Exercici 14. Siguin a, b nombres naturals no nuls, i siguin

$$a = \prod_p p^{v_p(a)} \quad b = \prod_p p^{v_p(b)}$$

les descomposicions de a i b com a producte de nombres primers. Proveu que

$$\text{mcd}(a,b) = \prod_p p^{\min(v_p(a),v_p(b))} \quad \text{mcm}(a,b) = \prod_p p^{\max(v_p(a),v_p(b))}$$

Solucio 14.

Tenim que $\prod_p p^{\min(v_p(a),v_p(b))} = p_1^{\min(v_{p1}(a),v_{p1}(b))} \cdot \ldots \cdot p_n^{\min(v_{pn}(a),v_{pn}(b))}*$, clarament $p_1^{\min(v_{p1}(a),v_{p1}(b))} \cdot \ldots \cdot p_n^{\min(v_{pn}(a),v_{pn}(b))} | a$ i $p_1^{\min(v_{p1}(a),v_{p1}(b))} \cdot \ldots \cdot p_n^{\min(v_{pn}(a),v_{pn}(b))} | b$, ja que al escolllir sempre el minim exponent per cada factor primer de la descomposicio tenim que si per a, agafem el seguent productori $p_i^{v_{pi}(a)-\min(v_{pi}(a),v_{pi}(b))}$ per $1 \leq i \leq n$, i tenim que $p_i^{v_{pi}(a)-\min(v_{pi}(a),v_{pi}(b))} \in \mathbb{N}$ ja que si $\min(v_{pi}(a), v_{pi}(b)) = v_{pi}(a)$ aleshores $v_{pi}(a) - \min(v_{pi}(a), v_{pi}(b)) = 0$ i $p_i^{v_{pi}(a)-\min(v_{pi}(a),v_{pi}(b))} \in \mathbb{N}$, pero si $\min(v_{pi}(a), v_{pi}(b)) = v_{pi}(b) \implies v_{pi}(a) > v_{pi}(b)$, i per tant $v_{pi}(a) - v_{pi}(b) \in \mathbb{N}$, i per tant $p_i^{v_{pi}(a)-\min(v_{pi}(a),v_{pi}(b))} \in \mathbb{N}$ ara clarament $p_i^{v_{pi}(a)-\min(v_{pi}(a),v_{pi}(b))} \cdot p_1^{\min(v_{p1}(a),v_{p1}(b))} \cdot \ldots \cdot p_n^{\min(v_{pn}(a),v_{pn}(b))} = a$ $1 \leq i \leq n$, per un raonament analog podem veure que $p_1^{\min(v_{p1}(a),v_{p1}(b))} \cdot \ldots \cdot p_n^{\min(v_{pn}(a),v_{pn}(b))} | b$.

Ara provarem que $\nexists\ c \in \mathbb{N}$ tal que $c|a$ i $c|b$ i $c > p_1^{\min(v_{p1}(a),v_{p1}(b))} \cdot \ldots \cdot p_n^{\min(v_{pn}(a),v_{pn}(b))}$. Suposem per reduccio a l'absurd que si que existeix aquest c, aleshores com $c|a$ la descomposicio en factors primers de c, no pot tenir factors que no tingui a** i per tant $\exists\ p_1^{v_{p1}(c)} \cdot \ldots \cdot p_n^{v_{pn}(c)} = c$, aleshores si $c > p_1^{\min(v_{p1}(a),v_{p1}(b))} \cdot \ldots \cdot p_n^{\min(v_{pn}(a),v_{pn}(b))}$, $\implies$ existeix almenys un $v_{pi}(c)$ tal que $v_{pi}(c) > \min(v_{pn}(a), v_{pn}(b))$, pero llavors c no dividira a b o a a***, i per tant hem arribat a una contadiccio. I queda demostrat el que voliem:

$$\text{mcd}(a,b) = \prod_p p^{\min(v_p(a),v_p(b))}$$

Ara, sabem que el $\text{mcm}(a,b) = \frac{a \cdot b}{\text{mcd}(a,b)}$ i per tant $\frac{\prod_p p^{v_p(a)} \cdot \prod_p p^{v_p(b)}}{\prod_p p^{\min(v_p(a),v_p(b))}} = \prod_p p^{\max(v_p(a),v_p(b))}$, ja que per cada p_i $1 \leq i \leq n$, tenim que es cancel·la el que te menor grau i per tant ens quendem amb el que te major grau per la definicio del mcd.

* considerem $p_1, .., p_n$ els factors primers que apareixen en les descomposicons en factors primers de a i b, de manera que si algun factor p_i, no hi es en una descomposicio d'un dels dos nombres el seu exponent es 0.

** Ja que $\forall$ q primer, tal que apareix en la descomposicio de c tenim que $q|c$ i $c|a \implies q|a$.

*** Ja que si $v_{pi}(c) > \min(v_{pn}(a), v_{pn}(b))$ per un cert i, tenim que si $\min(v_{pn}(a), v_{pn}(b)) = v_{pn}(b)$ tenim que $p_{i\,pi}^{v}(c) | \prod_p p^{v_p(b)} \implies p_{i\,pi}^{v}(c) | p_{i\,pi}^{v}(b)$, i si existis un k tal que $p_{i\,pi}^{v}(c)k = p_{i\,pi}^{v}(b)$ aleshores $k = p_i^{v_{pi}(b)-v_{pi}(c)}$ es un racional, ja que l'exponent de p_i es negatiu.