Décomposition en facteurs premiers et valuation p-adique

Th Soit $n \in \mathbb{N}$ et $n \geq 2$. $\exists\, r \in \mathbb{N}^*$ ainsi que des nombres premiers $p_1 < p_2 < \dots < p_r$ et des entiers naturels $\alpha_1, \dots \alpha_r$ non nuls tels que
$$n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$$
Cette décomposition est unique. Les nombres $p_1, \dots, p_r$ sont appelés les facteurs premiers de n.

Soit p un nombre premier. Pour tout entier naturel n non nul, l'ensemble des entiers naturels k tels que $p^k \mid n$ est non vide (il contient 0) et majoré (par exemple par n puisque $p^n \geq n$ par récurrence immédiate). Il possède donc un plus grand élément.

Déf : Soit p un nombre premier. Pour tout entier naturel n non nul, on appelle valuation p-adique de n, noté $v_p(n)$ le plus grand entier $k \in \mathbb{N}$ tel que $p^k \mid n$.

Lemme = Etant donné $p \in \mathcal{P}$ et $n \in \mathbb{N}^*$, on a
$$v_p(n) = k \iff \exists\, q \text{ premier avec } p \text{ tel que } n = p^k q$$

Preuve : Si $k = v_p(n)$ alors $p^k \mid n$. Ecrivons donc $n = p^k q$
$p^{k+1} \nmid n$ donc p ne divise pas q
et comme p est premier alors $p \wedge q = 1$

Réciproquement, supposons $n = p^k q$ avec $p \wedge q = 1$
donc $p^k \mid n$ mais $p^{k+1} \nmid n$ puisque $p \nmid q$.

Rq : 1) Si $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ avec $p_1 < \dots < p_r$

Alors $\forall i \in [\![1, r]\!]$ $v_{p_i}(n) = \alpha_i$

En effet, $\forall i \in [\![1, r]\!]$ $n = p_i^{\alpha_i} q$ avec $q = \prod_{j \neq i} p_j^{\alpha_j}$ et $q \wedge p_i = 1$

Avec le lemme, on a :

$$n = \prod_{i=1}^{r} p_i^{v_{p_i}(n)}$$

2) $\forall p \in \mathcal{P} \setminus \{p_1 \dots p_r\}$ $v_p(n) = 0$

donc $n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$ a un sens car il y a un nombre fini de termes non nul.

Prop : Etant donné un nombre premier p et deux entiers naturels a, b non nuls, on a $v_p(ab) = v_p(a) + v_p(b)$

Prop : Etant donné deux entiers naturels non nuls, a et b on a

1) $b \mid a \iff \forall p \in \mathcal{P}$ $v_p(b) \leq v_p(a)$

2) $\forall p \in \mathcal{P}$ $v_p(a \wedge b) = \min(v_p(a), v_p(b))$.

et $v_p(a \vee b) = \max(v_p(a), v_p(b))$

preuve : 1) $\Rightarrow$: $b \mid a$ alors pour tout $p \in \mathcal{P}$ $p^{v_p(b)}$ divise b donc divise a

d'où $v_p(a) \geq v_p(b)$

Réciproquement, supposons $\forall p \in \mathcal{P}$ $v_p(b) \leq v_p(a)$

posons $c = \prod_{p \in \mathcal{P}} p^{v_p(a) - v_p(b)}$ puisque $\{p \in \mathcal{P} \mid v_p(a) - v_p(b) > 0\} \subset \{p \in \mathcal{P} \mid v_p(a) > 0\}$

c est un entier ($\in \mathbb{N}$).

donc $a = bc$

2) Posons $d = \prod_{p \in \mathcal{P}} p^{\min(v_p(a), v_p(b))}$ et $m = \prod_{p \in \mathcal{P}} p^{\max(v_p(a), v_p(b))}$

Calculons car :

$$\{p \in \mathcal{P} \mid \min(v_p(a), v_p(b)) > 0\} \subset \{p \in \mathcal{P} \mid \max(v_p(b), v_p(a)) > 0\}$$
$$\subset \{p \in \mathcal{P} \mid v_p(a) > 0\} \cup \{p \in \mathcal{P} \mid v_p(b) > 0\}$$

Ce qui prouve que tous ces ensembles sont finis.

Le premier point prouve que d est un diviseur de a et b et que tout diviseur commun de a et b divise d. Donc $d = a \wedge b$.

De même sans doute $m = a \vee b$.

Ainsi si $a = p_1^{\alpha_1} \cdots p_\ell^{\alpha_\ell}$ et $b = p_1^{\beta_1} \cdots p_\ell^{\beta_\ell}$

avec $p_1, \dots, p_\ell$ nombres premiers distincts.

1) $a \mid b \iff \forall i \in [\![1, \ell]\!] \quad \alpha_i \leq \beta_i$

2) $a \wedge b = \prod_{i=1}^{\ell} p_i^{\min(\alpha_i, \beta_i)}$ $\quad a \vee b = \prod_{i=1}^{\ell} p_i^{\max(\alpha_i, \beta_i)}$

Rq importante : $n = p_1^{\alpha_1} \cdots p_\ell^{\alpha_\ell}$

Les diviseurs d de a s'écrivent

$d = p_1^{\delta_1} \cdots p_\ell^{\delta_\ell}$ avec $\forall i \in [\![1, \ell]\!] \quad \delta_i \leq \alpha_i$

Un diviseur de a est donc déterminé par un ℓ-uplet $(\delta_1, \dots, \delta_\ell)$ appartenant à $E = [\![0, \alpha_1]\!] \times \cdots \times [\![0, \alpha_\ell]\!]$

Le nombre de diviseurs de n est le cardinal de $E = \prod_{i=1}^{\ell} (1 + \alpha_i)$