1. **Existence de la décomposition en facteurs premiers**
   Par récurrence forte sur $n \geq 2$, montrons que n peut s'écrire comme produit de nombres premiers. Il suffira ensuite de regrouper entre eux les nombres premiers égaux pour obtenir la formule proposée.
   La propriété est vraie pour $n = 2$.
   Supposons la propriété vraie jusqu'au rang $n \geq 2$.
   Si $n + 1$ est un nombre premier, alors la propriété est vraie.
   Si $n + 1$ est un nombre composé alors on peut écrire $n + 1 = ab$ avec $2 \leq a \leq n$ et $2 \leq b \leq n$.
   Par hypothèse de récurrence forte, on peut écrire a et b comme produit de nombres premiers et l'on obtient donc $n + 1 = ab$ est un produit de nombres premiers.
   Récurrence établie.

   Unicité de la décomposition en facteurs premiers (à l'ordre près des facteurs)
   Supposons deux écritures $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_N^{\alpha_N}$ et $n = q_1^{\beta_1} q_2^{\beta_2} \cdots q_M^{\beta_M}$ de la forme annoncée.
   Pour tout $1 \leq i \leq n$, on a $p_i | n$ donc p_i divise nécessairement l'un des q_j et dès lors, lui est égal car ce sont des nombres premiers.
   Ainsi $\{p_1, \cdots, p_N\} \subset \{q_1, \cdots, q_M\}$.
   Par un raisonnement symétrique, on obtient l'autre inclusion et donc l'égalité.
   En particulier $M = N$.
   Quitte à permuter les couples (q_j, β_j), on peut supposer $q_1 = p_1, \ldots, q_N = p_N$.
   On a alors $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_N^{\alpha_N} = p_1^{\beta_1} p_2^{\beta_2} \cdots p_N^{\beta_N}$.
   Pour tout $1 \leq i \leq n$, $p_i^{\alpha_i} | n$ et $n = p_1^{\beta_1} p_2^{\beta_2} \cdots p_N^{\beta_N} = p_i^{\beta_i} k$ avec $p_i \wedge k = 1$,
   donc $p_i^{\alpha_i} | p_i^{\beta_i}$ puis $\alpha_i \leq \beta_i$.
   De manière symétrique $\beta_i \leq \alpha_i$ et finalement l'égalité $\alpha_i = \beta_i$.

2. **<u>Enoncé :</u>**

Soit p un nombre premier. Soient a et b deux entiers naturels non nuls. Alors $v_p(ab) = v_p(a) + v_p(b)$

   <u>Démonstration :</u> on note $k = v_p(a)$ et $k' = v_p(b)$.
   D'après le lemme, on peut écrire $a = p^k q$ et $b = p^{k'} r$ avec $p \wedge q = 1$ et $p \wedge r = 1$.
   On a alors $p \wedge qr = 1$ et $ab = p^{k+k'} qr$.
   Le même lemme permet alors de déduire que $v_p(ab) = k + k'$.

3. **<u>Enoncé :</u>**

Soient a et b deux entiers naturels non nuls. $a \mid b \iff \forall p \in \mathbb{P} \quad v_p(a) \leq v_p(b)$

   <u>Démonstration :</u>
   • Supposons que a divise b.
   Alors, pour tout $p \in \mathbb{P}$, $p^{v_p(a)}$ divise a, donc divise b. Par conséquent, $v_p(a) \leq v_p(b)$.

   • Supposons que $\forall p \in \mathbb{P} \quad v_p(a) \leq v_p(b)$.
   On note $\mathbb{P}_b$ l'ensemble des nombres premiers inférieurs à b.
   D'après la décomposition en facteurs premiers, on a :
   $$b = \prod_{p \in \mathbb{P}_b} p^{v_p(b)}$$
   Comme pour tout $p \in \mathbb{P} \setminus \mathbb{P}_b$, on a $v_p(b) = 0$, alors $v_p(a) = 0$.

   Par conséquent, $\quad a = \displaystyle\prod_{p \in \mathbb{P}_b} p^{v_p(a)}$. On pose $c = \displaystyle\prod_{p \in \mathbb{P}_b} p^{v_p(b) - v_p(a)}$

   Alors $c \in \mathbb{N}^*$ (car pour tout $p \in \mathbb{P}_b$, $v_p(b) - v_p(a) \geq 0$) et $ac = b$, donc a divise b.