Valuación p-ádica

Por Denisse A. Escobar Parra y César E. Rodríguez Angón

Una forma de obtener información cuando se trabaja con ecuaciones con enteros es la que se conoce como la valuación p-ádica. Aunque el nombre puede parecer extravagante, en realidad es algo que aparece desde los primeros problemas de teoría de números, por ejemplo al revisar la paridad de ambos lados en una igualdad con enteros. La valuación p-ádica no es otra cosa que calcular la máxima potencia de un primo p que divide a cierto número entero a. Se suele escribir $\nu_p(a) = m$ para indicar que $a = p^m \cdot b$, donde mcd$(p, b) = 1$. También se utiliza la notación $p^m || a$, que se lee: p^m divide exactamente al entero a. A manera de ejemplo, tenemos que $\nu_3(9) = 2$, $\nu_{13}(39) = 1$, $\nu_5(4625) = 3$ y $\nu_{37}(4625) = 1$.
Un ejemplo clásico del uso de la valuación p-ádica, en el que no se hace uso explícito de la definición, es la demostración de que $\sqrt{2}$ es irracional.

Ejemplo 1. *Demuestra que el número $\sqrt{2}$ no puede expresarse en la forma $\frac{a}{b}$ con a, b enteros y $b \neq 0$.*

Solución. Supongamos, por contradicción, que $\sqrt{2} = \frac{a}{b}$, con a y b enteros positivos y primos relativos. Elevamos ambos lados de la igualdad al cuadrado y obtenemos que $2 = \frac{a^2}{b^2}$. Multiplicando esta igualdad por b^2, obtenemos que $b^2 \cdot 2 = a^2$. La contradicción llega básicamente por fijarnos en la máxima potencia de 2 que divide a cada lado de la igualdad, ya que los cuadrados son divisibles por una potencia par de 2, por lo que un lado es divisible por una potencia par de 2 y el otro lado por una potencia impar. Esto se puede ver de forma incluso más explícita ya que, al considerar que mcd$(a, b) = 1$, a lo más uno de ellos es par. Según la igualdad debería ser a, pero entonces al ser 2 un primo, se debería tener que 2^2 divide a a^2, pero en el lado izquierdo b es impar, por lo que el lado izquierdo de la igualdad solo es divisible por 2, pero no por 4, lo cual es una contradicción.

A continuación veremos algunos resultados importantes a cerca de la valuación p-ádica.

Teorema 1. *Sean a y b enteros positivos y sea p un número primo. Entonces,*

a) $\nu_p(ab) = \nu_p(a) + \nu_p(b)$.

b) Si $b \mid a$, entonces $\nu_p(\frac{a}{b}) = \nu_p(a) - \nu_p(b)$.

c) $\nu_p(mcd(a,b)) = min(\nu_p(a), \nu_p(b))$. *Análogamente sucede que* $\nu_p(mcm(a,b)) = max(\nu_p(a), \nu_p(b))$.

d) $\nu_p(a+b) \geq min(\nu_p(a), \nu_p(b))$. *Más aún, si* $\nu_p(a) \neq \nu_p(b)$, *entonces* $\nu_p(a+b) = min(\nu_p(a), \nu_p(b))$.

Demostración. a) Sean $a = p^\alpha a_1$ y $b = p^\beta b_1$, con $\text{mcd}(a_1, p) = 1 = \text{mcd}(b_1, p)$, esto es, $\nu_p(a) = \alpha$ y $\nu_p(b) = \beta$. Cuando multiplicamos ambos número obtenemos $ab = p^{\alpha+\beta} a_1 b_1$. Por lo que, $\nu_p(ab) = \alpha + \beta = \nu_p(a) + \nu_p(b)$.

b) Sean $a = p^\alpha a_1$ y $b = p^\beta b_1$, con $\text{mcd}(a_1, p) = 1$ y $\text{mcd}(b_1, p) = 1$. Entonces, $\frac{a}{b} = \frac{p^\alpha a_1}{p^\beta b_1} = \frac{p^{\alpha-\beta} a_1}{b_1}$, lo cual implica que $\nu_p(\frac{a}{b}) = \nu_p(a) - \nu_p(b)$.

c) Sean $a = p^\alpha a_1$ y $b = p^\beta b_1$, con $\text{mcd}(a_1, p) = 1$ y $\text{mcd}(b_1, p) = 1$. Supongamos, sin pérdida de generalidad, que $\alpha \leq \beta$. Entonces, $\text{mín}(\nu_p(a), \nu_p(b)) = \text{mín}(\alpha, \beta) = \alpha$. Por otro lado, por la forma en la que definimos α y β, tenemos que $p^\alpha \mid a$ y $p^\alpha \mid b$, pero $p^{\alpha+1} \nmid a$. Por lo tanto, el exponente de p en $\text{mcd}(a, b)$ es α, es decir $\nu_p(\text{mcd}(a, b)) = \alpha = \text{mín}(\nu_p(a), \nu_p(b))$. La demostración de $\nu_p(\text{mcm}(a, b)) = \text{máx}(\nu_p(a), \nu_p(b))$ se hace de manera análoga.

d) Sean $a = p^\alpha a_1$ y $b = p^\beta b_1$, con $\text{mcd}(a_1, p) = 1$ y $\text{mcd}(b_1, p) = 1$. Sin pérdida de generalidad, podemos suponer que $\alpha \geq \beta$. Notemos que $a + b = p^\alpha a_1 + p^\beta b_1 = p^\beta(p^{\alpha-\beta} a_1 + b_1)$, por lo que

$$\begin{aligned} \nu_p(a+b) &= \nu_p(p^\beta(p^{\alpha-\beta} a_1 + b_1)) = \nu_p(p^\beta) + \nu_p(p^{\alpha-\beta} a_1 + b_1) \\ &= \beta + \nu_p(p^{\alpha-\beta} a_1 + b_1), \end{aligned}$$

de donde concluimos que $\nu_p(a+b) \geq \text{mín}(\nu_p(a), \nu_p(b)) = \beta$. Además, si suponemos que $\alpha > \beta$, entonces $\alpha - \beta \geq 1$ y $p \mid p^{\alpha-\beta} a_1$ y, como $\text{mcd}(b_1, p) = 1$, entonces $p \nmid p^{\alpha-\beta} a_1 + b_1$ y, por lo tanto, $\nu_p(p^{\alpha-\beta} a_1 + b_1) = 0$. De lo anterior, si $\nu_p(a) \neq \nu_p(b)$, entonces $\nu_p(a+b) = \text{mín}(\nu_p(a), \nu_p(b))$.

□

Con las pruebas del teorema anterior, podemos extender la definición de valuación p-ádica a los números racionales de la siguiente forma, si $r = \frac{a}{b}$, con a y b enteros, se define $\nu_p(r) = \nu_p\left(\frac{a}{b}\right) = \nu_p(a) - \nu_p(b)$. Siguiendo las ideas de la demostración del teorema anterior, se puede ver que la valuación p-ádica no depende de la representación de r como fracción. De igual forma, es fácil ver que las propiedades a) y d) del teorema 1 se cumplen para cualesquiera números racionales a y b.

Teorema 2. *Un número racional $\frac{a}{b}$ es entero si y solo si $\nu_p\left(\frac{a}{b}\right) \geq 0$ para todo número primo p.*

Demostración. Es claro que si $\frac{a}{b} = n$ es un entero, entonces $\nu_p\left(\frac{a}{b}\right) = \nu_p(n) \geq 0$. Por otro lado, supongamos que $\nu_p\left(\frac{a}{b}\right) \geq 0$ para un primo arbitrario p. Notemos que podemos suponer sin pérdida de generalidad que $\text{mcd}(a, b) = 1$. Se tiene entonces que

$$0 \leq \nu_p\left(\frac{a}{b}\right) = \nu_p(a) - \nu_p(b)$$

y, como $\text{mcd}(a, b) = 1$, entonces a lo más uno de $\nu_p(a)$ o $\nu_p(b)$ es distinto de cero, pero la desigualdad de arriba solo se cumple si $\nu_p(a) \geq 0$ y $\nu_p(b) = 0$, porque como a y b son enteros, entonces $\nu_p(a) \geq 0$ y $\nu_p(b) \geq 0$. Como lo anterior sucede para cualquier primo p, podemos concluir que $b = \pm 1$ y, por lo tanto, $\frac{a}{b} = \pm a$ es un entero. □

Teorema 3 (Legendre)**.** *Para cada entero positivo n y cada número primo p, tenemos que*

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

Demostración. Consideremos un primo p que divide a $n!$. La cantidad de veces que hay un factor p entre los números del 1 al n, se puede contar como $\left\lfloor \frac{n}{p} \right\rfloor$, es decir, estamos contando todos los múltiplos de p. Luego debemos contar los múltiplos de p^2, ya que cada vez que los contamos en el parráfo anterior únicamente tomamos en cuenta uno de los factores p.
Siguiendo con este razonamiento, aunque ya hemos contado dos de los factores p de los números múltiplos de p^3, al contar cuántos múltiplos de p^3 hay entre 1 y n, estaremos contando un tercer factor p para dichos números. Los múltiplos de p^3 entre 1 y n son precisamente $\left\lfloor \frac{n}{p^3} \right\rfloor$. Si repetimos este proceso hasta la k-ésima potencia de p tal que $p^k \leq n < p^{k+1}$, contaremos todos los factores p en $n!$
Cabe notar que si r es tal que $p^r > n$, entonces $\left\lfloor \frac{n}{p^r} \right\rfloor = 0$. Por lo tanto, se tiene

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

□

Con este resultado en mente, revisitamos un problema elemental en la olimpiada de matemáticas.

Ejemplo 2. *Encuentra la cantidad de ceros en los que termina el número* 2022!

Solución. Notemos que la cantidad de ceros al final de un número depende de la cantidad de factores 10, sin embargo como hay mayor cantidad de factores 2 que factores 5 en un factorial, debemos calcular la valuación 5-ádica. Notemos que las primeras potencias de 5 son $5^1 = 5, 5^2 = 25, 5^3 = 125, 5^4 = 625$ y $5^5 = 3125 > 2022$. Entonces,

$$\begin{aligned}\nu_p(2022!) &= \sum_{k=1}^{4} \left\lfloor \frac{2022}{5^k} \right\rfloor = \left\lfloor \frac{2022}{5} \right\rfloor + \left\lfloor \frac{2022}{5^2} \right\rfloor + \left\lfloor \frac{2022}{5^3} \right\rfloor + \left\lfloor \frac{2022}{5^4} \right\rfloor \\ &= 404 + 80 + 16 + 3 = 503.\end{aligned}$$

Por lo que la cantidad de ceros en los que termina el número $2022!$ es 503.

Ejemplo 3 (Olimpiada Austriaca de Matemáticas 2016, Problema 6)**.** *Sea a, b y c tres números enteros tales que $\frac{ab}{c}+\frac{ac}{b}+\frac{bc}{a}$ es un entero. Demuestra que cada uno de los números $\frac{ab}{c}$, $\frac{ac}{b}$ y $\frac{bc}{a}$ es un entero.*

Solución. Como $\frac{ab}{c}+\frac{ac}{b}+\frac{bc}{a}=\frac{(ab)^2+(ac)^2+(bc)^2}{abc}$ es un entero, tenemos que

$$\nu_p(abc)=\nu_p(a)+\nu_p(b)+\nu_p(c)\leq \nu_p((ab)^2+(ac)^2+(bc)^2)$$

para todo número primo p.
Supongamos, sin pérdida de generalidad, que $\nu_p(a)\geq\nu_p(b)\geq\nu_p(c)$. Entonces, $\nu_p(ab)=\nu_p(a)+\nu_p(b)\geq\nu_p(c)$, de donde $\nu_p\left(\frac{ab}{c}\right)\geq 0$. Análogamente, obtenemos que $\nu_p\left(\frac{ac}{b}\right)\geq 0$.
Supongamos que $\nu_p(a)>\nu_p(b)$. Entonces,

$$\begin{aligned}\nu_p(a^2b^2+a^2c^2+b^2c^2)&=\min(\nu_p(a^2b^2),\nu_p(a^2c^2),\nu_p(b^2c^2))=\nu_p(b^2c^2)\\&=2\nu_p(bc)=2(\nu_p(b)+\nu_p(c))\\&\geq\nu_p(a)+\nu_p(b)+\nu_p(c)=\nu_p(abc),\end{aligned}$$

lo cual implica que $\nu_p(b)+\nu_p(c)\geq\nu_p(a)$, por lo que $\nu_p\left(\frac{bc}{a}\right)\geq 0$. Como p es un primo arbitrario y, hemos probado que cada uno de $\nu_p\left(\frac{ab}{c}\right)$, $\nu_p\left(\frac{ac}{b}\right)$ y $\nu_p\left(\frac{bc}{a}\right)$ es mayor o igual que 0, entonces cada uno de $\frac{ab}{c}$, $\frac{ac}{b}$ y $\frac{bc}{a}$ es un número entero.

Ejemplo 4. *Encuentra todas las funciones $f:\mathbb{Z}^+\to\mathbb{Z}^+$ que cumplen las siguientes condiciones:*

1) $f(a)^2+f(b)^2=f(a+b)^2-2^{2011}f(ab)$ para cualesquiera enteros positivos a y b.

2) $f(2010)=2^{2010}\cdot 2010$.

Solución. Sustituyendo $a=b$ en la igualdad de la condición 1), obtenemos que

$$2f(a)^2=f(2a)^2-2^{2011}f(a^2). \tag{1}$$

Si $\nu_2(f(a))=k$ y $\nu_2(f(2a))=l$, entonces $\nu_2(2f(a)^2)=2k+1$ y $\nu_2(f(2a)^2)=2l$. En particular, $\nu_2(2f(a)^2)\neq\nu_2(f(2a)^2)$. Notemos que la ecuación (1) es equivalente a la ecuación

$$2^{2011}f(a^2)=f(2a^2)-2f(a)^2, \tag{2}$$

lo cual implica que $2011\leq\nu_2\left(f(2a^2)-2f(a)^2\right)=\min\{2k+1,2l\}$. En particular, se tiene que $2k+1\geq 2011$, esto es, $k\geq 1005$. Dado que a es un entero positivo arbitrario, lo anterior demuestra que $\nu_2(c)\geq 1005$ para todo entero positivo c. Tomemos a tal que $\nu_2(a)=x\geq 1005$ es mínimo. Se tiene entonces que $\nu_2\left(2^{2011}f(a^2)\right)\geq 2011+x$ y, nuevamente, tomando la valuación 2-ádica en la ecuación (2), se tiene que

$$2011+x\leq\nu_2\left(2^{2011}f(a^2)\right)=\nu_2\left(f(2a)^2-2f(a)^2\right)=\min\{2x+1,2l\}.$$

De lo anterior podemos concluir que $2011 + x \leq 2x + 1$, lo que equivale a $x \geq 2010$. Por lo tanto, hemos probado que $2^{2010} \mid f(n)$ para todo entero positivo n.
Si hacemos $b = 1$ en la ecuación 1) del problema y despejamos $f(a+1)^2$, obtenemos

$$f(a)^2 < f(a)^2 + f(1)^2 + 2^{2011} f(a) = f(a+1)^2,$$

de donde se sigue que la función es creciente, esto es, $f(a) < f(b)$ si y solo si $a < b$. Con esto y, usando que $2^{2010} \mid f(n)$, podemos concluir que $2^{2010} \cdot n \leq f(n)$, pero la segunda condición del problema nos dice que $f(2010) = 2^{2010} \cdot 2010$, lo cual a la vez nos dice que $f(i) = 2^{2010} i$ para todo $1 \leq i \leq 2010$, ya que es la única forma de que se cumpla que $2^{2010} i \leq f(i) < 2^{2010}(i+1)$ para todo $1 \leq i \leq 2009$.
Finalmente, probaremos por inducción que $f(n) = 2^{2010} n$ para todo entero positivo n. Tomemos como base $n = 1$ y supongamos que $f(i) = 2^{2010} i$ para todo $1 \leq i \leq n-1$. Tomemos $a = 1$ y $b = n-1$ en la igualdad de la condición 1). De esta forma obtenemos

$$f(1)^2 + f(n-1)^2 = f(n)^2 - 2^{2011} f(n-1).$$

Despejando $f(n)^2$ y usando la hipótesis de inducción, tenemos

$$(2^{2010} \cdot 1)^2 + (2^{2010}(n-1))^2 + 2^{2011}(2^{2010}(n-1)) = f(n)^2.$$

Factorizando 2^{4020} y reagrupando, obtenemos que $2^{2010} n = f(n)$.
Finalmente, es fácil ver que dicha función cumple las condiciones del problema.

Ejemplo 5 (Olimpiada regional zona centro, México, 2019)**.** *Determina todos los enteros positivos m con la siguiente propiedad: Si d es un entero positivo menor o igual que m y no es coprimo con m, entonces existen enteros positivos $a_1, a_2, \ldots, a_{2019}$, todos ellos coprimos con m, tales que*

$$m + a_1 d + a_2 d^2 + \cdots + a_{2019} d^{2019}$$

es una potencia perfecta.

Solución. Supongamos que m cumple la propiedad. Como $\text{mcd}(d, m) \neq 1$, entonces existe un primo p que divide a ambos números d y m. Notemos que $\nu_p(a_i d^i) = \nu_p(d^i)$, porque $\text{mcd}(a_i, m) = 1$ y, por lo tanto, cada a_i es primo relativo con cualquier divisor de m. Más aún, $\nu_p(d^i) \leq \nu_p(d^j)$ si y solo si $0 < i \leq j$. Juntando las observaciones anteriores y usando la propiedad d) del Teorema 1, tenemos que

$$\nu_p\big(a_1 d + a_2 d^2 + \cdots + a_{2019} d^{2019}\big) = \nu_p(d).$$

Notemos que lo anterior implica que si $\nu_p(m) > \nu_p(d)$, entonces

$$\nu_p\big(m + a_1 d + a_2 d^2 + \cdots + a_{2019} d^{2019}\big) = \nu_p(d)$$

y, si $\nu_p(m) < \nu_p(d)$, entonces

$$\nu_p\big(m + a_1 d + a_2 d^2 + \cdots + a_{2019} d^{2019}\big) = \nu_p(m).$$

Como d puede ser cualquier entero que no sea primo relativo con m y $p \mid m$, podemos elegir $p = d$ y concluir que si $\nu_p(m) > 1$, entonces

$$\nu_p\big(m + a_1 p + a_2 p^2 + \cdots + a_{2019} p^{2019}\big) = \nu_p(p) = 1,$$

por lo que la suma $m + a_1 p + a_2 p^2 + \cdots + a_{2019} p^{2019}$ no podría ser una potencia perfecta. Es decir, hemos visto que si m tiene algún divisor primo p, tal que $p^2 \mid m$, entonces, eligiendo $d = p$, obtenemos un entero cuya valuación p-ádica es 1 y, por lo tanto, no puede ser una potencia perfecta. Con esto concluimos que si m cumple la propiedad buscada, entonces m es de la forma $m = p_1 p_2 \cdots p_k$, donde los p_i's son primos distintos.
De lo anterior se sigue que si m no es primo, entonces es un producto de al menos dos primos p y q con $p < q$. De esta forma, tenemos que $p^2 < pq \leq m$. Tomando $d = p^2$ y usando el hecho de que $1 = \nu_p(m) < \nu_p(p^2)$, obtenemos que

$$\nu_p\big(m + a_1 (p^2) + a_2 (p^2)^2 + \cdots + a_{2019} (p^2)^{2019}\big) = \nu_p(m) = 1,$$

por lo que nuevamente el número obtenido no sería una potencia perfecta. Esto contradice el hecho de que m puede tener más de un factor primo.
Finalmente, mostraremos que si $m = p$, es primo, entonces cumple la propiedad buscada. Como el único número menor o igual a p que no es primo relativo con p es el mismo p, basta mostrar que para $d = p$ se pueden elegir las a_i's de forma que se cumpla la propiedad. Para ello tomaremos $a_i = p - 1$. De esta forma obtenemos que

$$\begin{aligned} & p + (p-1)p + (p-1)p^2 + \cdots + (p-1)p^{2019} \\ &= p + p^2 - p + p^3 - p^2 + \cdots + p^{2020} - p^{2019} \\ &= p^{2020}, \end{aligned}$$

que es una potencia perfecta, por lo que los valores de m que satisfacen la condición del problema son los números primos.

Ejemplo 6 (Examen selectivo de Perú para la EGMO, 2021)**.** *Determina todos los enteros positivos b para los cuales existe un entero positivo a con las siguientes propiedades:*

1) a no es un divisor de b,

2) a^a es un divisor de b^b.

Solución. Aunque es claro que la valuación p-ádica está involucrada, no siempre es lo más conveniente usar dicha notación, en particular, en este problema usaremos la notación usual para la descomposición canónica de un entero. Por un lado, si a y b cumplen las condiciones, entonces los primos que dividen a a también dividen a b. Sin embargo, para algún primo p tal que $p \mid a$ y $p \mid b$, se debe cumplir que $\nu_p(a) > \nu_p(b)$. Supongamos que $p^\alpha || a$ y que $p^\beta || b$. Más aún, sean $a = p^\alpha T$ y $b = p^\beta S$, con $\text{mcd}(T, p) = 1 = \text{mcd}(S, p)$. Si nos fijamos solamente en el primo p, las condiciones del problema se traducen en

1) $\alpha > \beta$,

2) $\alpha T p^{\alpha} \leq \beta S p^{\beta}$.

En particular, podemos notar que si para b existe un entero positivo a tal que $a \nmid b$ pero $a^a \mid b^b$, entonces se puede elegir una potencia de un primo, digamos p^{α}, en lugar de a, de tal forma que p^{α} y b cumplen las condiciones del problema. Ahora supongamos que $b = p^{\beta} S$ y $a = p^{\alpha}$ cumplen que $p^{\alpha} \nmid b$ y $(p^{\alpha})^{(p^{\alpha})} \mid b^b$. Como $\alpha \geq \beta + 1$, podemos cambiar α por $\beta + 1$ y los números $a = p^{\beta+1}$ y b siguen cumpliendo las condiciones.
Con lo anterior hemos probado que si para cierto entero positivo b existe un entero positivo a tal que $a \nmid b$ y $a^a \mid b^b$, entonces, para el mismo b, se puede elegir $a = p^{\beta+1}$, donde p es un primo tal que $p^{\beta} || b$.
Ahora notemos que dicho par cumple las condiciones si y solo si $(\beta+1)p^{\beta+1} \leq \beta p^{\beta} S$, lo cual sucede si y solo si $(\beta+1)p \leq \beta S$. En particular, si p es el menor divisor primo de b y S es el producto de al menos dos primos, entonces $S \geq 2p$ y $(\beta+1)p \leq 2\beta p \leq \beta S$.
Por lo tanto, hemos probado que si b es el producto de al menos tres números primos y al menos dos de ellos son distintos, entonces existe un entero a que satisface las condiciones.
Ahora notemos que si $b = p^{\beta}$, entonces no puede existir un número a que no divida a b pero que una de sus potencias sí divida a b^b, ya que los divisores de p^{β} son de la forma p^{α}, pero si $a = p^{\alpha}$ no divide a p^{β}, entonces $\alpha > \beta$, lo cual implica que $a > b$ y, por lo tanto, $a^a > b^a > b^b$.
Solo hace falta resolver el caso cuando $b = pq$, con p y q primos distintos. Como vimos anteriormente, si $p < q$, entonces $a = p^2$ debería cumplir que $a \nmid b$ pero $a^a \mid b^b$. Lo anterior es equivalente a $2p^2 \leq pq$, lo cual es cierto si y solo si $2p \leq q$.
Concluimos que los enteros que cumplen lo buscado son todos los enteros positivos que no son potencias de primos ni son de la forma pq con p y q primos tales que $p < q < 2p$.

Ejemplo 7 (Lista corta ELMO 2017, N3)**.** *Para cada entero $C > 1$ determina si existe una sucesión de enteros positivos distintos $a_1, a_2, a_3, \ldots$ tales que para todo $k \geq 1$, $a_{k+1}^k \mid C^k a_1 a_2 \cdots a_k$.*

Solución. Demostraremos que no existe tal sucesión. Supongamos, por contradicción, que hay una sucesión que cumple las condiciones del problema. Primero demostraremos por inducción que si $p \mid a_k$, entonces $p \mid Ca_1$. El resultado es claramente cierto para a_2, ya que $a_2^2 \mid Ca_1$. Ahora, supongamos que el resultado es cierto para todo $1 \leq i \leq k$. Si $p \mid a_{k+1}$, entonces $p \mid C^k a_1 a_2 \cdots a_k$, por lo que p divide a alguno de los a_i's, con $1 \leq i \leq k$, o p divide a C y el resultado se sigue de la hipótesis de inducción.
Con lo anterior podemos concluir que los a_i's tienen como factores primos solo a un número finito de primos, digamos $p_1, p_2, \ldots, p_t$.
Sea p un número primo y sean $\nu_p(C) = c$, $x_i = \nu_p(a_i)$ para cada $i \geq 1$. La divisibilidad planteada se traduce en la siguiente desigualdad en la valuación p-ádica:

$$kx_{k+1} \leq kc + x_1 + \cdots + x_k.$$

Para cada entero $n \geq 2$, definimos

$$H_n = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n-1} + \frac{1}{n}.$$

Demostraremos el siguiente lema.

Lema 1. $x_n \leq cH_{n-1} + x_1$ para cada entero $n \geq 2$.

Demostración. Primero notemos que cambiar x_i por $x_i - r$, no cambia la relación

$$kx_{k+1} \leq kc + x_1 + \cdots + x_k, \tag{3}$$

por lo que, sin pérdida de generalidad, podemos suponer que $x_1 = 0$. Con esto en mente, usaremos inducción fuerte. El caso base $n = 2$ se sigue de la desigualdad (3): $x_2 \leq c + x_1 = cH_1 + x_1$. Ahora suponemos el resultado cierto para todo $1 \leq i \leq n-1$. Entonces,

$$\begin{aligned}(n-1)c + x_1 + \cdots + x_{n-1} &\leq (n-1)c + c\left(1 + \left(1 + \frac{1}{2}\right) + \cdots + \left(1 + \cdots + \frac{1}{n-2}\right)\right) \\ &= c\left(1 + (n-2) + \frac{n-2}{1} + \frac{n-3}{2} + \cdots + \frac{1}{n-2}\right) \\ &= c\left(\frac{n-1}{1} + \frac{n-1}{2} + \cdots + \frac{n-1}{n-2} + \frac{n-1}{n-1}\right) \\ &= c(n-1)H_{n-1}.\end{aligned}$$

□

Ahora fijemos N en la desigualdad $x_N \leq cH_N + x_1$ y sea $a = cH_N + x_1$. Tenemos entonces que $x_N \leq a$. Notemos que

$$H_{N+N} - H_N = \frac{1}{N+1} + \frac{1}{N+2} + \cdots + \frac{1}{N+N} < 1.$$

Con esto y la desigualdad del Lema 1, existen $N(k+1)$ términos de los x_i's menores o iguales que $a + ck$.
Ahora demostraremos el siguiente lema.

Lema 2. Para cualquier número d, existen números N y k tales que $d < \frac{N(k+1)}{a+ck}$.

Demostración. La desigualdad es equivalente a $da + dck < N(k+1)$. Si tomamos $N > dc$ y aumentamos k en 1, el lado izquierdo aumenta en dc, mientras que el lado derecho aumenta en N, por lo se obtiene la desigualdad para k suficientemente grande. □

El Lema 2 implica que el número $\frac{n}{cH_n + x_1}$ es arbitrariamente grande. Recordando que $x_i = \nu_p(a_i)$, lo anterior se traduce en que para un primo fijo p, se puede elegir una cantidad arbitrariamente grande de los a_i's tales que su valuación p-ádica es igual. Finalmente, recordando que existen solo t primos que dividen a los a_i's, por el principio de las casillas existen a_i y a_j tales que su valuación p-ádica es igual para todos los primos p, pero esto implica que $a_i = a_j$, lo cual es una contradicción.

Teorema 4 (Lifting the Exponent Lemma, LTE)**.** *a) Sea p un primo impar que no divide a los enteros a y b. Si $p \mid a - b$ y n es un entero no negativo, entonces*

$$\nu_p(a^n - b^n) = \nu_p(a - b) + \nu_p(n).$$

b) Sea p un primo impar que no divide a los enteros a y b. Si $p \mid a+b$ y n es un entero positivo impar, entonces

$$\nu_p(a^n + b^n) = \nu_p(a+b) + \nu_p(n).$$

c) Sean $p = 2$, n un entero par y a, b enteros tales que $p \nmid a$ y $p \nmid b$.

1) Si $4 \mid a-b$, entonces $\nu_2(a^n - b^n) = \nu_2(a-b) + \nu_2(n)$.

2) Si $4 \mid a+b$, entonces $\nu_2(a^n + b^n) = \nu_2(a+b) + \nu_2(n)$.

Demostración. a) Haremos inducción sobre $\nu_p(n)$. Primero haremos el caso en el que $\nu_p(n) = 0$. Notemos que $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + b^{n-1})$, por lo que

$$\begin{aligned}\nu_p(a^n - b^n) &= \nu_p((a-b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + b^{n-1})) \\ &= \nu_p(a-b) + \nu_p(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + b^{n-1}).\end{aligned}$$

Analicemos el segundo término módulo p. Como $a \equiv b \pmod p$, tenemos que $a^{n-k}b^{k-1} \equiv a^{n-1} \pmod p$, lo cual implica que

$$a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + b^{n-1} \equiv na^{n-1} \pmod p.$$

Como a y n son primos relativos con p, concluimos que $\nu_p(na^{n-1}) = 0$ y, por lo tanto, $\nu_p(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + b^{n-1}) = 0$, de donde se sigue que $\nu_p(a^n - b^n) = \nu_p(a-b) + \nu_p(n)$.

Ahora supongamos que $n = p$. Como $p \mid a-b$, se tiene entonces que $b = a + p^k b_1$, donde $\text{mcd}(b_1, p) = 1$ y, además, $\nu_p(a-b) = \nu_p(-p^k b_1) = k$. Usando el teorema del binomio de Newton, tenemos:

$$\begin{aligned}a^p - b^p &= a^p - (a + p^k b_1)^p \\ &= a^p - \binom{p}{0}a^p - \binom{p}{1}a^{p-1}p^k b_1 - \binom{p}{2}a^{p-2}p^{2k}b_1^2 - \cdots - \binom{p}{p}p^{pk}b_1^p \\ &= -pa^{p-1}p^k b_1 - \binom{p}{2}a^{p-2}p^{2k}b_1^2 - \cdots - \binom{p}{p}p^{pk}b_1^p.\end{aligned}$$

De lo anterior se sigue que

$$\nu_p(a^p - b^p) = \nu_p\left(-pa^{p-1}p^k b_1 - \binom{p}{2}a^{p-2}p^{2k}b_1^2 - \cdots - \binom{p}{p}p^{pk}b_1^p\right).$$

Notemos que p^{2k+1} divide a todos los términos, excepto a $-pa^{p-1}p^k b_1$, por lo que

$$\begin{aligned}\nu_p(a^p - b^p) &= \nu_p\left(-pa^{p-1}p^k b_1 - \binom{p}{2}a^{p-2}p^{2k}b_1^2 - \cdots - \binom{p}{p}p^{pk}b_1^p\right) \\ &= \nu_p\left(pa^{p-1}p^k b_1\right) = \nu_p(p) + \nu_p(a^{p-1}) + \nu_p(p^k) + \nu_p(b_1) \\ &= \nu_p(p) + 0 + \nu_p(p^k) + 0 = \nu_p(p) + k \\ &= \nu_p(p) + \nu_p(a-b).\end{aligned}$$

Finalmente, supongamos que el resultado es cierto para $\nu_p(n) = m - 1$. Sea n tal que $\nu_p(n) = m$ y escribamos $n = p^m c$, con mcd$(c, p) = 1$. Utilizando lo anterior, tenemos que

$$\begin{aligned}\nu_p(a^n - b^n) = \nu_p(a^{p^m c} - b^{p^m c}) &= \nu_p\left((a^{p^{m-1}c})^p - (b^{p^{m-1}c})^p\right) \\ &= \nu_p(p) + \nu_p(a^{p^{m-1}c} - b^{p^{m-1}c}).\end{aligned}$$

Pero, por la hipótesis de inducción se tiene

$$\begin{aligned}\nu_p(p) + \nu_p(a^{p^{m-1}c} - b^{p^{m-1}c}) &= \nu_p(p) + \nu_p(p^{m-1}c) + \nu_p(a-b) \\ &= 1 + m - 1 + \nu_p(a-b) \\ &= m + \nu_p(a-b) \\ &= \nu_p(n) + \nu_p(a-b).\end{aligned}$$

b) La demostración es análoga a la anterior, usando ahora la factorización $a^n + b^n = (a+b)(a^{n-1} - a^{n-2}b + a^{n-3}b^2 - \cdots + b^{n-1})$, válida para n impar.

c) En los casos anteriores, supusimos que p es un primo impar. Notemos que en este caso, $p = 2$.

1) Al igual que en la prueba de la primera parte de este lema, si mcd$(p, n) = 1$, entonces $\nu_p(a^n - b^n) = \nu_p(a-b)$. Así, tomamos $n = 2^k m$ con mcd$(m, 2) = 1$, por lo que $\nu_2(a^{(2^k)^m} - b^{(2^k)^m}) = \nu_2(a^{2^k} - b^{2^k})$.
Notemos que $a^{2^k} - b^{2^k} = (a^{2^{k-1}} + b^{2^{k-1}})(a^{2^{k-2}} + b^{2^{k-2}}) \cdots (a+b)(a-b)$ y, como $a - b \equiv 0 \pmod 4$, resulta que $a \equiv b \pmod 4$, lo cual implica que $a^{2^t} \equiv b^{2^t} \pmod 4$ y $a^{2^t} + b^{2^t} \equiv 2a^{2^t} \not\equiv 0 \pmod 4$, esta última congruencia se debe a que $2 \nmid a$. Esto implica que $\nu_2(a^{2^t} - b^{2^t}) = 1$ para todo t. Entonces,

$$\begin{aligned}\nu_p(a^{2^k} - b^{2^k}) &= \nu_p((a^{2^{k-1}} - b^{2^{k-1}})(a^{2^{k-2}} - b^{2^{k-2}}) \cdots (a-b)(a+b)) \\ &= \nu_p(a^{2^{k-1}} - b^{2^{k-1}}) + \cdots + \nu_p(a-b) + \nu_p(a+b) \\ &= \nu_p(a-b) + k = \nu_p(a-b) + \nu_p(n).\end{aligned}$$

2) La demostración es análoga a la anterior.

□

Ejemplo 8 (Lista Corta, Olimpiada de Matemáticas de los Balcanes 2017, N3)**.** *Demuestra que para todo entero positivo n, existe un entero m tal que $7^n \mid 3^m + 5^m - 1$.*

Solución. Demostraremos que para cada entero positivo n, el número $m = 7^{n-1}$ cumple. Utilicemos la segunda versión de LTE con $p = 7$. Tenemos que

$$\begin{aligned}\nu_7(3^m + 4^m) = \nu_7(3+4) + \nu_7(m) = \nu_7(3^{7^{n-1}} + 4^{7^{n-1}}) &= \nu_7(3+4) + \nu_7(7^{n-1}) \\ = 1 + n - 1 = n.\end{aligned}$$

Notemos que esto implica que $3^{7^{n-1}} + 4^{7^{n-1}} \equiv 0 \pmod{7^n}$. Utilizando de nuevo la segunda versión de LTE con $p = 7$ obtenemos que

$$\begin{aligned}\nu_7(5^m + 2^m) &= \nu_7(5+2) + \nu_7(m) = \nu_7(5^{7^{n-1}} + 2^{7^{n-1}}) = \nu_7(5+2) + \nu_7(7^{n-1}) \\ &= 1 + n - 1 = n.\end{aligned}$$

Esto implica que $5^{7^{n-1}} + 2^{7^{n-1}} \equiv 0 \pmod{7^n}$. Sumando ambas congruencias obtenemos que $3^{7^{n-1}} + 4^{7^{n-1}} + 5^{7^{n-1}} + 2^{7^{n-1}} \equiv 0 \pmod{7^n}$, esto es, $3^{7^{n-1}} + 5^{7^{n-1}} \equiv -(4^{7^{n-1}} + 2^{7^{n-1}}) \pmod{7^n}$, de donde obtenemos que

$$3^{7^{n-1}} + 5^{7^{n-1}} - 1 \equiv -(4^{7^{n-1}} + 2^{7^{n-1}} + 1) \pmod{7^n}.$$

Ahora, módulo 7 tenemos que $2^0 \equiv 1$, $2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 1$, etc. Como $7^{n-1} \equiv 1^{n-1} \equiv 1 \pmod 3$, tenemos que $2^{7^{n-1}} - 1 \equiv 1 \pmod 7$, lo cual implica que

$$\begin{aligned}4^{7^{n-1}} + 2^{7^{n-1}} + 1 &\equiv (4^{7^{n-1}} + 2^{7^{n-1}} + 1)(2^{7^{n-1}} - 1) \\ &\equiv 8^{7^{n-1}} + 4^{7^{n-1}} + 2^{7^{n-1}} - 4^{7^{n-1}} - 2^{7^{n-1}} - 1 \\ &\equiv 8^{7^{n-1}} - 1 \\ &\equiv 0 \pmod 7.\end{aligned}$$

Utilizando LTE con $p = 7$ una vez más obtenemos que

$$\nu_7(8^{7^{n-1}} - 1) = \nu_7(8-1) + \nu_7(7^{n-1}) = 1 + n - 1 = n.$$

Por lo que, $3^{7^{n-1}} + 5^{7^{n-1}} - 1 \equiv 0 \pmod{7^n}$.

Ejemplo 9 (IMO 2019, Problema 2)**.** *Encuentra todos los pares (k, n) de enteros positivos tales que $k! = (2^n - 1)(2^n - 2)(2^n - 4) \cdots (2^n - 2^{n-1})$.*

Solución. Notemos que $\nu_2(2^n - 2^k) = k$, por lo que

$$\begin{aligned}&\nu_2((2^n - 1)(2^n - 2)(2^n - 4) \cdots (2^n - 2^{n-1})) \\ &= \nu_2(2^n - 1) + \nu_2(2^n - 2) + \cdots + \nu_2(2^n - 2^{n-1}) \\ &= 0 + 1 + 2 + \cdots + n - 1 \\ &= \frac{(n-1)n}{2}.\end{aligned}$$

Por el teorema de Legendre, tenemos que

$$\nu_2(k!) = \sum_{m=1}^{\infty} \left\lfloor \frac{k}{2^m} \right\rfloor \leq \sum_{m=1}^{\infty} \frac{k}{2^m} = k \sum_{m=1}^{\infty} \frac{1}{2^m} < k.$$

Con esto concluimos que $k > \dfrac{(n-1)n}{2}$.
Ahora analizando $p = 3$, obtenemos que

$$\nu_3(2^n - 2^k) = \nu_3(2^k(2^{n-k} - 1)) = \nu_3(2^k) + \nu_3(2^{n-k} - 1) = \nu_3(2^{n-k} - 1).$$

Además, es fácil ver que $2^n \equiv 1 \pmod 3$ si n es par y $2^n \equiv 2 \pmod 3$ si n es impar. Luego, si $n-k$ es impar, $\nu_3(2^{n-k}-1) = 0$ y, si $n-k = 2t$ es par, podemos utilizar LTE para ver que $\nu_3(2^{n-k}-1) = \nu_3(2^{2t}-1) = \nu_3(4^t-1) = \nu_3(4-1)+\nu_3(t) = 1+\nu_3(t)$. Por lo que tomando la valuación 3-ádica de la multiplicación, tenemos que

$$\begin{aligned}
&\nu_3((2^n-1)(2^n-2)(2^n-4)\cdots(2^n-2^{n-1})) \\
&= \nu_3(2^n-1) + \nu_3(2^n-2) + \cdots + \nu_3(2^n-2^{n-1}) \\
&= \sum_{t=1}^{\lfloor \frac{n}{2} \rfloor} 1 + \nu_3(t) = \left\lfloor \frac{n}{2} \right\rfloor + \nu_3\left(\left\lfloor \frac{n}{2} \right\rfloor !\right) \\
&= \left\lfloor \frac{n}{2} \right\rfloor + \left\lfloor \frac{\lfloor \frac{n}{2} \rfloor}{3} \right\rfloor + \left\lfloor \frac{\lfloor \frac{n}{2} \rfloor}{3^2} \right\rfloor + \cdots \\
&< \frac{n}{2} + \frac{n}{6} + \frac{n}{18} + \cdots \\
&= \frac{n}{2}\left(\sum_{i=0}^{\infty} \frac{1}{3^i}\right) = \frac{n}{2}\left(\frac{1}{1-\frac{1}{3}}\right) = \frac{3n}{4}.
\end{aligned}$$

Además, sabemos que $\nu_3(k!) \geq \lfloor \frac{k}{3} \rfloor > \frac{k}{3} - 1$. Luego, $\frac{k}{3} - 1 < \nu_3(k!) < \frac{3n}{4} < n$, lo cual implica que $\frac{(n-1)n}{2} < k < 3n+3$. Así, $n(n-1) < 6(n+1)$, esto es,

$$n^2 - 7n - 6 < 0,$$

de donde se sigue que $n < 7$. Finalmente, revisando los casos donde $n \leq 6$, obtenemos que las únicas soluciones son $(1,1)$ y $(3,2)$.

Ejercicios

1) Considera el conjunto L que contiene a los enteros $1, 2, \ldots, n$, para algún entero positivo n. Sea 2^k la máxima potencia de 2 que pertenece a L. Prueba que 2^k no es divisor de ningún otro entero en L. Usa lo anterior para probar que la suma

$$\sum_{j=1}^{n} \frac{1}{j}.$$

no es un entero si $n > 1$.

2) Sea $p > 2013$ un primo. Sean a y b enteros positivos tales que $p \mid a+b$ pero $p^2 \nmid a+b$. Si $p^2 \mid a^{2013}+b^{2013}$, encuentra el número de enteros positivos $n \leq 2013$ tales que $p^n \mid a^{2013}+b^{2013}$.

3) (OMM 2005, Concurso Nacional, Problema 3) Determina todos los pares (a,b) de enteros diferentes de 0 para los cuales es posible encontrar un entero positivo x y un entero y de tal forma que x es primo relativo con b y en la siguiente lista hay una infinidad de enteros:

$$\frac{a+xy}{b}, \frac{a+xy^2}{b^2}, \frac{a+xy^3}{b^3}, \ldots, \frac{a+xy^n}{b^n}, \ldots$$

4) (Lista corta IMO 2015, N1) Determina todos los enteros positivos M tales que la sucesión $a_0, a_1, a_2, \ldots$ definida por $a_0 = M + \frac{1}{2}$ y

$$a_{k+1} = a_k \lfloor a_k \rfloor \quad \text{para } k = 0, 1, 2, \ldots$$

contiene al menos un entero.

5) (IMO 2018, Problema 5) Sean a_1, a_2, $\ldots$ una sucesión infinita de enteros positivos. Suponga que existe un entero $N > 1$ tal que, para cada $n \geq N$, 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. Demuestra que existe un entero M tal que $a_m = a_{m+1}$ para todo $m \geq M$.

6) (EGMO 2022, Problema 2) Sea $\mathbb{N} = \{1, 2, 3, \ldots\}$ el conjunto de los enteros positivos. Encuentra todas las funciones $f : \mathbb{N} \to \mathbb{N}$ tales que para cualesquiera enteros positivos a y b, se satisfacen las siguientes condiciones:
(1) $f(ab) = f(a)f(b)$, y
(2) al menos dos de los números $f(a)$, $f(b)$ y $f(a + b)$ son iguales.

7) (Olimpiada China de Matemáticas 2018, Problema 1) Sean n un entero positvo y A_n el conjunto de los primos p tales que existen enteros positivos a, b que satisfacen que $\frac{a+b}{p}$ y $\frac{a^n+b^n}{p^2}$ son ambos enteros coprimos con p. Si A_n es finito, $f(n)$ denota $|A_n|$.

a) Prueba que A_n es finito si y solo si $n \neq 2$.

b) Sean m, k enteros positovs impares y sea d su máximo común divisor. Demuestra que

$$f(d) \leq f(k) + f(m) - f(km) \leq 2f(d).$$

8) (APMO 2017, Problema 4) Llamamos a un número racional r poderoso si r puede expresarse en la forma $\frac{p^k}{q}$ para algunos enteros positivos p y q primos relativos y algún entero $k > 1$. Sean a, b, c números racionales positivos tales que $abc = 1$. Supón que existen enteros positivos x, y, z tales que $a^x + b^y + c^z$ es un entero. Prueba que a, b y c son poderosos.

9) (IMO 2022, Problema 5) Determina todas las ternas (a, b, p) de enteros positivos, con p primo, que satisfacen $a^p = b! + p$.

Bibliografía

1) I. Niven, H. S. Zuckerman, H. L. Montgomery. *An introduction to the Theory of Numbers*. 5th edition, John Wiley & Sons, 1991.

2) Justin Stevens. *Olympiad number theory through challenging problems*. https://s3.amazonaws.com/aops-cdn.artofproblemsolving.com/resources/articles/olymp

3) M. L. Pérez Seguí. *Teoría de números*. Cuadernos de Olimpiadas de Matemáticas, Instituto de Matemáticas, UNAM, 2004.