

Solution du devoir 2

Auteur : Alexandre Blondin Massé

1. Soient a, b, m sont des nombres naturels quelconques, où $m \neq 0$ et $(a, b) \neq (0, 0)$. Démontrez les deux identités suivantes à propos de la fonction pgcd.

- (a) (5 points) $\text{pgcd}(ma, mb) = m \cdot \text{pgcd}(a, b)$ *Suggestion* : Posez $a = p_1^{x_1} p_2^{x_2} \cdots p_k^{x_k}$, $b = p_1^{y_1} p_2^{y_2} \cdots p_k^{y_k}$ et $m = p_1^{z_1} p_2^{z_2} \cdots p_k^{z_k}$, où k est un nombre positif, les exposants x_k , y_k et z_k sont des nombres entiers positifs ou nuls et p_i est un nombre premier pour $i = 1, 2, \dots, k$, puis calculez les pgcd en fonction des exposants.

Solution: Comme le suggère l'indice, posons

$$\begin{aligned} a &= p_1^{x_1} p_2^{x_2} \cdots p_k^{x_k} \\ b &= p_1^{y_1} p_2^{y_2} \cdots p_k^{y_k} \\ m &= p_1^{z_1} p_2^{z_2} \cdots p_k^{z_k} \end{aligned}$$

où k est un entier positif, p_i est un nombre premier et x_i, y_i et z_i sont des nombres positifs ou nuls, pour $i = 1, 2, \dots, k$. Nous savons que de telles factorisations existent par le théorème fondamental de l'arithmétique. On obtient alors

$$\begin{aligned} \text{pgcd}(ma, mb) &= \text{pgcd}(p_1^{z_1} p_2^{z_2} \cdots p_k^{z_k} p_1^{x_1} p_2^{x_2} \cdots p_k^{x_k}, p_1^{z_1} p_2^{z_2} \cdots p_k^{z_k} p_1^{y_1} p_2^{y_2} \cdots p_k^{y_k}) \\ &= \text{pgcd}(p_1^{x_1+z_1} p_2^{x_2+z_2} \cdots p_k^{x_k+z_k}, p_1^{y_1+z_1} p_2^{y_2+z_2} \cdots p_k^{y_k+z_k}) \\ &= p_1^{\min(x_1+z_1, y_1+z_1)} p_2^{\min(x_2+z_2, y_2+z_2)} \cdots p_k^{\min(x_k+z_k, y_k+z_k)} \\ &= p_1^{z_1+\min(x_1, y_1)} p_2^{z_2+\min(x_2, y_2)} \cdots p_k^{z_k+\min(x_k, y_k)} \\ &= p_1^{z_1} p_2^{z_2} \cdots p_k^{z_k} p_1^{\min(x_1, y_1)} p_2^{\min(x_2, y_2)} \cdots p_k^{\min(x_k, y_k)} \\ &= m \cdot \text{pgcd}(p_1^{x_1} p_2^{x_2} \cdots p_k^{x_k}, p_1^{y_1} p_2^{y_2} \cdots p_k^{y_k}) \\ &= m \cdot \text{pgcd}(a, b) \end{aligned}$$

tel que voulu.

- (b) (5 points) $\text{pgcd}(a, b) = \text{pgcd}(a + b, b)$ *Suggestion* : Montrez que les diviseurs communs de a et b sont exactement les diviseurs communs de $a + b$ et b et donc les pgcd doivent être les mêmes.

Solution: Soit $d = \text{pgcd}(a, b)$ et $e = \text{pgcd}(a + b, b)$. Par définition, d divise a et b , donc d divise $a + b$ et b , de sorte que $d \leq e$ (e étant le *plus grand* diviseur commun de $a + b$ et b). De la même façon, par définition, e divise $a + b$ et b , de sorte que e divise $(a + b) - b = a$ et b . On en conclut que $e \leq d$ (puisque

d est le *plus grand* diviseur commun de a et b). Comme $d \leq e$ et $e \leq d$, on a nécessairement $d = e$.

2. (20 points) Les *mots de Fibonacci* sont définis récursivement comme suit :

$$f_1 = 1, \quad f_2 = 0 \quad \text{et} \quad f_n = f_{n-1} \cdot f_{n-2}, \quad \text{pour tout } n \geq 3,$$

où \cdot est la concaténation de deux mots. Par exemple, $f_3 = f_2 \cdot f_1 = 0 \cdot 1 = 01$, $f_4 = f_3 \cdot f_2 = 01 \cdot 0 = 010$, et ainsi de suite.

- (a) (5 points) Calculez les mots f_n pour $1 \leq n \leq 8$. Pour chacun, indiquez leur longueur ainsi que le nombre de 0 et le nombre de 1 qu'on y trouve. Présentez vos résultats sous la forme d'un tableau.

Solution:

n	f_n	$ f_n $
1	1	1
2	0	1
3	01	2
4	010	3
5	01001	5
6	01001010	8
7	0100101001001	13
8	010010100100101001010	21

- (b) (5 points) Montrez par induction que $|f_n|$ est le n -ième nombre de Fibonacci, pour tout entier $n \geq 1$.

Solution: Rappelons que la suite de Fibonacci est définie par

$$F_1 = F_2 = 1 \quad \text{et} \quad F_n = F_{n-1} + F_{n-2}, \quad \text{pour } n \geq 3.$$

On doit montrer par induction sur n que $|f_n| = F_n$ pour tout entier $n \geq 1$.

CAS DE BASE. On a $|f_1| = |1| = 1$ et $|f_2| = |0| = 1$.

HYPOTHÈSE D'INDUCTION. Il faut utiliser l'induction généralisée dans ce cas.

Supposons que $|f_m| = F_m$ pour tout entier m tel que $1 \leq m < n$.

ÉTAPE INDUCTIVE. On doit montrer que $|f_n| = F_n$ pour tout entier $n \geq 3$. Or,

$$\begin{aligned} |f_n| &= |f_{n-1} \cdot f_{n-2}| \\ &= |f_{n-1}| + |f_{n-2}| \\ &= F_{n-1} + F_{n-2} \\ &= F_n. \end{aligned}$$

L'hypothèse d'induction a été utilisée à la troisième égalité. De plus, nous avons utilisé la propriété $|uv| = |u| + |v|$, qui est assez facile à démontrer.

- (c) (5 points) Montrez par induction que pour tout $n \geq 3$, le mot f_n termine par 01 si n est impair et par 10 si n est pair.

Solution: CAS DE BASE. Nous avons $f_3 = 01$ qui termine bien par 01 et $f_4 = 010$ qui termine par 10.

HYPOTHÈSE D'INDUCTION. Supposons que pour tout entier m tel que $3 \leq m < n$, nous avons que f_m termine par 01 ou 10 selon que m est impair ou pair.

ÉTAPE INDUCTIVE. Il y a deux cas à considérer. Tout d'abord, rappelons que, par définition de la suite $\{f_n\}$, nous avons $f_n = f_{n-1} \cdot f_{n-2}$. Ainsi, f_n termine par f_{n-2} . Supposons d'abord que n est impair. Alors par hypothèse d'induction, f_{n-2} termine par 01 et donc f_n aussi termine par 01. D'autre part, si n est pair, alors l'hypothèse d'induction entraîne que f_{n-2} termine par 10 et donc f_n aussi termine par 10.

- (d) (5 points) Montrez par induction que pour tout entier $n \geq 3$, il existe un palindrome p et deux lettres a et b telles que $f_n = pab$. *Indice :* Utilisez (c) et le fait que $f_n = f_{n-2}f_{n-3}f_{n-2}$ pour $n \geq 4$.

Solution: Tout d'abord, remarquons que l'indice est correct, puisque, pour $n \geq 4$, nous avons

$$f_n = f_{n-1}f_{n-2} = f_{n-2}f_{n-3}f_{n-2}.$$

Maintenant, procédons par induction généralisée.

CAS DE BASE. Nous avons que $f_3 = 01 = \varepsilon \cdot 01$. En supprimant les deux dernières lettres, on a bien que ε est un palindrome. De la même façon, $f_4 = 010 = 0 \cdot 10$ et on voit que 0 aussi est un palindrome.

HYPOTHÈSE D'INDUCTION. Supposons que pour tout entier m tel que $3 \leq m < n$, nous avons que le préfixe obtenu de f_m en supprimant les deux dernières lettres est bien un palindrome.

ÉTAPE INDUCTIVE. Comme $f_n = f_{n-2}f_{n-3}f_{n-2}$, l'hypothèse d'induction entraîne qu'il existe deux palindromes p et q ainsi que des lettres a et b telles que

$$f_n = pab \cdot qba \cdot pab.$$

En supprimant les dernières lettres, il reste à montrer que le mot $pabqba$ est un palindrome. Or,

$$\widetilde{pabqba} = \widetilde{pabqba} = pabqba,$$

ce qui termine la démonstration.

3. On dit d'un arbre binaire qu'il est *parfait* si chacun de ses noeuds possède zéro ou deux enfants (autrement dit, il n'y a aucun noeud qui possède exactement un enfant).
- (a) (8 points) Soit T un arbre binaire parfait non vide de n noeuds, dont i noeuds sont internes et f sont des feuilles. Montrez par induction sur n que $f = i + 1$.

Solution: CAS DE BASE. Si $n = 1$, alors $f = 1$ et $i = 0$, de sorte que $f = 1 = 0 + 1 = i + 1$, tel que voulu.

HYPOTHÈSE D'INDUCTION. On suppose que tout arbre binaire parfait T' de n' noeuds, avec $n' < n$ vérifie $f' = i' + 1$, où f' est le nombre de feuilles de T' et i' est son nombre de noeuds internes.

INDUCTION. Comme $n \geq 2$, alors la racine de T possède nécessairement deux enfants. Soient G et D les sous-arbres gauche et droit de T . Notons que G et D sont des arbres parfaits. Soient i_G et f_G (respectivement i_D et f_D) le nombre de noeuds internes et le nombre de feuilles de G (respectivement de D).

Alors les relations suivantes sont satisfaites :

$$\begin{aligned} f &= f_G + f_D; \\ i &= i_G + i_D + 1. \end{aligned}$$

De plus, par hypothèse d'induction, nous avons

$$f_G = i_G + 1 \quad \text{et} \quad f_D = i_D + 1.$$

Par conséquent,

$$\begin{aligned} f &= f_G + f_D \\ &= (i_G + 1) + (i_D + 1) \\ &= (i_G + i_D + 1) + 1 \\ &= i + 1, \end{aligned}$$

ce qui termine la démonstration.

- (b) (7 points) Donnez le pseudocode d'un algorithme qui vérifie si un arbre binaire T est parfait ou non. Utilisez l'en-tête de fonction

fonction ESTPARFAIT(T : arbre binaire) : booléen

Solution: Notons qu'un arbre vide est, par définition, parfait. Si un arbre est non vide, on vérifie s'il est parfait en inspectant ses deux sous-arbres, et en s'assurant qu'ils sont soit tous deux vides, soit tous deux non vides. Une solution possible est donc :

```

1: fonction ESTPARFAIT( $T$  : arbre binaire) : booléen
2:   si  $T$ .ESTVIDE() alors
3:     retourner vrai
4:   sinon si  $T$ .GAUCHE().ESTVIDE() alors
5:     retourner  $T$ .DROIT().ESTVIDE()

```

```

6:   sinon si  $T.DROIT().ESTVIDE()$  alors
7:     retourner faux
8:   sinon
9:     retourner  $ESTPARFAIT(T.GAUCHE())$  et  $ESTPARFAIT(T.DROIT())$ 
10:  fin si
11: fin fonction

```

4. Soit $\Sigma = \{0, 1\}$ l'alphabet binaire. Pour tout mot u sur Σ et pour tout entier positif n , on définit $W(u, n)$ comme l'ensemble des mots de longueur n sur Σ qui évitent le facteur u et $P(u, n)$ comme l'ensemble des mots de $W(u, n)$ qui sont des palindromes.

Par exemple,

$$W(00, 4) = \{0101, 0110, 0111, 1010, 1011, 1101, 1110, 1111\}.$$

et

$$P(00, 4) = \{0110, 1111\}.$$

- (a) (3 points) Calculez $|W(00, n)|$ pour $0 \leq n \leq 6$.

Solution: Énumérons les éléments de $W(00, n)$, c'est-à-dire l'ensemble des mots binaires qui évitent le facteur 00 de longueur $n = 0, 1, 2, 3, 4, 5, 6$. On trouve

$$W(00, 0) = \{\varepsilon\}$$

$$W(00, 1) = \{0, 1\}$$

$$W(00, 2) = \{01, 10, 11\}$$

$$W(00, 3) = \{010, 011, 101, 110, 111\}$$

$$W(00, 4) = \{0101, 0110, 0111, 1010, 1011, 1101, 1110, 1111\}$$

$$W(00, 5) = \{01010, 01011, 01101, 01110, 01111, 10101, 10110, 10111, 11010, 11011, 11101, 11110, 11111\}$$

$$W(00, 6) = \{010101, 010110, 010111, 011010, 011011, 011101, 011110, 011111, 101010, 101011, 101101, 101110, 101111, 110101, 110110, 110111, 111010, 111011, 111101, 111110, 111111\}$$

On obtient donc

$$|W(00, 0)| = 1$$

$$|W(00, 1)| = 2$$

$$|W(00, 2)| = 3$$

$$|W(00, 3)| = 5$$

$$|W(00, 4)| = 8$$

$$|W(00, 5)| = 13$$

$$|W(00, 6)| = 21.$$

(b) (2 points) Calculez $|P(00, n)|$ pour $0 \leq n \leq 6$.

Solution: Il suffit de conserver les palindromes parmi les mots énumérés en (a) :

$$\begin{aligned} P(00, 0) &= \{\varepsilon\} \\ P(00, 1) &= \{0, 1\} \\ P(00, 2) &= \{11\} \\ P(00, 3) &= \{010, 101, 111\} \\ P(00, 4) &= \{0110, 1111\} \\ P(00, 5) &= \{01010, 01110, 10101, 11011, 11111\} \\ P(00, 6) &= \{011110, 101101, 111111\} \end{aligned}$$

On obtient alors

$$\begin{aligned} |P(00, 0)| &= 1 \\ |P(00, 1)| &= 2 \\ |P(00, 2)| &= 1 \\ |P(00, 3)| &= 3 \\ |P(00, 4)| &= 2 \\ |P(00, 5)| &= 5 \\ |P(00, 6)| &= 3 \end{aligned}$$

(c) (5 points) Proposez une formule générale donnant la valeur de $|W(00, n)|$, pour $n \geq 0$ et démontrez-la par induction.

Solution: On voit les premiers termes de la suite de Fibonacci apparaître en calculant les longueurs successives. Par conséquent, il semblerait que

$$|W(00, n)| = f_{n+1},$$

où f_n est le n -ième nombre de Fibonacci, c'est-à-dire la suite $\{f_n\}_{n \geq 0}$ définie par $f_0 = f_1 = 1$ et $f_n = f_{n-1} + f_{n-2}$ pour $n \geq 2$. Démontrons-le par induction généralisée sur n .

CAS DE BASE. On a vu en (a) que $|W(00, 0)| = 1 = f_1$ et $|W(00, 1)| = 2 = f_2$.

HYPOTHÈSE D'INDUCTION. On suppose que pour tout naturel m tel que $0 \leq m < n$, on ait $|W(00, m)| = f_{m+1}$.

INDUCTION. Soit $w \in W(00, n)$. Alors il y a deux cas possibles :

- Le mot w termine par 1, c'est-à-dire que $w = w'1$ pour un certain $w' \in W(00, n-1)$.

- Le mot w termine par 0. Or, comme w évite le facteur 00, w doit nécessairement terminer par 10, de sorte que $w = w'10$ pour un certain $w' \in W(00, n-2)$.

Comme les deux scénarios sont mutuellement exclusifs, nous avons

$$\begin{aligned} |W(00, n)| &= |W(00, n-1)| + |W(00, n-2)| && \text{(par le principe de la somme)} \\ &= f_{(n-1)+1} + f_{(n-2)+1} && \text{(par hypothèse d'induction)} \\ &= f_n + f_{n-1} \\ &= f_{n+1} && \text{(par définition de } f_{n+1}) \end{aligned}$$

tel que voulu.

- (d) (5 points) Proposez une formule générale donnant la valeur de $|P(00, n)|$, pour $n \geq 0$ et démontrez-la par induction.

Solution: Ce problème est un peu plus compliqué. On voit bien que les nombres de Fibonacci apparaissent, mais pas de façon aussi régulière qu'en (a). Par contre, si on sépare les cas selon la parité de la longueur, on constate que la suite de Fibonacci apparaît de façon entrelacée. Plus précisément, nous allons montrer que

$$|P(00, n)| = \begin{cases} f_{n/2}, & \text{si } n \text{ est pair;} \\ f_{(n+3)/2}, & \text{si } n \text{ est impair.} \end{cases}$$

où $f_0 = f_1 = 1$ et $f_n = f_{n-1} + f_{n-2}$ pour $n \geq 2$.

Solution 1: On procède par induction, tel que précisé dans l'énoncé.

CAS DE BASE. La formule est vérifiée en (b) pour $n = 0, 1, 2, 3$.

HYPOTHÈSE D'INDUCTION. Supposons que pour tout naturel m tel que $0 \leq m < n$, on ait

$$|P(00, m)| = \begin{cases} f_{m/2}, & \text{si } m \text{ est pair;} \\ f_{(m+3)/2}, & \text{si } m \text{ est impair.} \end{cases}$$

INDUCTION. Soit $w \in P(00, n)$, avec $n \geq 4$ (car nous avons vérifié les cas $n \leq 3$). Il y a deux cas à considérer selon que n est pair ou impair :

- Si n est pair, alors le facteur central de longueur 4 de w est 0110 ou 1111, puisque w évite le motif 00. Par conséquent, soit $w = u0110\tilde{u}$ pour un certain mot u tel que $u\tilde{u} \in P(00, n-4)$ ou bien $w = u1111\tilde{u}$ pour un certain mot u tel que $u11\tilde{u} \in P(00, n-2)$, les deux cas étant mutuellement

exclusifs. Par le principe de la somme, on obtient donc

$$\begin{aligned}
 |P(00, n)| &= |P(00, n-2)| + |P(00, n-4)| && \text{(par le principe de la somme)} \\
 &= f_{(n-2)/2} + f_{(n-4)/2} && \text{(par hypothèse d'induction)} \\
 &= f_{n/2-1} + f_{n/2-2} \\
 &= f_{n/2} && \text{(par définition de } f_{n/2}\text{)}
 \end{aligned}$$

- Si n est impair, alors soit $w = u0\tilde{u}$ pour un certain mot u tel que $u\tilde{u} \in P(00, n-1)$, ou bien $w = u010\tilde{u}$ pour un certain mot u tel que $u\tilde{u} \in P(00, n-3)$ ou encore $w = u111\tilde{u}$ pour un certain mot u tel que $u11\tilde{u} \in P(00, n-1)$, les trois cas étant mutuellement exclusifs. Comme $n-1$ et $n-3$ sont tous deux pairs, on en déduit que

$$\begin{aligned}
 |P(00, n)| &= 2|P(00, n-1)| + |P(00, n-3)| && \text{(par le principe de la somme)} \\
 &= 2f_{(n-1)/2} + f_{(n-3)/2} && \text{(par hypothèse d'induction)} \\
 &= f_{(n-1)/2} + f_{(n+1)/2} && \text{(par définition de } f_{(n+1)/2}\text{)} \\
 &= f_{(n+3)/2} && \text{(par définition de } f_{(n+3)/2}\text{)}
 \end{aligned}$$

ce qui termine la démonstration.

Solution 2: On utilise le résultat obtenu en (c). Soit $w \in P(00, n)$, avec $n \geq 4$. D'une part, si n est pair, alors $w = u11\tilde{u}$ pour un certain mot $u \in W(00, (n-2)/2)$. Par conséquent, dans ce cas,

$$|P(00, n)| = |W(00, (n-2)/2)| = f_{(n-2)/2+1} = f_{n/2},$$

tel que voulu. D'autre part, si n est impair, alors $w = u1\tilde{u}$ pour un certain mot $u \in W(00, (n-1)/2)$ ou bien $w = u101\tilde{u}$ pour un certain mot $u \in W(00, (n-3)/2)$, les deux cas étant mutuellement exclusifs. Par le principe de la somme, on trouve donc

$$\begin{aligned}
 |P(00, n)| &= |W(00, (n-1)/2)| + |W(00, (n-3)/2)| \\
 &= f_{(n-1)/2+1} + f_{(n-3)/2+1} \\
 &= f_{(n+1)/2} + f_{(n-1)/2} \\
 &= f_{(n+3)/2},
 \end{aligned}$$

ce qui conclut la démonstration.

5. (10 points) Dans une région mystérieuse de notre planète, un numéro de téléphone est valide si et seulement s'il vérifie les conditions suivantes :

- Il est formé de 10 chiffres consécutifs entre 0 et 9;

- Chaque chiffre impair (1, 3, 5, 7 et 9) doit apparaître au moins une fois.

Par exemple, le numéro 4189375351 est valide, puisqu'il contient les chiffres 1, 3, 5, 7 et 9, mais pas le numéro 012345678, car il ne contient pas le chiffre 9.

Combien existe-t-il de numéros de téléphone valides dans cette région? *Indice* : Principe d'inclusion-exclusion. *Suggestion* : Vous pouvez écrire un programme qui énumère les numéros, mais il prendra sans doute beaucoup de temps pour terminer. Si vous êtes patient, vous pourrez donc l'utiliser pour confirmer votre solution.

Solution: Il est plus facile de compter d'abord le nombre n de numéros de téléphones pour lesquels il manque au moins un chiffre impair. Dénotons par N_i l'ensemble des numéros de téléphone dans lesquels le chiffre i n'apparaît pas. Alors clairement,

$$n = |N_1 \cup N_3 \cup N_5 \cup N_7 \cup N_9|.$$

Évidemment, les ensembles N_1, N_3, N_5, N_7 et N_9 ne sont pas disjoints et donc on doit utiliser le principe d'inclusion-exclusion. Tout d'abord, notons que $|N_i| = 9^{10}$ pour $i = 1, 3, 5, 7, 9$ puisqu'il suffit d'exclure, à chaque position, le chiffre interdit (on a donc 9 choix à chaque position). En suivant cette logique, on remarque que $|N_i \cap N_j| = 8^{10}$ pour i, j impairs et distincts, puis $|N_i \cap N_j \cap N_k| = 7^{10}$, $|N_i \cap N_j \cap N_k \cap N_\ell| = 6^{10}$ et finalement $|N_i \cap N_j \cap N_k \cap N_\ell \cap N_m| = 5^{10}$.

Il ne nous reste qu'à utiliser le principe d'inclusion-exclusion. On obtient

$$\begin{aligned} n &= |N_1 \cup N_3 \cup N_5 \cup N_7 \cup N_9| \\ &= (|N_1| + |N_3| + |N_5| + |N_7| + |N_9|) \\ &\quad - (|N_1 \cap N_3| + |N_1 \cap N_5| + |N_1 \cap N_7| + \dots + |N_7 \cap N_9|) \\ &\quad + (|N_1 \cap N_3 \cap N_5| + |N_1 \cap N_3 \cap N_7| + \dots + |N_3 \cap N_5 \cap N_7|) \\ &\quad - (|N_1 \cap N_3 \cap N_5 \cap N_7| + |N_1 \cap N_3 \cap N_5 \cap N_9| + \dots + |N_3 \cap N_5 \cap N_7 \cap N_9|) \\ &\quad + |N_1 \cap N_3 \cap N_5 \cap N_7 \cap N_9| \\ &= C(5, 1) \cdot 9^{10} - C(5, 2) \cdot 8^{10} + C(5, 3) \cdot 7^{10} - C(5, 4) \cdot 6^{10} + C(5, 5) \cdot 5^{10} \\ &= 9228691000. \end{aligned}$$

Le nombre de numéros de téléphone cherché est donc

$$10^{10} - 9228691000 = 771309000.$$

6. (10 points) Soit n un entier strictement positif et $A = \{1, 2, 3, \dots, 2n\}$. Montrez à l'aide du principe des tiroirs que si on choisit un sous-ensemble B de A constitué de $n + 1$ éléments, alors il en existe au moins 2 qui sont premiers entre eux.

Solution: Il suffit de partitionner l'ensemble A en prenant les ensembles $A_i = \{2i - 1, 2i\}$ pour $i = 1, 2, \dots, n$. Clairement, $\text{pgcd}(2i - 1, 2i) = 1$ puisqu'il s'agit de deux nombres consécutifs. En effet, si d divise $2i - 1$ et $2i$, alors d divise la différence $2i - (2i - 1) = 1$ et donc $d = 1$ nécessairement. Par conséquent, si on choisit un sous-ensemble B de A formé de $n + 1$ éléments, alors, par le principe des tiroirs, il y a nécessairement deux nombres de B qui sont tous deux dans l'ensemble A_i , pour un certain indice $i \in \{1, 2, \dots, n\}$. Ces deux nombres sont donc premiers entre eux, tel que voulu.