Preuves supplémentaires du chapitre 3
Arithmétique

Proposition 10

Soient $a, b \in \mathbb{N}^*$, on a :

$$\text{pgcd}(a,b).\text{ppcm}(a,b) = a.b.$$

Preuve. Posons $d = \text{pgcd}(a,b)$ et $m = \text{ppcm}(a,b)$. Alors, il existe $\alpha, \beta, \gamma, \delta \in \mathbb{N}$ tels que :

$$a = \alpha d,\ b = \beta d,\ m = \gamma a,\ m = \delta b.$$

- $\alpha\beta d = \beta a = \alpha b$ donc $a|\alpha\beta d$ et $b|\alpha\beta d$, ainsi $m|\alpha\beta d$. Donc, il existe $k \in \mathbb{N}$ tel que : $mk = \alpha\beta d$.
- $mk = \gamma ak = a\beta$ donc $\beta = \gamma k$, donc $k|\beta$.
- $mk = \delta bk = b\alpha$ donc $\alpha = \delta k$, donc $k|\alpha$.
- Ainsi $k|\text{pgcd}(\alpha,\beta)$. Or $\text{pgcd}(a,b) = d = \text{pgcd}(\alpha d, \beta d) = d\text{pgcd}(\alpha,\beta)$. Donc : $\text{pgcd}(\alpha,\beta) = 1$, ainsi $k = 1$.
- D'où $m = \alpha\beta d$, ainsi $md = \alpha d\beta d = ab$.

□

Proposition 13

Soient $a, b \in \mathbb{N} \setminus \{0,1\}$ tels que $a = p_1^{\alpha_1} \dots p_r^{\alpha_r} = \prod_{i=1}^{r} p_i^{\alpha_i}$ et $b = p_1^{\beta_1} \dots p_r^{\beta_r} = \prod_{i=1}^{r} p_i^{\beta_i}$ où $p_1,\ p_2, ...,\ p_r$ est sont des nombres premiers distincts deux à deux, et $\alpha_1, ..., \alpha_r \in \mathbb{N}$, $\beta_1, ..., \beta_r \in \mathbb{N}$ (éventuellement nuls pour tenir compte d'un nombre premier qui pourrait ne diviser qu'un seul des deux entiers a ou b). Alors :

$$\text{pgcd}(a,b) = p_1^{\min(\alpha_1,\beta_1)} \dots p_r^{\min(\alpha_r,\beta_r)} = \prod_{i=1}^{r} p_i^{\min(\alpha_i,\beta_i)}$$

$$\text{ppcm}(a,b) = p_1^{\max(\alpha_1,\beta_1)} \dots p_r^{\max(\alpha_r,\beta_r)} = \prod_{i=1}^{r} p_i^{\max(\alpha_i,\beta_i)}$$

Preuve.

- Posons $d = \prod_{i=1}^{r} p_i^{\min(\alpha_i,\beta_i)}$.
  - Pour tout $i \in [\![1,r]\!]$, $\min(\alpha_i,\beta_i) \leq \alpha_i$. Donc : $a = \prod_{i=1}^{r} p_i^{\alpha_i - \min(\alpha_i,\beta_i) + \min(\alpha_i,\beta_i)} = d.\prod_{i=1}^{r} p_i^{\alpha_i - \min(\alpha_i,\beta_i)}$.
    Ainsi, $d|a$ et, de même, $d|b$.
  - Posons $\alpha = \frac{a}{d}$ et $\beta = \frac{b}{d}$. On a $\alpha, \beta \in \mathbb{N}^*$ et : $\alpha = \prod_{i=1}^{r} p_i^{\alpha_i - \min(\alpha_i,\beta_i)}$ et $\beta = \prod_{i=1}^{r} p_i^{\beta_i - \min(\alpha_i,\beta_i)}$.
    Soit $i \in [\![1,r]\!]$, on a : $\alpha_i - \min(\alpha_i,\beta_i) = 0$ ou $\beta_i - \min(\alpha_i,\beta_i) = 0$ ainsi $p_i \not| \alpha$ ou $p_i \not| \beta$.
    Ainsi α et β n'ont pas de facteur premier commun donc $\text{pgcd}(\alpha,\beta) = 1$.
  - Donc :
    $$\text{pgcd}(a,b) = \text{pgcd}(d\alpha, d\beta) = d\text{pgcd}(\alpha,\beta) = d.$$
- On a : $\text{pgcd}(a,b)\text{ppcm}(a,b) = ab = \prod_{i=1}^{r} p_i^{\alpha_i+\beta_i}$.
  D'où $\text{ppcm}(a,b) \prod_{i=1}^{r} p_i^{\min(\alpha_i,\beta_i)} = \prod_{i=1}^{r} p_i^{\alpha_i+\beta_i}$.
  Ainsi, $\text{ppcm}(a,b) = \prod_{i=1}^{r} p_i^{\alpha_i+\beta_i-\min(\alpha_i,\beta_i)}$.
  Soit $i \in [\![1,r]\!]$, on a : $\alpha_i + \beta_i - \min(\alpha_i,\beta_i) = \max(\alpha_i,\beta_i)$. En effet :
  - Si $\alpha_i \geq \beta_i$. Alors, $\min(\alpha_i,\beta_i) = \beta_i$ et $\max(\alpha_i,\beta_i) = \alpha_i$.
    Ainsi, $\alpha_i + \beta_i - \min(\alpha_i,\beta_i) = \alpha_i + \beta_i - \beta_i = \alpha_i = \max(\alpha_i,\beta_i)$.
  - Si $\alpha_i < \beta_i$. Alors, $\min(\alpha_i,\beta_i) = \alpha_i$ et $\max(\alpha_i,\beta_i) = \beta_i$.
    Ainsi, $\alpha_i + \beta_i - \min(\alpha_i,\beta_i) = \alpha_i + \beta_i - \alpha_i = \beta_i = \max(\alpha_i,\beta_i)$.

□