III. Théorème fondamental de l'arithmétique

III. Théorème fondamental de l'arithmétique

Théorème et définition 21. — Théorème fondamental de l'arithmétique

Tout entier $n \geqslant 2$ peut s'écrire comme un produit de nombres premiers (éventuellement réduit à un seul facteur). De plus, cette écriture est unique à l'ordre des facteurs près.
Cette écriture s'appelle la décomposition de n en produit de facteurs premiers.

Avant de démontrer le théorème, expliquons ce que signifie « cette écriture est unique à l'ordre des facteurs près ».

Avant de démontrer le théorème, expliquons ce que signifie « cette écriture est unique à l'ordre des facteurs près ». Considérons, par exemple, $n = 100$.

Avant de démontrer le théorème, expliquons ce que signifie « cette écriture est unique à l'ordre des facteurs près ». Considérons, par exemple, $n = 100$. Pour décomposer n en produit de facteurs premiers, on peut commencer par remarquer que n est divisible par $2 : n = 2 \times 50$.

Avant de démontrer le théorème, expliquons ce que signifie « cette écriture est unique à l'ordre des facteurs près ». Considérons, par exemple, $n = 100$. Pour décomposer n en produit de facteurs premiers, on peut commencer par remarquer que n est divisible par 2 : $n = 2 \times 50$. Ensuite, voir que 50 est lui-même divisible par 2 : $50 = 2 \times 25$

Avant de démontrer le théorème, expliquons ce que signifie « cette écriture est unique à l'ordre des facteurs près ». Considérons, par exemple, $n = 100$. Pour décomposer n en produit de facteurs premiers, on peut commencer par remarquer que n est divisible par 2 : $n = 2 \times 50$. Ensuite, voir que 50 est lui-même divisible par 2 : $50 = 2 \times 25$ donc $n = 2 \times 2 \times 25$.

Avant de démontrer le théorème, expliquons ce que signifie « cette écriture est unique à l'ordre des facteurs près ». Considérons, par exemple, $n = 100$. Pour décomposer n en produit de facteurs premiers, on peut commencer par remarquer que n est divisible par 2 : $n = 2 \times 50$. Ensuite, voir que 50 est lui-même divisible par 2 : $50 = 2 \times 25$ donc $n = 2 \times 2 \times 25$. Enfin, conclure en écrivant $25 = 5 \times 5$.

Avant de démontrer le théorème, expliquons ce que signifie « cette écriture est unique à l'ordre des facteurs près ». Considérons, par exemple, $n = 100$. Pour décomposer n en produit de facteurs premiers, on peut commencer par remarquer que n est divisible par 2 : $n = 2 \times 50$. Ensuite, voir que 50 est lui-même divisible par 2 : $50 = 2 \times 25$ donc $n = 2 \times 2 \times 25$. Enfin, conclure en écrivant $25 = 5 \times 5$. Ainsi, n se décompose en $n = 2 \times 2 \times 5 \times 5$.

Avant de démontrer le théorème, expliquons ce que signifie « cette écriture est unique à l'ordre des facteurs près ». Considérons, par exemple, $n = 100$. Pour décomposer n en produit de facteurs premiers, on peut commencer par remarquer que n est divisible par 2 : $n = 2 \times 50$. Ensuite, voir que 50 est lui-même divisible par 2 : $50 = 2 \times 25$ donc $n = 2 \times 2 \times 25$. Enfin, conclure en écrivant $25 = 5 \times 5$. Ainsi, n se décompose en $n = 2 \times 2 \times 5 \times 5$.
Une autre façon de procéder aurait été d'écrire $n = 10 \times 10$

Avant de démontrer le théorème, expliquons ce que signifie « cette écriture est unique à l'ordre des facteurs près ». Considérons, par exemple, $n = 100$. Pour décomposer n en produit de facteurs premiers, on peut commencer par remarquer que n est divisible par 2 : $n = 2 \times 50$. Ensuite, voir que 50 est lui-même divisible par 2 : $50 = 2 \times 25$ donc $n = 2 \times 2 \times 25$. Enfin, conclure en écrivant $25 = 5 \times 5$. Ainsi, n se décompose en $n = 2 \times 2 \times 5 \times 5$.
Une autre façon de procéder aurait été d'écrire $n = 10 \times 10$ et, comme $10 = 2 \times 5$,

Avant de démontrer le théorème, expliquons ce que signifie « cette écriture est unique à l'ordre des facteurs près ». Considérons, par exemple, $n = 100$. Pour décomposer n en produit de facteurs premiers, on peut commencer par remarquer que n est divisible par 2 : $n = 2 \times 50$. Ensuite, voir que 50 est lui-même divisible par 2 : $50 = 2 \times 25$ donc $n = 2 \times 2 \times 25$. Enfin, conclure en écrivant $25 = 5 \times 5$. Ainsi, n se décompose en $n = 2 \times 2 \times 5 \times 5$.
Une autre façon de procéder aurait été d'écrire $n = 10 \times 10$ et, comme $10 = 2 \times 5$, $100 = 2 \times 5 \times 2 \times 5$.

Avant de démontrer le théorème, expliquons ce que signifie « cette écriture est unique à l'ordre des facteurs près ». Considérons, par exemple, $n = 100$. Pour décomposer n en produit de facteurs premiers, on peut commencer par remarquer que n est divisible par 2 : $n = 2 \times 50$. Ensuite, voir que 50 est lui-même divisible par 2 : $50 = 2 \times 25$ donc $n = 2 \times 2 \times 25$. Enfin, conclure en écrivant $25 = 5 \times 5$. Ainsi, n se décompose en $n = 2 \times 2 \times 5 \times 5$.
Une autre façon de procéder aurait été d'écrire $n = 10 \times 10$ et, comme $10 = 2 \times 5$, $100 = 2 \times 5 \times 2 \times 5$.
On obtient ainsi « deux » façons d'écrire 100 comme un produit de facteurs premiers.

Avant de démontrer le théorème, expliquons ce que signifie « cette écriture est unique à l'ordre des facteurs près ». Considérons, par exemple, $n = 100$. Pour décomposer n en produit de facteurs premiers, on peut commencer par remarquer que n est divisible par 2 : $n = 2 \times 50$. Ensuite, voir que 50 est lui-même divisible par 2 : $50 = 2 \times 25$ donc $n = 2 \times 2 \times 25$. Enfin, conclure en écrivant $25 = 5 \times 5$. Ainsi, n se décompose en $n = 2 \times 2 \times 5 \times 5$.
Une autre façon de procéder aurait été d'écrire $n = 10 \times 10$ et, comme $10 = 2 \times 5$, $100 = 2 \times 5 \times 2 \times 5$.
On obtient ainsi « deux » façons d'écrire 100 comme un produit de facteurs premiers. Cependant, ce sont essentiellement les mêmes :

Avant de démontrer le théorème, expliquons ce que signifie « cette écriture est unique à l'ordre des facteurs près ». Considérons, par exemple, $n = 100$. Pour décomposer n en produit de facteurs premiers, on peut commencer par remarquer que n est divisible par 2 : $n = 2 \times 50$. Ensuite, voir que 50 est lui-même divisible par 2 : $50 = 2 \times 25$ donc $n = 2 \times 2 \times 25$. Enfin, conclure en écrivant $25 = 5 \times 5$. Ainsi, n se décompose en $n = 2 \times 2 \times 5 \times 5$.
Une autre façon de procéder aurait été d'écrire $n = 10 \times 10$ et, comme $10 = 2 \times 5$, $100 = 2 \times 5 \times 2 \times 5$.
On obtient ainsi « deux » façons d'écrire 100 comme un produit de facteurs premiers. Cependant, ce sont essentiellement les mêmes : la seule chose qui varie est l'ordre des facteurs.

Pour éviter ce genre de distinction, on prendra l'habitude

Pour éviter ce genre de distinction, on prendra l'habitude

1. d'ordonner les facteurs premiers du plus petit au plus grand ;

Pour éviter ce genre de distinction, on prendra l'habitude

1. d'ordonner les facteurs premiers du plus petit au plus grand ;
2. de rassembler les facteurs identiques en une seule puissance.

Pour éviter ce genre de distinction, on prendra l'habitude

1. d'ordonner les facteurs premiers du plus petit au plus grand ;
2. de rassembler les facteurs identiques en une seule puissance.

Avec ses conventions supplémentaires, on écrira $100 = 2^2 \times 5^2$

Pour éviter ce genre de distinction, on prendra l'habitude

1. d'ordonner les facteurs premiers du plus petit au plus grand ;
2. de rassembler les facteurs identiques en une seule puissance.

Avec ses conventions supplémentaires, on écrira $100 = 2^2 \times 5^2$ et c'est la seule écriture possible !

Démonstration du théorème 21

On doit montrer à la fois l'existence et l'unicité de la décomposition.

Démonstration du théorème 21

On doit montrer à la fois l'existence et l'unicité de la décomposition.

Existence.

Démonstration du théorème 21

On doit montrer à la fois l'existence et l'unicité de la décomposition.

Existence. On raisonne par l'absurde en supposant que l'ensemble E des entiers $n \geqslant 2$ qui ne peuvent pas s'écrire comme produit de nombres premiers est non vide.

Démonstration du théorème 21

On doit montrer à la fois l'existence et l'unicité de la décomposition.

Existence. On raisonne par l'absurde en supposant que l'ensemble E des entiers $n \geqslant 2$ qui ne peuvent pas s'écrire comme produit de nombres premiers est non vide. Alors, E est une partie non vide de $\mathbb{N}$ donc E admet un plus petit élément n.

Démonstration du théorème 21

On doit montrer à la fois l'existence et l'unicité de la décomposition.

Existence. On raisonne par l'absurde en supposant que l'ensemble E des entiers $n \geqslant 2$ qui ne peuvent pas s'écrire comme produit de nombres premiers est non vide. Alors, E est une partie non vide de $\mathbb{N}$ donc E admet un plus petit élément n. Comme $n \geqslant 2$, d'après la propriété 5, n admet un diviseur premier p.

Démonstration du théorème 21

On doit montrer à la fois l'existence et l'unicité de la décomposition.

Existence. On raisonne par l'absurde en supposant que l'ensemble E des entiers $n \geqslant 2$ qui ne peuvent pas s'écrire comme produit de nombres premiers est non vide. Alors, E est une partie non vide de $\mathbb{N}$ donc E admet un plus petit élément n. Comme $n \geqslant 2$, d'après la propriété 5, n admet un diviseur premier p. Si $n = p$ alors n serait le produit d'un seul nombre premier donc $n \notin E$.

Démonstration du théorème 21

On doit montrer à la fois l'existence et l'unicité de la décomposition.

Existence. On raisonne par l'absurde en supposant que l'ensemble E des entiers $n \geqslant 2$ qui ne peuvent pas s'écrire comme produit de nombres premiers est non vide. Alors, E est une partie non vide de $\mathbb{N}$ donc E admet un plus petit élément n. Comme $n \geqslant 2$, d'après la propriété 5, n admet un diviseur premier p. Si $n = p$ alors n serait le produit d'un seul nombre premier donc $n \notin E$. Ainsi, $p < n$ donc il existe un entier $m \geqslant 2$ tel que $n = pm$.

Démonstration du théorème 21

On doit montrer à la fois l'existence et l'unicité de la décomposition.

Existence. On raisonne par l'absurde en supposant que l'ensemble E des entiers $n \geqslant 2$ qui ne peuvent pas s'écrire comme produit de nombres premiers est non vide. Alors, E est une partie non vide de $\mathbb{N}$ donc E admet un plus petit élément n. Comme $n \geqslant 2$, d'après la propriété 5, n admet un diviseur premier p. Si $n = p$ alors n serait le produit d'un seul nombre premier donc $n \notin E$. Ainsi, $p < n$ donc il existe un entier $m \geqslant 2$ tel que $n = pm$. De plus, comme $p > 1$, $m < n$ donc, par minimalité de n, $m \notin E$.

Démonstration du théorème 21

On doit montrer à la fois l'existence et l'unicité de la décomposition.

Existence. On raisonne par l'absurde en supposant que l'ensemble E des entiers $n \geqslant 2$ qui ne peuvent pas s'écrire comme produit de nombres premiers est non vide. Alors, E est une partie non vide de $\mathbb{N}$ donc E admet un plus petit élément n. Comme $n \geqslant 2$, d'après la propriété 5, n admet un diviseur premier p. Si $n = p$ alors n serait le produit d'un seul nombre premier donc $n \notin E$. Ainsi, $p < n$ donc il existe un entier $m \geqslant 2$ tel que $n = pm$. De plus, comme $p > 1$, $m < n$ donc, par minimalité de n, $m \notin E$. Ainsi, il existe des nombres premiers p_1, p_2, ..., p_k (pas forcément distincts) tels que $m = p_1 p_2 \cdots p_k$.

Démonstration du théorème 21

On doit montrer à la fois l'existence et l'unicité de la décomposition.

Existence. On raisonne par l'absurde en supposant que l'ensemble E des entiers $n \geqslant 2$ qui ne peuvent pas s'écrire comme produit de nombres premiers est non vide. Alors, E est une partie non vide de $\mathbb{N}$ donc E admet un plus petit élément n. Comme $n \geqslant 2$, d'après la propriété 5, n admet un diviseur premier p. Si $n = p$ alors n serait le produit d'un seul nombre premier donc $n \notin E$. Ainsi, $p < n$ donc il existe un entier $m \geqslant 2$ tel que $n = pm$. De plus, comme $p > 1$, $m < n$ donc, par minimalité de n, $m \notin E$. Ainsi, il existe des nombres premiers p_1, p_2, ..., p_k (pas forcément distincts) tels que $m = p_1 p_2 \cdots p_k$. Mais alors $n = pm = p p_1 p_2 \cdots p_k$ est un produit de nombres premiers, ce qui est absurde.

Démonstration du théorème 21

On doit montrer à la fois l'existence et l'unicité de la décomposition.

Existence. On raisonne par l'absurde en supposant que l'ensemble E des entiers $n \geqslant 2$ qui ne peuvent pas s'écrire comme produit de nombres premiers est non vide. Alors, E est une partie non vide de $\mathbb{N}$ donc E admet un plus petit élément n. Comme $n \geqslant 2$, d'après la propriété 5, n admet un diviseur premier p. Si $n = p$ alors n serait le produit d'un seul nombre premier donc $n \notin E$. Ainsi, $p < n$ donc il existe un entier $m \geqslant 2$ tel que $n = pm$. De plus, comme $p > 1$, $m < n$ donc, par minimalité de n, $m \notin E$. Ainsi, il existe des nombres premiers p_1, p_2, ..., p_k (pas forcément distincts) tels que $m = p_1 p_2 \cdots p_k$. Mais alors $n = pm = p p_1 p_2 \cdots p_k$ est un produit de nombres premiers, ce qui est absurde. Ainsi, $E = \varnothing$ et donc, tout entier $n \geqslant 2$ s'écrit comme un produit de nombres premiers.

Unicité.

Unicité. Pour montrer l'unicité, on va supposer qu'un entier $n \geqslant 2$ peut s'écrire à la fois $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ et $n = q_1^{\beta_1} q_2^{\beta_2} \cdots q_\ell^{\beta_\ell}$ où $p_1 < p_2 < \cdots < p_k$ et $q_1 < q_2 < \cdots < q_\ell$ sont des nombres premiers et α_1, α_2, ..., α_k, β_1, β_2, ..., β_ℓ sont des entiers naturels non nuls.

Soit $i \in [\![1, k]\!]$.

Soit $i \in [\![1, k]\!]$. Alors, p_i divise n donc p_i divise $q_1^{\beta_1} q_2^{\beta_2} \cdots q_\ell^{\beta_\ell}$

Soit $i \in [\![1, k]\!]$. Alors, p_i divise n donc p_i divise $q_1^{\beta_1} q_2^{\beta_2} \cdots q_\ell^{\beta_\ell}$ donc, par le corollaire 17, il existe un entier $j \in [\![1, \ell]\!]$ tel que $p_i = q_j$.

Soit $i \in [\![1, k]\!]$. Alors, p_i divise n donc p_i divise $q_1^{\beta_1} q_2^{\beta_2} \cdots q_\ell^{\beta_\ell}$ donc, par le corollaire 17, il existe un entier $j \in [\![1, \ell]\!]$ tel que $p_i = q_j$. De même, on montre que, pour tout $j \in [\![1, \ell]\!]$, il existe un entier $i \in [\![1, k]\!]$ tel que $q_j = p_i$.

Soit $i \in [\![1, k]\!]$. Alors, p_i divise n donc p_i divise $q_1^{\beta_1} q_2^{\beta_2} \cdots q_\ell^{\beta_\ell}$ donc, par le corollaire 17, il existe un entier $j \in [\![1, \ell]\!]$ tel que $p_i = q_j$. De même, on montre que, pour tout $j \in [\![1, \ell]\!]$, il existe un entier $i \in [\![1, k]\!]$ tel que $q_j = p_i$. Ceci implique $\{p_1, p_2, ..., p_k\} = \{q_1, q_2, ..., q_\ell\}$

Soit $i \in [\![1, k]\!]$. Alors, p_i divise n donc p_i divise $q_1^{\beta_1} q_2^{\beta_2} \cdots q_\ell^{\beta_\ell}$ donc, par le corollaire 17, il existe un entier $j \in [\![1, \ell]\!]$ tel que $p_i = q_j$. De même, on montre que, pour tout $j \in [\![1, \ell]\!]$, il existe un entier $i \in [\![1, k]\!]$ tel que $q_j = p_i$. Ceci implique $\{p_1, p_2, ..., p_k\} = \{q_1, q_2, ..., q_\ell\}$ et, par conséquent, $k = \ell$ et,

Soit $i \in [\![1, k]\!]$. Alors, p_i divise n donc p_i divise $q_1^{\beta_1} q_2^{\beta_2} \cdots q_\ell^{\beta_\ell}$ donc, par le corollaire 17, il existe un entier $j \in [\![1, \ell]\!]$ tel que $p_i = q_j$. De même, on montre que, pour tout $j \in [\![1, \ell]\!]$, il existe un entier $i \in [\![1, k]\!]$ tel que $q_j = p_i$. Ceci implique $\{p_1, p_2, ..., p_k\} = \{q_1, q_2, ..., q_\ell\}$ et, par conséquent, $k = \ell$ et, pour tout $i \in [\![1, k]\!]$, $p_i = q_i$.

Soit $i \in [\![1, k]\!]$. Alors, p_i divise n donc p_i divise $q_1^{\beta_1} q_2^{\beta_2} \cdots q_\ell^{\beta_\ell}$ donc, par le corollaire 17, il existe un entier $j \in [\![1, \ell]\!]$ tel que $p_i = q_j$. De même, on montre que, pour tout $j \in [\![1, \ell]\!]$, il existe un entier $i \in [\![1, k]\!]$ tel que $q_j = p_i$. Ceci implique $\{p_1, p_2, ..., p_k\} = \{q_1, q_2, ..., q_\ell\}$ et, par conséquent, $k = \ell$ et, pour tout $i \in [\![1, k]\!]$, $p_i = q_i$. Ainsi, $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$.

Soit $i \in [\![1, k]\!]$. Alors, p_i divise n donc p_i divise $q_1^{\beta_1} q_2^{\beta_2} \cdots q_\ell^{\beta_\ell}$ donc, par le corollaire 17, il existe un entier $j \in [\![1, \ell]\!]$ tel que $p_i = q_j$. De même, on montre que, pour tout $j \in [\![1, \ell]\!]$, il existe un entier $i \in [\![1, k]\!]$ tel que $q_j = p_i$. Ceci implique $\{p_1, p_2, ..., p_k\} = \{q_1, q_2, ..., q_\ell\}$ et, par conséquent, $k = \ell$ et, pour tout $i \in [\![1, k]\!]$, $p_i = q_i$. Ainsi, $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$. Soit un entier $i \in [\![1, k]\!]$.

Soit $i \in [\![1, k]\!]$. Alors, p_i divise n donc p_i divise $q_1^{\beta_1} q_2^{\beta_2} \cdots q_\ell^{\beta_\ell}$ donc, par le corollaire 17, il existe un entier $j \in [\![1, \ell]\!]$ tel que $p_i = q_j$. De même, on montre que, pour tout $j \in [\![1, \ell]\!]$, il existe un entier $i \in [\![1, k]\!]$ tel que $q_j = p_i$. Ceci implique $\{p_1, p_2, ..., p_k\} = \{q_1, q_2, ..., q_\ell\}$ et, par conséquent, $k = \ell$ et, pour tout $i \in [\![1, k]\!]$, $p_i = q_i$. Ainsi, $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$. Soit un entier $i \in [\![1, k]\!]$. Quitte à échanger α_i et β_i, on peut toujours supposer que $\alpha_i \leqslant \beta_i$.

Soit $i \in [\![1, k]\!]$. Alors, p_i divise n donc p_i divise $q_1^{\beta_1} q_2^{\beta_2} \cdots q_\ell^{\beta_\ell}$ donc, par le corollaire 17, il existe un entier $j \in [\![1, \ell]\!]$ tel que $p_i = q_j$. De même, on montre que, pour tout $j \in [\![1, \ell]\!]$, il existe un entier $i \in [\![1, k]\!]$ tel que $q_j = p_i$. Ceci implique $\{p_1, p_2, ..., p_k\} = \{q_1, q_2, ..., q_\ell\}$ et, par conséquent, $k = \ell$ et, pour tout $i \in [\![1, k]\!]$, $p_i = q_i$. Ainsi, $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$. Soit un entier $i \in [\![1, k]\!]$. Quitte à échanger α_i et β_i, on peut toujours supposer que $\alpha_i \leqslant \beta_i$. Si on divise $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ par $p_i^{\alpha_i}$ alors on obtient un produit de nombres premiers qui ne contient plus p_i :

Soit $i \in [\![1, k]\!]$. Alors, p_i divise n donc p_i divise $q_1^{\beta_1} q_2^{\beta_2} \cdots q_\ell^{\beta_\ell}$ donc, par le corollaire 17, il existe un entier $j \in [\![1, \ell]\!]$ tel que $p_i = q_j$. De même, on montre que, pour tout $j \in [\![1, \ell]\!]$, il existe un entier $i \in [\![1, k]\!]$ tel que $q_j = p_i$. Ceci implique $\{p_1, p_2, ..., p_k\} = \{q_1, q_2, ..., q_\ell\}$ et, par conséquent, $k = \ell$ et, pour tout $i \in [\![1, k]\!]$, $p_i = q_i$. Ainsi, $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$. Soit un entier $i \in [\![1, k]\!]$. Quitte à échanger α_i et β_i, on peut toujours supposer que $\alpha_i \leqslant \beta_i$. Si on divise $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ par $p_i^{\alpha_i}$ alors on obtient un produit de nombres premiers qui ne contient plus p_i : ce nombre n'est donc pas divisible par p_i (car $p_i \neq p_j$ si $i \neq j$).

Soit $i \in [\![1, k]\!]$. Alors, p_i divise n donc p_i divise $q_1^{\beta_1} q_2^{\beta_2} \cdots q_\ell^{\beta_\ell}$ donc, par le corollaire 17, il existe un entier $j \in [\![1, \ell]\!]$ tel que $p_i = q_j$. De même, on montre que, pour tout $j \in [\![1, \ell]\!]$, il existe un entier $i \in [\![1, k]\!]$ tel que $q_j = p_i$. Ceci implique $\{p_1, p_2, ..., p_k\} = \{q_1, q_2, ..., q_\ell\}$ et, par conséquent, $k = \ell$ et, pour tout $i \in [\![1, k]\!]$, $p_i = q_i$. Ainsi, $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$. Soit un entier $i \in [\![1, k]\!]$. Quitte à échanger α_i et β_i, on peut toujours supposer que $\alpha_i \leqslant \beta_i$. Si on divise $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ par $p_i^{\alpha_i}$ alors on obtient un produit de nombres premiers qui ne contient plus p_i : ce nombre n'est donc pas divisible par p_i (car $p_i \neq p_j$ si $i \neq j$). Mais, d'un autre côté, si on divise $n = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$ par $p_i^{\alpha_i}$, on obtient un produit de nombres premiers qui fait apparaître $p_i^{\beta_i - \alpha_i}$.

Soit $i \in [\![1, k]\!]$. Alors, p_i divise n donc p_i divise $q_1^{\beta_1} q_2^{\beta_2} \cdots q_\ell^{\beta_\ell}$ donc, par le corollaire 17, il existe un entier $j \in [\![1, \ell]\!]$ tel que $p_i = q_j$. De même, on montre que, pour tout $j \in [\![1, \ell]\!]$, il existe un entier $i \in [\![1, k]\!]$ tel que $q_j = p_i$. Ceci implique $\{p_1, p_2, ..., p_k\} = \{q_1, q_2, ..., q_\ell\}$ et, par conséquent, $k = \ell$ et, pour tout $i \in [\![1, k]\!]$, $p_i = q_i$. Ainsi, $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$. Soit un entier $i \in [\![1, k]\!]$. Quitte à échanger α_i et β_i, on peut toujours supposer que $\alpha_i \leqslant \beta_i$. Si on divise $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ par $p_i^{\alpha_i}$ alors on obtient un produit de nombres premiers qui ne contient plus p_i : ce nombre n'est donc pas divisible par p_i (car $p_i \neq p_j$ si $i \neq j$). Mais, d'un autre côté, si on divise $n = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$ par $p_i^{\alpha_i}$, on obtient un produit de nombres premiers qui fait apparaître $p_i^{\beta_i - \alpha_i}$. Comme ce produit n'est pas divisible par p_i, on en déduit que $\beta_i - \alpha_i = 0$ i.e. $\alpha_i = \beta_i$.

Soit $i \in [\![1, k]\!]$. Alors, p_i divise n donc p_i divise $q_1^{\beta_1} q_2^{\beta_2} \cdots q_\ell^{\beta_\ell}$ donc, par le corollaire 17, il existe un entier $j \in [\![1, \ell]\!]$ tel que $p_i = q_j$. De même, on montre que, pour tout $j \in [\![1, \ell]\!]$, il existe un entier $i \in [\![1, k]\!]$ tel que $q_j = p_i$. Ceci implique $\{p_1, p_2, ..., p_k\} = \{q_1, q_2, ..., q_\ell\}$ et, par conséquent, $k = \ell$ et, pour tout $i \in [\![1, k]\!]$, $p_i = q_i$. Ainsi, $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$. Soit un entier $i \in [\![1, k]\!]$. Quitte à échanger α_i et β_i, on peut toujours supposer que $\alpha_i \leqslant \beta_i$. Si on divise $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ par $p_i^{\alpha_i}$ alors on obtient un produit de nombres premiers qui ne contient plus p_i : ce nombre n'est donc pas divisible par p_i (car $p_i \neq p_j$ si $i \neq j$). Mais, d'un autre côté, si on divise $n = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$ par $p_i^{\alpha_i}$, on obtient un produit de nombres premiers qui fait apparaître $p_i^{\beta_i - \alpha_i}$. Comme ce produit n'est pas divisible par p_i, on en déduit que $\beta_i - \alpha_i = 0$ i.e. $\alpha_i = \beta_i$.
On conclut donc que l'écriture de n sous la forme $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ est unique.

Exemple 22

Décomposer 4312 en produit de facteurs premiers.

Exemple 22

Décomposer 4312 en produit de facteurs premiers.
Pour cela, on teste tous les diviseurs premiers successivement et autant de fois que possible.

Exemple 22

Décomposer 4312 en produit de facteurs premiers.
Pour cela, on teste tous les diviseurs premiers successivement et autant de fois que possible. Une présentation pratique est la suivante :

Exemple 22

Décomposer 4312 en produit de facteurs premiers.
Pour cela, on teste tous les diviseurs premiers successivement et autant de fois que possible. Une présentation pratique est la suivante :

$$4312 \mid$$

Exemple 22

Décomposer 4312 en produit de facteurs premiers.
Pour cela, on teste tous les diviseurs premiers successivement et autant de fois que possible. Une présentation pratique est la suivante :

$$4312 \mid 2$$

Exemple 22

Décomposer 4312 en produit de facteurs premiers.
Pour cela, on teste tous les diviseurs premiers successivement et autant de fois que possible. Une présentation pratique est la suivante :

$$\begin{array}{r|l} 4312 & 2 \\ 2156 & \\ \end{array}$$

Exemple 22

Décomposer 4312 en produit de facteurs premiers.
Pour cela, on teste tous les diviseurs premiers successivement et autant de fois que possible. Une présentation pratique est la suivante :

$$\begin{array}{r|l} 4312 & 2 \\ 2156 & 2 \end{array}$$

Exemple 22

Décomposer 4312 en produit de facteurs premiers.
Pour cela, on teste tous les diviseurs premiers successivement et autant de fois que possible. Une présentation pratique est la suivante :

4312	2
2156	2
1078	

Exemple 22

Décomposer 4312 en produit de facteurs premiers.
Pour cela, on teste tous les diviseurs premiers successivement et autant de fois que possible. Une présentation pratique est la suivante :

4312	2
2156	2
1078	2

Exemple 22

Décomposer 4312 en produit de facteurs premiers.
Pour cela, on teste tous les diviseurs premiers successivement et autant de fois que possible. Une présentation pratique est la suivante :

4312	2
2156	2
1078	2
539	

Exemple 22

Décomposer 4312 en produit de facteurs premiers.
Pour cela, on teste tous les diviseurs premiers successivement et autant de fois que possible. Une présentation pratique est la suivante :

4312	2
2156	2
1078	2
539	7

Exemple 22

Décomposer 4312 en produit de facteurs premiers.
Pour cela, on teste tous les diviseurs premiers successivement et autant de fois que possible. Une présentation pratique est la suivante :

4312	2
2156	2
1078	2
539	7
77	

Exemple 22

Décomposer 4312 en produit de facteurs premiers.
Pour cela, on teste tous les diviseurs premiers successivement et autant de fois que possible. Une présentation pratique est la suivante :

4312	2
2156	2
1078	2
539	7
77	7

Exemple 22

Décomposer 4312 en produit de facteurs premiers.
Pour cela, on teste tous les diviseurs premiers successivement et autant de fois que possible. Une présentation pratique est la suivante :

4312	2
2156	2
1078	2
539	7
77	7
11	

Exemple 22

Décomposer 4312 en produit de facteurs premiers.
Pour cela, on teste tous les diviseurs premiers successivement et autant de fois que possible. Une présentation pratique est la suivante :

4312	2
2156	2
1078	2
539	7
77	7
11	11

Exemple 22

Décomposer 4312 en produit de facteurs premiers.
Pour cela, on teste tous les diviseurs premiers successivement et autant de fois que possible. Une présentation pratique est la suivante :

4312	2
2156	2
1078	2
539	7
77	7
11	11
1	

Exemple 22

Décomposer 4312 en produit de facteurs premiers.
Pour cela, on teste tous les diviseurs premiers successivement et autant de fois que possible. Une présentation pratique est la suivante :

4312	2
2156	2
1078	2
539	7
77	7
11	11
1	

À droite, on met les diviseurs premiers successifs et à gauche les quotients obtenus.

Exemple 22

Décomposer 4312 en produit de facteurs premiers.
Pour cela, on teste tous les diviseurs premiers successivement et autant de fois que possible. Une présentation pratique est la suivante :

4312	2
2156	2
1078	2
539	7
77	7
11	11
1	

À droite, on met les diviseurs premiers successifs et à gauche les quotients obtenus. La colonne de droite contient la décomposition produit de facteurs premiers : $4312 = 2^3 \times 7^2 \times 11$.

Définition 23

Soit un entier $n \geqslant 2$ et un nombre premier p. La puissance de p dans la décomposition de n en produit de facteurs premiers est appelée la valuation $p-$adique de n. On la note $v_p(n)$.

Définition 23

Soit un entier $n \geqslant 2$ et un nombre premier p. La puissance de p dans la décomposition de n en produit de facteurs premiers est appelée la valuation $p-$adique de n. On la note $v_p(n)$.

Exemple 24

$v_2(4312) =$

Définition 23

Soit un entier $n \geqslant 2$ et un nombre premier p. La puissance de p dans la décomposition de n en produit de facteurs premiers est appelée la valuation $p-$adique de n. On la note $v_p(n)$.

Exemple 24

$v_2(4312) = 3$, $v_{11}(4312) =$

Définition 23

Soit un entier $n \geqslant 2$ et un nombre premier p. La puissance de p dans la décomposition de n en produit de facteurs premiers est appelée la valuation $p-$adique de n. On la note $v_p(n)$.

Exemple 24

$v_2(4312) = 3$, $v_{11}(4312) = 1$.

Définition 23

Soit un entier $n \geqslant 2$ et un nombre premier p. La puissance de p dans la décomposition de n en produit de facteurs premiers est appelée la valuation $p-$adique de n. On la note $v_p(n)$.

Exemple 24

$v_2(4312) = 3$, $v_{11}(4312) = 1$.

Remarque 25

On convient que si p n'apparaît pas dans la décomposition d'un entier $n \geqslant 2$ en produit de facteurs premiers alors $v_p(n) = 0$. De plus, on convient que, pour tout nombre premier p, $v_p(1) = 0$.

Lemme 26

Soit n et m deux entiers naturels non nuls. Alors, $v_p(n \times m) = v_p(n) + v_p(m)$.

Lemme 26

Soit n et m deux entiers naturels non nuls. Alors, $v_p(n \times m) = v_p(n) + v_p(m)$.

Démonstration.

Lemme 26

Soit n et m deux entiers naturels non nuls. Alors, $v_p(n \times m) = v_p(n) + v_p(m)$.

Démonstration.

Par définition, il existe deux entiers n' et m' premiers avec p tels que $n = p^{v_p(n)}n'$ et $m = p^{v_p(m)}m'$.

Lemme 26

Soit n et m deux entiers naturels non nuls. Alors, $v_p(n \times m) = v_p(n) + v_p(m)$.

Démonstration.

Par définition, il existe deux entiers n' et m' premiers avec p tels que $n = p^{v_p(n)}n'$ et $m = p^{v_p(m)}m'$. Ainsi,
$n \times m =$

Lemme 26

Soit n et m deux entiers naturels non nuls. Alors, $v_p(n \times m) = v_p(n) + v_p(m)$.

Démonstration.

Par définition, il existe deux entiers n' et m' premiers avec p tels que $n = p^{v_p(n)}n'$ et $m = p^{v_p(m)}m'$. Ainsi,
$n \times m = (p^{v_p(n)}n')(p^{v_p(m)}m') =$

Lemme 26

Soit n et m deux entiers naturels non nuls. Alors, $v_p(n \times m) = v_p(n) + v_p(m)$.

Démonstration.

Par définition, il existe deux entiers n' et m' premiers avec p tels que $n = p^{v_p(n)}n'$ et $m = p^{v_p(m)}m'$. Ainsi,
$n \times m = (p^{v_p(n)}n')(p^{v_p(m)}m') = p^{v_p(n)+v_p(m)}n'm'$

Lemme 26

Soit n et m deux entiers naturels non nuls. Alors, $v_p(n \times m) = v_p(n) + v_p(m)$.

Démonstration.

Par définition, il existe deux entiers n' et m' premiers avec p tels que $n = p^{v_p(n)}n'$ et $m = p^{v_p(m)}m'$. Ainsi,
$n \times m = (p^{v_p(n)}n')(p^{v_p(m)}m') = p^{v_p(n)+v_p(m)}n'm'$ et, d'après le corollaire 18, p est premier avec $n'm'$

Lemme 26

Soit n et m deux entiers naturels non nuls. Alors, $v_p(n \times m) = v_p(n) + v_p(m)$.

Démonstration.

Par définition, il existe deux entiers n' et m' premiers avec p tels que $n = p^{v_p(n)}n'$ et $m = p^{v_p(m)}m'$. Ainsi,
$n \times m = (p^{v_p(n)}n')(p^{v_p(m)}m') = p^{v_p(n)+v_p(m)}n'm'$ et, d'après le corollaire 18, p est premier avec $n'm'$ donc
$v_p(m \times m) = v_p(n) + v_p(m)$. □

Propriété 27

Soit a et b deux entiers supérieurs ou égaux à 1. Alors, b divise a si et seulement si, pour tout nombre premier p, $v_p(b) \leqslant v_p(a)$.

Démonstration.

Démonstration.

Supposons que b divise a.

Démonstration.

Supposons que b divise a. Alors, il existe un entier $d \geqslant 1$ tel que $a = bd$.

Démonstration.

Supposons que b divise a. Alors, il existe un entier $d \geqslant 1$ tel que $a = bd$. Grâce au lemme 26, $v_p(a) =$

Démonstration.

Supposons que b divise a. Alors, il existe un entier $d \geqslant 1$ tel que $a = bd$. Grâce au lemme 26, $v_p(a) = v_p(b) + v_p(d)$

Démonstration.

Supposons que b divise a. Alors, il existe un entier $d \geqslant 1$ tel que $a = bd$. Grâce au lemme 26, $v_p(a) = v_p(b) + v_p(d) \geqslant v_p(b)$ car $v_p(d) \geqslant 0$.
Réciproquement, supposons que, pour tout nombre premier p, $v_p(b) \leqslant v_p(a)$.

Démonstration.

Supposons que b divise a. Alors, il existe un entier $d \geqslant 1$ tel que $a = bd$. Grâce au lemme 26, $v_p(a) = v_p(b) + v_p(d) \geqslant v_p(b)$ car $v_p(d) \geqslant 0$.
Réciproquement, supposons que, pour tout nombre premier p, $v_p(b) \leqslant v_p(a)$. Alors, tout nombre premier qui apparaît dans la décomposition de b apparaît aussi dans celle de a.

Démonstration.

Supposons que b divise a. Alors, il existe un entier $d \geqslant 1$ tel que $a = bd$. Grâce au lemme 26, $v_p(a) = v_p(b) + v_p(d) \geqslant v_p(b)$ car $v_p(d) \geqslant 0$.
Réciproquement, supposons que, pour tout nombre premier p, $v_p(b) \leqslant v_p(a)$. Alors, tout nombre premier qui apparaît dans la décomposition de b apparaît aussi dans celle de a. Écrivons $a = p_1^{v_{p_1}(a)} p_2^{v_{p_2}(a)} \cdots p_k^{v_{p_k}(a)}$.

Démonstration.

Supposons que b divise a. Alors, il existe un entier $d \geqslant 1$ tel que $a = bd$. Grâce au lemme 26, $v_p(a) = v_p(b) + v_p(d) \geqslant v_p(b)$ car $v_p(d) \geqslant 0$.
Réciproquement, supposons que, pour tout nombre premier p, $v_p(b) \leqslant v_p(a)$. Alors, tout nombre premier qui apparaît dans la décomposition de b apparaît aussi dans celle de a. Écrivons $a = p_1^{v_{p_1}(a)} p_2^{v_{p_2}(a)} \cdots p_k^{v_{p_k}(a)}$. Alors, $b = p_1^{v_{p_1}(b)} p_2^{v_{p_2}(b)} \cdots p_k^{v_{p_k}(b)}$

Démonstration.

Supposons que b divise a. Alors, il existe un entier $d \geqslant 1$ tel que $a = bd$. Grâce au lemme 26, $v_p(a) = v_p(b) + v_p(d) \geqslant v_p(b)$ car $v_p(d) \geqslant 0$.
Réciproquement, supposons que, pour tout nombre premier p, $v_p(b) \leqslant v_p(a)$. Alors, tout nombre premier qui apparaît dans la décomposition de b apparaît aussi dans celle de a. Écrivons $a = p_1^{v_{p_1}(a)} p_2^{v_{p_2}(a)} \cdots p_k^{v_{p_k}(a)}$. Alors, $b = p_1^{v_{p_1}(b)} p_2^{v_{p_2}(b)} \cdots p_k^{v_{p_k}(b)}$ donc

$$\frac{a}{b} = \frac{p_1^{v_{p_1}(a)} p_2^{v_{p_2}(a)} \cdots p_k^{v_{p_k}(a)}}{p_1^{v_{p_1}(b)} p_2^{v_{p_2}(b)} \cdots p_k^{v_{p_k}(b)}}$$

Démonstration.

Supposons que b divise a. Alors, il existe un entier $d \geqslant 1$ tel que $a = bd$. Grâce au lemme 26, $v_p(a) = v_p(b) + v_p(d) \geqslant v_p(b)$ car $v_p(d) \geqslant 0$.
Réciproquement, supposons que, pour tout nombre premier p, $v_p(b) \leqslant v_p(a)$. Alors, tout nombre premier qui apparaît dans la décomposition de b apparaît aussi dans celle de a. Écrivons $a = p_1^{v_{p_1}(a)} p_2^{v_{p_2}(a)} \cdots p_k^{v_{p_k}(a)}$. Alors, $b = p_1^{v_{p_1}(b)} p_2^{v_{p_2}(b)} \cdots p_k^{v_{p_k}(b)}$ donc

$$\begin{aligned} \frac{a}{b} &= \frac{p_1^{v_{p_1}(a)} p_2^{v_{p_2}(a)} \cdots p_k^{v_{p_k}(a)}}{p_1^{v_{p_1}(b)} p_2^{v_{p_2}(b)} \cdots p_k^{v_{p_k}(b)}} \\ &= p_1^{v_{p_1}(a)-v_{p_1}(b)} p_2^{v_{p_2}(a)-v_{p_2}(b)} \cdots p_k^{v_{p_k}(a)-v_{p_k}(b)}. \end{aligned}$$

Démonstration.

Supposons que b divise a. Alors, il existe un entier $d \geqslant 1$ tel que $a = bd$. Grâce au lemme 26, $v_p(a) = v_p(b) + v_p(d) \geqslant v_p(b)$ car $v_p(d) \geqslant 0$.
Réciproquement, supposons que, pour tout nombre premier p, $v_p(b) \leqslant v_p(a)$. Alors, tout nombre premier qui apparaît dans la décomposition de b apparaît aussi dans celle de a. Écrivons $a = p_1^{v_{p_1}(a)} p_2^{v_{p_2}(a)} \cdots p_k^{v_{p_k}(a)}$. Alors, $b = p_1^{v_{p_1}(b)} p_2^{v_{p_2}(b)} \cdots p_k^{v_{p_k}(b)}$ donc

$$\begin{aligned}\frac{a}{b} &= \frac{p_1^{v_{p_1}(a)} p_2^{v_{p_2}(a)} \cdots p_k^{v_{p_k}(a)}}{p_1^{v_{p_1}(b)} p_2^{v_{p_2}(b)} \cdots p_k^{v_{p_k}(b)}} \\ &= p_1^{v_{p_1}(a)-v_{p_1}(b)} p_2^{v_{p_2}(a)-v_{p_2}(b)} \cdots p_k^{v_{p_k}(a)-v_{p_k}(b)}.\end{aligned}$$

Comme, pour tout $i \in [\![1, k]\!]$, $v_{p_i}(a) \geqslant v_{p_i}(b)$, toutes les puissances qui apparaissent dans le produit précédent sont positives

Démonstration.

Supposons que b divise a. Alors, il existe un entier $d \geqslant 1$ tel que $a = bd$. Grâce au lemme 26, $v_p(a) = v_p(b) + v_p(d) \geqslant v_p(b)$ car $v_p(d) \geqslant 0$.
Réciproquement, supposons que, pour tout nombre premier p, $v_p(b) \leqslant v_p(a)$. Alors, tout nombre premier qui apparaît dans la décomposition de b apparaît aussi dans celle de a. Écrivons $a = p_1^{v_{p_1}(a)} p_2^{v_{p_2}(a)} \cdots p_k^{v_{p_k}(a)}$. Alors, $b = p_1^{v_{p_1}(b)} p_2^{v_{p_2}(b)} \cdots p_k^{v_{p_k}(b)}$ donc

$$\begin{aligned} \frac{a}{b} &= \frac{p_1^{v_{p_1}(a)} p_2^{v_{p_2}(a)} \cdots p_k^{v_{p_k}(a)}}{p_1^{v_{p_1}(b)} p_2^{v_{p_2}(b)} \cdots p_k^{v_{p_k}(b)}} \\ &= p_1^{v_{p_1}(a)-v_{p_1}(b)} p_2^{v_{p_2}(a)-v_{p_2}(b)} \cdots p_k^{v_{p_k}(a)-v_{p_k}(b)}. \end{aligned}$$

Comme, pour tout $i \in [\![1, k]\!]$, $v_{p_i}(a) \geqslant v_{p_i}(b)$, toutes les puissances qui apparaissent dans le produit précédent sont positives donc ce nombre est un entier.

Démonstration.

Supposons que b divise a. Alors, il existe un entier $d \geqslant 1$ tel que $a = bd$. Grâce au lemme 26, $v_p(a) = v_p(b) + v_p(d) \geqslant v_p(b)$ car $v_p(d) \geqslant 0$.
Réciproquement, supposons que, pour tout nombre premier p, $v_p(b) \leqslant v_p(a)$. Alors, tout nombre premier qui apparaît dans la décomposition de b apparaît aussi dans celle de a. Écrivons $a = p_1^{v_{p_1}(a)} p_2^{v_{p_2}(a)} \cdots p_k^{v_{p_k}(a)}$. Alors, $b = p_1^{v_{p_1}(b)} p_2^{v_{p_2}(b)} \cdots p_k^{v_{p_k}(b)}$ donc

$$\begin{aligned}\frac{a}{b} &= \frac{p_1^{v_{p_1}(a)} p_2^{v_{p_2}(a)} \cdots p_k^{v_{p_k}(a)}}{p_1^{v_{p_1}(b)} p_2^{v_{p_2}(b)} \cdots p_k^{v_{p_k}(b)}} \\ &= p_1^{v_{p_1}(a)-v_{p_1}(b)} p_2^{v_{p_2}(a)-v_{p_2}(b)} \cdots p_k^{v_{p_k}(a)-v_{p_k}(b)}.\end{aligned}$$

Comme, pour tout $i \in [\![1, k]\!]$, $v_{p_i}(a) \geqslant v_{p_i}(b)$, toutes les puissances qui apparaissent dans le produit précédent sont positives donc ce nombre est un entier. Ainsi, b divise a. □

Propriété 28

Soit a et b deux entiers supérieurs ou égaux à 2 et $\{p_1, p_2, ..., p_k\}$ l'ensemble de tous les nombres premiers qui apparaissent dans la décomposition en produit de facteurs premiers de a ou dans celle de b. Si on note, pour tout $i \in [\![1, k]\!]$, m_i le plus petit des deux nombres $v_{p_i}(a)$ et $v_{p_i}(b)$ et M_i le plus grand des deux nombres $v_{p_i}(a)$ et $v_{p_i}(b)$ alors

$$\mathrm{PGCD}(a, b) = p_1^{m_1} p_2^{m_2} ... p_k^{m_k}$$

et

$$\mathrm{PPCM}(a, b) = p_1^{M_1} p_2^{M_2} ... p_k^{M_k}$$

Démonstration.

Démonstration.

Notons $d = \text{PGCD}(a, b)$ et $\delta = p_1^{m_1} p_2^{m_2} ... p_k^{m_k}$.

Démonstration.

Notons $d = \text{PGCD}(a, b)$ et $\delta = p_1^{m_1} p_2^{m_2} ... p_k^{m_k}$. Pour tout $i \in [\![1, k]\!]$, $v_{p_i}(\delta) = m_i \leqslant v_{p_i}(a)$ et $v_{p_i}(\delta) = m_i \leqslant v_{p_i}(b)$ donc, d'après la propriété 27, δ divise a et b et ainsi δ divise d.

Démonstration.

Notons $d = \text{PGCD}(a, b)$ et $\delta = p_1^{m_1} p_2^{m_2} ... p_k^{m_k}$. Pour tout $i \in [\![1, k]\!]$, $v_{p_i}(\delta) = m_i \leqslant v_{p_i}(a)$ et $v_{p_i}(\delta) = m_i \leqslant v_{p_i}(b)$ donc, d'après la propriété 27, δ divise a et b et ainsi δ divise d. Réciproquement, d divise a et b donc, d'après la propriété 27, pour tout $i \in [\![1, k]\!]$, $v_{p_i}(d) \leqslant v_{p_i}(a)$ et $v_{p_i}(d) \leqslant v_{p_i}(b)$ donc $v_{p_i}(d) \leqslant m_i$.

Démonstration.

Notons $d = \text{PGCD}(a, b)$ et $\delta = p_1^{m_1} p_2^{m_2} ... p_k^{m_k}$. Pour tout $i \in [\![1, k]\!]$, $v_{p_i}(\delta) = m_i \leqslant v_{p_i}(a)$ et $v_{p_i}(\delta) = m_i \leqslant v_{p_i}(b)$ donc, d'après la propriété 27, δ divise a et b et ainsi δ divise d. Réciproquement, d divise a et b donc, d'après la propriété 27, pour tout $i \in [\![1, k]\!]$, $v_{p_i}(d) \leqslant v_{p_i}(a)$ et $v_{p_i}(d) \leqslant v_{p_i}(b)$ donc $v_{p_i}(d) \leqslant m_i$. Ainsi, toujours d'après la propriété 27, d divise δ. Comme $d > 0$ et $\delta > 0$, on conclut que $d = \delta$.

Démonstration.

Notons $d = \text{PGCD}(a, b)$ et $\delta = p_1^{m_1} p_2^{m_2} ... p_k^{m_k}$. Pour tout $i \in [\![1, k]\!]$, $v_{p_i}(\delta) = m_i \leqslant v_{p_i}(a)$ et $v_{p_i}(\delta) = m_i \leqslant v_{p_i}(b)$ donc, d'après la propriété 27, δ divise a et b et ainsi δ divise d. Réciproquement, d divise a et b donc, d'après la propriété 27, pour tout $i \in [\![1, k]\!]$, $v_{p_i}(d) \leqslant v_{p_i}(a)$ et $v_{p_i}(d) \leqslant v_{p_i}(b)$ donc $v_{p_i}(d) \leqslant m_i$. Ainsi, toujours d'après la propriété 27, d divise δ. Comme $d > 0$ et $\delta > 0$, on conclut que $d = \delta$.

Notons $m = \text{PPCM}(a, b)$ et $\mu = p_1^{M_1} p_2^{M_2} ... p_k^{M_k}$.

Démonstration.

Notons $d = \text{PGCD}(a, b)$ et $\delta = p_1^{m_1} p_2^{m_2} ... p_k^{m_k}$. Pour tout $i \in [\![1, k]\!]$, $v_{p_i}(\delta) = m_i \leqslant v_{p_i}(a)$ et $v_{p_i}(\delta) = m_i \leqslant v_{p_i}(b)$ donc, d'après la propriété 27, δ divise a et b et ainsi δ divise d. Réciproquement, d divise a et b donc, d'après la propriété 27, pour tout $i \in [\![1, k]\!]$, $v_{p_i}(d) \leqslant v_{p_i}(a)$ et $v_{p_i}(d) \leqslant v_{p_i}(b)$ donc $v_{p_i}(d) \leqslant m_i$. Ainsi, toujours d'après la propriété 27, d divise δ. Comme $d > 0$ et $\delta > 0$, on conclut que $d = \delta$.

Notons $m = \text{PPCM}(a, b)$ et $\mu = p_1^{M_1} p_2^{M_2} ... p_k^{M_k}$. Pour tout $i \in [\![1, k]\!]$, $v_{p_i}(\mu) = M_i \geqslant v_{p_i}(a)$ et $v_{p_i}(\mu) = M_i \geqslant v_{p_i}(b)$ donc, d'après la propriété 27, a et b divise μ et ainsi m divise μ.

Démonstration.

Notons $d = \text{PGCD}(a, b)$ et $\delta = p_1^{m_1} p_2^{m_2} ... p_k^{m_k}$. Pour tout $i \in [\![1, k]\!]$, $v_{p_i}(\delta) = m_i \leqslant v_{p_i}(a)$ et $v_{p_i}(\delta) = m_i \leqslant v_{p_i}(b)$ donc, d'après la propriété 27, δ divise a et b et ainsi δ divise d. Réciproquement, d divise a et b donc, d'après la propriété 27, pour tout $i \in [\![1, k]\!]$, $v_{p_i}(d) \leqslant v_{p_i}(a)$ et $v_{p_i}(d) \leqslant v_{p_i}(b)$ donc $v_{p_i}(d) \leqslant m_i$. Ainsi, toujours d'après la propriété 27, d divise δ. Comme $d > 0$ et $\delta > 0$, on conclut que $d = \delta$.

Notons $m = \text{PPCM}(a, b)$ et $\mu = p_1^{M_1} p_2^{M_2} ... p_k^{M_k}$. Pour tout $i \in [\![1, k]\!]$, $v_{p_i}(\mu) = M_i \geqslant v_{p_i}(a)$ et $v_{p_i}(\mu) = M_i \geqslant v_{p_i}(b)$ donc, d'après la propriété 27, a et b divise μ et ainsi m divise μ. Réciproquement, a et b divise m donc, d'après la propriété 27, pour tout $i \in [\![1, k]\!]$, $v_{p_i}(m) \geqslant v_{p_i}(a)$ et $v_{p_i}(m) \geqslant v_{p_i}(b)$ donc $v_{p_i}(m) \geqslant M_i$.

Démonstration.

Notons $d = \text{PGCD}(a, b)$ et $\delta = p_1^{m_1} p_2^{m_2} ... p_k^{m_k}$. Pour tout $i \in [\![1, k]\!]$, $v_{p_i}(\delta) = m_i \leqslant v_{p_i}(a)$ et $v_{p_i}(\delta) = m_i \leqslant v_{p_i}(b)$ donc, d'après la propriété 27, δ divise a et b et ainsi δ divise d. Réciproquement, d divise a et b donc, d'après la propriété 27, pour tout $i \in [\![1, k]\!]$, $v_{p_i}(d) \leqslant v_{p_i}(a)$ et $v_{p_i}(d) \leqslant v_{p_i}(b)$ donc $v_{p_i}(d) \leqslant m_i$. Ainsi, toujours d'après la propriété 27, d divise δ. Comme $d > 0$ et $\delta > 0$, on conclut que $d = \delta$.

Notons $m = \text{PPCM}(a, b)$ et $\mu = p_1^{M_1} p_2^{M_2} ... p_k^{M_k}$. Pour tout $i \in [\![1, k]\!]$, $v_{p_i}(\mu) = M_i \geqslant v_{p_i}(a)$ et $v_{p_i}(\mu) = M_i \geqslant v_{p_i}(b)$ donc, d'après la propriété 27, a et b divise μ et ainsi m divise μ. Réciproquement, a et b divise m donc, d'après la propriété 27, pour tout $i \in [\![1, k]\!]$, $v_{p_i}(m) \geqslant v_{p_i}(a)$ et $v_{p_i}(m) \geqslant v_{p_i}(b)$ donc $v_{p_i}(m) \geqslant M_i$. Ainsi, toujours d'après la propriété 27, μ divise m.

Démonstration.

Notons $d = \text{PGCD}(a, b)$ et $\delta = p_1^{m_1} p_2^{m_2} ... p_k^{m_k}$. Pour tout $i \in [\![1, k]\!]$, $v_{p_i}(\delta) = m_i \leqslant v_{p_i}(a)$ et $v_{p_i}(\delta) = m_i \leqslant v_{p_i}(b)$ donc, d'après la propriété 27, δ divise a et b et ainsi δ divise d. Réciproquement, d divise a et b donc, d'après la propriété 27, pour tout $i \in [\![1, k]\!]$, $v_{p_i}(d) \leqslant v_{p_i}(a)$ et $v_{p_i}(d) \leqslant v_{p_i}(b)$ donc $v_{p_i}(d) \leqslant m_i$. Ainsi, toujours d'après la propriété 27, d divise δ. Comme $d > 0$ et $\delta > 0$, on conclut que $d = \delta$.

Notons $m = \text{PPCM}(a, b)$ et $\mu = p_1^{M_1} p_2^{M_2} ... p_k^{M_k}$. Pour tout $i \in [\![1, k]\!]$, $v_{p_i}(\mu) = M_i \geqslant v_{p_i}(a)$ et $v_{p_i}(\mu) = M_i \geqslant v_{p_i}(b)$ donc, d'après la propriété 27, a et b divise μ et ainsi m divise μ. Réciproquement, a et b divise m donc, d'après la propriété 27, pour tout $i \in [\![1, k]\!]$, $v_{p_i}(m) \geqslant v_{p_i}(a)$ et $v_{p_i}(m) \geqslant v_{p_i}(b)$ donc $v_{p_i}(m) \geqslant M_i$. Ainsi, toujours d'après la propriété 27, μ divise m. Comme $m > 0$ et $\mu > 0$, on conclut que $m = \mu$. □

Exemple 29

Déterminer le P.G.C.D. et le P.P.C.M. de 4312 et 1000.

Exemple 29

Déterminer le P.G.C.D. et le P.P.C.M. de 4312 et 1000.
Comme $4312 = 2^3 \times 7^2 \times 11$ et $1000 = 10^3 = (2 \times 5)^3 = 2^3 \times 5^3$,

Exemple 29

Déterminer le P.G.C.D. et le P.P.C.M. de 4312 et 1000.
Comme $4312 = 2^3 \times 7^2 \times 11$ et $1000 = 10^3 = (2 \times 5)^3 = 2^3 \times 5^3$, on a PGCD$(4312, 1000) =$

Exemple 29

Déterminer le P.G.C.D. et le P.P.C.M. de 4312 et 1000.
Comme $4312 = 2^3 \times 7^2 \times 11$ et $1000 = 10^3 = (2 \times 5)^3 = 2^3 \times 5^3$, on a PGCD$(4312, 1000) = 2^3 \times 5^0 \times 7^0 \times 11^0 =$

Exemple 29

Déterminer le P.G.C.D. et le P.P.C.M. de 4312 et 1000.
Comme $4312 = 2^3 \times 7^2 \times 11$ et $1000 = 10^3 = (2 \times 5)^3 = 2^3 \times 5^3$,
on a PGCD$(4312, 1000) = 2^3 \times 5^0 \times 7^0 \times 11^0 = 8$

Exemple 29

Déterminer le P.G.C.D. et le P.P.C.M. de 4312 et 1000.
Comme $4312 = 2^3 \times 7^2 \times 11$ et $1000 = 10^3 = (2 \times 5)^3 = 2^3 \times 5^3$, on a PGCD$(4312, 1000) = 2^3 \times 5^0 \times 7^0 \times 11^0 = 8$ et PPCM$(4312, 1000) =$

Exemple 29

Déterminer le P.G.C.D. et le P.P.C.M. de 4312 et 1000.
Comme $4312 = 2^3 \times 7^2 \times 11$ et $1000 = 10^3 = (2 \times 5)^3 = 2^3 \times 5^3$,
on a PGCD$(4312, 1000) = 2^3 \times 5^0 \times 7^0 \times 11^0 = 8$ et
PPCM$(4312, 1000) = 2^3 \times 5^3 \times 7^2 \times 11^1 =$

Exemple 29

Déterminer le P.G.C.D. et le P.P.C.M. de 4312 et 1000.
Comme $4312 = 2^3 \times 7^2 \times 11$ et $1000 = 10^3 = (2 \times 5)^3 = 2^3 \times 5^3$, on a PGCD$(4312, 1000) = 2^3 \times 5^0 \times 7^0 \times 11^0 = 8$ et PPCM$(4312, 1000) = 2^3 \times 5^3 \times 7^2 \times 11^1 = 539000$.

Correction des exercices

Exercice 89 p. 30

Exercice 89 p. 30

Considérons trois entiers naturels impairs consécutifs :

Exercice 89 p. 30

Considérons trois entiers naturels impairs consécutifs : a, $a+2$ et $a+4$.

Exercice 89 p. 30

Considérons trois entiers naturels impairs consécutifs : a, $a+2$ et $a+4$. Alors, leur somme est

$$S =$$

Exercice 89 p. 30

Considérons trois entiers naturels impairs consécutifs : a, $a+2$ et $a+4$. Alors, leur somme est

$$S = a + (a+2) + (a+4) =$$

Exercice 89 p. 30

Considérons trois entiers naturels impairs consécutifs : a, $a+2$ et $a+4$. Alors, leur somme est

$$S = a + (a+2) + (a+4) = 3a + 6 =$$

Exercice 89 p. 30

Considérons trois entiers naturels impairs consécutifs : a, $a+2$ et $a+4$. Alors, leur somme est

$$S = a + (a+2) + (a+4) = 3a + 6 = 3(a+2).$$

Exercice 89 p. 30

Considérons trois entiers naturels impairs consécutifs : a, $a+2$ et $a+4$. Alors, leur somme est

$$S = a + (a+2) + (a+4) = 3a + 6 = 3(a+2).$$

De plus, $a \geqslant 1$ donc $a + 2 \geqslant 3$.

Exercice 89 p. 30

Considérons trois entiers naturels impairs consécutifs : a, $a+2$ et $a+4$. Alors, leur somme est

$$S = a + (a+2) + (a+4) = 3a + 6 = 3(a+2).$$

De plus, $a \geqslant 1$ donc $a + 2 \geqslant 3$. Ainsi, S est divisible par 3

Exercice 89 p. 30

Considérons trois entiers naturels impairs consécutifs : a, $a+2$ et $a+4$. Alors, leur somme est

$$S = a + (a+2) + (a+4) = 3a + 6 = 3(a+2).$$

De plus, $a \geqslant 1$ donc $a + 2 \geqslant 3$. Ainsi, S est divisible par 3 et $S > 3$

Exercice 89 p. 30

Considérons trois entiers naturels impairs consécutifs : a, $a+2$ et $a+4$. Alors, leur somme est

$$S = a + (a+2) + (a+4) = 3a + 6 = 3(a+2).$$

De plus, $a \geqslant 1$ donc $a+2 \geqslant 3$. Ainsi, S est divisible par 3 et $S > 3$ donc S n'est pas premier.

Exercice 92 p. 30

Exercice 92 p. 30

1. Supposons que $f : x \mapsto ax + b$ vérifie : pour tout entier naturel n, $f(n)$ est premier.

Exercice 92 p. 30

1. Supposons que $f : x \mapsto ax + b$ vérifie : pour tout entier naturel n, $f(n)$ est premier. Alors, en particulier, $f(0) = b$ est premier.

Exercice 92 p. 30

1. Supposons que $f : x \mapsto ax + b$ vérifie : pour tout entier naturel n, $f(n)$ est premier. Alors, en particulier, $f(0) = b$ est premier.
2. Avec les mêmes hypothèses, $f(b) = ab + b = (a + 1)b$ est premier

Exercice 92 p. 30

1. Supposons que $f : x \mapsto ax + b$ vérifie : pour tout entier naturel n, $f(n)$ est premier. Alors, en particulier, $f(0) = b$ est premier.
2. Avec les mêmes hypothèses, $f(b) = ab + b = (a + 1)b$ est premier donc, comme $b > 1$,

Exercice 92 p. 30

1. Supposons que $f : x \mapsto ax + b$ vérifie : pour tout entier naturel n, $f(n)$ est premier. Alors, en particulier, $f(0) = b$ est premier.
2. Avec les mêmes hypothèses, $f(b) = ab + b = (a + 1)b$ est premier donc, comme $b > 1$, cela impose que $a + 1 = 1$

Exercice 92 p. 30

1. Supposons que $f : x \mapsto ax + b$ vérifie : pour tout entier naturel n, $f(n)$ est premier. Alors, en particulier, $f(0) = b$ est premier.
2. Avec les mêmes hypothèses, $f(b) = ab + b = (a + 1)b$ est premier donc, comme $b > 1$, cela impose que $a + 1 = 1$ i.e. $a = 0$.

Exercice 92 p. 30

1. Supposons que $f : x \mapsto ax + b$ vérifie : pour tout entier naturel n, $f(n)$ est premier. Alors, en particulier, $f(0) = b$ est premier.
2. Avec les mêmes hypothèses, $f(b) = ab + b = (a + 1)b$ est premier donc, comme $b > 1$, cela impose que $a + 1 = 1$ i.e. $a = 0$.
   Ainsi, si f est solution du problème alors f est constante égale à un nombre premier.

Exercice 92 p. 30

1. Supposons que $f : x \mapsto ax + b$ vérifie : pour tout entier naturel n, $f(n)$ est premier. Alors, en particulier, $f(0) = b$ est premier.
2. Avec les mêmes hypothèses, $f(b) = ab + b = (a + 1)b$ est premier donc, comme $b > 1$, cela impose que $a + 1 = 1$ i.e. $a = 0$.
   Ainsi, si f est solution du problème alors f est constante égale à un nombre premier.
   La réciproque est évidente donc les seules fonctions solutions sont les fonctions constantes égales à des nombres premiers.

Exercice 102 p. 31.

Exercice 102 p. 31. Supposons que x et y sont deux entiers naturels tels que $x^2 - y^2 = p$.

Exercice 102 p. 31. Supposons que x et y sont deux entiers naturels tels que $x^2 - y^2 = p$. Alors,$(x - y)(x + y) = p$

Exercice 102 p. 31. Supposons que x et y sont deux entiers naturels tels que $x^2 - y^2 = p$. Alors,$(x - y)(x + y) = p$ donc, comme p est premier

Exercice 102 p. 31. Supposons que x et y sont deux entiers naturels tels que $x^2 - y^2 = p$. Alors,$(x-y)(x+y) = p$ donc, comme p est premier et comme $x - y \leqslant x + y$ (car $y \geqslant 0$),

Exercice 102 p. 31. Supposons que x et y sont deux entiers naturels tels que $x^2 - y^2 = p$. Alors,$(x-y)(x+y) = p$ donc, comme p est premier et comme $x - y \leqslant x + y$ (car $y \geqslant 0$), on conclut que $x - y = 1$ et $x + y = p$.

Exercice 102 p. 31. Supposons que x et y sont deux entiers naturels tels que $x^2 - y^2 = p$. Alors,$(x-y)(x+y) = p$ donc, comme p est premier et comme $x - y \leqslant x + y$ (car $y \geqslant 0$), on conclut que $x - y = 1$ et $x + y = p$. Dès lors,
$x =$

Exercice 102 p. 31. Supposons que x et y sont deux entiers naturels tels que $x^2 - y^2 = p$. Alors,$(x-y)(x+y) = p$ donc, comme p est premier et comme $x - y \leqslant x + y$ (car $y \geqslant 0$), on conclut que $x - y = 1$ et $x + y = p$. Dès lors,
$x = \frac{(x+y)+(x-y)}{2} =$

Exercice 102 p. 31. Supposons que x et y sont deux entiers naturels tels que $x^2 - y^2 = p$. Alors,$(x-y)(x+y) = p$ donc, comme p est premier et comme $x - y \leqslant x + y$ (car $y \geqslant 0$), on conclut que $x - y = 1$ et $x + y = p$. Dès lors,
$x = \frac{(x+y)+(x-y)}{2} = \frac{p+1}{2}$ et $y =$

Exercice 102 p. 31. Supposons que x et y sont deux entiers naturels tels que $x^2 - y^2 = p$. Alors,$(x-y)(x+y) = p$ donc, comme p est premier et comme $x - y \leqslant x + y$ (car $y \geqslant 0$), on conclut que $x - y = 1$ et $x + y = p$. Dès lors,
$x = \frac{(x+y)+(x-y)}{2} = \frac{p+1}{2}$ et $y = \frac{(x+y)-(x-y)}{2} =$

Exercice 102 p. 31. Supposons que x et y sont deux entiers naturels tels que $x^2 - y^2 = p$. Alors,$(x-y)(x+y) = p$ donc, comme p est premier et comme $x - y \leqslant x + y$ (car $y \geqslant 0$), on conclut que $x - y = 1$ et $x + y = p$. Dès lors, $x = \frac{(x+y)+(x-y)}{2} = \frac{p+1}{2}$ et $y = \frac{(x+y)-(x-y)}{2} = \frac{p-1}{2}$.

Exercice 102 p. 31. Supposons que x et y sont deux entiers naturels tels que $x^2 - y^2 = p$. Alors,$(x-y)(x+y) = p$ donc, comme p est premier et comme $x - y \leqslant x + y$ (car $y \geqslant 0$), on conclut que $x - y = 1$ et $x + y = p$. Dès lors,
$x = \frac{(x+y)+(x-y)}{2} = \frac{p+1}{2}$ et $y = \frac{(x+y)-(x-y)}{2} = \frac{p-1}{2}$.
Réciproquement, considérons $x = \frac{p+1}{2}$ et $y = \frac{p-1}{2}$.

Exercice 102 p. 31. Supposons que x et y sont deux entiers naturels tels que $x^2 - y^2 = p$. Alors,$(x-y)(x+y) = p$ donc, comme p est premier et comme $x - y \leqslant x + y$ (car $y \geqslant 0$), on conclut que $x - y = 1$ et $x + y = p$. Dès lors,
$x = \frac{(x+y)+(x-y)}{2} = \frac{p+1}{2}$ et $y = \frac{(x+y)-(x-y)}{2} = \frac{p-1}{2}$.
Réciproquement, considérons $x = \frac{p+1}{2}$ et $y = \frac{p-1}{2}$. Si $p = 2$ alors $x = \frac{3}{2}$ n'est pas entier

Exercice 102 p. 31. Supposons que x et y sont deux entiers naturels tels que $x^2 - y^2 = p$. Alors,$(x-y)(x+y) = p$ donc, comme p est premier et comme $x - y \leqslant x + y$ (car $y \geqslant 0$), on conclut que $x - y = 1$ et $x + y = p$. Dès lors,
$x = \frac{(x+y)+(x-y)}{2} = \frac{p+1}{2}$ et $y = \frac{(x+y)-(x-y)}{2} = \frac{p-1}{2}$.
Réciproquement, considérons $x = \frac{p+1}{2}$ et $y = \frac{p-1}{2}$. Si $p = 2$ alors $x = \frac{3}{2}$ n'est pas entier donc l'équation n'a pas de solution dans $\mathbb{N}^2$.

Exercice 102 p. 31. Supposons que x et y sont deux entiers naturels tels que $x^2 - y^2 = p$. Alors,$(x-y)(x+y) = p$ donc, comme p est premier et comme $x - y \leqslant x + y$ (car $y \geqslant 0$), on conclut que $x - y = 1$ et $x + y = p$. Dès lors,
$x = \frac{(x+y)+(x-y)}{2} = \frac{p+1}{2}$ et $y = \frac{(x+y)-(x-y)}{2} = \frac{p-1}{2}$.
Réciproquement, considérons $x = \frac{p+1}{2}$ et $y = \frac{p-1}{2}$. Si $p = 2$ alors $x = \frac{3}{2}$ n'est pas entier donc l'équation n'a pas de solution dans $\mathbb{N}^2$.
Si $p > 2$ alors p est impair

Exercice 102 p. 31. Supposons que x et y sont deux entiers naturels tels que $x^2 - y^2 = p$. Alors,$(x-y)(x+y) = p$ donc, comme p est premier et comme $x - y \leqslant x + y$ (car $y \geqslant 0$), on conclut que $x - y = 1$ et $x + y = p$. Dès lors,
$x = \frac{(x+y)+(x-y)}{2} = \frac{p+1}{2}$ et $y = \frac{(x+y)-(x-y)}{2} = \frac{p-1}{2}$.
Réciproquement, considérons $x = \frac{p+1}{2}$ et $y = \frac{p-1}{2}$. Si $p = 2$ alors $x = \frac{3}{2}$ n'est pas entier donc l'équation n'a pas de solution dans $\mathbb{N}^2$.
Si $p > 2$ alors p est impair donc $p + 1$ et $p - 1$ sont pairs

Exercice 102 p. 31. Supposons que x et y sont deux entiers naturels tels que $x^2 - y^2 = p$. Alors,$(x-y)(x+y) = p$ donc, comme p est premier et comme $x - y \leqslant x + y$ (car $y \geqslant 0$), on conclut que $x - y = 1$ et $x + y = p$. Dès lors,
$x = \frac{(x+y)+(x-y)}{2} = \frac{p+1}{2}$ et $y = \frac{(x+y)-(x-y)}{2} = \frac{p-1}{2}$.
Réciproquement, considérons $x = \frac{p+1}{2}$ et $y = \frac{p-1}{2}$. Si $p = 2$ alors $x = \frac{3}{2}$ n'est pas entier donc l'équation n'a pas de solution dans $\mathbb{N}^2$. Si $p > 2$ alors p est impair donc $p + 1$ et $p - 1$ sont pairs et ainsi x et y sont entiers.

Exercice 102 p. 31. Supposons que x et y sont deux entiers naturels tels que $x^2 - y^2 = p$. Alors,$(x-y)(x+y) = p$ donc, comme p est premier et comme $x - y \leqslant x + y$ (car $y \geqslant 0$), on conclut que $x - y = 1$ et $x + y = p$. Dès lors,
$x = \frac{(x+y)+(x-y)}{2} = \frac{p+1}{2}$ et $y = \frac{(x+y)-(x-y)}{2} = \frac{p-1}{2}$.
Réciproquement, considérons $x = \frac{p+1}{2}$ et $y = \frac{p-1}{2}$. Si $p = 2$ alors $x = \frac{3}{2}$ n'est pas entier donc l'équation n'a pas de solution dans $\mathbb{N}^2$.
Si $p > 2$ alors p est impair donc $p + 1$ et $p - 1$ sont pairs et ainsi x et y sont entiers. De plus, $x - y = 1$ et $x + y = p$

Exercice 102 p. 31. Supposons que x et y sont deux entiers naturels tels que $x^2 - y^2 = p$. Alors,$(x-y)(x+y) = p$ donc, comme p est premier et comme $x - y \leqslant x + y$ (car $y \geqslant 0$), on conclut que $x - y = 1$ et $x + y = p$. Dès lors,
$x = \frac{(x+y)+(x-y)}{2} = \frac{p+1}{2}$ et $y = \frac{(x+y)-(x-y)}{2} = \frac{p-1}{2}$.
Réciproquement, considérons $x = \frac{p+1}{2}$ et $y = \frac{p-1}{2}$. Si $p = 2$ alors $x = \frac{3}{2}$ n'est pas entier donc l'équation n'a pas de solution dans $\mathbb{N}^2$.
Si $p > 2$ alors p est impair donc $p + 1$ et $p - 1$ sont pairs et ainsi x et y sont entiers. De plus, $x - y = 1$ et $x + y = p$ donc
$x^2 - y^2 = (x - y)(x + y) = p$

Exercice 102 p. 31. Supposons que x et y sont deux entiers naturels tels que $x^2 - y^2 = p$. Alors,$(x-y)(x+y) = p$ donc, comme p est premier et comme $x - y \leqslant x + y$ (car $y \geqslant 0$), on conclut que $x - y = 1$ et $x + y = p$. Dès lors, $x = \frac{(x+y)+(x-y)}{2} = \frac{p+1}{2}$ et $y = \frac{(x+y)-(x-y)}{2} = \frac{p-1}{2}$.
Réciproquement, considérons $x = \frac{p+1}{2}$ et $y = \frac{p-1}{2}$. Si $p = 2$ alors $x = \frac{3}{2}$ n'est pas entier donc l'équation n'a pas de solution dans $\mathbb{N}^2$.
Si $p > 2$ alors p est impair donc $p + 1$ et $p - 1$ sont pairs et ainsi x et y sont entiers. De plus, $x - y = 1$ et $x + y = p$ donc $x^2 - y^2 = (x - y)(x + y) = p$ et ainsi x et y sont solutions de l'équation.

Exercice 102 p. 31. Supposons que x et y sont deux entiers naturels tels que $x^2 - y^2 = p$. Alors,$(x-y)(x+y) = p$ donc, comme p est premier et comme $x - y \leqslant x + y$ (car $y \geqslant 0$), on conclut que $x - y = 1$ et $x + y = p$. Dès lors,
$x = \frac{(x+y)+(x-y)}{2} = \frac{p+1}{2}$ et $y = \frac{(x+y)-(x-y)}{2} = \frac{p-1}{2}$.
Réciproquement, considérons $x = \frac{p+1}{2}$ et $y = \frac{p-1}{2}$. Si $p = 2$ alors $x = \frac{3}{2}$ n'est pas entier donc l'équation n'a pas de solution dans $\mathbb{N}^2$.
Si $p > 2$ alors p est impair donc $p + 1$ et $p - 1$ sont pairs et ainsi x et y sont entiers. De plus, $x - y = 1$ et $x + y = p$ donc $x^2 - y^2 = (x - y)(x + y) = p$ et ainsi x et y sont solutions de l'équation.
On conclut que l'équation n'a pas de solution dans $\mathbb{N}^2$ si $p = 2$ et que l'unique solution de l'équation dans $\mathbb{N}^2$ est $\left(\frac{p+1}{2} ; \frac{p-1}{2}\right)$ si $p > 2$.

Sujet C p. 37

1. On a $u_1 = 10 \times 1 + 21 = 31$,

Sujet C p. 37

1. On a $u_1 = 10 \times 1 + 21 = 31$, $u_2 = 10 \times 31 + 21 = 331$

Sujet C p. 37

1. On a $u_1 = 10 \times 1 + 21 = 31$, $u_2 = 10 \times 31 + 21 = 331$ et $u_3 = 10 \times 331 + 21 = 3331$.

Sujet C p. 37

1. On a $u_1 = 10 \times 1 + 21 = 31$, $u_2 = 10 \times 31 + 21 = 331$ et $u_3 = 10 \times 331 + 21 = 3331$.
2. a. Considérons, pour tout $n \in \mathbb{N}$, la proposition P_n :
« $3u_n = 10^{n+1} - 7$ »

Sujet C p. 37

1. On a $u_1 = 10 \times 1 + 21 = 31$, $u_2 = 10 \times 31 + 21 = 331$ et $u_3 = 10 \times 331 + 21 = 3331$.

2. a. Considérons, pour tout $n \in \mathbb{N}$, la proposition P_n :
« $3u_n = 10^{n+1} - 7$ »
Comme $10^{0+1} - 7 = 3 = 3 \times u_0$, P_0 est vraie.

Sujet C p. 37

1. On a $u_1 = 10 \times 1 + 21 = 31$, $u_2 = 10 \times 31 + 21 = 331$ et $u_3 = 10 \times 331 + 21 = 3331$.

2. a. Considérons, pour tout $n \in \mathbb{N}$, la proposition P_n :
« $3u_n = 10^{n+1} - 7$ »
Comme $10^{0+1} - 7 = 3 = 3 \times u_0$, P_0 est vraie.
Supposons que P_k est vraie pour un certain $k \in \mathbb{N}$.

Sujet C p. 37

1. On a $u_1 = 10 \times 1 + 21 = 31$, $u_2 = 10 \times 31 + 21 = 331$ et $u_3 = 10 \times 331 + 21 = 3331$.

2. a. Considérons, pour tout $n \in \mathbb{N}$, la proposition P_n :
« $3u_n = 10^{n+1} - 7$ »
Comme $10^{0+1} - 7 = 3 = 3 \times u_0$, P_0 est vraie.
Supposons que P_k est vraie pour un certain $k \in \mathbb{N}$.
Alors,

$3u_{k+1} =$

Sujet C p. 37

1. On a $u_1 = 10 \times 1 + 21 = 31$, $u_2 = 10 \times 31 + 21 = 331$ et $u_3 = 10 \times 331 + 21 = 3331$.

2. a. Considérons, pour tout $n \in \mathbb{N}$, la proposition P_n :
« $3u_n = 10^{n+1} - 7$ »
Comme $10^{0+1} - 7 = 3 = 3 \times u_0$, P_0 est vraie.
Supposons que P_k est vraie pour un certain $k \in \mathbb{N}$.
Alors,

$$3u_{k+1} = 3(10u_n + 21) =$$

Sujet C p. 37

1. On a $u_1 = 10 \times 1 + 21 = 31$, $u_2 = 10 \times 31 + 21 = 331$ et $u_3 = 10 \times 331 + 21 = 3331$.

2. a. Considérons, pour tout $n \in \mathbb{N}$, la proposition P_n :
« $3u_n = 10^{n+1} - 7$ »
Comme $10^{0+1} - 7 = 3 = 3 \times u_0$, P_0 est vraie.
Supposons que P_k est vraie pour un certain $k \in \mathbb{N}$.
Alors,

$$3u_{k+1} = 3(10u_n + 21) = 10 \times (3u_k) + 63$$

Sujet C p. 37

1. On a $u_1 = 10 \times 1 + 21 = 31$, $u_2 = 10 \times 31 + 21 = 331$ et $u_3 = 10 \times 331 + 21 = 3331$.

2. a. Considérons, pour tout $n \in \mathbb{N}$, la proposition P_n :
« $3u_n = 10^{n+1} - 7$ »
Comme $10^{0+1} - 7 = 3 = 3 \times u_0$, P_0 est vraie.
Supposons que P_k est vraie pour un certain $k \in \mathbb{N}$.
Alors,

$$\begin{aligned} 3u_{k+1} &= 3(10u_n + 21) = 10 \times (3u_k) + 63 \\ &= 10 \times (10^{k+1} - 7) + 63 = \end{aligned}$$

Sujet C p. 37

1. On a $u_1 = 10 \times 1 + 21 = 31$, $u_2 = 10 \times 31 + 21 = 331$ et $u_3 = 10 \times 331 + 21 = 3331$.

2. a. Considérons, pour tout $n \in \mathbb{N}$, la proposition P_n :
« $3u_n = 10^{n+1} - 7$ »
Comme $10^{0+1} - 7 = 3 = 3 \times u_0$, P_0 est vraie.
Supposons que P_k est vraie pour un certain $k \in \mathbb{N}$.
Alors,

$$\begin{aligned} 3u_{k+1} &= 3(10u_n + 21) = 10 \times (3u_k) + 63 \\ &= 10 \times (10^{k+1} - 7) + 63 = 10^{k+2} - 70 + 63 = \end{aligned}$$

Sujet C p. 37

1. On a $u_1 = 10 \times 1 + 21 = 31$, $u_2 = 10 \times 31 + 21 = 331$ et $u_3 = 10 \times 331 + 21 = 3331$.

2. a. Considérons, pour tout $n \in \mathbb{N}$, la proposition P_n :
« $3u_n = 10^{n+1} - 7$ »
Comme $10^{0+1} - 7 = 3 = 3 \times u_0$, P_0 est vraie.
Supposons que P_k est vraie pour un certain $k \in \mathbb{N}$.
Alors,

$$\begin{aligned} 3u_{k+1} &= 3(10u_n + 21) = 10 \times (3u_k) + 63 \\ &= 10 \times (10^{k+1} - 7) + 63 = 10^{k+2} - 70 + 63 = 10^{k+2} - 7 \end{aligned}$$

Sujet C p. 37

1. On a $u_1 = 10 \times 1 + 21 = 31$, $u_2 = 10 \times 31 + 21 = 331$ et $u_3 = 10 \times 331 + 21 = 3331$.

2. a. Considérons, pour tout $n \in \mathbb{N}$, la proposition P_n :
« $3u_n = 10^{n+1} - 7$ »
Comme $10^{0+1} - 7 = 3 = 3 \times u_0$, P_0 est vraie.
Supposons que P_k est vraie pour un certain $k \in \mathbb{N}$.
Alors,

$$\begin{aligned} 3u_{k+1} &= 3(10u_n + 21) = 10 \times (3u_k) + 63 \\ &= 10 \times (10^{k+1} - 7) + 63 = 10^{k+2} - 70 + 63 = 10^{k+2} - 7 \end{aligned}$$

donc P_{k+1} est vraie.

Sujet C p. 37

1. On a $u_1 = 10 \times 1 + 21 = 31$, $u_2 = 10 \times 31 + 21 = 331$ et $u_3 = 10 \times 331 + 21 = 3331$.

2. a. Considérons, pour tout $n \in \mathbb{N}$, la proposition P_n :
« $3u_n = 10^{n+1} - 7$ »
Comme $10^{0+1} - 7 = 3 = 3 \times u_0$, P_0 est vraie.
Supposons que P_k est vraie pour un certain $k \in \mathbb{N}$.
Alors,

$$\begin{aligned} 3u_{k+1} &= 3(10u_n + 21) = 10 \times (3u_k) + 63 \\ &= 10 \times (10^{k+1} - 7) + 63 = 10^{k+2} - 70 + 63 = 10^{k+2} - 7 \end{aligned}$$

donc P_{k+1} est vraie.
On a donc montré par récurrence que, pour tout $n \in \mathbb{N}$,
$3u_n = 10^{n+1} - 7$.

Sujet C p. 37

1. On a $u_1 = 10 \times 1 + 21 = 31$, $u_2 = 10 \times 31 + 21 = 331$ et $u_3 = 10 \times 331 + 21 = 3331$.
2. a. Considérons, pour tout $n \in \mathbb{N}$, la proposition P_n :
« $3u_n = 10^{n+1} - 7$ »
Comme $10^{0+1} - 7 = 3 = 3 \times u_0$, P_0 est vraie.
Supposons que P_k est vraie pour un certain $k \in \mathbb{N}$.
Alors,

$$\begin{aligned} 3u_{k+1} &= 3(10u_n + 21) = 10 \times (3u_k) + 63 \\ &= 10 \times (10^{k+1} - 7) + 63 = 10^{k+2} - 70 + 63 = 10^{k+2} - 7 \end{aligned}$$

donc P_{k+1} est vraie.
On a donc montré par récurrence que, pour tout $n \in \mathbb{N}$, $3u_n = 10^{n+1} - 7$.

b. Soit $n \in \mathbb{N}$.

Sujet C p. 37

1. On a $u_1 = 10 \times 1 + 21 = 31$, $u_2 = 10 \times 31 + 21 = 331$ et $u_3 = 10 \times 331 + 21 = 3331$.

2. a. Considérons, pour tout $n \in \mathbb{N}$, la proposition P_n :
« $3u_n = 10^{n+1} - 7$ »
Comme $10^{0+1} - 7 = 3 = 3 \times u_0$, P_0 est vraie.
Supposons que P_k est vraie pour un certain $k \in \mathbb{N}$.
Alors,

$$\begin{aligned} 3u_{k+1} &= 3(10u_n + 21) = 10 \times (3u_k) + 63 \\ &= 10 \times (10^{k+1} - 7) + 63 = 10^{k+2} - 70 + 63 = 10^{k+2} - 7 \end{aligned}$$

donc P_{k+1} est vraie.
On a donc montré par récurrence que, pour tout $n \in \mathbb{N}$, $3u_n = 10^{n+1} - 7$.

b. Soit $n \in \mathbb{N}$. Le nombre 10^{n+1} s'écrit $1\underbrace{000\cdots0}_{n+1 \text{ fois}}$

Sujet C p. 37

1. On a $u_1 = 10 \times 1 + 21 = 31$, $u_2 = 10 \times 31 + 21 = 331$ et $u_3 = 10 \times 331 + 21 = 3331$.

2. a. Considérons, pour tout $n \in \mathbb{N}$, la proposition P_n :
« $3u_n = 10^{n+1} - 7$ »
Comme $10^{0+1} - 7 = 3 = 3 \times u_0$, P_0 est vraie.
Supposons que P_k est vraie pour un certain $k \in \mathbb{N}$.
Alors,

$$\begin{aligned} 3u_{k+1} &= 3(10u_n + 21) = 10 \times (3u_k) + 63 \\ &= 10 \times (10^{k+1} - 7) + 63 = 10^{k+2} - 70 + 63 = 10^{k+2} - 7 \end{aligned}$$

donc P_{k+1} est vraie.
On a donc montré par récurrence que, pour tout $n \in \mathbb{N}$, $3u_n = 10^{n+1} - 7$.

b. Soit $n \in \mathbb{N}$. Le nombre 10^{n+1} s'écrit $1\underbrace{000\cdots0}_{n+1 \text{ fois}}$ donc $10^{n+1} - 7$ s'écrit $\underbrace{999\cdots9}_{n \text{ fois}}3$.

Sujet C p. 37

1. On a $u_1 = 10 \times 1 + 21 = 31$, $u_2 = 10 \times 31 + 21 = 331$ et $u_3 = 10 \times 331 + 21 = 3331$.

2. a. Considérons, pour tout $n \in \mathbb{N}$, la proposition P_n :
« $3u_n = 10^{n+1} - 7$ »
Comme $10^{0+1} - 7 = 3 = 3 \times u_0$, P_0 est vraie.
Supposons que P_k est vraie pour un certain $k \in \mathbb{N}$.
Alors,

$$\begin{aligned} 3u_{k+1} &= 3(10u_n + 21) = 10 \times (3u_k) + 63 \\ &= 10 \times (10^{k+1} - 7) + 63 = 10^{k+2} - 70 + 63 = 10^{k+2} - 7 \end{aligned}$$

donc P_{k+1} est vraie.
On a donc montré par récurrence que, pour tout $n \in \mathbb{N}$, $3u_n = 10^{n+1} - 7$.

b. Soit $n \in \mathbb{N}$. Le nombre 10^{n+1} s'écrit $1\underbrace{000\cdots0}_{n+1 \text{ fois}}$ donc $10^{n+1} - 7$ s'écrit $\underbrace{999\cdots9}_{n \text{ fois}}3$. En divisant par 3, on en déduit que $u_n = \underbrace{333\cdots3}_{n \text{ fois}}1$.

3. La partie entière de $\sqrt{331}$ est 18.

3. La partie entière de $\sqrt{331}$ est 18. On vérifie que 331 n'est pas divisible 2, 3, 5, 7, 11, 13 et 17

3. La partie entière de $\sqrt{331}$ est 18. On vérifie que 331 n'est pas divisible 2, 3, 5, 7, 11, 13 et 17 donc 331 est un nombre premier.

3. La partie entière de $\sqrt{331}$ est 18. On vérifie que 331 n'est pas divisible 2, 3, 5, 7, 11, 13 et 17 donc 331 est un nombre premier.
4. Soit $n \in \mathbb{N}$.

3. La partie entière de $\sqrt{331}$ est 18. On vérifie que 331 n'est pas divisible 2, 3, 5, 7, 11, 13 et 17 donc 331 est un nombre premier.
4. Soit $n \in \mathbb{N}$. L'écriture décimale de u_n se termine par 1

3. La partie entière de $\sqrt{331}$ est 18. On vérifie que 331 n'est pas divisible 2, 3, 5, 7, 11, 13 et 17 donc 331 est un nombre premier.
4. Soit $n \in \mathbb{N}$. L'écriture décimale de u_n se termine par 1 donc u_n n'est divisible ni par 2 ni par 5.

3. La partie entière de $\sqrt{331}$ est 18. On vérifie que 331 n'est pas divisible 2, 3, 5, 7, 11, 13 et 17 donc 331 est un nombre premier.
4. Soit $n \in \mathbb{N}$. L'écriture décimale de u_n se termine par 1 donc u_n n'est divisible ni par 2 ni par 5. De plus, la somme des chiffres de u_n est $3n + 1$

3. La partie entière de $\sqrt{331}$ est 18. On vérifie que 331 n'est pas divisible 2, 3, 5, 7, 11, 13 et 17 donc 331 est un nombre premier.
4. Soit $n \in \mathbb{N}$. L'écriture décimale de u_n se termine par 1 donc u_n n'est divisible ni par 2 ni par 5. De plus, la somme des chiffres de u_n est $3n+1$ qui n'est pas divisible par 3 (puisque son reste modulo 3 est 1)

3. La partie entière de $\sqrt{331}$ est 18. On vérifie que 331 n'est pas divisible 2, 3, 5, 7, 11, 13 et 17 donc 331 est un nombre premier.
4. Soit $n \in \mathbb{N}$. L'écriture décimale de u_n se termine par 1 donc u_n n'est divisible ni par 2 ni par 5. De plus, la somme des chiffres de u_n est $3n+1$ qui n'est pas divisible par 3 (puisque son reste modulo 3 est 1) donc u_n n'est pas divisible par 3.

3. La partie entière de $\sqrt{331}$ est 18. On vérifie que 331 n'est pas divisible 2, 3, 5, 7, 11, 13 et 17 donc 331 est un nombre premier.
4. Soit $n \in \mathbb{N}$. L'écriture décimale de u_n se termine par 1 donc u_n n'est divisible ni par 2 ni par 5. De plus, la somme des chiffres de u_n est $3n+1$ qui n'est pas divisible par 3 (puisque son reste modulo 3 est 1) donc u_n n'est pas divisible par 3.
5. a. Soit $n \in \mathbb{N}$.

3. La partie entière de $\sqrt{331}$ est 18. On vérifie que 331 n'est pas divisible 2, 3, 5, 7, 11, 13 et 17 donc 331 est un nombre premier.
4. Soit $n \in \mathbb{N}$. L'écriture décimale de u_n se termine par 1 donc u_n n'est divisible ni par 2 ni par 5. De plus, la somme des chiffres de u_n est $3n+1$ qui n'est pas divisible par 3 (puisque son reste modulo 3 est 1) donc u_n n'est pas divisible par 3.
5. a. Soit $n \in \mathbb{N}$. Alors, d'après la question **2.a.**, $3u_n = 10^{n+1} - 7$.

3. La partie entière de $\sqrt{331}$ est 18. On vérifie que 331 n'est pas divisible 2, 3, 5, 7, 11, 13 et 17 donc 331 est un nombre premier.
4. Soit $n \in \mathbb{N}$. L'écriture décimale de u_n se termine par 1 donc u_n n'est divisible ni par 2 ni par 5. De plus, la somme des chiffres de u_n est $3n+1$ qui n'est pas divisible par 3 (puisque son reste modulo 3 est 1) donc u_n n'est pas divisible par 3.
5. a. Soit $n \in \mathbb{N}$. Alors, d'après la question **2.a.**, $3u_n = 10^{n+1} - 7$. Or, $10 \equiv -1\ [11]$

3. La partie entière de $\sqrt{331}$ est 18. On vérifie que 331 n'est pas divisible 2, 3, 5, 7, 11, 13 et 17 donc 331 est un nombre premier.
4. Soit $n \in \mathbb{N}$. L'écriture décimale de u_n se termine par 1 donc u_n n'est divisible ni par 2 ni par 5. De plus, la somme des chiffres de u_n est $3n+1$ qui n'est pas divisible par 3 (puisque son reste modulo 3 est 1) donc u_n n'est pas divisible par 3.
5. a. Soit $n \in \mathbb{N}$. Alors, d'après la question **2.a.**, $3u_n = 10^{n+1} - 7$. Or, $10 \equiv -1\ [11]$ et $-7 \equiv 4\ [11]$

3. La partie entière de $\sqrt{331}$ est 18. On vérifie que 331 n'est pas divisible 2, 3, 5, 7, 11, 13 et 17 donc 331 est un nombre premier.
4. Soit $n \in \mathbb{N}$. L'écriture décimale de u_n se termine par 1 donc u_n n'est divisible ni par 2 ni par 5. De plus, la somme des chiffres de u_n est $3n+1$ qui n'est pas divisible par 3 (puisque son reste modulo 3 est 1) donc u_n n'est pas divisible par 3.
5. a. Soit $n \in \mathbb{N}$. Alors, d'après la question **2.a.**, $3u_n = 10^{n+1} - 7$. Or, $10 \equiv -1\ [11]$ et $-7 \equiv 4\ [11]$ donc $3u_n \equiv (-1)^{n+1} + 4\ [11]$

3. La partie entière de $\sqrt{331}$ est 18. On vérifie que 331 n'est pas divisible 2, 3, 5, 7, 11, 13 et 17 donc 331 est un nombre premier.

4. Soit $n \in \mathbb{N}$. L'écriture décimale de u_n se termine par 1 donc u_n n'est divisible ni par 2 ni par 5. De plus, la somme des chiffres de u_n est $3n+1$ qui n'est pas divisible par 3 (puisque son reste modulo 3 est 1) donc u_n n'est pas divisible par 3.

5. a. Soit $n \in \mathbb{N}$. Alors, d'après la question **2.a.**, $3u_n = 10^{n+1} - 7$. Or, $10 \equiv -1\ [11]$ et $-7 \equiv 4\ [11]$ donc $3u_n \equiv (-1)^{n+1} + 4\ [11]$ i.e. puisque $(-1)^{n+1} = (-1) \times (-1)^n = -(-1)^n$, $3u_n \equiv 4 - (-1)^n\ [11]$.

3. La partie entière de $\sqrt{331}$ est 18. On vérifie que 331 n'est pas divisible 2, 3, 5, 7, 11, 13 et 17 donc 331 est un nombre premier.
4. Soit $n \in \mathbb{N}$. L'écriture décimale de u_n se termine par 1 donc u_n n'est divisible ni par 2 ni par 5. De plus, la somme des chiffres de u_n est $3n+1$ qui n'est pas divisible par 3 (puisque son reste modulo 3 est 1) donc u_n n'est pas divisible par 3.
5. a. Soit $n \in \mathbb{N}$. Alors, d'après la question **2.a.**, $3u_n = 10^{n+1} - 7$. Or, $10 \equiv -1\ [11]$ et $-7 \equiv 4\ [11]$ donc $3u_n \equiv (-1)^{n+1} + 4\ [11]$ i.e. puisque $(-1)^{n+1} = (-1) \times (-1)^n = -(-1)^n$, $3u_n \equiv 4 - (-1)^n\ [11]$.

   b. Soit $n \in \mathbb{N}$.

3. La partie entière de $\sqrt{331}$ est 18. On vérifie que 331 n'est pas divisible 2, 3, 5, 7, 11, 13 et 17 donc 331 est un nombre premier.
4. Soit $n \in \mathbb{N}$. L'écriture décimale de u_n se termine par 1 donc u_n n'est divisible ni par 2 ni par 5. De plus, la somme des chiffres de u_n est $3n+1$ qui n'est pas divisible par 3 (puisque son reste modulo 3 est 1) donc u_n n'est pas divisible par 3.
5. a. Soit $n \in \mathbb{N}$. Alors, d'après la question **2.a.**, $3u_n = 10^{n+1} - 7$. Or, $10 \equiv -1\ [11]$ et $-7 \equiv 4\ [11]$ donc $3u_n \equiv (-1)^{n+1} + 4\ [11]$ i.e. puisque $(-1)^{n+1} = (-1) \times (-1)^n = -(-1)^n$, $3u_n \equiv 4 - (-1)^n\ [11]$.
   b. Soit $n \in \mathbb{N}$. Si n est pair alors $3u_n \equiv 4 - 1\ [11] \equiv 3\ [11]$

3. La partie entière de $\sqrt{331}$ est 18. On vérifie que 331 n'est pas divisible 2, 3, 5, 7, 11, 13 et 17 donc 331 est un nombre premier.
4. Soit $n \in \mathbb{N}$. L'écriture décimale de u_n se termine par 1 donc u_n n'est divisible ni par 2 ni par 5. De plus, la somme des chiffres de u_n est $3n+1$ qui n'est pas divisible par 3 (puisque son reste modulo 3 est 1) donc u_n n'est pas divisible par 3.
5. a. Soit $n \in \mathbb{N}$. Alors, d'après la question **2.a.**, $3u_n = 10^{n+1} - 7$. Or, $10 \equiv -1\ [11]$ et $-7 \equiv 4\ [11]$ donc $3u_n \equiv (-1)^{n+1} + 4\ [11]$ i.e. puisque $(-1)^{n+1} = (-1) \times (-1)^n = -(-1)^n$, $3u_n \equiv 4 - (-1)^n\ [11]$.
   b. Soit $n \in \mathbb{N}$. Si n est pair alors $3u_n \equiv 4 - 1\ [11] \equiv 3\ [11]$ et si n est impair alors $3u_n \equiv 4 + 1\ [11] \equiv 5\ [11]$.

3. La partie entière de $\sqrt{331}$ est 18. On vérifie que 331 n'est pas divisible 2, 3, 5, 7, 11, 13 et 17 donc 331 est un nombre premier.

4. Soit $n \in \mathbb{N}$. L'écriture décimale de u_n se termine par 1 donc u_n n'est divisible ni par 2 ni par 5. De plus, la somme des chiffres de u_n est $3n+1$ qui n'est pas divisible par 3 (puisque son reste modulo 3 est 1) donc u_n n'est pas divisible par 3.

5. a. Soit $n \in \mathbb{N}$. Alors, d'après la question **2.a.**, $3u_n = 10^{n+1} - 7$. Or, $10 \equiv -1\ [11]$ et $-7 \equiv 4\ [11]$ donc $3u_n \equiv (-1)^{n+1} + 4\ [11]$ i.e. puisque $(-1)^{n+1} = (-1) \times (-1)^n = -(-1)^n$, $3u_n \equiv 4 - (-1)^n\ [11]$.

   b. Soit $n \in \mathbb{N}$. Si n est pair alors $3u_n \equiv 4 - 1\ [11] \equiv 3\ [11]$ et si n est impair alors $3u_n \equiv 4 + 1\ [11] \equiv 5\ [11]$. Comme 3 et 5 sont compris entre 0 et 10, on en déduit que le reste de $3u_n$ modulo 11 est soit 3 soit 5.

3. La partie entière de $\sqrt{331}$ est 18. On vérifie que 331 n'est pas divisible 2, 3, 5, 7, 11, 13 et 17 donc 331 est un nombre premier.

4. Soit $n \in \mathbb{N}$. L'écriture décimale de u_n se termine par 1 donc u_n n'est divisible ni par 2 ni par 5. De plus, la somme des chiffres de u_n est $3n+1$ qui n'est pas divisible par 3 (puisque son reste modulo 3 est 1) donc u_n n'est pas divisible par 3.

5. a. Soit $n \in \mathbb{N}$. Alors, d'après la question **2.a.**, $3u_n = 10^{n+1} - 7$. Or, $10 \equiv -1\ [11]$ et $-7 \equiv 4\ [11]$ donc $3u_n \equiv (-1)^{n+1} + 4\ [11]$ i.e. puisque $(-1)^{n+1} = (-1) \times (-1)^n = -(-1)^n$, $3u_n \equiv 4 - (-1)^n\ [11]$.

   b. Soit $n \in \mathbb{N}$. Si n est pair alors $3u_n \equiv 4 - 1\ [11] \equiv 3\ [11]$ et si n est impair alors $3u_n \equiv 4 + 1\ [11] \equiv 5\ [11]$. Comme 3 et 5 sont compris entre 0 et 10, on en déduit que le reste de $3u_n$ modulo 11 est soit 3 soit 5. En tout cas, ce reste n'est pas 0 donc 11 ne divise pas $3u_n$.

3. La partie entière de $\sqrt{331}$ est 18. On vérifie que 331 n'est pas divisible 2, 3, 5, 7, 11, 13 et 17 donc 331 est un nombre premier.

4. Soit $n \in \mathbb{N}$. L'écriture décimale de u_n se termine par 1 donc u_n n'est divisible ni par 2 ni par 5. De plus, la somme des chiffres de u_n est $3n+1$ qui n'est pas divisible par 3 (puisque son reste modulo 3 est 1) donc u_n n'est pas divisible par 3.

5. a. Soit $n \in \mathbb{N}$. Alors, d'après la question **2.a.**, $3u_n = 10^{n+1} - 7$. Or, $10 \equiv -1\ [11]$ et $-7 \equiv 4\ [11]$ donc $3u_n \equiv (-1)^{n+1} + 4\ [11]$ i.e. puisque $(-1)^{n+1} = (-1) \times (-1)^n = -(-1)^n$, $3u_n \equiv 4 - (-1)^n\ [11]$.

   b. Soit $n \in \mathbb{N}$. Si n est pair alors $3u_n \equiv 4 - 1\ [11] \equiv 3\ [11]$ et si n est impair alors $3u_n \equiv 4 + 1\ [11] \equiv 5\ [11]$. Comme 3 et 5 sont compris entre 0 et 10, on en déduit que le reste de $3u_n$ modulo 11 est soit 3 soit 5. En tout cas, ce reste n'est pas 0 donc 11 ne divise pas $3u_n$. Il s'ensuit que 11 ne divise pas u_n.

6. a. Comme $10^4 = 17 \times 588 + 4$ et $0 \leqslant 4 < 17$,

6. a. Comme $10^4 = 17 \times 588 + 4$ et $0 \leqslant 4 < 17$, le reste de 10^4 modulo 17 est 4.

6. a. Comme $10^4 = 17 \times 588 + 4$ et $0 \leqslant 4 < 17$, le reste de 10^4 modulo 17 est 4.
Dès lors $10^{16} =$

6. a. Comme $10^4 = 17 \times 588 + 4$ et $0 \leqslant 4 < 17$, le reste de 10^4 modulo 17 est 4.
Dès lors $10^{16} = (10^4)^4 \equiv 4^4\ [17]$

6. a. Comme $10^4 = 17 \times 588 + 4$ et $0 \leqslant 4 < 17$, le reste de 10^4 modulo 17 est 4.
Dès lors $10^{16} = (10^4)^4 \equiv 4^4\ [17] \equiv 256\ [17]$.

6. a. Comme $10^4 = 17 \times 588 + 4$ et $0 \leqslant 4 < 17$, le reste de 10^4 modulo 17 est 4.
Dès lors $10^{16} = (10^4)^4 \equiv 4^4\ [17] \equiv 256\ [17]$. Or,
$256 = 17 \times 15 + 1$

6. a. Comme $10^4 = 17 \times 588 + 4$ et $0 \leqslant 4 < 17$, le reste de 10^4 modulo 17 est 4.
Dès lors $10^{16} = (10^4)^4 \equiv 4^4\ [17] \equiv 256\ [17]$. Or,
$256 = 17 \times 15 + 1$ donc $256 \equiv 1\ [17]$

6. a. Comme $10^4 = 17 \times 588 + 4$ et $0 \leqslant 4 < 17$, le reste de 10^4 modulo 17 est 4.
Dès lors $10^{16} = (10^4)^4 \equiv 4^4\ [17] \equiv 256\ [17]$. Or,
$256 = 17 \times 15 + 1$ donc $256 \equiv 1\ [17]$ et donc $10^{16} \equiv 1\ [17]$.

6. a. Comme $10^4 = 17 \times 588 + 4$ et $0 \leqslant 4 < 17$, le reste de 10^4 modulo 17 est 4.
   Dès lors $10^{16} = (10^4)^4 \equiv 4^4\ [17] \equiv 256\ [17]$. Or,
   $256 = 17 \times 15 + 1$ donc $256 \equiv 1\ [17]$ et donc $10^{16} \equiv 1\ [17]$.
   b. Soit $k \in \mathbb{N}$.

6. a. Comme $10^4 = 17 \times 588 + 4$ et $0 \leqslant 4 < 17$, le reste de 10^4 modulo 17 est 4.
   Dès lors $10^{16} = (10^4)^4 \equiv 4^4\ [17] \equiv 256\ [17]$. Or,
   $256 = 17 \times 15 + 1$ donc $256 \equiv 1\ [17]$ et donc $10^{16} \equiv 1\ [17]$.
   b. Soit $k \in \mathbb{N}$. Alors,

$$3u_{16k+8} =$$

6. a. Comme $10^4 = 17 \times 588 + 4$ et $0 \leqslant 4 < 17$, le reste de 10^4 modulo 17 est 4.
   Dès lors $10^{16} = (10^4)^4 \equiv 4^4\ [17] \equiv 256\ [17]$. Or,
   $256 = 17 \times 15 + 1$ donc $256 \equiv 1\ [17]$ et donc $10^{16} \equiv 1\ [17]$.
   b. Soit $k \in \mathbb{N}$. Alors,

$$3u_{16k+8} = 10^{(16k+8)+1} - 7 =$$

6. a. Comme $10^4 = 17 \times 588 + 4$ et $0 \leqslant 4 < 17$, le reste de 10^4 modulo 17 est 4.
   Dès lors $10^{16} = (10^4)^4 \equiv 4^4\ [17] \equiv 256\ [17]$. Or,
   $256 = 17 \times 15 + 1$ donc $256 \equiv 1\ [17]$ et donc $10^{16} \equiv 1\ [17]$.
   b. Soit $k \in \mathbb{N}$. Alors,

$$3u_{16k+8} = 10^{(16k+8)+1} - 7 = 10^{16k+9} - 7$$

6. a. Comme $10^4 = 17 \times 588 + 4$ et $0 \leqslant 4 < 17$, le reste de 10^4 modulo 17 est 4.
   Dès lors $10^{16} = (10^4)^4 \equiv 4^4\ [17] \equiv 256\ [17]$. Or,
   $256 = 17 \times 15 + 1$ donc $256 \equiv 1\ [17]$ et donc $10^{16} \equiv 1\ [17]$.
   b. Soit $k \in \mathbb{N}$. Alors,

$$\begin{aligned} 3u_{16k+8} &= 10^{(16k+8)+1} - 7 = 10^{16k+9} - 7 \\ &= (10^{16})^k \times 10^9 - 7 \end{aligned}$$

6. a. Comme $10^4 = 17 \times 588 + 4$ et $0 \leqslant 4 < 17$, le reste de 10^4 modulo 17 est 4.
   Dès lors $10^{16} = (10^4)^4 \equiv 4^4\ [17] \equiv 256\ [17]$. Or,
   $256 = 17 \times 15 + 1$ donc $256 \equiv 1\ [17]$ et donc $10^{16} \equiv 1\ [17]$.
   b. Soit $k \in \mathbb{N}$. Alors,

$$\begin{aligned} 3u_{16k+8} &= 10^{(16k+8)+1} - 7 = 10^{16k+9} - 7 \\ &= (10^{16})^k \times 10^9 - 7 \equiv 1^k \times 10^9 - 7\ [17] \end{aligned}$$

6. a. Comme $10^4 = 17 \times 588 + 4$ et $0 \leqslant 4 < 17$, le reste de 10^4 modulo 17 est 4.
   Dès lors $10^{16} = (10^4)^4 \equiv 4^4\ [17] \equiv 256\ [17]$. Or,
   $256 = 17 \times 15 + 1$ donc $256 \equiv 1\ [17]$ et donc $10^{16} \equiv 1\ [17]$.
   b. Soit $k \in \mathbb{N}$. Alors,

$$\begin{aligned} 3u_{16k+8} &= 10^{(16k+8)+1} - 7 = 10^{16k+9} - 7 \\ &= (10^{16})^k \times 10^9 - 7 \equiv 1^k \times 10^9 - 7\ [17] \\ &\equiv 10^9 - 7\ [17] \end{aligned}$$

6. a. Comme $10^4 = 17 \times 588 + 4$ et $0 \leqslant 4 < 17$, le reste de 10^4 modulo 17 est 4.
Dès lors $10^{16} = (10^4)^4 \equiv 4^4\ [17] \equiv 256\ [17]$. Or,
$256 = 17 \times 15 + 1$ donc $256 \equiv 1\ [17]$ et donc $10^{16} \equiv 1\ [17]$.

b. Soit $k \in \mathbb{N}$. Alors,

$$\begin{aligned} 3u_{16k+8} &= 10^{(16k+8)+1} - 7 = 10^{16k+9} - 7 \\ &= (10^{16})^k \times 10^9 - 7 \equiv 1^k \times 10^9 - 7\ [17] \\ &\equiv 10^9 - 7\ [17] \end{aligned}$$

Or,
$10^9 = 10^{2\times 4+1} =$

6. a. Comme $10^4 = 17 \times 588 + 4$ et $0 \leqslant 4 < 17$, le reste de 10^4 modulo 17 est 4.
Dès lors $10^{16} = (10^4)^4 \equiv 4^4\ [17] \equiv 256\ [17]$. Or,
$256 = 17 \times 15 + 1$ donc $256 \equiv 1\ [17]$ et donc $10^{16} \equiv 1\ [17]$.

b. Soit $k \in \mathbb{N}$. Alors,

$$\begin{aligned} 3u_{16k+8} &= 10^{(16k+8)+1} - 7 = 10^{16k+9} - 7 \\ &= (10^{16})^k \times 10^9 - 7 \equiv 1^k \times 10^9 - 7\ [17] \\ &\equiv 10^9 - 7\ [17] \end{aligned}$$

Or,
$10^9 = 10^{2\times 4+1} = (10^4)^2 \times 10 =$

6. a. Comme $10^4 = 17 \times 588 + 4$ et $0 \leqslant 4 < 17$, le reste de 10^4 modulo 17 est 4.
Dès lors $10^{16} = (10^4)^4 \equiv 4^4\ [17] \equiv 256\ [17]$. Or,
$256 = 17 \times 15 + 1$ donc $256 \equiv 1\ [17]$ et donc $10^{16} \equiv 1\ [17]$.

b. Soit $k \in \mathbb{N}$. Alors,

$$\begin{aligned} 3u_{16k+8} &= 10^{(16k+8)+1} - 7 = 10^{16k+9} - 7 \\ &= (10^{16})^k \times 10^9 - 7 \equiv 1^k \times 10^9 - 7\ [17] \\ &\equiv 10^9 - 7\ [17] \end{aligned}$$

Or,
$10^9 = 10^{2\times 4+1} = (10^4)^2 \times 10 = 4^2 \times 10\ [17]$

6. a. Comme $10^4 = 17 \times 588 + 4$ et $0 \leqslant 4 < 17$, le reste de 10^4 modulo 17 est 4.
Dès lors $10^{16} = (10^4)^4 \equiv 4^4\ [17] \equiv 256\ [17]$. Or,
$256 = 17 \times 15 + 1$ donc $256 \equiv 1\ [17]$ et donc $10^{16} \equiv 1\ [17]$.

b. Soit $k \in \mathbb{N}$. Alors,

$$\begin{aligned} 3u_{16k+8} &= 10^{(16k+8)+1} - 7 = 10^{16k+9} - 7 \\ &= (10^{16})^k \times 10^9 - 7 \equiv 1^k \times 10^9 - 7\ [17] \\ &\equiv 10^9 - 7\ [17] \end{aligned}$$

Or,
$10^9 = 10^{2\times 4+1} = (10^4)^2 \times 10 = 4^2 \times 10\ [17] \equiv 160\ [17]$

6. a. Comme $10^4 = 17 \times 588 + 4$ et $0 \leqslant 4 < 17$, le reste de 10^4 modulo 17 est 4.
Dès lors $10^{16} = (10^4)^4 \equiv 4^4\ [17] \equiv 256\ [17]$. Or,
$256 = 17 \times 15 + 1$ donc $256 \equiv 1\ [17]$ et donc $10^{16} \equiv 1\ [17]$.

b. Soit $k \in \mathbb{N}$. Alors,

$$\begin{aligned} 3u_{16k+8} &= 10^{(16k+8)+1} - 7 = 10^{16k+9} - 7 \\ &= (10^{16})^k \times 10^9 - 7 \equiv 1^k \times 10^9 - 7\ [17] \\ &\equiv 10^9 - 7\ [17] \end{aligned}$$

Or,
$10^9 = 10^{2\times 4+1} = (10^4)^2 \times 10 = 4^2 \times 10\ [17] \equiv 160\ [17] \equiv 7\ [17]$
donc $3u_{16k+8} \equiv$

6. a. Comme $10^4 = 17 \times 588 + 4$ et $0 \leqslant 4 < 17$, le reste de 10^4 modulo 17 est 4.
Dès lors $10^{16} = (10^4)^4 \equiv 4^4\ [17] \equiv 256\ [17]$. Or,
$256 = 17 \times 15 + 1$ donc $256 \equiv 1\ [17]$ et donc $10^{16} \equiv 1\ [17]$.

b. Soit $k \in \mathbb{N}$. Alors,

$$\begin{aligned} 3u_{16k+8} &= 10^{(16k+8)+1} - 7 = 10^{16k+9} - 7 \\ &= (10^{16})^k \times 10^9 - 7 \equiv 1^k \times 10^9 - 7\ [17] \\ &\equiv 10^9 - 7\ [17] \end{aligned}$$

Or,
$10^9 = 10^{2\times 4+1} = (10^4)^2 \times 10 = 4^2 \times 10\ [17] \equiv 160\ [17] \equiv 7\ [17]$
donc $3u_{16k+8} \equiv 7 - 7\ [17]$

6. a. Comme $10^4 = 17 \times 588 + 4$ et $0 \leqslant 4 < 17$, le reste de 10^4 modulo 17 est 4.
Dès lors $10^{16} = (10^4)^4 \equiv 4^4\ [17] \equiv 256\ [17]$. Or,
$256 = 17 \times 15 + 1$ donc $256 \equiv 1\ [17]$ et donc $10^{16} \equiv 1\ [17]$.

b. Soit $k \in \mathbb{N}$. Alors,

$$\begin{aligned} 3u_{16k+8} &= 10^{(16k+8)+1} - 7 = 10^{16k+9} - 7 \\ &= (10^{16})^k \times 10^9 - 7 \equiv 1^k \times 10^9 - 7\ [17] \\ &\equiv 10^9 - 7\ [17] \end{aligned}$$

Or,
$10^9 = 10^{2\times 4+1} = (10^4)^2 \times 10 = 4^2 \times 10\ [17] \equiv 160\ [17] \equiv 7\ [17]$
donc $3u_{16k+8} \equiv 7 - 7\ [17] \equiv 0\ [17]$.

6. a. Comme $10^4 = 17 \times 588 + 4$ et $0 \leqslant 4 < 17$, le reste de 10^4 modulo 17 est 4.
Dès lors $10^{16} = (10^4)^4 \equiv 4^4\ [17] \equiv 256\ [17]$. Or,
$256 = 17 \times 15 + 1$ donc $256 \equiv 1\ [17]$ et donc $10^{16} \equiv 1\ [17]$.

b. Soit $k \in \mathbb{N}$. Alors,

$$\begin{aligned} 3u_{16k+8} &= 10^{(16k+8)+1} - 7 = 10^{16k+9} - 7 \\ &= (10^{16})^k \times 10^9 - 7 \equiv 1^k \times 10^9 - 7\ [17] \\ &\equiv 10^9 - 7\ [17] \end{aligned}$$

Or,
$10^9 = 10^{2\times 4+1} = (10^4)^2 \times 10 = 4^2 \times 10\ [17] \equiv 160\ [17] \equiv 7\ [17]$
donc $3u_{16k+8} \equiv 7 - 7\ [17] \equiv 0\ [17]$. Ainsi, 17 divise $3u_n$

6. a. Comme $10^4 = 17 \times 588 + 4$ et $0 \leqslant 4 < 17$, le reste de 10^4 modulo 17 est 4.
Dès lors $10^{16} = (10^4)^4 \equiv 4^4\ [17] \equiv 256\ [17]$. Or,
$256 = 17 \times 15 + 1$ donc $256 \equiv 1\ [17]$ et donc $10^{16} \equiv 1\ [17]$.

b. Soit $k \in \mathbb{N}$. Alors,

$$\begin{aligned} 3u_{16k+8} &= 10^{(16k+8)+1} - 7 = 10^{16k+9} - 7 \\ &= (10^{16})^k \times 10^9 - 7 \equiv 1^k \times 10^9 - 7\ [17] \\ &\equiv 10^9 - 7\ [17] \end{aligned}$$

Or,
$10^9 = 10^{2\times 4+1} = (10^4)^2 \times 10 = 4^2 \times 10\ [17] \equiv 160\ [17] \equiv 7\ [17]$
donc $3u_{16k+8} \equiv 7 - 7\ [17] \equiv 0\ [17]$. Ainsi, 17 divise $3u_n$ donc, comme 17 est premier,

6. a. Comme $10^4 = 17 \times 588 + 4$ et $0 \leqslant 4 < 17$, le reste de 10^4 modulo 17 est 4.
Dès lors $10^{16} = (10^4)^4 \equiv 4^4\ [17] \equiv 256\ [17]$. Or,
$256 = 17 \times 15 + 1$ donc $256 \equiv 1\ [17]$ et donc $10^{16} \equiv 1\ [17]$.

b. Soit $k \in \mathbb{N}$. Alors,

$$\begin{aligned} 3u_{16k+8} &= 10^{(16k+8)+1} - 7 = 10^{16k+9} - 7 \\ &= (10^{16})^k \times 10^9 - 7 \equiv 1^k \times 10^9 - 7\ [17] \\ &\equiv 10^9 - 7\ [17] \end{aligned}$$

Or,
$10^9 = 10^{2\times 4+1} = (10^4)^2 \times 10 = 4^2 \times 10\ [17] \equiv 160\ [17] \equiv 7\ [17]$
donc $3u_{16k+8} \equiv 7 - 7\ [17] \equiv 0\ [17]$. Ainsi, 17 divise $3u_n$ donc, comme 17 est premier, par le lemme d'Euclide, 17 divise 3 ou divise u_{16k+8}.

6. a. Comme $10^4 = 17 \times 588 + 4$ et $0 \leqslant 4 < 17$, le reste de 10^4 modulo 17 est 4.
Dès lors $10^{16} = (10^4)^4 \equiv 4^4\ [17] \equiv 256\ [17]$. Or,
$256 = 17 \times 15 + 1$ donc $256 \equiv 1\ [17]$ et donc $10^{16} \equiv 1\ [17]$.

b. Soit $k \in \mathbb{N}$. Alors,

$$\begin{aligned} 3u_{16k+8} &= 10^{(16k+8)+1} - 7 = 10^{16k+9} - 7 \\ &= (10^{16})^k \times 10^9 - 7 \equiv 1^k \times 10^9 - 7\ [17] \\ &\equiv 10^9 - 7\ [17] \end{aligned}$$

Or,
$10^9 = 10^{2\times 4+1} = (10^4)^2 \times 10 = 4^2 \times 10\ [17] \equiv 160\ [17] \equiv 7\ [17]$
donc $3u_{16k+8} \equiv 7 - 7\ [17] \equiv 0\ [17]$. Ainsi, 17 divise $3u_n$ donc, comme 17 est premier, par le lemme d'Euclide, 17 divise 3 ou divise u_{16k+8}. De plus, $0 < 3 < 17$ donc 17 ne divise par 3

6. a. Comme $10^4 = 17 \times 588 + 4$ et $0 \leqslant 4 < 17$, le reste de 10^4 modulo 17 est 4.
Dès lors $10^{16} = (10^4)^4 \equiv 4^4\ [17] \equiv 256\ [17]$. Or,
$256 = 17 \times 15 + 1$ donc $256 \equiv 1\ [17]$ et donc $10^{16} \equiv 1\ [17]$.

b. Soit $k \in \mathbb{N}$. Alors,

$$\begin{aligned} 3u_{16k+8} &= 10^{(16k+8)+1} - 7 = 10^{16k+9} - 7 \\ &= (10^{16})^k \times 10^9 - 7 \equiv 1^k \times 10^9 - 7\ [17] \\ &\equiv 10^9 - 7\ [17] \end{aligned}$$

Or,
$10^9 = 10^{2\times 4+1} = (10^4)^2 \times 10 = 4^2 \times 10\ [17] \equiv 160\ [17] \equiv 7\ [17]$
donc $3u_{16k+8} \equiv 7 - 7\ [17] \equiv 0\ [17]$. Ainsi, 17 divise $3u_n$ donc, comme 17 est premier, par le lemme d'Euclide, 17 divise 3 ou divise u_{16k+8}. De plus, $0 < 3 < 17$ donc 17 ne divise par 3 et ainsi 17 divise u_{16k+8}.

6. a. Comme $10^4 = 17 \times 588 + 4$ et $0 \leqslant 4 < 17$, le reste de 10^4 modulo 17 est 4.
Dès lors $10^{16} = (10^4)^4 \equiv 4^4\ [17] \equiv 256\ [17]$. Or,
$256 = 17 \times 15 + 1$ donc $256 \equiv 1\ [17]$ et donc $10^{16} \equiv 1\ [17]$.

b. Soit $k \in \mathbb{N}$. Alors,

$$\begin{aligned} 3u_{16k+8} &= 10^{(16k+8)+1} - 7 = 10^{16k+9} - 7 \\ &= (10^{16})^k \times 10^9 - 7 \equiv 1^k \times 10^9 - 7\ [17] \\ &\equiv 10^9 - 7\ [17] \end{aligned}$$

Or,
$10^9 = 10^{2\times 4+1} = (10^4)^2 \times 10 = 4^2 \times 10\ [17] \equiv 160\ [17] \equiv 7\ [17]$
donc $3u_{16k+8} \equiv 7 - 7\ [17] \equiv 0\ [17]$. Ainsi, 17 divise $3u_n$ donc, comme 17 est premier, par le lemme d'Euclide, 17 divise 3 ou divise u_{16k+8}. De plus, $0 < 3 < 17$ donc 17 ne divise par 3 et ainsi 17 divise u_{16k+8}.
On a donc bien montré que, pour tout $k \in \mathbb{N}$, 17 divise u_{16k+8}.