HOJA 3 – ALGORITMOS POLINOMIALES Y ALGORITMOS DE FACTORIZACIÓN

1. Decide si $f(n_1, n_2, \log(n_3)) = n_1^2 + m_3 n_2^5$ es $\to O(n_1 n_2)$, $\to O(n_1^2 n_2^3)$, $\to O(n_1^2 n_2^5 m_3)$

$$\frac{n_1^2 + m_3 n_2^5}{n_1 n_2} \xrightarrow[n_2 \to \infty]{n_1 \to \infty} \infty \qquad \text{NO es } O(n_1 n_2)$$

$$\frac{n_1^2 + m_3 n_2^5}{n_1^2 n_2^3} \xrightarrow{n_2 \to \infty} \infty \qquad \text{NO es } O(n_1^2 n_2^3)$$

$$\frac{n_1^2 + m_3 n_2^5}{n_1^2 n_2^5 m_3} = \frac{1}{n_2^5 m_3} + \frac{1}{n_1^2} \underset{\substack{n_1, n_2, n_3 \geq 1 \\ m_3 > e}}{<} 2 \implies \underline{\text{es } O(n_1^2 n_2^5 m_3)}$$

2.

i) $p^a \| n \implies \exists K \in \mathbb{N} : Kp^a = n \wedge p \nmid K$

$p^b \| m \implies \exists q \in \mathbb{N} : qp^b = m \wedge p \nmid q$

$nm = Kp^a qp^b = (Kq)\underbrace{p^a p^b}_{p^{a+b}} \wedge p \nmid (Kq) \implies$

$\implies p^{a+b} \| nm \wedge p^{a+b+1} \nmid nm$ porque $p \nmid (Kq)$ $\blacksquare$

ii) $p^a \| n \implies \exists K \in \mathbb{N} : Kp^a = n \wedge p \nmid K$

$p^b \| m \implies \exists q \in \mathbb{N} : qp^b = m \wedge p \| q$

$n+m = Kp^a + qp^b$

Como $a < b \implies b = a + c$ para algún $c \in \mathbb{N}$

$n+m = Kp^a + qp^b = Kp^a + qp^{a+c} = Kp^a + qp^a p^c = p^a(K + qp^c)$

$\implies p^a \| p^a(K + qp^c) \implies p^a \| nm$, porque $p \nmid (K + qp^c)$ porque $p \nmid K$ $\blacksquare$

Contraejemplo: $p = 2$, $a = 3$, $b = 2$

$\boxed{3.}$ i) Llamemos $d < \sqrt{n}$ un divisor de n.

La biyección $f(d) = \frac{n}{d}$ cumple la condición pues

$$\frac{n}{d} > \frac{n}{\sqrt{n}} = \sqrt{n}$$

La inyectividad se cumple ya que $f(d_1) = f(d_2) \Rightarrow$

$$\Rightarrow \frac{n}{d_1} = \frac{n}{d_2} \Rightarrow d_1 = d_2$$

La sobreyectividad también ya que sea $d' > \sqrt{n}$ un divisor de n, entonces $\exists d < \sqrt{n} : f(d) = d'$, con $d = \frac{n}{d'}$ ya que:

① $d = \frac{n}{d'} \underset{\substack{\uparrow \\ d' > \sqrt{n}}}{<} \frac{n}{\sqrt{n}} = \sqrt{2}$ ② $f(d) = f(n/d') = n/(n/d') = d'$

ii) $n = s^2 - t^2 = (s+t)(s-t)$, donde $s+t = a$ y $s-t = b$

a, b son divisores de n. Como hemos visto en el ejercicio anterior, $a \geq \sqrt{n}$ y queda fijado $b \leq n$ mediante una biyección. Resolviendo el sistema anterior $\begin{cases} s = \frac{a+b}{2} \\ t = \frac{a-b}{2} \end{cases}$

Como s, t son combinaciones lineales $a \longrightarrow (a,b) \longrightarrow \left(\frac{a+b}{2}, \frac{a-b}{2}\right)$

Además, $s, t \in \mathbb{Z}$ ya que como n es impar $\Rightarrow a, b$ impares.

iii) • $n = 15 = 3.5$

$$\begin{matrix} a = 5 \\ b = 3 \end{matrix} \Rightarrow \begin{matrix} s = \frac{5+3}{2} = 4 \\ t = \frac{5-3}{2} = 1 \end{matrix} \rightarrow n = 15 = 4^2 - 1^2 = 16 - 1$$

• $n = 45 = 9.5 = 3^2.5$; $\sqrt{45} \approx 6'71$

$$\begin{matrix} a = 9 \\ b = 5 \end{matrix} \Rightarrow \begin{matrix} s = \frac{9+5}{2} = 7 \\ t = \frac{9-5}{2} = 2 \end{matrix} \rightarrow n = 45 = 7^2 - 2^2 = 49 - 4$$

iv) divisores de 225: 1, 3, 5, 9, 15, 25, 45, 75, 225; $\sqrt{225} = 15$

$n = 25.9 \rightarrow \begin{cases} a = 25 \\ b = 9 \end{cases} \Rightarrow \begin{cases} s = \frac{25+9}{2} = 17 \\ t = \frac{25-9}{2} = 8 \end{cases} \Rightarrow n = 225 = 17^2 - 8^2 = 289 - 64$

$n = 45.5 \rightarrow \begin{cases} a = 45 \\ b = 5 \end{cases} \Rightarrow \begin{cases} s = \frac{45+5}{2} = 25 \\ t = \frac{45-5}{2} = 20 \end{cases} \Rightarrow n = 225 = 25^2 - 20^2 = 625 - 400$

$n = 75.3 \rightarrow \begin{cases} a = 75 \\ b = 3 \end{cases} \Rightarrow \begin{cases} s = \frac{75+3}{2} = 39 \\ t = \frac{75-3}{2} = 36 \end{cases} \Rightarrow n = 225 = 39^2 - 36^2 = 1521 - 1296$

$n = 225.1 \rightarrow \begin{cases} a = 225 \\ b = 1 \end{cases} \Rightarrow \begin{cases} s = \frac{225+1}{2} = 113 \\ t = \frac{225-1}{2} = 112 \end{cases} \Rightarrow n = 225 = 113^2 - 112^2 = 12769 - 12544$

$\boxed{4.}$

i) $187 = 5.34 + 17 \longrightarrow 17 = \underbrace{187}_{a} - 5.\overbrace{34}^{b}$

ii) $841 = 5.160 + 41$ $(**) \equiv 41 = 841 - 5.160$

$160 = 3.41 + 37$ $(*)$

$41 = 1.37 + 4 \longrightarrow 4 = 41 - 37$

$37 = 9.4 + 1 \longrightarrow 37 - 9.4 = 1$

$4 = 4.1 + 0$

$\Rightarrow 37 - 9.(41 - 37) = 1 \Rightarrow$

$\Rightarrow 10.37 - 9.41 = 1$

$(*)$ $37 = 160 - 3.41$

$\Rightarrow 10(160 - 3.41) - 9.41 = 1 \Rightarrow 10.160 - 39.41 = 1$

$\overset{(**)}{\Rightarrow} 10.160 - 39(841 - 5.160) = 1 \Rightarrow$

$\Rightarrow \boxed{-39.\underbrace{841}_{a} + 205.\underbrace{160}_{b} = 1}$

$\boxed{5.}$

i) $360 = 2^3 . 3^2 . 5$
$294 = 2.3.7$ $\Big\} \Rightarrow mcd(360,294) = 2.3 = 6$

ii) $360 = 1.294 + 66$

$294 = 4.66 + 30$

$66 = 2.33 + 6 \longrightarrow mcd(360,294) = 6$

$30 = 5.6 + 0$

$\boxed{6.}$ n impar

$$(b+1)(b^{n-1} - b^{n-2} + \cdots + b^2 - b + 1) = b^n \cancel{- b^{n-1}} \underbrace{\cancel{+ b^{n-2}} - \cdots \cancel{- b^4}}_{\#\text{ impar}} \cancel{+ b^3} \cancel{- b^2} \cancel{+ b}$$
$$\cancel{+ b^{n-1}} \cancel{- b^{n-2}} \underbrace{\cancel{+ b^{n-3}} - \cdots \cancel{- b^3}}_{\#\text{impar}} \cancel{+ b^2} \cancel{- b} + 1 = (b^n + 1)$$

$\boxed{7.}$ $$(b-1)(b^{n-1} + b^{n-2} + \cdots + b^2 + b + 1) = b^n \cancel{+ b^{n-1}} \cancel{+ b^{n-2}} + \cdots \cancel{+ b^3} \cancel{+ b^2} +$$
$$\cancel{+ b} \cancel{- b^{n-1}} \cancel{- b^{n-2}} - \cdots \cancel{- b^2} \cancel{- b} - 1 = b^n - 1$$

$\boxed{8.}$ Contrarecíproco: Si $n \geq 2$ es no primo, entonces $2^n - 1$ no es primo tampoco

Si $n \geq 2$ no es primo, existen $x, y > 1$ tal que $n = xy$.

Tenemos $2^n - 1 = 2^{xy} - 1 = (2^y)^x - 1 = (2^y - 1)(2^{y(x-1)} + 2^{y(x-2)} + \cdots +$
$+ 2^{y.1} + 2^{y.0})$. Como $y > 1$, entonces $2^y - 1 > 1$. Como $x > 1$,
entonces $2^y - 1 < 2^n - 1$.

$2^n - 1$ tiene un propio divisor $2^y - 1 > 1$, por lo que hemos mostrado que $2^n - 1$ es compuesto. ($\equiv$ no primo).

■

$\boxed{9.}$ Para cualquier natural impar a, el polinomio $x+1$ divide a x^a+1.

En particular, tenemos:

$$\frac{x^a+1}{x+1} = \frac{(-x)^a-1}{(-x)-1} = 1-x+x^2-\cdots+(-x)^{a-1}$$

Por la fórmula de la suma geométrica.

En este caso, para $x = 2^{2^m}$ tenemos un divisor no trivial. ∎