

4.8 Initialisation : Supposons $n = p_1 = q_1 \cdot \dots \cdot q_s$.

Pour tout $1 \leq i \leq s$, on a $q_i \neq 1$ et $q_i \mid p_1$.

Puisque p_1 est premier, il n'admet que 1 et p_1 pour diviseurs.

C'est pourquoi $s = 1$ et $q_1 = p_1$.

Hérédité : L'égalité $p_1 \cdot \dots \cdot p_r = q_1 \cdot \dots \cdot q_s$ implique que p_r divise $q_1 \cdot \dots \cdot q_s$.

Montrons par récurrence sur s que p_r divise l'un des q_i .

Initialisation : Si $s = 1$, c'est trivial : p_r divise q_1 .

Hérédité : Si p_r divise q_1 , alors le résultat est établi.

Si p_r ne divise pas q_1 , alors p_r et q_1 sont premiers entre eux.

Vu le lemme de Gauss, p_r divise $q_2 \cdot \dots \cdot q_s$.

L'hypothèse de récurrence implique que p_r divise l'un des facteurs premiers q_i ($2 \leq i \leq s$).

Quitte à changer l'ordre des facteurs premiers q_i , on peut supposer que p_r divise q_s .

Comme $p_r \neq 1$, on doit avoir $p_r = q_s$, car q_s n'est divisible que par 1 et q_s .

L'égalité $p_1 \cdot \dots \cdot p_r = q_1 \cdot \dots \cdot q_s = q_1 \cdot \dots \cdot q_{s-1} \cdot p_r$ peut être divisée par p_r pour devenir $p_1 \cdot \dots \cdot p_{r-1} = q_1 \cdot \dots \cdot q_{s-1}$.

L'hypothèse de récurrence implique alors que $r - 1 = s - 1$, c'est-à-dire $r = s$ et que $p_i = q_i$ pour tout $1 \leq i \leq r - 1$, quitte à changer l'ordre des facteurs premiers q_i .