Orden de un número

Por Carlos Jacob Rubio Barrios y Emerson Lucas Soriano Pérez

Nivel Avanzado

Para explicar de manera sencilla la motivación de este artículo, diremos que un entero positivo es *bueno* si todos sus dígitos son iguales a 9. Por ejemplo, los números $9;\ 999$ y 9999 son números buenos.

Se observa que 3 posee un múltiplo bueno, ya que 9 es múltiplo de 3. El número 7 también posee un múltiplo bueno, pues 999999 es múltiplo de 7. En general, si n es coprimo con 10, entonces, por el teorema de Euler[2], tenemos que $10^{\phi(n)} \equiv 1 \pmod{n}$, lo cual significa que

$$n \mid \underbrace{999\ldots99}_{\phi(n) \text{ veces}}.$$

Este hecho nos garantiza que cualquier entero positivo n que es coprimo con 10 posee un múltiplo bueno. Además, es fácil notar que si n posee un múltiplo bueno, entonces posee infinitos múltiplos buenos, pero, ¿cuál de todos los múltiplos buenos tiene la menor cantidad de dígitos? En este artículo mostraremos cómo calcular la cantidad de dígitos de ese menor múltiplo bueno de n.

Para mayor facilidad, mencionaremos algunas notaciones usadas a lo largo de este escrito.

- $a \mid b$ significa que a divide a b, a es divisor de b o que b es múltiplo de a.
- Para cada entero positivo n, $\phi(n)$ denota el número de enteros positivos menores o iguales que n, que son coprimos con n. Por ejemplo, si p es un número primo, es fácil demostrar que $\phi(p) = p - 1$ y $\phi(p^k) = p^{k-1}(p-1)$ para todo entero positivo k.

[2]El teorema de Euler afirma que si a y n son enteros positivos coprimos, entonces $a^{\phi(n)} \equiv 1 \pmod{n}$.

- Si p es un número primo y a es un entero positivo, entonces $\nu_p(a)$ denota al mayor entero no negativo tal que $p^{\nu_p(a)} \mid a$.

Teoría y Ejemplos

Para cada par a y n de enteros positivos coprimos, sea $A(a,n)$ el conjunto de los números naturales k tales que $a^k \equiv 1 \pmod{n}$, esto es,

$$A(a,n) = \left\{k \in \mathbb{N} \mid a^k \equiv 1 \pmod{n}\right\}.$$

Ahora, consideremos la siguiente sucesión de números:

$$a^1, a^2, a^3, \ldots, a^n, a^{n+1}.$$

Por el principio de las casillas, existen índices $i > j$ tales que $a^i \equiv a^j \pmod{n}$. Como a y n son coprimos, se tiene que $a^{i-j} \equiv 1 \pmod{n}$. Por lo tanto, $i-j$ es un elemento de $A(a,n)$, y en consecuencia, $A(a,n)$ es un conjunto no vacío de números naturales. Luego, $A(a,n)$ tiene un elemento mínimo. A dicho elemento mínimo se le conoce como *orden de a módulo n* y se denota por $ord_n a$.

Teorema 1. *Si a, n y k son enteros positivos tales que $a^k \equiv 1 \pmod{n}$, entonces $ord_n a \mid k$.*

Demostración. Sea $d = \text{ord}_n a$. Por el algoritmo de la división, existen enteros no negativos q y r tales que $k = dq + r$, donde $0 \leq r < d$. Como $a^d \equiv 1 \pmod{n}$, tenemos que

$$1 \equiv a^k = a^{dq+r} = (a^d)^q \cdot a^r \equiv a^r \pmod{n}.$$

Si $r > 0$, entonces r es elemento de $A(a,n)$, y como d es el elemento mínimo de $A(a,n)$, tenemos que $d \leq r$. Pero esto es una contradicción, pues $r < d$. Por lo tanto, $r = 0$, y en consecuencia $d \mid k$. □

Teorema 2. *Si a y n son enteros positivos coprimos, entonces $ord_n a \mid \phi(n)$.*

Demostración. Si a y n son coprimos, entonces $a^{\phi(n)} \equiv 1 \pmod{n}$ por el teorema de Euler. Luego, por el Teorema 1, se sigue que $\text{ord}_n a \mid \phi(n)$. □

Ejemplo 1. *Encontrar el menor múltiplo de 19 cuyos dígitos son todos iguales a 1.*

Solución. Sea N el menor múltiplo de 19 conformado únicamente por dígitos 1 y sea m la cantidad de dígitos de N. Como $19 \mid 9N$ y $9N = 10^m - 1$, se tiene que $10^m \equiv 1 \pmod{19}$. Luego, $m = \text{ord}_{19}10$, pues N es mínimo.
Para hallar N, básicamente tenemos que encontrar m, es decir, todo se reduce a calcular el valor de $\text{ord}_{19}10$. En efecto, por el Teorema 2 tenemos que $\text{ord}_{19}10 \mid 18$ (pues $\phi(19) = 18$), y, en consecuencia, $\text{ord}_{19}10 \in \{1,\ 2,\ 3,\ 6,\ 9,\ 18\}$. Como

$$10 - 1 = 9 \equiv 9 \pmod{19},$$
$$10^2 - 1 = 99 \equiv 4 \pmod{19},$$
$$10^3 - 1 = 999 \equiv 11 \pmod{19},$$
$$10^6 - 1 = 999\,999 \equiv 10 \pmod{19},$$
$$10^9 - 1 = 999\,999\,999 \equiv -1 \pmod{19},$$

concluimos que $10^m \not\equiv 1 \pmod{19}$ para $m = 1, 2, 3, 6$ y 9. Por lo tanto, $\text{ord}_{19}10 = 18$, y así $N = \underbrace{111\ldots11}_{18 \text{ veces}}$. □

Ejemplo 2. *Hallar el valor de* $ord_{101}2$.

Demostración. Sea $d = \text{ord}_{101}2$. Como 101 es primo, tenemos que $\phi(101) = 100$ y, por el teorema de Euler, $2^{100} \equiv 1 \pmod{101}$. Luego, por el Teorema 1 se sigue que $d \mid 100$, esto es, $d \in \{1, 2, 4, 5, 10, 20, 25, 50, 100\}$. Como $0 < 2^d < 101$ si $d = 1, 2, 4, 5$, se sigue que d no puede ser igual a ninguno de estos números. Además, como

$$\begin{aligned} 2^{10} &\equiv 14 \pmod{101}, \\ 2^{20} &\equiv 95 \pmod{101}, \\ 2^{25} &\equiv 10 \pmod{101}, \\ 2^{50} &\equiv 100 \pmod{101}, \end{aligned}$$

se sigue que d tampoco puede ser igual a $10, 20, 25$ o 50. Por lo tanto, $d = 100$. □

Ejemplo 3. *Encontrar el menor entero positivo* n *tal que* 2^{2016} *divide a* $17^n - 1$.

Solución. El problema equivale a determinar el valor de $n = \text{ord}_{2^{2016}}17$. Por el teorema de Euler y el Teorema 1, tenemos que

$$n \mid \phi(2^{2016}) = 2^{2015}.$$

Así, $n = 2^k$, para algún $k \in \{1, 2, 3, \ldots, 2015\}$. Tenemos que $2^{2016} \mid 17^{2^k} - 1$. Notemos lo siguiente:

$$17^{2^k} - 1 = (17 - 1)(17 + 1)(17^2 + 1) \cdots (17^{2^{k-1}} + 1).$$

Buscaremos el exponente de 2 en cada uno de los factores del producto. Como $17 \equiv 1 \pmod 4$, tenemos que $17^{2^i} + 1 \equiv 1 + 1 \equiv 2 \pmod 4$ para todo entero $i \geq 0$. Así, el número $17^{2^i} + 1$ es múltiplo de 2, pero no de 4 para todo entero $i \geq 0$. Por lo tanto, $\nu_2(17^{2^k} - 1) = k + 4$, y en consecuencia, $k + 4 \geq 2016$. Luego, se concluye que $n = 2^{2012}$. □

Ejemplo 4. [*Leningrado, 1990*] *Sea* n *un entero positivo. Demostrar que* $n \mid \phi(a^n - 1)$ *para todo entero positivo* $a > 1$.

Demostración. Sea $d = \text{ord}_{(a^n-1)}a$. Como a y $a^n - 1$ son coprimos, por el teorema de Euler tenemos que $a^{\phi(a^n-1)} \equiv 1 \pmod{a^n - 1}$, y por el Teorema 1, $d \mid \phi(a^n - 1)$. Basta demostrar entonces que $d = n$.
Como $a^n \equiv 1 \pmod{a^n - 1}$, el Teorema 1 implica que $d \mid n$, y en consecuencia, $d \leq n$. Si $d < n$, entonces $0 < a^d - 1 < a^n - 1$ y por lo tanto $a^d \not\equiv 1 \pmod{a^n - 1}$, lo que es una contradicción. Por lo tanto, $d = n$. □

Ejemplo 5. [*Putnam, 1972*] *Demostrar que no existe entero* $n > 1$ *tal que* $n \mid (2^n - 1)$.

Demostración. Supongamos lo contrario, esto es, que existe un entero $n > 1$ tal que $2^n \equiv 1 \pmod{n}$, y sea k el menor de tales enteros. Es claro que 2 y k son coprimos. Sea $d = \text{ord}_k 2$. Como $2^d \equiv 1 \pmod{k}$ y $k > 1$, se sigue que $d > 1$.
Por otro lado, como $2^k \equiv 1 \pmod{k}$, se tiene que $d \mid k$ por el Teorema 1. Luego, $d \leq k$. Como $2^d \equiv 1 \pmod{k}$ y $d \mid k$, se sigue que $2^d \equiv 1 \pmod{d}$ con $d > 1$. Entonces, por definición de k tenemos que $k \leq d$. Concluimos que $d = k$.
Como 2 y k son coprimos, el Teorema 2 garantiza que $d \mid \phi(k)$, esto es, $k \mid \phi(k)$. Luego, $1 < k \leq \phi(k)$, lo cual es una contradicción, ya que $\phi(i) \leq i - 1$ para todo entero $i > 1$. Por lo tanto, no existe ningún entero $n > 1$ tal que $n \mid (2^n - 1)$. □

Ejemplo 6. *Demostrar que si p es un número primo mayor que 3, entonces cualquier divisor positivo del número*

$$\frac{2^p + 1}{3}$$

es de la forma $2kp + 1$, donde k es un entero no negativo.

Demostración. Sea $p > 3$ un número primo arbitrario y sea $m = \frac{2^p+1}{3}$. Es claro que el número 1 es un divisor positivo de m y es de la forma $2kp + 1$ para algún entero no negativo k, a saber $1 = 2p \cdot 0 + 1$. Como el producto de dos números de la forma $2kp + 1$ es de la misma forma, basta demostrar el resultado para los divisores primos de m.
Como $p > 3$, tenemos que $p \equiv 1 \pmod{6}$ o $p \equiv -1 \pmod{6}$. Si $p \equiv 1 \pmod{6}$, entonces $2^p \equiv 2 \pmod{9}$, pues $2^6 = 64 \equiv 1 \pmod{9}$. Así, $2^p + 1 \equiv 3 \pmod{9}$. De manera análoga, si $p \equiv -1 \pmod{6}$, entonces $2^p + 1 \equiv -3 \pmod{9}$. Luego, $2^p + 1$ es múltiplo de 3, pero no de 9. De esta manera, todo divisor primo de m es mayor o igual que 5.
Sea q un divisor primo de m y sea $d = \text{ord}_q 2$. Como $\frac{2^p+1}{3} \equiv 0 \pmod{q}$, tenemos que $2^p \equiv -1 \pmod{q}$ y $2^{2p} \equiv 1 \pmod{q}$. Luego, por el Teorema 1, tenemos que $d \mid 2p$. De aquí que $d \in \{1, 2, p, 2p\}$. Como $2^1 \equiv 2 \pmod{q}$, $2^2 \equiv 4 \pmod{q}$, $2^p \equiv -1 \pmod{q}$ y $q \geq 5$, tenemos que $d \neq 1, 2$ y p. Por lo tanto, $d = 2p$. Aplicando el Teorema 2, se sigue que $2p \mid \phi(q)$ (pues 2 y q son coprimos), esto es, $2p \mid (q - 1)$, ya que q es primo. Concluimos que $q = 2pk + 1$ para algún entero positivo k.
Por lo tanto, cada divisor positivo de m es de la forma $2pk+1$ con k entero no negativo. □

Ejemplo 7. *Demostrar que si p es un número primo mayor que 2, entonces cualquier divisor positivo del número $2^p - 1$ es de la forma $2kp + 1$, donde k es un entero no negativo.*

Demostración. Se deja de ejercicio al lector. □

Ejemplo 8. [*Lista larga, IMO 1985*] *Sea $k \geq 2$ un número entero y sean $n_1, n_2, \ldots, n_k$ enteros positivos tales que*

$$n_1 \mid (2^{n_2} - 1),\ n_2 \mid (2^{n_3} - 1),\ \ldots,\ n_k \mid (2^{n_1} - 1).$$

Demostrar que $n_1 = n_2 = \cdots = n_k = 1$.

Demostración. Sea $n_{k+1} = n_1$. Si existe i tal que $n_i = 1$, entonces necesariamente $n_1 = n_2 = \cdots = n_k = 1$. Ahora, supongamos que ninguno de los n_i es igual a 1. Para cada $1 \leqslant i \leqslant k$, sea p_i el menor primo que divide a n_i. Luego, como $2^{n_{i+1}} \equiv 1 \pmod{p_i}$, se tiene que 2 y p_i son coprimos, y por el Teorema 1, $\text{ord}_{p_i} 2 \mid n_{i+1}$. Note que $\text{ord}_{p_i} 2 > 1$. En consecuencia, $p_{i+1} \leq \text{ord}_{p_i} 2$ (si $p_{i+1} > \text{ord}_{p_i} 2$, entonces $\text{ord}_{p_i} 2$ tendría un divisor primo menor que p_{i+1}, y por lo tanto, n_{i+1} tendría un divisor primo menor que p_{i+1}, lo que contradice la definición del primo p_{i+1}). Por otra parte, por el teorema pequeño de Fermat[3] tenemos que $2^{p_i - 1} \equiv 1 \pmod{p_i}$, y por el Teorema 1, se sigue que $\text{ord}_{p_i} 2 \mid (p_i - 1)$. De aquí que $\text{ord}_{p_i} 2 \leq p_i - 1 < p_i$. Por lo tanto, $p_{i+1} < p_i$ para todo $i = 1, 2, \ldots, k$. Pero esto es una contradicción, pues se tendría que

$$p_1 > p_2 > \cdots > p_k > p_{k+1} = p_1.$$

Finalmente, concluimos que $n_1 = n_2 = \cdots = n_k = 1$. □

Ejemplo 9. *Encontrar el menor entero $n > 1$ que no es una potencia de 3 tal que*

$$n \mid (2^n + 1).$$

Solución. Claramente n es impar. Como n no es una potencia de 3, entonces n tiene al menos un factor primo distinto de 3. Supongamos que p es el menor de ellos y sea $d = \text{ord}_p 2$. Como $2^n \equiv -1 \pmod{n}$ y $p \mid n$, tenemos que $2^n \equiv -1 \pmod{p}$, de donde $2^{2n} \equiv 1 \pmod{p}$. Luego, por el Teorema 1, $d \mid 2n$.
Si d es impar, entonces $d \mid n$, y como $2^d \equiv 1 \pmod{p}$, concluimos que $2^n \equiv 1 \pmod{p}$. Pero entonces, $-1 \equiv 1 \pmod{p}$, lo cual no puede ser porque $p > 3$. Esto demuestra que d es par, esto es, $d = 2k$ para algún entero positivo k. Tenemos entonces que $2k \mid 2n$, lo que implica que $k \mid n$. Como n es impar, k también es impar. Por otro lado, por el teorema pequeño de Fermat tenemos que $2^{p-1} \equiv 1 \pmod{p}$, de modo que por el Teorema 1, $d \mid (p-1)$, esto es, $2k \mid (p-1)$. Como $\frac{p-1}{2}$ es entero, concluimos que k divide a $\frac{p-1}{2}$. Si existe un primo $q \geq 5$ tal que $q \mid k$, entonces $q \mid d$ y en consecuencia, $q \mid n$. Pero también, q divide a $\frac{p-1}{2}$. Luego, $q \leq \frac{p-1}{2} < p$ y $q \mid n$, lo que contradice la definición de p. Esto demuestra que k debe ser una potencia de 3. Analizaremos cuatro casos:

1) Si $k = 3$, entonces $d = 6$ y $2^6 \equiv 1 \pmod{p}$ de donde $p = 7$. Esto quiere decir que $n = 21r$, para algún entero positivo r (pues n es múltiplo de p y de k). Como $2^3 \equiv 1 \pmod{7}$, tenemos que $-1 \equiv 2^n = 2^{21r} = (2^3)^{7r} \equiv 1 \pmod{7}$, lo cual es un absurdo. Luego, en este caso no existe tal n.

2) Si $k = 9$, entonces $d = 18$ y $2^{18} \equiv 1 \pmod{p}$. Luego, p divide a

$$\begin{aligned} 2^{18} - 1 &= (2^9 + 1)(2^9 - 1) \\ &= (2^3 + 1)(2^6 - 2^3 + 1)(2^3 - 1)(2^6 + 2^3 + 1) = 9 \cdot 57 \cdot 7 \cdot 73 \\ &= 3^3 \cdot 7 \cdot 19 \cdot 73. \end{aligned}$$

[3] Ver en el apéndice el teorema 2.

Como $p > 3$, se sigue que $p \in \{7, 19, 73\}$.
Si $p = 7$, entonces $n = 7 \cdot 9 \cdot r = 63r$ para algún entero positivo r. Sin embargo, ya que $2^3 \equiv 1 \pmod 7$, tenemos que $2^{63r} + 1 = (2^3)^{21r} + 1 \equiv 1 + 1 \equiv 2 \pmod 7$ para todo entero positivo r. Esto demuestra que $7 \nmid (2^{63r} + 1)$ para todo entero positivo r, de modo que no hay valores de n con $p = 7$.
Si $p = 19$, veamos que $n = 9 \cdot 19 = 171$ sí cumple. Tenemos que $2^3 \equiv -1 \pmod 9$ implica que $2^9 \equiv (-1)^3 \equiv -1 \pmod 9$ y $2^{9 \cdot 19} + 1 \equiv (-1)^{19} + 1 \equiv 0 \pmod 9$, lo que demuestra que $9 \mid (2^{9 \cdot 19} + 1)$. Además, como $2^9 + 1 = 513 = 19 \cdot 27$ y $2^{19} + 1 \mid (2^{9 \cdot 19} + 1)$, tenemos que $19 \mid (2^{9 \cdot 19} + 1)$. Por lo tanto, $n = 171$ satisface las condiciones del problema.
No estamos interesados en buscar valores de n en el caso $p = 73$, pues si existe algún n que cumpla, este es de la forma $n = 9 \cdot 73r$, para algún entero positivo r, pero $n = 9 \cdot 73r \geq 9 \cdot 73 = 657$, es decir, en este caso los n que cumplen (si los hay) son mayores que 171.

3) Si $k = 27$, entonces $d = 54$ y $2^{54} \equiv 1 \pmod p$. Es claro que $p \neq 2$.
Si $p = 3$, entonces $n = 3 \cdot 27r = 3^4 r$ para algún entero positivo r. Como n no puede ser potencia de 3, se debe tener que $r \geq 2$. Si $r = 2$, entonces $n = 81 \cdot 2 = 3(54)$ y $2^{3(54)} + 1 \equiv (2^3)^{54} + 1 \equiv (-1)^{54} + 1 \equiv 2 \pmod 9$. Esto implica que $n = 3(54)$ no divide a $2^n + 1$. Ahora, si $r > 2$, entonces $n > 81 \cdot 3 = 243 > 171$, de manera que en este caso los n que cumplen (si los hay) son mayores que 171.
Sea $p = 5$. Por el teorema pequeño de Fermat, tenemos que $2^4 \equiv 1 \pmod 5$, lo cual implica que $2^{54} = (2^4)^{13} \cdot 2^2 \equiv 4 \pmod 5$. Esto es una contradicción, pues $2^{54} \equiv 1 \pmod p$. Luego, en este caso, no hay soluciones.
Si $p \geq 7$, entonces $n \geq 27 \cdot 7 = 189 > 171$.

4) Si $k = 3^i$ para algún entero $i \geqslant 4$, entonces $k \geq 3^4$ y $p \geq 5$, de modo que por ser coprimos k y p, y ambos divisores de n, tenemos que $n \geq kp \geq 3^4 \cdot 5 = 405 > 171$.

Por lo tanto, concluimos que el menor valor que puede tomar n es $9 \cdot 19 = 171$. □

Ejemplo 10. [*Selectivo Brasil, Cono Sur 2002*] *Encontrar el periodo en la representación decimal de*

$$\frac{1}{3^{2002}}.$$

Solución. Para cada entero $n \geqslant 1$, sea $d_n = \operatorname{ord}_{3^n} 10$. Notemos que d_n es impar, pues si d_n fuera par, entonces como $\operatorname{mcd}(3, 10^{\frac{d_n}{2}} + 1) = 1$, se tendría que

$$\begin{aligned} 10^{d_n} &\equiv 1 \pmod{3^n}, \\ \left(10^{\frac{d_n}{2}} + 1\right)\left(10^{\frac{d_n}{2}} - 1\right) &\equiv 0 \pmod{3^n}, \\ \left(10^{\frac{d_n}{2}} - 1\right) &\equiv 0 \pmod{3^n}, \\ 10^{\frac{d_n}{2}} &\equiv 1 \pmod{3^n}, \end{aligned}$$

lo que contradice la minimalidad de d_n.
Es claro que $d_1 = 1$. Demostraremos que $d_n = 3^{n-2}$ y $\nu_3(10^{d_n} - 1) = n$ para todo entero $n \geqslant 2$ por inducción sobre n. En efecto, tenemos que $d_2 = 3^0$ y $\nu_3(10^{d_2} - 1) =$

2. Supongamos que existe un entero $k \geq 2$ tal que $d_k = 3^{k-2}$ y $\nu_3(10^{d_k} - 1) = k$. Observemos que

$$10^{d_{k+1}} \equiv 1 \pmod{3^{k+1}} \Longrightarrow 10^{d_{k+1}} \equiv 1 \pmod{3^k}.$$

Luego, por el Teorema 1, $3^{k-2} \mid d_{k+1}$; y por el Teorema 2, $d_{k+1} \mid \phi(3^{k+1})$, esto es, $d_{k+1} \mid 2 \cdot 3^k$. Como d_{k+1} es impar, se sigue que $d_{k+1} \mid 3^k$, lo que significa que d_{k+1} es una potencia de 3. Tenemos entonces que $3^{k-2} \leq d_{k+1} \leq 3^k$ con d_{k+1} una potencia de 3. Por lo tanto, $d_{k+1} = 3^i$ para algún $i \in \{k-2, k-1, k\}$. Pero $d_{k+1} = 3^{k-2}$ no puede ocurrir, pues

$$\nu_3(10^{d_k} - 1) = \nu_3(10^{3^{k-2}} - 1) = k < k + 1.$$

Esto quiere decir que $d_{k+1} \geq 3^{k-1}$.
Ahora, como $10^{3^{k-1}} - 1 = \left(10^{3^{k-2}} - 1\right)\left(10^{2 \cdot 3^{k-2}} + 10^{3^{k-2}} + 1\right)$, tenemos que

$$\nu_3(10^{3^{k-1}} - 1) = \nu_3(10^{3^{k-2}} - 1) + \nu_3(10^{2 \cdot 3^{k-2}} + 10^{3^{k-2}} + 1)$$

y por la hipótesis de inducción, se sigue que $\nu_3(10^{3^{k-1}} - 1) = k + 1$ (observe que $\nu_3(10^{2 \cdot 3^{k-2}} + 10^{3^{k-2}} + 1) = 1$ ya que $10^{2 \cdot 3^{k-2}} + 10^{3^{k-2}} + 1$ es múltiplo de 3 pero no de 9).
Por lo tanto, $d_{k+1} = 3^{k-1}$ y $\nu_3(10^{d_{k+1}} - 1) = k + 1$, quedando completa la inducción. En particular, la respuesta al problema es $d_{2002} = 3^{2000}$. □

Ejemplo 11. *Demostrar que el número $3^n - 2^n$ no es divisible por n para todo entero $n \geqslant 2$.*

Demostración. Supongamos lo contrario, y sea $n \geq 2$ el menor entero tal que n divide a $3^n - 2^n$. Es claro que n es coprimo con 2 y 3. Luego, existe un entero a tal que $2a \equiv 1 \pmod{n}$, de donde a y n también son coprimos. De aquí que,

$$3^n \equiv 2^n \pmod{n} \Longleftrightarrow (3a)^n \equiv 1 \pmod{n}.$$

Sea $d = \text{ord}_n 3a$. Por el Teorema 1, tenemos que $d \mid n$.
Por otro lado, el teorema de Euler implica que $3^{\phi(n)} \equiv 2^{\phi(n)} \pmod{n}$, esto es, $(3a)^{\phi(n)} \equiv 1 \pmod{n}$. Nuevamente por el Teorema 1, tenemos que $d \mid \phi(n)$, de donde $d \leq \phi(n) \leq n - 1 < n$ (observe que $\phi(n) \leq n - 1$ ya que $n \geq 2$).
Como $3^d \equiv 2^d \pmod{n}$ (pues $(3a)^d \equiv 1 \pmod{n}$) y $d \mid n$, tenemos que $3^d \equiv 2^d \pmod{d}$. Notemos que d no puede ser 1, pues de lo contrario se tendría que $n \mid (3 - 2)$ y $n \geq 2$. Por lo tanto, $2 \leqslant d < n$ y $3^d \equiv 2^d \pmod{d}$, lo que contradice la minimalidad de n. En conclusión, no existe tal n. □

Ejemplo 12. *Demostrar que*

(a) $ord_{3^n} 2 = 2 \cdot 3^{n-1}$.

(b) Si $2^m \equiv -1$ *(mod* 3^n*), entonces* $3^{n-1} \mid m$.

Demostración. Comenzamos demostrando el siguiente lema.

Lema. Para cada entero positivo n, se cumple que $\nu_3(2^{3^n}+1) = n+1$.

Prueba. La prueba la haremos por inducción en n. En efecto, si $n = 1$ el resultado es inmediato, pues $\nu_3(2^{3^1}+1) = \nu_3(9) = 2$. Supongamos que $\nu_3(2^{3^k}+1) = k+1$ para algún entero positivo k.
Como $2^{3^{k+1}}+1 = (2^{3^k}+1)(2^{2\cdot 3^k} - 2^{3^k}+1)$, tenemos que

$$\nu_3(2^{3^{k+1}}+1) = \nu_3(2^{3^k}+1) + \nu_3(2^{2\cdot 3^k} - 2^{3^k}+1). \tag{1}$$

Es fácil ver que $2^{2\cdot 3^k} - 2^{3^k} + 1$ es múltiplo de 3, pero no es múltiplo de 9, pues $2^{3^k} = 8^{3^{k-1}} \equiv -1 \pmod 9$, y en consecuencia,

$$2^{2\cdot 3^k} - 2^{3^k} + 1 \equiv (-1)^2 - (-1) + 1 \equiv 3 \pmod 9.$$

Por lo tanto, $\nu_3(2^{2\cdot 3^k} - 2^{3^k}+1) = 1$, y por la hipótesis de inducción y la relación (1) se tiene que

$$\nu_3(2^{3^{k+1}}+1) = (k+1)+1 = k+2.$$

Esto completa la inducción. □

(a) Sea $d = \operatorname{ord}_{3^n} 2$. Por el Teorema 2 tenemos que $d \mid \phi(3^n)$, esto es, $d \mid 2\cdot 3^{n-1}$. Luego, existe un entero i tal que $d = 3^i$ o $d = 2\cdot 3^i$, con $1 \le i \le n-1$.
Por el lema anterior, tenemos que $2^{3^n} \equiv -1 \pmod{3^{n+1}}$ para todo entero positivo n. En particular, $2^{3^i} \equiv -1 \pmod{3^i}$ para $1 \le i \le n-1$. Luego, $d \neq 3^i$. Entonces, $d = 2\cdot 3^i$ para algún $1 \le i \le n-1$, y por lo tanto, $\nu_3(2^{2\cdot 3^i} - 1) \geqslant n$. Esto es, $\nu_3(2^{3^i}+1)+\nu_3(2^{3^i}-1) \ge n$. Por el lema anterior, tenemos que $\nu_3(2^{3^i}+1) = i+1$; y como 3 no divide a $2^{3^i}-1$, tenemos que $\nu_3(2^{3^i}-1) = 0$. Luego, $i+1 \ge n$ de donde $i \ge n-1$. Concluimos que $i = n-1$. Así, $d = 2\cdot 3^{n-1}$.

(b) Si $2^m \equiv -1 \pmod{3^n}$, entonces $2^{2m} \equiv 1 \pmod{3^n}$. Luego, el Teorema 1 y el inciso anterior, implican que $\operatorname{ord}_{3^n} 2 = 2\cdot 3^{n-1}$ divide a $2m$. Por lo tanto, $3^{n-1} \mid m$.

□

Ejemplo 13. [*Bulgaria, 1997*] *Determinar todos los enteros positivos $m \ge 2$ y $n \ge 2$, tales que*

$$\frac{1 + m^{3^n} + m^{2\cdot 3^n}}{n}$$

es un número entero.

Solución. Claramente n es impar, $\operatorname{mcd}(m,n) = 1$ y $n \geqslant 3$. Supongamos que $n = 3$. Como m y n son coprimos, tenemos que $m \equiv 1$ o $-1 \pmod 3$. Si $m \equiv -1 \pmod 3$, entonces

$$1 + m^{3^n} + m^{2\cdot 3^n} \equiv 1 - 1 + 1 \equiv 1 \pmod 3,$$

lo que significa que $n = 3$ no divide a $1 + m^{3^n} + m^{2\cdot 3^n}$. Luego, $m \equiv 1 \pmod 3$ y $1 + m^{3^n} + m^{2\cdot 3^n} \equiv 1 + 1 + 1 \equiv 0 \pmod 3$. Por lo tanto, las parejas de la forma

$(m, n) = (3k + 1, 3)$, con k entero positivo, satisfacen la condición del problema.
Supongamos que $n > 3$ y sea $d = \text{ord}_n m$. Es claro que $d > 1$. Como

$$1 + m^{3^n} + m^{2\cdot 3^n} = \frac{m^{3^{n+1}} - 1}{m^{3^n} - 1}$$

y n debe dividir a $1+m^{3^n}+m^{2\cdot 3^n}$, se sigue que n divide a $m^{3^{n+1}}-1$, esto es, $m^{3^{n+1}} \equiv 1 \pmod{n}$. Luego, por el Teorema 1, tenemos que $d \mid 3^{n+1}$. En consecuencia, $d = 3^i$ para algún entero i con $1 \leq i \leq n + 1$. Si $i \leq n$, entonces $m^{3^n} \equiv 1 \pmod{n}$, y en consecuencia $0 \equiv 1 + m^{3^n} + m^{2\cdot 3^n} \equiv 3 \pmod{n}$, lo cual es imposible ya que $n > 3$. Por lo tanto, $i = n + 1$. Pero por el Teorema 2, tenemos que $d = 3^{n+1}$ divide a $\phi(n)$, lo cual implica que $3^{n+1} \leq \phi(n) \leq n - 1$. Esto es una contradicción, ya que $3^{n+1} \geq n + 3$ para todo entero $n \geq 0$. Por lo tanto, no existen enteros m y n que satisfagan las condiciones del problema si $n > 3$.
Concluimos que los pares que cumplen son $(m, n) = (3k+1, 3)$ con k entero positivo. □

Ejemplo 14. *Demostrar que si p es un número primo, entonces $p^p - 1$ tiene un factor de la forma $pk + 1$, donde k es un entero positivo.*

Demostración. Sea q un divisor primo de $\frac{p^p-1}{p-1}$ (tal divisor existe ya que $\frac{p^p-1}{p-1}$ es un entero mayor que 1). Entonces, $p^p \equiv 1 \pmod{q}$, y por el Teorema 1, $\text{ord}_q p \mid p$, lo cual implica que $\text{ord}_q p = 1$ o p.

Si $\text{ord}_q p = 1$, entonces $p \equiv 1 \pmod{q}$. Luego, $\sum_{i=0}^{p-1} p^i \equiv p \pmod{q}$. Pero, como

$$\sum_{i=0}^{p-1} p^i = \frac{p^p - 1}{p - 1} \equiv 0 \pmod{q},$$

se sigue que $p \equiv 0 \pmod{q}$. Así, $1 \equiv 0 \pmod{q}$ lo cual es imposible.
Por lo tanto, $\text{ord}_q p = p$, y por el Teorema 2, p divide a $\phi(q) = q - 1$, esto es, $q \equiv 1 \pmod{p}$, de donde se sigue el resultado. □

Ejemplo 15. *Para cada entero no negativo n, sea $F_n = 2^{2^n} + 1$.*

(a) Demostrar que cualquier divisor positivo de F_n es de la forma $2^{n+1}k + 1$ donde k es un entero no negativo.

(b) Demostrar que para cada entero $n \geq 1$ hay una infinidad de números primos de la forma $2^n k + 1$ con k entero positivo.

Demostración.

(a) Sean n un entero no negativo y p un divisor primo de F_n. Como $2^{2^n} \equiv -1 \pmod{p}$, tenemos que $p > 2$ y $2^{2^{n+1}} \equiv 1 \pmod{p}$. Luego, por el Teorema 1, $\text{ord}_p 2 \mid 2^{n+1}$, esto es, existe un entero positivo k tal que $\text{ord}_p 2 = 2^k$ con $k \leq n + 1$. Si $k \leqslant n$, entonces

$$2^{2^k} \equiv 1 \pmod{p} \Longrightarrow -1 \equiv 2^{2^n} \equiv (2^{2^k})^{2^{n-k}} \equiv 1 \pmod{p} \Longrightarrow p = 2,$$

lo cual es una contradicción. Por lo tanto, $k = n + 1$, y por el Teorema 2, $\text{ord}_p 2 \mid \phi(p)$, esto es, $2^{n+1} \mid (p-1)$. Por lo tanto, $p = 2^{n+1}k+1$ para algún entero positivo k.
Ahora, sea d un divisor de F_n. Si $d = 1$, tenemos que $1 = 2^{n+1} \cdot 0 + 1$. Si $d > 1$, entonces d es producto de números primos de la forma $2^{n+1}k + 1$, donde k es un entero positivo. Por lo tanto, cualquier divisor positivo de F_n se puede expresar de la forma pedida.

(b) Sean n un entero positivo fijo y r un entero tal que $r \geq n - 1$. Tomemos el menor divisor primo de F_r, digamos q_r. Por la parte (a) sabemos que $q_r \equiv 1 \pmod{2^{r+1}}$, y como $r + 1 \geq n$, en particular tenemos que $q_r \equiv 1 \pmod{2^n}$. Es conocido que si $i \neq j$, entonces F_i y F_j son coprimos[4]. Luego, cada número de la lista infinita

$$F_r, F_{r+1}, F_{r+2}, \ldots$$

tiene un divisor primo de la forma $2^n k + 1$ que no divide a ningún otro número de la lista, de donde se sigue el resultado.

□

Ejemplo 16. [*Bulgaria, 1995*] *Determinar todos los pares de números primos* (p, q) *tales que el número*

$$\frac{2^p + 2^q}{pq}$$

es entero.

Solución. Sean p y q números primos tales que $2^p + 2^q \equiv 0 \pmod{pq}$. Supongamos sin pérdida de generalidad que $p \leqslant q$. Si $p = 2$, entonces $2q \mid (2^2 + 2^q)$, esto es, $q \mid (2 + 2^{q-1})$. Es claro que $q = 2$ satisface esta relación de divisibilidad, y por consiguiente, el par $(p, q) = (2, 2)$ es una solución. Si $q > 2$, entonces por el teorema pequeño de Fermat tenemos que $2^{q-1} \equiv 1 \pmod{q}$, lo cual implica que

$$2 + 2^{q-1} \equiv 2 + 1 \equiv 3 \pmod{q}.$$

Como $2 + 2^{q-1} \equiv 0 \pmod{q}$, se sique que $3 \equiv 0 \pmod{q}$, y por lo tanto $q = 3$. De aquí que el par $(p, q) = (2, 3)$ también es solución.
Supongamos que $p > 2$. Sean $a = \text{ord}_q 2$ y $b = \text{ord}_p 2$.
Nuevamente, por el teorema pequeño de Fermat, tenemos que

$$0 \equiv 2^p + 2^q \equiv 2^p + 2 \pmod{q} \Longrightarrow 2^{p-1} \equiv -1 \pmod{q} \Longrightarrow 2^{2(p-1)} \equiv 1 \pmod{q}.$$

Luego, por el Teorema 1, tenemos que $a \mid 2(p-1)$, y en consecuencia,

$$\nu_2(a) \leq \nu_2(2(p-1)) = \nu_2(p-1) + 1.$$

[4]Se puede demostrar por inducción, que para cada entero $n \geq 1$, $F_n = F_0 \cdots F_{n-1} + 2$, lo cual implica que $F_k \mid (F_n - 2)$ para $k = 0, 1, \ldots, n-1$. De aquí que si p es un divisor primo de F_k y F_n, entonces $p \mid 2$, y por lo tanto $p = 2$. Pero esto es una contradicción, pues F_n es impar por definición. Esto muestra que para cada entero $n \geq 1$, F_n y F_k son coprimos para cada $k = 0, 1, \ldots, n-1$. De aquí se sigue que si $i \neq j$, entonces F_i y F_j son coprimos. A los números F_n se les conoce como *números de Fermat*.

Si $\nu_2(a) \leqslant \nu_2(p-1)$, entonces la mayor potencia de 2 que divide al entero a, también divide a $p-1$. Además, como $a \mid 2(p-1)$, la mayor potencia de cada primo impar que divide al entero a divide también a $p-1$, pues tales potencias son coprimos con 2. Luego, $a \mid (p-1)$. Esto implica que $2^{p-1} \equiv 1 \pmod{q}$, de donde $q > 2$. Esto contradice que $2^{p-1} \equiv -1 \pmod{q}$, pues tendríamos que $1 \equiv -1 \pmod{q}$ con $q > 2$. Por lo tanto, $\nu_2(a) = \nu_2(p-1) + 1$. Por el Teorema 2 tenemos que $a \mid (q-1)$, lo cual implica que $\nu_2(a) \leq \nu_2(q-1)$. De esta manera, tenemos que $\nu_2(p-1)+1 \leq \nu_2(q-1)$. Haciendo un razonamiento análogo módulo p, obtenemos que $\nu_2(q-1)+1 \leqslant \nu_2(p-1)$. Por lo tanto, $\nu_2(q-1)+1 \leqslant \nu_2(p-1) \leqslant \nu_2(q-1)-1$, que es una contradicción. Esto demuestra que no hay soluciones si $p > 2$.
Concluimos que las soluciones (p,q) con $p \leq q$ son $(2,2)$ y $(2,3)$. De manera análoga, las soluciones (p,q) con $p \geq q$ son $(2,2)$ y $(3,2)$. □

Ejemplo 17. [*Vietnam, 1997*] *Demostrar que para cada entero positivo n existe un entero positivo k tal que $19^k - 97$ es múltiplo de 2^n.*

Demostración. Si $n = 1, 2$ o 3, y $k = 2$, tenemos que $19^2 - 97 = 264 = 8 \cdot 33$ es múltiplo de 2, 2^2 y 2^3.
Supongamos que $n \geq 3$. Demostraremos que $\text{ord}_{2^n} 19 = 2^{n-2}$. Observemos que

$$\begin{aligned} 19^{2^{n-2}} - 1 &= (19-1)(19^{2^0}+1)(19^{2^1}+1)\cdots(19^{2^{n-3}}+1), \\ &= 2^3 \cdot 5 \cdot 9 \cdot (19^{2^1}+1)(19^{2^2}+1)\cdots(19^{2^{n-3}}+1). \end{aligned}$$

Como $19 \equiv 3 \pmod{4}$, tenemos que $19^2 \equiv 9 \equiv 1 \pmod{4}$ y

$$19^{2^i} + 1 = (19^2)^{2^{i-1}} + 1 \equiv 1^{2^{i-1}} + 1 \equiv 1 + 1 \equiv 2 \pmod{4}.$$

para todo entero $i \geq 1$. Luego, $2^2 \nmid 19^{2^i} + 1$ para todo entero $i \geq 1$. Esto significa que $\nu_2(19^{2^{n-2}} - 1) = n$ para todo entero $n \geq 3$. En particular, tenemos que $19^{2^{n-2}} \equiv 1 \pmod{2^n}$, y por el Teorema 1, $\text{ord}_{2^n} 19 \mid 2^{n-2}$. De aquí que $\text{ord}_{2^n} 19 = 2^r$ para algún entero $r \leq n-2$. Es fácil ver que $r > 0$. Además,

$$19^{2^r} \equiv 1 \pmod{2^n} \Longrightarrow 19^{2^{r+1}} \equiv 1 \pmod{2^{n+1}},$$

pues en general, es un ejercicio demostrar que si $a \equiv b \pmod{2^n}$, entonces $a^2 \equiv b^2 \pmod{2^{n+1}}$.
Luego, si $r \leq n-3$, entonces $r+1 \leq n-2$ y

$$19^{2^{r+1}} \equiv 1 \pmod{2^{n+1}} \Longrightarrow 19^{2^{n-2}} \equiv 1 \pmod{2^{n+1}},$$

lo que contradice que $\nu_2(19^{2^{n-2}} - 1) = n$. Por lo tanto, $r = n-2$ y $\text{ord}_{2^n} 19 = 2^{n-2}$.
Regresando al problema, procederemos por inducción en n. El caso $n = 3$ ya se hizo antes. Supongamos que para algún entero $n \geq 3$, existe un entero positivo k tal que $19^k \equiv 97 \pmod{2^n}$. Como $19^{2^{n-2}} \equiv 1 \pmod{2^n}$, se sigue que $19^{k+2^i} \equiv 97 \pmod{2^n}$, para todo entero $i \geqslant n-2$. En particular, para $i = n-2$ e $i = n-1$, tenemos que

$$19^{k+2^{n-2}} - 97 \equiv 0 \pmod{2^n} \text{ y } 19^{k+2^{n-1}} - 97 \equiv 0 \pmod{2^n},$$

las cuales implican[5] que

$$19^{k+2^{n-2}} - 97 \equiv 0 \text{ o } 2^n \pmod{2^{n+1}} \text{ y } 19^{k+2^{n-1}} - 97 \equiv 0 \text{ o } 2^n \pmod{2^{n+1}}.$$

Supongamos que $19^{k+2^{n-2}} - 97 \equiv 19^{k+2^{n-1}} - 97 \equiv 2^n \pmod{2^{n+1}}$. Entonces, $19^{2^{n-1}-2^{n-2}} \equiv 1 \pmod{2^{n+1}}$ y por el Teorema 1, $\text{ord}_{2^{n+1}} 19 \mid (2^{n-1} - 2^{n-2})$, esto es, $2^{n-1} \mid (2^{n-1} - 2^{n-2})$. Pero esto implica que $2^{n-1} \mid 2^{n-2}$, lo cual es una contradicción. Por lo tanto, $19^{k+2^{n-2}} \equiv 97 \pmod{2^{n+1}}$ o $19^{k+2^{n-1}} \equiv 97 \pmod{2^{n+1}}$, lo cual completa la inducción. □

Ejemplo 18. [*Colombia, 2009*] *Determinar todas las ternas* (a, b, n) *de enteros positivos tales que*

$$a^b = 1 + b + b^2 + \cdots + b^n.$$

Solución. Si $b = 1$, entonces $a = n + 1$. Luego, en este caso las soluciones son las ternas de la forma $(n + 1, 1, n)$, donde n es un entero positivo.
Si $b \geq 2$, consideremos el menor número primo q que divide a b. Tenemos entonces que $a^b \equiv 1 \pmod{q}$, lo cual implica que a y q son coprimos. Luego, por el Teorema 2 se sigue que $\text{ord}_q a \mid \phi(q)$ y por el Teorema 1, tenemos que $\text{ord}_q a \mid b$. Como q es el menor divisor primo de b, resulta que $\text{ord}_q a$ y $\phi(q) = q - 1$ son coprimos. Así, tenemos que $\text{ord}_q a = 1$ y, por lo tanto, $a \equiv 1 \pmod{q}$.
Por otra parte, podemos escribir b en la forma $b = q^k M$ con k entero positivo y $\text{mcd}(M, q) = 1$. Notemos que

$$a^b - 1 = (a-1)(1 + a + a^2 + \cdots + a^{n-1}) = b(1 + b + b^2 + \cdots + b^{n-1}), \quad (2)$$

lo cual implica que $\nu_q(a^b - 1) = \nu_q(b) = k$.
De (2) tenemos también que $a^b \equiv 1 \pmod{b}$, de donde $a^b \equiv 1 \pmod{q^k}$. Nuevamente por el Teorema 2, tenemos que $\text{ord}_{q^k} a \mid \phi(q^k)$ y por el Teorema 1, tenemos que $\text{ord}_{q^k} a \mid b$. Como $\text{ord}_{q^k} a$ y $q - 1$ son coprimos (pues $\text{ord}_q a$ y $q - 1$ son coprimos), y $\phi(q^k) = q^{k-1}(q - 1)$, resulta que $\text{ord}_{q^k} a = q^m$ para algún entero m con $1 \leq m \leq k - 1$.
Entonces,

$$E = \frac{a^b - 1}{a^{q^m} - 1} = \frac{(a^{q^m})^{q^{k-m}M} - 1}{a^{q^m} - 1} = 1 + a^{q^m} + (a^{q^m})^2 + \cdots + (a^{q^m})^{q^{k-m}M - 1}.$$

Como $a \equiv 1 \pmod{q}$, se sigue que

$$E \equiv \underbrace{1 + 1 + \cdots + 1}_{q^{k-m}M} \equiv q^{k-m}M \equiv 0 \pmod{q},$$

pues $k - m \geq 1$. Esto es, $q \mid E$ y así, $\nu_q(E) \geq 1$.
Como $a^b - 1 = (a^{q^m} - 1)E$, tenemos que $\nu_q(a^b - 1) = \nu_q(a^{q^m} - 1) + \nu_q(E) \geq k + 1$, lo que es una contradicción. Esto demuestra que no hay soluciones si $b \geq 2$.
Finalmente, se concluye que las soluciones son las ternas de la forma $(n + 1, 1, n)$, donde n es cualquier entero positivo. □

[5] Si a es un entero tal que $a \equiv 0 \pmod{2^n}$, es fácil demostrar que $a \equiv 0 \text{ o } 2^n \pmod{2^{n+1}}$.

Ejemplo 19. [*APMO, 2016*] *Un entero positivo se llama* alegre *si puede expresarse en la forma* $2^{a_1} + 2^{a_2} + \cdots + 2^{a_{100}}$ *donde* $a_1, a_2, \ldots, a_{100}$ *son enteros no negativos no necesariamente distintos.*
Determinar el menor entero positivo n *tal que ningún múltiplo de* n *es un número alegre.*

Solución. En primer lugar probaremos que si $n < 2^0 + 2^1 + 2^2 + \cdots + 2^{100}$, entonces n es alegre. En efecto, como $2^0 + 2^1 + 2^2 + \cdots + 2^{100}$ es el primer entero positivo que se puede expresar como la suma de 101 potencias distintas de 2 (incluyendo al 1), entonces al escribir a n en base 2, tendrá a lo más 100 cifras, esto es, $n = 2^{x_1} + 2^{x_2} + \cdots + 2^{x_k}$, donde $k \leq 100$ y $x_1 < x_2 < \cdots < x_k \leq 100$.
Si t es un entero positivo, entonces $2^t = 2^{t-1} + 2^{t-1}$, esto es, lo podemos escribir como suma de dos potencias de 2. Consideremos el número

$$n \cdot 2^{100} = 2^{100+x_1} + 2^{100+x_2} + \cdots + 2^{100+x_k}.$$

No es difícil darse cuenta que 2^{100+x_k} lo podemos escribir como suma de exactamente $101 - k$ potencias de 2. Por lo tanto, $n \cdot 2^{100}$ es alegre.
Demostraremos que $2^0 + 2^1 + 2^2 + \cdots + 2^{100} = 2^{101} - 1$ es el mínimo entero positivo tal que todos sus múltiplos no son alegres. En efecto, como $2^{101} \equiv 1 \pmod{2^{101} - 1}$, el Teorema 1 implica que $\text{ord}_{2^{101}-1}2 \mid 101$, de modo que la única posibilidad es $\text{ord}_{2^{101}-1}2 = 101$, ya que 101 es primo.
Es fácil ver que los posibles residuos distintos para una potencia de 2 módulo $2^{101} - 1$ son: $2^0, 2^1, 2^2, \ldots, 2^{100}$.
Ahora, supongamos que existe un entero positivo k tal que $(2^{101} - 1)k$ es alegre, esto es, existen $w \leqslant 100$ y $y_1 < y_2 < \cdots < y_w$ tales que

$$(2^{101} - 1)k = 2^{y_1} + 2^{y_2} + \cdots + 2^{y_w},$$

y consideremos que k es tal que $y_1 + y_2 + \cdots + y_w$ es mínimo. Como $2^{101} - 1$ divide a $2^{y_1} + 2^{y_2} + \cdots + 2^{y_w}$, resulta que $2^{y_1} + 2^{y_2} + \cdots + 2^{y_w} \geq 2^{101} - 1$. Esto nos dice que existe un entero j, con $1 \leqslant j \leqslant w$, tal que $y_j > 100$, pues de lo contrario $2^{y_1} + 2^{y_2} + \cdots + 2^{y_w} \leqslant 2^1 + \cdots + 2^{100} = 2^{101} - 2$, lo cual es una contradicción.
Por el algoritmo de la división, para cada $i = 1, 2, \ldots, w$, existen enteros no negativos q_i y r_i tales que $y_i = 101q_i + r_i$, con $0 \leqslant r_i < 101$. Por lo tanto,

$$2^{y_i} \equiv (2^{101})^{q_i} \cdot 2^{r_i} \equiv 2^{r_i} \pmod{2^{101} - 1}.$$

En consecuencia, $2^{101}-1 \mid 2^{r_1}+2^{r_2}+\cdots+2^{r_w}$, lo cual implica que $y_1+y_2+\cdots+y_w \leqslant r_1 + r_2 + \cdots + r_w$, pues $y_1 + y_2 + \cdots + y_w$ es mínimo. Pero como existe j tal que $y_j > 100$, entonces

$$\sum_{s=1}^{w} y_s = 101 \sum_{s=1}^{w} q_s + \sum_{s=1}^{w} r_s > \sum_{s=1}^{w} r_s,$$

lo que es una contradicción.
Finalmente, se concluye que el mínimo número buscado es $2^{101} - 1$. □

Ejemplo 20. [*APMO, 2015*] *Una sucesión de números reales* $a_0, a_1, \ldots$ *es llamada* buena *si cumple las siguientes tres condiciones:*

- *El valor de* a_0 *es un entero positivo.*
- *Para cada entero no negativo* i*, se tiene* $a_{i+1} = 2a_i + 1$ *o* $a_{i+1} = \dfrac{a_i}{a_i + 2}$.
- *Existe un entero positivo* k *tal que* $a_k = 2014$.

Determinar el menor entero positivo n *tal que existe una sucesión buena* $a_0, a_1, \ldots$ *de números reales con la propiedad de que* $a_n = 2014$.

Solución. Para mayor comodidad y entendimiento, definamos $w(\frac{a}{b}) = a+b$ para todas las fracciones irreducibles $\frac{a}{b}$.
Como a_0 es un entero positivo, ningún otro término de la sucesión es negativo, 0 o 1. Si el siguiente término de a_i es $2a_i + 1$ diremos que se aplicó el paso (1), y si es $\frac{a_i}{a_i+2}$ diremos que se aplicó el paso (2). Sea $i \geq 1$. Notemos que si $a_i > 1$, entonces al término a_{i-1} se le ha tenido que aplicar el paso (1), pues si se hubiera aplicado el paso (2), a_i sería menor que 1. Si $0 < a_i < 1$, entonces al término a_{i-1} se le aplicó el paso (2), pues si se le hubiera aplicado el paso (1), entonces $2a_{i-1} + 1 = a_i$, y en consecuencia $2a_{i-1} = a_i - 1 < 0$, lo cual no puede ocurrir.
Supongamos que $j \geq 1$ y $a_j = \frac{p}{q}$, con $\text{mcd}(p, q) = 1$. Si $p > q$, entonces $a_{j-1} = \frac{p-q}{2q}$; y si $p < q$, entonces $a_{j-1} = \frac{2p}{q-p}$. Pero en ambos casos, como p y q son coprimos, el numerador y el denominador de a_{j-1} también son coprimos. Además, es claro que $w(a_i) = w(a_{i-1}) = p + q$.
Ya que la sucesión es buena, existe un entero positivo k tal que $a_k = 2014 = \frac{2014}{1}$, y consideremos al menor de tales enteros k. Observe que $w(a_k) = 2015$. Si encontramos el valor irreducible de los términos $a_{k-1}, a_{k-2}, \ldots, a_1, a_0$, se tendrá que

$$2015 = w(a_k) = w(a_{k-1}) = \cdots = w(a_1) = w(a_0).$$

Supongamos que $a_1 = \frac{m}{n}$, con m y n coprimos. Si $m > n$, entonces $a_0 = \frac{m-n}{2n}$ y $w(a_0) = (m - n) + 2n = m + n = 2015$, de donde se puede observar que $m - n$ es impar. Como a_0 es entero, entonces $2n \mid m - n$, pero esto es imposible, pues $m - n$ es impar. Con esto se deduce que $a_0 = \frac{2m}{n-m}$, y como a_0 es entero, se tiene que $n - m \mid 2m$, pero ya que $n - m$ es impar, se tiene que $n - m \mid m$, y usando que m y n son coprimos se llega a que $n - m = 1$, pero como $n + m = 2015$, entonces $n = 1008$ y $m = 1007$. Así, $a_0 = 2014$.
Por otro lado, si $j \geq 1$ y $a_j = \frac{p}{q}$, con p y q coprimos, se sabe que el numerador de a_{j-1} es $p - q$ o $2p$, pero como $p - q \equiv 2p \pmod{2015}$, entonces el numerador de a_{j-1} siempre es congruente con el doble del numerador de a_j módulo 2015.
Luego, como el numerador de a_0 es 2014 y el numerador de a_k es 2014, entonces $2014 \cdot 2^k \equiv 2014 \pmod{2015}$, de donde $2^k \equiv 1 \pmod{2015}$. Como k es el menor posible, entonces $k = \text{ord}_{2015}2$.
Para calcular el valor de $\text{ord}_{2015}2$, primero notemos que $2015 = 5 \cdot 13 \cdot 31$. Es fácil calcular que $\text{ord}_5 2 = 4$, $\text{ord}_{13}2 = 12$ y $\text{ord}_{31}2 = 5$. Como $2^k \equiv 1 \pmod{5}$, $2^k \equiv 1 \pmod{13}$ y $2^k \equiv 1 \pmod{31}$, tenemos que k es divisible por 4, 12 y 5, esto es, k es divisible por $\text{mcm}(4, 12, 5) = 60$. Luego, al verificar que $2^{60} \equiv 1 \pmod{2015}$, se concluye que $k = \text{ord}_{2015}2 = 60$. □

Ejercicios

1) Determine el menor factor primo del número $12^{2^{15}} + 1$.

2) Sea $k \geqslant 2$ un número entero. Pruebe que existen infinitos números compuestos n tales que $n \mid (a^{n-k} - 1)$ para cualquier entero positivo a coprimo con n.

3) [*Selectivo Perú, Ibero 2010*] Determine el menor entero $k > 1$ para el cual $n^k - n$ es múltiplo de 2010 para todo entero positivo n.

4) Pruebe que si p es un número primo de la forma $4k + 3$, entonces $2p + 1$ también es primo si y solo si $2p + 1$ divide a $2^p - 1$.

5) [*IMO, 1990*] Encuentre todos los enteros $n > 1$ tales que $\dfrac{2^n + 1}{n^2}$ es un número entero.

6) [*Selectivo EUA, IMO 2003*] Determine todas las ternas (p, q, r) de números primos tales que $p \mid (q^r + 1)$, $q \mid (r^p + 1)$ y $r \mid (p^q + 1)$.

7) [*Selectivo China, IMO 2005*] Pruebe que para todo entero $n > 2$, el mayor factor primo de $2^{2^n} + 1$ es mayor o igual que $n \cdot 2^{n+2} + 1$.

8) Encuentre todos los números primos p y q tales que $p^2 + 1$ divide a $2003^q + 1$ y $q^2 + 1$ divide a $2003^p + 1$.

9) Para cada número primo p, sea $f_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$. Demuestre que

   (a) Si m es un entero positivo tal que $p \mid m$, entonces $f_p(m)$ es coprimo con $m(m - 1)$.

   (b) Hay una infinidad de enteros positivos n tales que $pn + 1$ es un número primo.

10) [*Selectivo Irán, IMO 2009*] Sea a un entero positivo fijo, y sea A el conjunto de todos los números primos que dividen a alguno de los términos de la secuencia $(a_n)_{n \geqslant 1}$ definida por $a_n = 2^{2^n} + a$ para $n \geqslant 1$. Demuestre que A es infinito.

11) Sea $n > 1$ un número entero. Pruebe que $2^{n-1} \not\equiv -1 \pmod{n}$.

12) [*IMO, 2003*] Sea p un número primo. Demuestre que existe un número primo q tal que, para todo entero n, el número $n^p - p$ no es divisible por q.

Bibliografía

1. TITU ANDREESCU, DORIN ANDRICA, *Number Theory*, Structures, Examples, and Problems.

2. TITU ANDREESCU, GABRIEL DOSPINESCU, *Problems From The Book*.

3. ARTHUR ENGEL, *Problems Solving Strategies*.

4. XIONG BIN, LEE PENG YEE, *Mathematical Olympiad in China*.

5. PIERRE BORNSZTEIN, XAVIER CARUSO, PIERRE NOLIN, MEHDI TIBOUCHI, *Cours d-arithmétique*, Première Partie.