

Rq2: Si d et d' sont des PGCD de a et b , alors $d|a$, $d|b$ donc $d'|d$, mais $d'|a$, $d'|b$, donc $d|d'$.

Ex 3: • Soit $d \in \mathbb{Z}[i\sqrt{5}]$ tel que $d|3$ et $d|2+i\sqrt{5}$, écrivons $d=a+ib\sqrt{5}$.

• Soit $x \in \mathbb{Z}[i\sqrt{5}]^\times$. Alors $1 = |xx^{-1}|^2 = |x|^2 \cdot |x^{-1}|^2$, donc $|x|^2 \in \mathbb{Z}^\times = \{\pm 1\}$.
Or les solutions de $a^2 + 5b^2 = 1$ sont $(1,0)$ et $(-1,0)$, et $a^2 + 5b^2 = -1$ n'a pas de solution dans $\mathbb{Z}^2$, donc $x = \pm 1$. Ainsi $\mathbb{Z}[i\sqrt{5}]^\times = \{\pm 1\}$.

• On a $|d|^2 |3|^2 = 9$, donc $|d|^2 = a^2 + 5b^2 \in \{1, 3, 9\}$.

▷ L'équation $x^2 + 5y^2 = 3$ n'admet pas de solution dans $\mathbb{Z}^2$.

▷ Les solutions de $x^2 + 5y^2 = 9$ sont $(3,0)$ et $(-3,0)$.

Donc $d \in \mathbb{Z}[i\sqrt{5}]^\times$ ou $d = \pm 3$, ce qui montre que 3 est irréductible.

• De même, $|d|^2 |2+i\sqrt{5}|^2 = 9$, donc de même $d = \pm 1$ ou $d = \pm 3$.

Or $3 \nmid 2+i\sqrt{5}$ (car $3 \nmid 2$), donc $d = \pm 1$.

Finalement, $\boxed{3 \nmid (2+i\sqrt{5}) = 1}$

► Par l'absurde, supposons que 3 et $2+i\sqrt{5}$ admettent un PPCM $\mu = a+ib\sqrt{5} \in \mathbb{Z}[i\sqrt{5}]$.

Alors $3(2+i\sqrt{5}) = \pm (3 \nmid (2+i\sqrt{5})) \mu = \pm \mu$

Or $9 = 3 \times 3 = (2+i\sqrt{5})(2-i\sqrt{5})$ donc $\mu | 9$, donc $2+i\sqrt{5} | 3$, mais

$2+i\sqrt{5}$ est non inversible et non associé à 3, et 3 irréductible: Absurde.

► Soit $d = a+ib\sqrt{3} \in \mathbb{Z}[i\sqrt{3}]$ un diviseur commun à 4 et $2+2i\sqrt{3}$.

Alors $d|4$ et $d|2+2i\sqrt{3}$, donc $|d|^2 |16| = |4|^2 = |2+2i\sqrt{3}|^2$, donc $|d|^2 \in \{1, 2, 4, 8, 16\}$.

Or $\forall (x,y) \in \mathbb{Z}^2$, $x^2 + 3y^2 \notin \{2, 8\}$ donc $|d|^2 \in \{1, 4, 16\}$, donc $d = \pm 1$

ou $d \in \{\pm 2, \pm 1 \pm i\sqrt{3}\}$ ou $d \in \{\pm 4, \pm 2 \pm 2i\sqrt{3}\}$. Or:

▷ $2|4$ et $2|2+2i\sqrt{3}$ donc $d \neq \pm 1$.

▷ $4 \nmid 2+2i\sqrt{3}$ et $2+2i\sqrt{3} \nmid 4$ donc $d \notin \{\pm 4, \pm 2 \pm 2i\sqrt{3}\}$.

Donc $d \in \{\pm 2, \pm 1 \pm i\sqrt{3}\}$, et réciproquement ce sont bien des diviseurs communs.

Ce sont donc les seuls. Par l'absurde, si $4 \nmid (2+2i\sqrt{3}) = 2$, alors $1+i\sqrt{3} | 2$, ce qui n'est pas, et si $4 \nmid (2+2i\sqrt{3}) = 1+i\sqrt{3}$, alors $2 | 1+i\sqrt{3}$, ce qui n'est pas non plus.

Prop 5: Soient a et b admettant un PPCM; posons $\delta = \frac{ab}{a \vee b}$, montrons que $\delta = a \wedge b$.
Si $ab = 0$, alors c'est bon. Supposons $ab \neq 0$.

► $ab \in a \wedge b A$, donc $a \vee b | ab$, donc δ est bien défini.

▷ $a \vee b \in aA$: écrivons $a \vee b = ua$.

▷ $a \vee b \in bA$: écrivons $a \vee b = vb$.

► $\delta | a$: $ab = \delta(a \vee b) = \delta vb$, mais $b \neq 0$ donc par intégrité $a = \delta v$.

► $\delta | b$: idem.

► Soit $d \in A$ divisant a et b , montrons que $d | \delta$.

Écrivons $a = d\alpha$ et $b = d\beta$. Alors $d\alpha\beta = a\beta = ab \in a \wedge b A$, donc

$(a \vee b) | d\alpha\beta$: écrivons $d\alpha\beta = w(a \vee b)$. Alors $\delta(a \vee b) = ab = d^2\alpha\beta = dw(a \vee b)$.
Or $a \vee b \neq 0$ (car $ab \neq 0 \in a \wedge b A$) donc par intégrité $\delta = dw$.

Thm 6 (Gauss): Supposons que $a | bc$ et $a \nmid b = 1$. On a $a \wedge bc = c$, mais $a | ac$ et $a | bc$ donc $a | ac \wedge bc = c$.

Prop 7: Supposons A à PGCD. Soit $(a,b) \in (A \setminus \{0\})^2$. Écrivons $a = (a \wedge b)\alpha$ et $b = (a \wedge b)\beta$.

Comme A est à PGCD, $\alpha \wedge \beta$ existe et vaut 1. Posons $\mu = \frac{ab}{\delta} = a \wedge b = a\beta$.

► $\mu \in a \wedge b A$

► Soit $m \in a \wedge b A$, montrons que $\mu | m$. Écrivons $m = u\alpha = v\beta$.

Alors $u\delta\alpha = v\delta\beta$, mais $\delta \neq 0$ donc par intégrité $u\alpha = v\beta$, donc $\alpha | v\beta$ mais $\alpha \wedge \beta = 1$ donc (Gauss) $\alpha | v$. Écrivons $v = \alpha w$. Alors $m = v\beta = \alpha w\beta = w\mu$ et donc $\mu | m$.

Prop 8: Soit $\delta = \prod_{p \in \mathcal{P}} p^{\min(v_p(a), v_p(b))}$. On a $\forall p \in \mathcal{P}$, $v_p(a), v_p(b) \geq \max(v_p(a), v_p(b)) = v_p(\delta)$ donc

$\delta | a$ et $\delta | b$. Soit $d \in A$ tel que $d | a$ et $d | b$. Alors $\forall p \in \mathcal{P}$, $v_p(d) \leq v_p(a), v_p(b)$ donc $\forall p \in \mathcal{P}$, $v_p(d) \leq \min(v_p(a), v_p(b)) = v_p(\delta)$, et $d | \delta$.

Prop 10: ► $a | a \vee b$ donc $(a \vee b)A \subseteq aA$; $b | a \vee b$ donc $(a \vee b)A \subseteq bA$; donc $(a \vee b)A \subseteq aA \cap bA$.

Soit $x \in aA \cap bA$. Alors $(a \vee b) | x$, donc $x \in (a \vee b)A$.

► Si $aA \cap bA = \mu A$, alors $\mu \in aA \cap bA$, et $\forall m \in aA \cap bA$, $\mu | m$, donc $\mu = a \wedge b$.

► Par principalit e, $aA + bA = \delta A$. Montrons que $\delta = a \wedge b$: $aA \subseteq \delta A$ donc $\delta | a$; $bA \subseteq \delta A$ donc $\delta | b$. Soit $d \in A$ tel que $d | a$ et $d | b$, donc $aA \subseteq dA$ et $bA \subseteq dA$, donc $aA + bA \subseteq dA$, i.e. $\delta A \subseteq dA$, i.e. $d | \delta$. La r e iproque est alors imm ediate.

Thm 11: $a \mid b = 1 \Rightarrow aA + bA = (a \mid b)A = A \Rightarrow \exists (u, v) \in A^2: au + bv = 1$

Supposons que $\exists (u, v) \in A^2: au + bv = 1$. Donc $1 \in aA + bA = (a \mid b)A$, donc $a \mid b = 1$.

Appli 15: Montrons que $\text{Ker}((PQ)(f)) = \text{Ker}(P(f)) \oplus \text{Ker}(Q(f))$ si $P \mid Q = 1$.

D'après le théorème de Bézout: $\exists (U, V) \in K[X]^2: PU + QV = 1$

Soit $x + y \in \text{Ker}(P(f)) + \text{Ker}(Q(f))$. Alors $(PQ)(f)(x + y) = (PQ)(f)(y) + (QP)(f)(x) = P(f) \circ Q(f)(y) + Q(f) \circ P(f)(x) = P(f)(0) + Q(f)(0) = 0$, donc $x + y \in \text{Ker}((PQ)(f))$.

Donc $\text{Ker}(P(f)) + \text{Ker}(Q(f)) \subseteq \text{Ker}((PQ)(f))$; en particulier $\text{Ker}(P(f)), \text{Ker}(Q(f)) \subseteq \text{Ker}((PQ)(f))$

Soit $x \in \text{Ker}(P(f)) \cap \text{Ker}(Q(f))$. Alors $1(f)(x) = \text{id}(x) = x = (PU + QV)(f)(x)$

i.e. $x = U(f) \circ P(f)(x) + V(f) \circ Q(f)(x) = U(f)(0) + V(f)(0) = 0$.

Donc $\text{Ker}(P(f)) \cap \text{Ker}(Q(f)) = \{0\}$.

On a montré que $\text{Ker}(P(f)) \oplus \text{Ker}(Q(f)) \subseteq \text{Ker}((PQ)(f))$. Montrons la réciproque: soit $x \in \text{Ker}((PQ)(f))$. Alors: $x = 1(f)(x) = U(f) \circ P(f)(x) + V(f) \circ Q(f)(x) = y + z$

Où $Q(f)(y) = (QUP)(f)(x) = U(f) \circ (PQ)(f)(x) = U(f)(0) = 0$

$P(f)(z) = (PVQ)(f)(x) = V(f) \circ (PQ)(f)(x) = V(f)(0) = 0$

Donc $x \in \text{Ker}(P(f)) \oplus \text{Ker}(Q(f))$

Prop 20: Pour $a \in \mathbb{Z}$, on note $\mathbb{Z}\{a\} = \frac{\mathbb{Z}}{a\mathbb{Z}}$. Pour $p \in \mathcal{P}$, on note $n_p = v_p(n)$ et $m_p = v_p(m)$

$$\begin{aligned} \mathbb{Z}\{nm\} \times \mathbb{Z}\{nm\} &= \mathbb{Z}\left\{\prod_{p \in \mathcal{P}} p^{\min\{n_p, m_p\}}\right\} \times \mathbb{Z}\left\{\prod_{p \in \mathcal{P}} p^{\max\{n_p, m_p\}}\right\} \\ &\stackrel{\text{TAC}}{\simeq} \prod_{p \in \mathcal{P}} \mathbb{Z}\{p^{\min\{n_p, m_p\}}\} \times \prod_{p \in \mathcal{P}} \mathbb{Z}\{p^{\max\{n_p, m_p\}}\} \\ &\simeq \prod_{\substack{p \in \mathcal{P} \\ n_p < m_p}} \mathbb{Z}\{p^{n_p}\} \times \prod_{\substack{p \in \mathcal{P} \\ n_p = m_p}} \mathbb{Z}\{p^{m_p}\} \times \prod_{\substack{p \in \mathcal{P} \\ n_p > m_p}} \mathbb{Z}\{p^{n_p}\} \times \prod_{\substack{p \in \mathcal{P} \\ n_p > m_p}} \mathbb{Z}\{p^{m_p}\} \\ &\stackrel{\text{TAC}}{\simeq} \prod_{p \in \mathcal{P}} \mathbb{Z}\{p^{n_p}\} \times \prod_{p \in \mathcal{P}} \mathbb{Z}\{p^{m_p}\} \\ &\stackrel{\text{TAC}}{\simeq} \mathbb{Z}\left\{\prod_{p \in \mathcal{P}} p^{n_p}\right\} \times \mathbb{Z}\left\{\prod_{p \in \mathcal{P}} p^{m_p}\right\} = \mathbb{Z}\{n\} \times \mathbb{Z}\{m\} \end{aligned}$$

Lemme 21: Supposons que $a = bq + r$. D'une part, $b \mid r$ et $b \mid a$ donc $b \mid a - bq = r$ donc $b \mid r$ et $a \mid b$ et $a \mid a$ donc $a \mid a - bq = r$, donc $a \mid r$. Donc $a \mid b$ et $b \mid r$ sont associés, donc $a \mid b = br$ (NB: un PGCD est défini à un inversible près.)

Algo 22: Soit φ un stathme euclidien définissant une division euclidienne sur A . Par l'absurde, si $\forall n \in \mathbb{N}, r_n \neq 0$, alors $(\varphi(n))_n$ est une suite d'entiers strictement décroissante et minorée par 0, ce qui est impossible. Donc l'algorithme termine.

Ex 23: Soit $(n, m) \in \mathbb{Z}^2$ tel que $n > m$. Soit $n = mq + r$ la division euclidienne de n par m . En notant $P_n = X^n - 1$:

$$\frac{P_n - P_r}{P_m} = \frac{(X^n - 1) - (X^r - 1)}{X^m - 1} = X^r \frac{X^{n-r} - 1}{X^m - 1} = X^r \frac{X^{mq} - 1}{X^m - 1} = X^r \sum_{k=0}^{q-1} (X^m)^k =: Q(X) \in K[X]$$

Donc $P_n = QP_m + P_r$, et $0 \leq r < m$ donc $0 \leq \deg(P_r) < \deg(P_m)$.

Donc P_r est le reste de la division euclidienne de P_n par P_m . En déroulant l'algorithme d'Euclide pour n et m , on le déroule pour P_n et P_m . Ainsi, $P_n \mid P_m = P_{nm} \mid P_0 = P_{nm}$

$M_n = P_n(2)$, donc le raisonnement précédent montre que $M_n = Q(2)M_m + M_r$, et que ceci est la division euclidienne de M_n par M_m . De même, $M_n \mid M_m = M_{n \mid m}$.

$$\begin{array}{r|l} \text{Appli 25: } X^2 - X - 1 & 2X + 1 \\ \hline -(X^2 + \frac{1}{2}X) & \frac{1}{2}X - \frac{3}{4} \\ \hline -\frac{3}{2}X - 1 & \\ \hline -(-\frac{3}{2}X - \frac{3}{4}) & \\ \hline & -\frac{1}{4} \end{array} \quad \begin{array}{l} \text{donc } X^2 - X - 1 = (2X + 1)(\frac{1}{2}X - \frac{3}{4}) - \frac{1}{4} \\ \text{donc } 0 = \varphi^2 - \varphi - 1 = (2\varphi - 1)(\frac{1}{2}\varphi - \frac{3}{4}) - \frac{1}{4} \\ \text{donc } 1 = (2\varphi - 1)(2\varphi - 3) \\ \text{donc } (2\varphi - 1)^{-1} = 2\varphi - 3. \end{array}$$

Prop 26: Soit $\begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2$, soit $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z})$ (donc $ad - bc = \pm 1$).

Vérifions que $x \wedge y = (ax + by) \wedge (cx + dy)$:

$\triangleright x \wedge y \mid x$ et $x \wedge y \mid y$ donc $x \wedge y \mid ax + by$ et $x \wedge y \mid cx + dy$

$\triangleright$ Soit $\delta \in \mathbb{Z}$ tel que $\delta \mid ax + by$ et $\delta \mid cx + dy$. Alors

$\triangleright \delta \mid d(ax + by) - b(cx + dy) = (ad - bc)x = \pm x$, donc $\delta \mid x$
 $\triangleright \delta \mid -c(ax + by) + a(cx + dy) = (ad - bc)y = \pm y$, donc $\delta \mid y$ } donc $\delta \mid x \wedge y$

Cor 27: Si $a = bq + r$, alors $\begin{pmatrix} a \\ r \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}$. D'après l'algo d'Euclide, il existe donc $P \in GL_2(\mathbb{Z})$ telle que $P \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a \mid b \\ 0 \end{pmatrix} \in GL_2(\mathbb{Z})$.

Appli 28: D'après Cor 27, il existe $(P_1, \dots, P_n) \in GL_2(\mathbb{Z})^n$ tel que:
 $\tilde{P}_1 \dots \tilde{P}_n^t(a_1 \dots a_n) = P_1 \dots P_{n-1}^t(a_1 \dots a_{n-2} \ a_{n-1}a_n \ 0)$ où $\tilde{P}_i = \begin{pmatrix} 0 & 1 \\ 0 & P_i \ 0 \end{pmatrix}$
 $= \dots$
 $= \begin{pmatrix} a_1 \dots a_n & 0 \dots 0 \end{pmatrix}$

Donc si $a_1 \dots a_n = 1$, alors il existe $P \in GL_n(\mathbb{Z})$: $P \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, donc $\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = P^{-1} \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ est la première colonne de P^{-1} . Or $P^{-1} \in GL_n(\mathbb{Z})$, donc la famille des colonnes de P^{-1} est une base de $\mathbb{Z}^n$ contenant $\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$. Réciproquement, si P est une matrice de $M_n(\mathbb{Z})$ dont les colonnes forment une base de $\mathbb{Z}^n$ contenant $\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$, alors en développant par rapport à la première colonne, on obtient $\pm 1 = \det(P) = \sum_{i=1}^n (-1)^{1+i} \Delta_{i1} a_i$ qui est une relation de Bézout indiquant que $a_1 \dots a_n = 1$.

Thm 29 (Lamé) : $P(k)$: " Si l'algorithme d'Euclide termine en au moins k étapes, alors $b \geq F_{k+1}$ (et $a \geq F_{k+2}$). "

- $P(1)$: $a > b \geq 1$ donc si l'algo d'Euclide termine en au moins 1 étape, alors $b \geq F_2 = 1$ et $a \geq F_3 = 2$.
 - Soit $k \in \mathbb{N}^*$, supposons $P(k-1)$. Supposons que l'algorithme d'Euclide termine en au moins k étapes. Soit r le reste de la division euclidienne de a par b . Alors l'algorithme d'Euclide pour b et r termine en au moins $k-1$ étapes, donc $b \geq F_{k+1}$ et $r \geq F_{k+2}$, donc $a = bq + r \geq 1 \times F_{k+1} + F_{k+2} = F_{k+3}$.
- (NB : $q \neq 0$ sinon l'algorithme d'Euclide finirait en moins de $k-1$ étapes).

Rq 30 : $\forall n \in \mathbb{N}$, $F_{n+2} = 1 \times F_{n+1} + F_n$, $0 \leq F_n < F_{n+1}$: c'est donc la division euclidienne de F_{n+2} par F_{n+1} , donc leur algo d'Euclide termine en n étapes.

Algo 31 :

- $2a \wedge 2b = 2(a \wedge b)$
- $2a \wedge (2b+1) = a \wedge (2b+1)$: se voit avec la factorisation en premiers
- $(2a+1) \wedge 2b = (2a+1) \wedge b$: idem
- $(2a+1) \wedge (2b+1) = (a-b) \wedge (2b+1)$: Soit $\delta = (2a+1) \wedge (2b+1)$. Alors $\delta | 2b+1$ et $\delta | (2a+1) - (2b+1) = 2(a-b)$. Or $\delta \wedge 2 = 1$ (cf. factorisation) donc (Gauss) $\delta | a-b$.

Soit $d \in \mathbb{Z}$ tel que $d | a-b$ et $d | 2b+1$. Alors $d | (2b+1) + 2(a-b) = 2a+1$, donc $d | \delta$. CQFD.

Prop 39 : Soit $\mu = \text{ppcm}(\{\text{ord}(g)\}_{g \in G})$. Soit $n = \#G$.

Soit $g_0 \in G$ tel que $\text{ord}(g_0) = \max_{g \in G} \text{ord}(g)$. Soit $g \in G$. Soit p un nombre premier. Écrivons $\text{ord}(g_0) = p^a r$, $r \wedge p = 1$ et $\text{ord}(g) = p^b s$, $p \nmid s = 1$.

Alors $\text{ord}(g_0^p) = r$ et $\text{ord}(g^p) = p^b$, $p^b \wedge r = 1$ donc $\text{ord}(g_0^p g^p) = p^b r$.

Or $\text{ord}(g_0)$ est maximal donc $p^b r \leq \text{ord}(g_0) = p^a r$, donc $b \leq a$.

On a montré que $\forall p \in P$, $v_p(\text{ord}(g)) \leq v_p(\text{ord}(g_0))$, donc $\text{ord}(g) | \text{ord}(g_0)$.

Ainsi, $\forall g \in G$, $\text{ord}(g) | \text{ord}(g_0)$, donc $\mu | \text{ord}(g_0)$. Par ailleurs, $\text{ord}(g_0) | \mu$ donc $\text{ord}(g_0) = \mu$.

Lemme 40 : Soit $\bar{d} \in \mathbb{Z}/n\mathbb{Z}$. Montrons que $\text{ord}(\bar{d}) = \frac{n}{n \wedge d}$: Soit $k \in \mathbb{Z}$ tel que $k\bar{d} = \bar{0}$. Alors $n | kd$, donc $\frac{n}{n \wedge d} | k \frac{d}{n \wedge d}$, mais $\frac{n}{n \wedge d} \wedge \frac{d}{n \wedge d} = 1$, donc (Gauss) $\frac{n}{n \wedge d} | k$.

Comme ce sont en fait des équivalences, on a donc bien $\text{ord}(\bar{d}) = \frac{n}{n \wedge d}$.

(Rq : on a montré que $\{k \in \mathbb{Z} | k\bar{d} = \bar{0}\} = \frac{n}{n \wedge d} \mathbb{Z}$, formellement).

Thm 41 : Supposons que $G \cong \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_s\mathbb{Z} \cong \mathbb{Z}/d'_1\mathbb{Z} \times \dots \times \mathbb{Z}/d'_t\mathbb{Z}$, avec $2 \leq d_1 | \dots | d_s$ et $2 \leq d'_1 | \dots | d'_t$. Quitte à échanger, supposons $s \geq t$. Alors :

$$d_s G \cong \frac{d_s \mathbb{Z}}{d_1 \mathbb{Z}} \times \dots \times \frac{d_s \mathbb{Z}}{d_s \mathbb{Z}} \cong \frac{d_s \mathbb{Z}}{d'_1 \mathbb{Z}} \times \dots \times \frac{d_s \mathbb{Z}}{d'_t \mathbb{Z}}$$

Or $\forall a \in \mathbb{N}^*$, $\forall b \in \mathbb{N}^*$, $\frac{b\mathbb{Z}}{a\mathbb{Z}} = \langle \bar{b} \rangle$ donc $\# \frac{b\mathbb{Z}}{a\mathbb{Z}} = \text{ord}(\bar{b}) = \frac{n}{n \wedge b}$.

De là, $\# d_s G = \frac{d_1}{d_1 \wedge d_1} \times \dots \times \frac{d_s}{d_s \wedge d_1} = \frac{\#G}{d_1^s}$ car $\forall i \in [1, s]$, $d_1 | d_i$ et $\#G = d_1 \dots d_s$.

De même, $\# d_s G = \frac{d'_1}{d'_1 \wedge d_1} \times \dots \times \frac{d'_t}{d'_t \wedge d_1} = \frac{\#G}{\prod_{i=1}^t d_1 \wedge d'_i}$ car $\#G = d_1 \dots d'_t$.

Donc $d_1^s = \prod_{i=1}^t d_1 \wedge d'_i \leq \prod_{i=1}^t d_1 = d_1^t$, et comme $d_1 \geq 2$, on en déduit que $s \leq t$, puis $s = t$. Par ailleurs, si $d_1 \nmid d'_1$, alors $d_1 \wedge d'_1 < d_1$, donc $d_1^s = \prod_{i=1}^t d_1 \wedge d'_i < \prod_{i=1}^t d_1 = d_1^t = d_1^s$, ce qui est absurde. Ainsi, $d_1 | d'_1$. Par symétrie, $d'_1 | d_1$, donc $d_1 = d'_1$. En itérant le procédé, on montre que $\forall i \in [1, s]$, $d_i = d'_i$.