(x, p) = (1, p), (2, 2), (3, 3)}$. □

5 Lista de Problemas

Problem 1. *Sean a, b enteros tales que $a|b^2|a^3|b^4\ldots$. Prueba que $a = b$.*

Problem 2. *Prueba que $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$ no es entero para ningún $n \geq 2$.*

Problem 3. *Prueba que para todo entero positivo n,*

$$\binom{2n}{n} | \operatorname{lcm}\{1, 2, 3, \ldots, 2n\}.$$

Problem 4. *Prueba que para todo entero positivo n,*

$$n!| \prod_{k=0}^{n-1} (2^n - 2^k).$$

Problem 5. *Encuentra todos los enteros positivos n tales que,*

$$n|(n-1)!.$$

Problem 6 (Putnam 2003)**.** *Prueba que para todo entero positivo n,*

$$n!| \prod_{i=0}^{n} \operatorname{lcm}\{1, 2, \ldots, \lfloor \frac{n}{i} \rfloor\}.$$

Problem 7 (Bulgaria 1997)**.** *Para algunos enteros positivos n el número $3^n - 2^n$ es potencia de un primo. Prueba que n es primo.*

Problem 8 (China tst 2009)**.** *Sean $a > b > 1$ enteros positivos con b impar y sea n entero positivo. Si $b^n|a^n - 1$ prueba que $a^b > \frac{3^n}{n}$.*

Problem 9 (Iran 2008)**.** *Sea a un número natural. Supongamos que $4(a^n + 1)$ es un cubo perfecto para todo natural n. Prueba que $a = 1$.*

Problem 10. *Sean a, b, c enteros positivos tales que $c|a^c - b^c$. Prueba que $c|\frac{a^c - b^c}{a-b}$.*

Problem 11 (AIME 2018)**.** *Encuentra el menor entero positivo n tal que 3^n termina en 01 cuando es escrito en base 143.*

Problem 12 (IMO Shortlist 1991)**.** *Encuentra el mayor entero k para el cual 1991^k divide a*

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

Problem 13 (IMO Shortlist 2014)**.** *Encuentra todos los primos p y enteros positivos (x, y) tales que $x^{p-1} + y$ y $y^{p-1} + x$ son potencias de p.*

Problem 14. *Sea $k > 1$ sea un entero. Prueba que existen infinitos enteros positivos n tales que*

$$n|1^n + 2^n + 3^n + dots + k^n.$$

Problem 15 (Rusia 1996)**.** *Encuentra todos los enteros positivos n para los cuales existen enteros positivos x, y, k tales que* $\gcd(x, y) = 1$, $k > 1$ *y* $3^n = x^k + y^k$.

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

Problem 16 (Checa Eslovaca 1997)**.** *Encuentra todos los enteros positivos (x, y) tal que $p^x - y^p = 1$, donde p es primo.*

Problem 17. *Encuentra todos los enteros positivos a tales que $\frac{5^a+1}{3^a}$ es entero positivo.*

References

[1] Justin Stevens, Olympiad Number Theory Through Challenging Problems.

[2] Aditya Khurmi, Modern Olympiad Number Theory

[3] Amir Hossein, Lifting the exponent lemma.

[4] Evan Chen, Orders Modulo a Prime,https://web.evanchen.cc/handouts/ORPR/ORPR.pdf

[5] Evan Chen, The OTIS Excerpts.

[6] https://artofproblemsolving.com