Seminario de problemas. Curso 2019–20. Soluciones Hoja 3

33. Escribimos n como suma de potencias de 10, $n = d_k 10^k + \cdots + d_1 10 + d_0$ donde $d_k, \ldots, d_1, d_0$ son los dígitos de n. Puesto que n es múltiplo de sí mismo, por cumplirse el criterio de divisibilidad, n divide a $d_k + \cdots + d_0$. Así, $d_k + \cdots + d_0 \geq d_k 10^k + \cdots + d_1 10 + d_0$. Esto solo es posible si $d_k = \cdots = d_1 = 0$. Así que $n = d_0 \in \{1, 2, \ldots, 9\}$. Para estos números la suma de los dígitos de $9n$ es 9. Así, por el criterio, 9 es múltiplo de n. Por tanto, la única posibilidad es $n = 3$ y $n = 9$.

34. Sacando factor común 2^{1002} nos queda $5^{1002} - 1$. Comprobamos la máxima potencia de 2 en $\{16, 8, 4, 2, 1\}$ que divide a $5^{1002} - 1$. Puesto que $5^8 \equiv 1 \pmod{16}$, el problema se reduce a comprobarlo para $5^2 - 1$, y esa potencia es 8. Por tanto la solución es la D.

35. Observa que si $n \geq 1$ y $n = cd + r$ con $0 \leq r < d$ entonces $\left[\frac{n}{d}\right] = c$ por lo que $d\left[\frac{n}{d}\right] = n - n\,\%d$ donde $n\,\%d$ denota el resto r de dividir n entre d. Multiplicando por 6, la igualdad del enunciado es equivalente a

$$6n + 2010 = 6\left[\frac{3n}{6}\right] + 6\left[\frac{4n}{6}\right] = 3n - (3n)\,\%6 + 4n - (4n)\,\%6$$

es decir, a

$$n = 2010 + (3n)\,\%6 + (4n)\,\%6. \tag{1}$$

Los valores posibles para $(3n)\,\%6$ son $0, 3$ mientras que para $(4n)\,\%6$ son $0, 2, 4$. Así pues las posibilidades son $n = 2010, 2012, 2013, 2014, 2015, 2017$, y todas cumplen (1).

36. La preguenta es la misma que hallar el número de divisores de $1000000 = 2^6 * 5^6$ **que sean** ≥ 64. Es decir, $7 * 7 = 49$ divisores de 1000000 menos los 12 que son ≤ 63 quedan 37. La respuesta es la B.

37. Sin pérdida de generalidad podemos asumir que $x \geq y$. Si $y = x$ entonces la igualdad queda $p^4 = 2x^3$ y la única solución en tal caso es $p = 2$, $x = y = 2$, que es una solución válida.

Asumamos $x > y$. Factorizamos $x^3 + y^3$ como $p^4 = x^3 + y^3 = (x + y)(x^2 - xy + y^2)$ donde ambos factores son ≥ 2. Así $y \equiv -x \pmod{p}$ y $3x^2 \equiv 0 \pmod{p}$. Esto nos deja dos posibilidades

1. Posibilidad $x \equiv 0 \pmod{p}$: esto también implica que $y \equiv 0 \pmod{p}$. Así, $x = px_1$, $y = py_1$ y $p = (x_1 + y_1)(x_1^2 - x_1 y_1 + y_1^2)$ con ambos factores ≥ 2, lo que no es posible al ser p primo.
2. Posiblidad $p = 3$. En este caso, $3^4 = x^3 + y^3$ no es tampoco posible sin más que examinar los posibles valores de x ($x = 2, 3, 4$).

Así pues, el único primo posible es $p = 2$.

38. Módulo 4, $3^a - 8 = x^2$ se convierte en $(-1)^a \equiv x^2$. Los cuadrados módulo 4 son $0, 1$, por lo que a es par; es decir, $a = 2b$. Cambiando x por $-x$ podemos asumir que $x \geq 1$ y así $-8 = x^2 - (3^b)^2 = (x - 3^b)(x + 3^b)$ implica que $(x + 3^b, x - 3^b) \in \{(1, -8), (2, -4), (4, -2), (8, -1)\}$. Sumando las componentes de la pareja tenemos $2x \in \{-7, -2, 2, 7\}$. Así, $x = 1$. Por tanto las soluciones para x son $x = \pm 1$ y las posibles potencias de 3 son $\{9\}$.

39. Supongamos que n sí divide a 2^n-1. Consideramos el menor primo p que divida a n. Por un lado, $2^n \equiv 1 \pmod{p}$ y por otro lado, por el pequeño teorema de Fermat, $2^{p-1} \equiv 1 \pmod{p}$. Así, por la identidad de Bézout, $2^{\mathrm{mcd}(n,p-1)} \equiv 1 \pmod{p}$. Ahora bien, al ser p el menor primo que divide a n, $\mathrm{mcd}(n, p-1) = 1$. Por tanto $2 \equiv 1 \pmod{p}$, lo que implica que $1 = 2-1$ es múltiplo de p. Imposible. Así que n no divide a 2^n-1.

40. Comprobando para $p = 2, 3, 5, 7$ vemos que $p = 3, 7$ son respuestas válidas pero $2, 5$ no. Nos fijamos en los primos $p = 2k+1 \geq 11$. Aquí $k \geq 5$.

Sabemos que $2^{p-1} - 1 = pm^2$ para algún m. Por tanto $pm^2 = 2^{2k} - 1 = (2^k-1)(2^k+1)$. Puesto que $\mathrm{mcd}(2^k-1, 2^k+1)$ divide a 2 pero 2^k+1 es impar, este mcd es 1. En particular, uno de ellos tiene que ser un cuadrado perfecto.

Si $2^k + 1 = a^2$ entonces, como $k \geq 5$, $a \geq 5$. Ahora bien, $2^k = a^2 - 1 = (a-1)(a+1)$ y $\mathrm{mcd}(a-1, a+1)$ divide a 2. Por tanto o bien $a-1 \in \{1, 2\}$ o bien $a+1 \in \{1, 2\}$, lo que es imposible ya que $a \geq 5$.

Si $2^k - 1 = a^2$ entonces, como $k \geq 5$, módulo 4 tendremos $-1 \equiv a^2$, lo que es también imposible.

Concluimos que los únicos primos que cumplen la condición son $p = 3, 7$.

41. El caso $(1, p)$ es válido para cualquier primo p. Mirando los posibles n para $p = 2$ y $p = 3$ obtenemos los casos $(2, 2)$ y $(3, 3)$. Nos centramos en primos $p \geq 5$ y $n \geq 2$. En tales casos, obviamente n es impar.

Elegimos un primo q mínimo que divida a n, así $(p-1)^n + 1 \equiv 0 \pmod{q}$. Por tanto, $p-1$ es primo con q y así también $(p-1)^{q-1} \equiv 1 \pmod{q}$. Puesto que $\mathrm{mcd}(2n, q-1) = 2$, por la identidad de Bézout deducimos que $(p-1)^2 \equiv 1 \pmod{q}$. Es decir, o bien $p-1 \equiv -1$ o bien $p-1 \equiv 1 \pmod{q}$. En el primer caso $p = q$ mientras que en el segundo $1 \equiv (p-1)^n \equiv -1 \pmod{q}$ implica que $q = 2$, lo que es imposible ya que n es impar. Concluimos que $p = q$ divide a n. Además, por la cota sobre n esto implica que $n = p$.

Hemos de ver ahora qué primos ≥ 5 cumplen que $(p-1)^p + 1$ es divisible por p^{p-1}. Una forma muy bonita es desarrollar

$$(p-1)^p + 1 = p^p - \binom{p}{1}p^{p-1} \pm \cdots + \binom{p}{p-1}p - 1 + 1$$

para observar que la mayor potencia de p que lo divide la determina $\binom{p}{p-1}p = p^2$. Por tanto $p - 1 \leq 2$, lo que es imposible. Así que solamente aparecen como soluciones $(1, p), (2, 2), (3, 3)$.

Otra forma es escribirse $(p-1)^p + 1 = cp^{p-1}$ para algún c. Módulo $p-1$ obtenemos que $c \equiv 1$. Por tanto $c \in \{1, p, 2p, \dots\}$. Puesto que $(p-1)^p + 1 < p^p$ obtenemos que $c = 1$, es decir $(p-1)^p + 1 = p^{p-1}$. En este punto puede usarse el lema LTE para concluir que $p - 1 = v_p((p-1)^p + 1)) = v_p(p) + v_p(p) = 2$, lo que implica que $p = 3$, imposible ya que $p \geq 5$.

Otra forma más es, en lugar de usar el lema LTE, escribirse $(p-1)^p = p^{p-1} - 1 = (p^k - 1)(p^k + 1)$ donde $2k = p - 1$ (aquí $k \geq 2$). El factor $p^k + 1$ tiene mcd máximo común divisor 2 con $p - 1$. Por tanto $p^k - 1$ es una potencia de 2 (y es ≥ 24). El factor

$p^k + 1$ también tiene mcd 2 con $p^k - 1$, así que $p^k - 1$ no puedes ser múltiplo de 4. Si k es par, $p^k - 1$ es múltiplo de 4, imposible. Si k es impar entonces $p^k + 1 = 2^{p-1}$ y así $(2k+1)^k + 1 = 4^k$. Esto implica $k \leq 1$ y por tanto $p \leq 3$, imposible.

42. Demostramos la sugerencia. Primero observamos que

$$\boxed{\text{mcd}(2^m - 1, 2^n - 1) = 2^{mcd(m,n)} - 1}$$

En efecto, si $d = \text{mcd}(2^m - 1, 2^n - 1)$ entonces $2^m \equiv 1$ y $2^n \equiv 1$ (mód d). Por tanto, usando la identidad de Bézout, $2^{\text{mcd}(m,n)} \equiv 1$ (mód d). Así que d divide a $2^{\text{mcd}(m,n)} - 1$. Ahora bien, $2^{\text{mcd}(m,n)} - 1$ es divisor común de $2^m - 1$ y $2^n - 1$ ya que $2^m \equiv 1, 2^n \equiv 1$ (mód $2^{\text{mcd}(m,n)} - 1$). Por tanto $\text{mcd}(2^m - 1, 2^n - 1) = 2^{\text{mcd}(m,n)} - 1$.

Como $\text{mcd}(2^a + 1, 2^b + 1)$ divide a $\text{mcd}(2^{2a} - 1, 2^{2b} - 1) = 2^{\text{mcd}(2a,2b)} - 1 = 2^2 - 1 = 3$ ya que a y b eran números impares primos entre sí podemos concluir que $\text{mcd}(2^a + 1, 2^b + 1)$ es a lo sumo 1 o 3. Como $2 \equiv -1$ (mód 3) entonces $2^a + 1 \equiv 0$ (mód 3), lo mismo que $2^b + 1$. Así que

$$\boxed{\text{mcd}(2^a + 1, 2^b + 1) = 3 \text{ si } a, b \text{ son impares primos entre sí}}$$

Basta demostrar que $2^{p_1 \cdots p_n} + 1$ tiene al menos $2n$ divisores primos distintos.

Examinamos el caso de un solo primo p_1. Hemos visto que $2^{p_1} + 1$ es múltiplo de 3 pero no de $9 = 2^3 + 1$ ya que p_1 es primo con 3. Como $2^{p_1} + 1 \equiv 1$ (mód 4) y $3 \equiv -1$ (mód 4) entonces $2^{p_1} + 1$ posee un divisor primo $\neq 3$ que es congruente con -1 módulo 4 y que aparece elevado a una potencia impar (a este tipo de divisores primos de un número los vamos a llamar **divisores buenos**). Puesto que $2^{p_1} + 1$ posee al menos dos divisores primos, tiene al menos 4 divisores.

Examinamos el caso general. Basta demostrar (por inducción) que $2^{p_1 \cdots p_n} + 1$ tiene al menos $2n - 1$ divisores buenos ya que junto con el 3 esto da al menos $2n$ divisores primos, y por tanto al menos 4^n divisores.

Que $2^{p_1} + 1$ tiene al menos $2 * 1 - 1 = 1$ divisores buenos lo hemos visto. Supuesto que $2^{p_1 \cdots p_{n-1}} + 1$ tiene al menos $2(n-1) - 1$, como $2^{p_1 \cdots p_{n-1}} + 1$ y $2^{p_n} + 1$ dividen a $2^{p_1 \cdots p_n} + 1$, usando la sugerencia obtenemos al menos $2n-2$ divisores buenos. Pero como $2^{p_1 \cdots p_n} + 1 \equiv 1$ (mód 4) entonces además del 3 y de esos $2n-2$ divisores buenos debe aparecer algún otro divisor bueno. Por tanto hay al menos $2n - 1$ divisores buenos para $2^{p_1 \cdots p_n} + 1$.

43. Consideramos cualquier p que divida a n. Módulo p se tiene que $2^n \equiv -1$. Así que $2^{2n} \equiv 1$, al igual que 2^{p-1}. Por la identidad de Bézout, $2^{\text{mcd}(2n,p-1)} \equiv 1$ (mód p).

Si p es el menor primo que divide a n entonces n es primo con $p - 1$ y así, por lo anterior, $2^2 \equiv -1$ (mód p). Es decir, $p = 3$. Para hallar el exponente de 3 como divisor de n observamos que por el lema LTE y por ser n^2 divisor de $2^n + 1$,

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

lo que implica que $v_3(n) = 1$. Por tanto podemos escribir n como $n = 3m$ donde m es primo con 3. Obtenemos que $9m^2$ divide a $8^m + 1$.

Si $m = 1$ entonces $n = 3$ y tenemos una solución correcta. Si $m \neq 1$ entonces nos volvemos a fijar en el menor primo q que divida a m. Por el mismo motivo que antes, $2^{\mathrm{mcd}(2n,q-1)} \equiv 1 \pmod{q}$ y como m es primo con $q-1$ entonces $2^{2*3} \equiv 1 \pmod{q}$. Esto implica que $q = 7$. Así pues, módulo 7, $9m^2 \equiv 0 \equiv 8^m + 1 \equiv 2$, lo que no es posible. Concluimos que $n = 3$ es la única solución.