Ejercicio 7. Sean a y b enteros positivos. Demostrar que: $\text{mcd}(a^n, b^n) = \text{mcd}(a, b)^n$, $\forall\, n \in \mathbb{Z}^+$.

$x = 2^2 \cdot 3^4 \cdot 7^0 \cdot 11$

$y = 2 \cdot 3^5 \cdot 7 \cdot 11^0$

$\text{mcd}(x, y) = 2 \cdot 3^4 \cdot 7^0 \cdot 11^0$

$a = p_1^{\alpha_1} \cdots p_e^{\alpha_e}$ con $\alpha_i \geq 0$

$b = p_1^{\beta_1} \cdots p_e^{\beta_e}$ con $\beta_i \geq 0$

$$\text{mcd}(a,b) = p_1^{\min\{\alpha_1,\beta_1\}} \cdot p_2^{\min\{\alpha_2,\beta_2\}} \cdots p_e^{\min\{\alpha_e,\beta_e\}}$$

$$\text{mcd}(a,b) = \prod_{i=1}^{e} p_i^{\min\{\alpha_i,\beta_i\}}$$

$$ab = \text{mcd}(a,b)\,\text{mcm}(a,b)$$

$$\underbrace{p_1^{\alpha_1} \cdots p_e^{\alpha_e}}_{a}\,\underbrace{p_1^{\beta_1} \cdots p_e^{\beta_e}}_{b} = \underbrace{p_1^{\min\{\alpha_1,\beta_1\}}\, p_2^{\min\{\alpha_2,\beta_2\}} \cdots p_e^{\min\{\alpha_e,\beta_e\}}}_{\text{mcd}(a,b)}\ \text{mcm}(a,b)$$

$p_1^{\min\{\alpha_1,\beta_1\}}\ p_1^{\max\{\alpha_1,\beta_1\}} \cdots$

$$\text{mcm}(a,b) = \prod_{i=1}^{e} p_i^{\max\{\alpha_i,\beta_i\}}$$

$x = 2^2 \cdot 3^4 \cdot 7^0 \cdot 11$

$y = 2 \cdot 3^5 \cdot 7 \cdot 11^0$

$\text{mcm}(x,y) = 2^2 \cdot 3^5 \cdot 7 \cdot 11$

---

a, b enteros positivos

queremos ver que: $\text{mcd}(a^n, b^n) = \text{mcd}(a,b)^n$ para $n \in \mathbb{Z}^+$

$a = p_1^{\alpha_1} \cdots p_e^{\alpha_e}$ con $\alpha_i \geq 0$

$b = p_1^{\beta_1} \cdots p_e^{\beta_e}$ con $\beta_i \geq 0$

$$\text{mcd}(a,b) = \prod_{i=1}^{e} p_i^{\min\{\alpha_i,\beta_i\}}$$

$$a^n = (p_1^{\alpha_1} \cdots p_\ell^{\alpha_\ell})^n = p_1^{n\alpha_1} \cdots p_\ell^{n\alpha_\ell}$$

$$\min\{3\alpha, 3\beta\} = 3\min\{\alpha, \beta\}$$

$$b^n = (p_1^{\beta_1} \cdots p_\ell^{\beta_\ell})^n = p_1^{n\beta_1} \cdots p_\ell^{n\beta_\ell}$$

$$\text{mcd}(a^n, b^n) = \prod_{i=1}^{\ell} p_i^{\min\{n\alpha_i, n\beta_i\}}$$

$$= \prod_{i=1}^{\ell} p_i^{n\cdot\min\{\alpha_i, \beta_i\}}$$

$$= p_1^{n\cdot\min\{\alpha_1, \beta_1\}} \, p_2^{n\cdot\min\{\alpha_2, \beta_2\}} \cdots p_\ell^{n\cdot\min\{\alpha_\ell, \beta_\ell\}}$$

$$= \left(p_1^{\min\{\alpha_1, \beta_1\}} \, p_2^{\min\{\alpha_2, \beta_2\}} \cdots p_\ell^{\min\{\alpha_\ell, \beta_\ell\}}\right)^n$$

$$= \left(\prod_{i=1}^{\ell} p_i^{\min\{\alpha_i, \beta_i\}}\right)^n$$

$$= \text{mcd}(a, b)^n$$

<u>otra forma</u>:

$d = \text{mcd}(a, b)$

$\Rightarrow a = da^*$, $b = db^*$ con a^* y b^* coprimos

$4 \mid 2^4$

$4 \nmid 2$

$$\text{mcd}(a^n, b^n) = \text{mcd}((da^*)^n, (db^*)^n)$$

$$= \text{mcd}(d^n (a^*)^n, d^n (b^*)^n)$$

$$= d^n \underbrace{\text{mcd}((a^*)^n, (b^*)^n)}_{=1}$$

$$= d^n$$

$$= \text{mcd}(a, b)^n$$

supongamos que a^* y b^* no son coprimos

$\Rightarrow p \mid (a^*)^n$ y $p \mid (b^*)^n$ p primo

$\Rightarrow p \mid a^*$ y $p \mid b^*$

pero a^* y b^* son coprimos

absurdo!

Ejercicio 9. Demostrar que $\sqrt{pq}$ y $\log_{30}(pq)$ son irracionales para cualquier par de primos distintos p, q.

p, q primos distintos

* $\log_{30}(pq)$ es irracionales

$$\log_{30}(pq) = a \iff 30^a = pq$$

Supongamos por absurdo que $\log_{30}(pq)$ es racional

$$\Rightarrow \log_{30}(pq) = \frac{m}{n} \quad \text{con } m, n \in \mathbb{Z}^+$$

$$\Rightarrow 30^{\frac{m}{n}} = pq$$

$$\Rightarrow 30^m = (pq)^n$$

$$\Rightarrow (2 \cdot 3 \cdot 5)^m = (pq)^n$$

$$\Rightarrow 2^m \cdot 3^m \cdot 5^m = p^n q^n$$

esto es absurdo por la unicidad de la descomposición en primos

* $\sqrt{pq}$ es irracional

Supongamos que $\sqrt{pq}$ es racional

$$\sqrt{pq} = \frac{m}{n} \quad \text{con } m, n \in \mathbb{Z}^+$$

$$\Rightarrow pq = \frac{m^2}{n^2}$$

$$\Rightarrow n^2 pq = m^2$$

p primo

$$\underline{p} n^2 q = m^2 \Rightarrow p \mid m^2 \Rightarrow p \mid m$$

$\Rightarrow p$ está en la descomposición en primos de m

$$\Rightarrow m = p^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_e^{\alpha_e}$$

$$\Rightarrow m^2 = p^{2\alpha_1} p_2^{2\alpha_2} p_3^{2\alpha_3} \cdots p_e^{2\alpha_e}$$ con $\alpha_1 \geq 1$

como n^2 es cuadrado perfecto

$$n^2 = p^{2\beta_1} q_2^{2\beta_2} q_3^{2\beta_3} \cdots q_k^{2\beta_k}$$ con $\beta_1 \geq 0$

$$n^2 pq = m^2$$

$$p^{2\beta_1} q_2^{2\beta_2} \cdots q_k^{2\beta_k}\, pq = p^{2\alpha_1} p_2^{2\alpha_2} \cdots p_e^{2\alpha_e}$$

$$\underbrace{p^{2\beta_1+1} q_2^{2\beta_2} \cdots q_k^{2\beta_k}\, q}_{\text{p está elevado a una potencia impar}} = \underbrace{p^{2\alpha_1} p_2^{2\alpha_2} \cdots p_e^{2\alpha_e}}_{\text{p está elevado a una potencia par}}$$

imposible por la unicidad de la descomposición en primos

Ejercicio 14.

a. Probar que si $p > 2$ es primo, entonces es de la forma $4k+1$ o $\overset{4k-1}{4k+3}$, para algún $k \in \mathbb{Z}$. Sugerencia: trabajar con el resto de una división entera, analizando cada posible valor del resto.

b. Probar que si $p > 3$ es primo, entonces es de la forma $6k+1$ o $6k+5$, para algún $k \in \mathbb{Z}$.

c. Probar que existen infinitos primos de la forma $4k+3$. Sugerencia: imitar la prueba de Euclides sobre la infinitud de primos.

a) p primo $p > 2$

tenemos 4 posibilidades al dividir entre 4:

1. $p = 4k$

$\Rightarrow 4 \mid p \Rightarrow p$ no es primo <u>absurdo</u>

2. $p = 4k+1$ ✓

3. $p = 4k+2 = 2(2k+1) \Rightarrow 2 \mid p$ → $p = 2$ ✗ ; → $p \neq 2$ y divisible entre 2 ✗

4. $p = 4k+3$ ✓ $\quad p = 4k+3 = 4k+4-1 = 4(k+1)-1$

entonces si $p > 2$ es primo se cumple que $p = 4k+1$ o $\underbrace{p = 4k+3}_{p = 4(k+1)-1}$

b) p primo, $p > 3$

tenemos 6 casos:

1. $p = 6k \Rightarrow 6 | p$ no puede ser porque p es primo

2. $p = 6k+1$

3. $p = 6k+2 = 2(3k+1) \Rightarrow 2|p$ X

4. $p = 6k+3 = 3(2k+1) \Rightarrow 3|p$ → $p=3$ X porque $p>3$; → $p \neq 3$ y divisible ente 3 X

5. $p = 6k+4 = 2(3k+2) \Rightarrow 2|p$ X

6. $p = 6k+5$

c) hay infinitos primos de la forma $4k-1$

supongamos que el conjunto de primos de la forma $4k-1$ es finito $\{p_1, p_2, \dots, p_k\}$

$n = 4 p_1 p_i p_k - 1$

como $n > p_i$ para todo i tenemos que n no es primo

los factores primos de n son de la forma $4k+1$ o $4k-1$

$$(4k-1)(4k_1+1)(4k_2+1) \cdots (4k_e+1) = 4(\quad) - 1$$

por lo menos uno de los factores primos de n es de la forma $4k-1$

entonces hay un p_i que es factor primo de n

$$\left.\begin{array}{l} p_i | n \\ p_i | 4 p_1 p_2 \cdots p_i \cdots p_k \end{array}\right\}$$

$$n = 4p_1 \cdots p_i \cdots p_k - 1$$

$$\underset{\substack{\uparrow \\ \text{divisible} \\ \text{entre } p_i}}{n} - \underbrace{4p_1 \cdots p_i \cdots p_k}_{\substack{\uparrow \\ \text{divisible} \\ \text{entre } p_i}} = -1$$

$\Rightarrow$ -1 es divisible entre p_i

absurdo porque p_i es primo

$\{p_1, \ldots, p_k\}$

$$n = p_1 p_2 \cdots p_k + 1$$