Arithmétique dans $\mathbb{Z}$

Chapitre 11

I Divisibilité et division euclidienne

1 Diviseurs, multiples

Définition 1

Soient $a, b \in \mathbb{Z}$. On dit que b *divise* a ou que a est un *multiple* de b si :

On note :

1 Diviseurs, multiples

Définition 1

Soient $a, b \in \mathbb{Z}$. On dit que b *divise* a ou que a est un *multiple* de b si : il existe $k \in \mathbb{Z}$ tel que $a = kb$.
On note :

1 Diviseurs, multiples

Définition 1

Soient $a, b \in \mathbb{Z}$. On dit que b *divise* a ou que a est un *multiple* de b si : il existe $k \in \mathbb{Z}$ tel que $a = kb$.
On note : $b \mid a$.

1 Diviseurs, multiples

Définition 1

Soient $a, b \in \mathbb{Z}$. On dit que b *divise* a ou que a est un *multiple* de b si : il existe $k \in \mathbb{Z}$ tel que $a = kb$.
On note : $b \mid a$.

Exemple 1

a) Donner l'ensemble des diviseurs de 8

b) Donner l'ensemble des diviseurs de 0

1 Diviseurs, multiples

Définition 1

Soient $a, b \in \mathbb{Z}$. On dit que b *divise* a ou que a est un *multiple* de b si : il existe $k \in \mathbb{Z}$ tel que $a = kb$.
On note : $b \mid a$.

Exemple 2

Soient $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. Montrer que $a - b$ divise $a^n - b^n$.

1 Diviseurs, multiples

Définition 1

Soient $a, b \in \mathbb{Z}$. On dit que b *divise* a ou que a est un *multiple* de b si : il existe $k \in \mathbb{Z}$ tel que $a = kb$.
On note : $b \mid a$.

Exemple 3 : Entiers associés

Montrer que si : $a \mid b$ et $b \mid a$, alors : $a = \pm b$

1 Diviseurs, multiples

Théorème 1 : Combinaisons linéaires.

Soient $a, b, d \in \mathbb{Z}$. Si $d \mid a$ et $d \mid b$, alors d divise toute combinaison linéaire de a et b :

1 Diviseurs, multiples

Théorème 1 : Combinaisons linéaires.

Soient $a, b, d \in \mathbb{Z}$. Si $d \mid a$ et $d \mid b$, alors d divise toute combinaison linéaire de a et b : $d \mid au + bv$ pour tous $u, v \in \mathbb{Z}$.

Exercice 1

Démontrer ce résultat.

2 Congruences

Définition 2

Soient $n \in \mathbb{N}$ et $a, b \in \mathbb{Z}$.

On dit que *a est congru à b modulo n* si :

2 Congruences

On note
$a \equiv b \ [n]$

Définition 2

Soient $n \in \mathbb{N}$ et $a, b \in \mathbb{Z}$.

On dit que a *est congru à* b *modulo* n si : $n \mid a - b$

2 Congruences

On note $a \equiv b \ [n]$

Définition 2

Soient $n \in \mathbb{N}$ et $a, b \in \mathbb{Z}$.

On dit que a *est congru à* b *modulo* n si : $n \mid a - b$

Rappel

La congruence modulo n est :

2 Congruences

On note $a \equiv b \ [n]$

Définition 2

Soient $n \in \mathbb{N}$ et $a, b \in \mathbb{Z}$.

On dit que a *est congru à* b *modulo* n si : $n \mid a - b$

Rappel

La congruence modulo n est : une relation d'équivalence sur $\mathbb{Z}$.

On note $a \equiv b \ [n]$

Définition 2

Soient $n \in \mathbb{N}$ et $a, b \in \mathbb{Z}$.

On dit que a *est congru à* b *modulo* n si : $n \mid a - b$

Rappel

La congruence modulo n est : une relation d'équivalence sur $\mathbb{Z}$.

Exemple 4 : Modulo 5

a) $7 \equiv \quad [5]$ b) $13 \equiv \quad [5]$ c) $4 \equiv \quad [5]$ d) $20 \equiv \quad [5]$

2 Congruences

On note $a \equiv b \ [n]$

Définition 2

Soient $n \in \mathbb{N}$ et $a, b \in \mathbb{Z}$.

On dit que a *est congru à* b *modulo* n si : $n \mid a - b$

Rappel

La congruence modulo n est : une relation d'équivalence sur $\mathbb{Z}$.

Exemple 4 : Modulo 5

a) $7 \equiv 2 \ [5]$ b) $13 \equiv \quad [5]$ c) $4 \equiv \quad [5]$ d) $20 \equiv \quad [5]$

On note $a \equiv b \ [n]$

Définition 2

Soient $n \in \mathbb{N}$ et $a, b \in \mathbb{Z}$.

On dit que a *est congru à* b *modulo* n si : $n \mid a - b$

Rappel

La congruence modulo n est : une relation d'équivalence sur $\mathbb{Z}$.

Exemple 4 : Modulo 5

a) $7 \equiv 2 \ [5]$ b) $13 \equiv 3 \ [5]$ c) $4 \equiv \quad [5]$ d) $20 \equiv \quad [5]$

2 Congruences

On note $a \equiv b \ [n]$

Définition 2

Soient $n \in \mathbb{N}$ et $a, b \in \mathbb{Z}$.

On dit que a *est congru à* b *modulo* n si : $n \mid a - b$

Rappel

La congruence modulo n est : une relation d'équivalence sur $\mathbb{Z}$.

Exemple 4 : Modulo 5

a) $7 \equiv 2 \ [5]$ b) $13 \equiv 3 \ [5]$ c) $4 \equiv -1 \ [5]$ d) $20 \equiv \quad [5]$

2 Congruences

On note $a \equiv b \ [n]$

Définition 2

Soient $n \in \mathbb{N}$ et $a, b \in \mathbb{Z}$.

On dit que a *est congru à* b *modulo* n si : $n \mid a - b$

Rappel

La congruence modulo n est : une relation d'équivalence sur $\mathbb{Z}$.

Exemple 4 : Modulo 5

a) $7 \equiv 2 \ [5]$ b) $13 \equiv 3 \ [5]$ c) $4 \equiv -1 \ [5]$ d) $20 \equiv 0 \ [5]$

Théorème 2 : Compatibilité avec les opérations

Soient $a, a', b, b' \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. Si $a \equiv b \ [n]$ et $a' \equiv b' \ [n]$ alors :

-
-
-

Théorème 2 : Compatibilité avec les opérations

Soient $a, a', b, b' \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. Si $a \equiv b \ [n]$ et $a' \equiv b' \ [n]$ alors :

- $a + a' \equiv b + b' \ [n]$
-
-

Théorème 2 : Compatibilité avec les opérations

Soient $a, a', b, b' \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. Si $a \equiv b \ [n]$ et $a' \equiv b' \ [n]$ alors :

- $a + a' \equiv b + b' \ [n]$
- $aa' \equiv bb' \ [n]$
-

Théorème 2 : Compatibilité avec les opérations

Soient $a, a', b, b' \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. Si $a \equiv b \ [n]$ et $a' \equiv b' \ [n]$ alors :

- $a + a' \equiv b + b' \ [n]$
- $aa' \equiv bb' \ [n]$
- $\boxed{a^k \equiv b^k \ [n]}$ pour tout $k \in \mathbb{N}$

Théorème 2 : Compatibilité avec les opérations

Soient $a, a', b, b' \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. Si $a \equiv b \ [n]$ et $a' \equiv b' \ [n]$ alors :

- $a + a' \equiv b + b' \ [n]$
- $aa' \equiv bb' \ [n]$
- $\boxed{a^k \equiv b^k \ [n]}$ pour tout $k \in \mathbb{N}$

Exercice 2

Démontrer ce théorème

Théorème 2 : Compatibilité avec les opérations

Soient $a, a', b, b' \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. Si $a \equiv b \ [n]$ et $a' \equiv b' \ [n]$ alors :

- $a + a' \equiv b + b' \ [n]$
- $aa' \equiv bb' \ [n]$
- $\boxed{a^k \equiv b^k \ [n]}$ pour tout $k \in \mathbb{N}$

SF 1 : congruences et divisibilité

n divise a si et seulement si :

Théorème 2 : Compatibilité avec les opérations

Soient $a, a', b, b' \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. Si $a \equiv b \ [n]$ et $a' \equiv b' \ [n]$ alors :

- $a + a' \equiv b + b' \ [n]$
- $aa' \equiv bb' \ [n]$
- $\boxed{a^k \equiv b^k \ [n]}$ pour tout $k \in \mathbb{N}$

SF 1 : congruences et divisibilité

n divise a si et seulement si : $a \equiv 0 \ [n]$.

Théorème 2 : Compatibilité avec les opérations

Soient $a, a', b, b' \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. Si $a \equiv b \ [n]$ et $a' \equiv b' \ [n]$ alors :

- $a + a' \equiv b + b' \ [n]$
- $aa' \equiv bb' \ [n]$
- $\boxed{a^k \equiv b^k \ [n]}$ pour tout $k \in \mathbb{N}$

SF 1 : congruences et divisibilité

n divise a si et seulement si : $a \equiv 0 \ [n]$.

Exemple 5

Montrer que $4^{345} + 9^{434}$ est divisible par 5.

3 Division euclidienne

Théorème 3

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Il existe un unique couple (q, r) d'entiers tels que :

1. 2.

3 Division euclidienne

Théorème 3

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Il existe un unique couple (q, r) d'entiers tels que :

1. $a = b\,q\,+\,r$ 2.

3 Division euclidienne

Théorème 3

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Il existe un unique couple (q, r) d'entiers tels que :

1. $a = b\,q\,+\,r$
2. $0 \leq r < b$ (ou encore $0 \leq r \leq b-1$)

3 Division euclidienne

Théorème 3

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Il existe un unique couple (q, r) d'entiers tels que :

1. $a = b\,q + r$ 2. $0 \leq r < b$ (ou encore $0 \leq r \leq b-1$)

quotient

reste

3 Division euclidienne

Théorème 3

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Il existe un unique couple (q, r) d'entiers tels que :

1. $a = bq + r$
2. $0 \leq r < b$ (ou encore $0 \leq r \leq b - 1$)

quotient

reste

3 Division euclidienne

Théorème 3

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Il existe un unique couple (q, r) d'entiers tels que :

1. $a = bq + r$
2. $0 \leq r < b$ (ou encore $0 \leq r \leq b-1$)

quotient

reste

Exercice 3

Etablir l'existence de cet unique couple par analyse-synthèse.

3 Division euclidienne

Théorème 3

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Il existe un unique couple (q, r) d'entiers tels que :

1. $a = bq + r$
2. $0 \leq r < b$ (ou encore $0 \leq r \leq b-1$)

quotient

reste

Exercice 3

Etablir l'existence de cet unique couple par analyse-synthèse.

Exemple 6

Effectuer la division euclidienne de : a) 16 par 3 b) 65362 par 3

3 Division euclidienne

SF 2 : congruences et reste

Modulo b, l'entier a est congru à un seul élément de $[\![0\,,b-1]\!]$:

3 Division euclidienne

SF 2 : congruences et reste

Modulo b, l'entier a est congru à un seul élément de $[\![0\,,b-1]\!]$:
le reste de la division euclidienne de a par b.

3 Division euclidienne

SF 2 : congruences et reste

Modulo b, l'entier a est congru à un seul élément de $[\![0\,,b-1]\!]$:
le reste de la division euclidienne de a par b.

Exemple 7

Trouver le reste de la division euclidienne de 2^{65362} par 7 .

3 Division euclidienne

SF 2 : congruences et reste

Modulo b, l'entier a est congru à un seul élément de $[\![0\,,b-1]\!]$:
le reste de la division euclidienne de a par b.

Exemple 8

$4^{345}+9^{434}$ est-il divisible par 7 ?

Exemple 9 : Tableau de congruence

Soit $n \in \mathbb{Z}$, impair. Montrer : $n^2 \equiv 1\ [8]$.

Exemple 9 : Tableau de congruence

Soit $n \in \mathbb{Z}$, impair. Montrer : $n^2 \equiv 1\ [8]$.

Exemple 10 : Tableau de congruence (bis)

Montrer que l'équation $x^2 - 3y^2 = 17$ n'a pas de solution dans $\mathbb{Z}^2$.

II PGCD et algorithme d'Euclide

1 Définition du PGCD

Notation

Pour $a \in \mathbb{Z}$, on note $\mathscr{D}(a)$ l'ensemble des diviseurs positifs de a.
Exemple : $\mathscr{D}(4) =$ $\mathscr{D}(0) =$

1 Définition du PGCD

Notation

Pour $a \in \mathbb{Z}$, on note $\mathscr{D}(a)$ l'ensemble des diviseurs positifs de a.
Exemple : $\mathscr{D}(4) = \{1, 2, 4\}$ $\mathscr{D}(0) =$

1 Définition du PGCD

Notation

Pour $a \in \mathbb{Z}$, on note $\mathscr{D}(a)$ l'ensemble des diviseurs positifs de a.
Exemple : $\mathscr{D}(4) = \{1, 2, 4\}$ $\quad$ $\mathscr{D}(0) = \mathbb{N}$

1 Définition du PGCD

Notation

Pour $a \in \mathbb{Z}$, on note $\mathscr{D}(a)$ l'ensemble des diviseurs positifs de a.
Exemple : $\mathscr{D}(4) = \{1, 2, 4\}$ $\qquad$ $\mathscr{D}(0) = \mathbb{N}$

Définition 1

Soient $a, b \in \mathbb{Z}$ avec $(a, b) \neq (0, 0)$.
On appelle PGCD de a et b le

1 Définition du PGCD

Notation

Pour $a \in \mathbb{Z}$, on note $\mathscr{D}(a)$ l'ensemble des diviseurs positifs de a.
Exemple : $\mathscr{D}(4) = \{1, 2, 4\}$ $\qquad$ $\mathscr{D}(0) = \mathbb{N}$

Définition 1

Soient $a, b \in \mathbb{Z}$ avec $(a, b) \neq (0, 0)$.
On appelle PGCD de a et b le plus grand diviseur commun à a et b

1 Définition du PGCD

Notation

Pour $a \in \mathbb{Z}$, on note $\mathscr{D}(a)$ l'ensemble des diviseurs positifs de a.
Exemple : $\mathscr{D}(4) = \{1, 2, 4\}$ $\qquad$ $\mathscr{D}(0) = \mathbb{N}$

Définition 1

Soient $a, b \in \mathbb{Z}$ avec $(a, b) \neq (0, 0)$.
On appelle PGCD de a et b le plus grand diviseur commun à a et b
On le note : $a \wedge b$.

1 Définition du PGCD

Notation

Pour $a \in \mathbb{Z}$, on note $\mathscr{D}(a)$ l'ensemble des diviseurs positifs de a.
Exemple : $\mathscr{D}(4) = \{1, 2, 4\}$ $\qquad$ $\mathscr{D}(0) = \mathbb{N}$

Définition 1

Soient $a, b \in \mathbb{Z}$ avec $(a, b) \neq (0, 0)$.
On appelle PGCD de a et b le plus grand diviseur commun à a et b
On le note : $a \wedge b$.

Exemple 1

Calculer le PGCD de 16 et 12.

1 Définition du PGCD

Remarque

1. Si $a \in \mathbb{N}^*$: $a \wedge 0 =$
2. Par convention : $0 \wedge 0 =$

1 Définition du PGCD

Remarque

1. Si $a \in \mathbb{N}^*$: $a \wedge 0 = a$
2. Par convention : $0 \wedge 0 =$

1 Définition du PGCD

Remarque

1. Si $a \in \mathbb{N}^*$: $a \wedge 0 = a$
2. Par convention : $0 \wedge 0 = 0$

1 Définition du PGCD

Remarque

1. Si $a \in \mathbb{N}^*$: $a \wedge 0 = a$
2. Par convention : $0 \wedge 0 = 0$

Remarque

On peut toujours supposer a et b positifs car : $a \wedge b =$

1 Définition du PGCD

Remarque

1. Si $a \in \mathbb{N}^*$: $a \wedge 0 = a$
2. Par convention : $0 \wedge 0 = 0$

Remarque

On peut toujours supposer a et b positifs car : $a \wedge b = |a| \wedge |b|$

1 Définition du PGCD

Remarque

1. Si $a \in \mathbb{N}^*$: $a \wedge 0 = a$
2. Par convention : $0 \wedge 0 = 0$

Remarque

On peut toujours supposer a et b positifs car : $a \wedge b = |a| \wedge |b|$

Théorème 1

Soient $a, b \in \mathbb{Z}$. Pour tout $k \in \mathbb{Z}$:

1 Définition du PGCD

Remarque

1. Si $a \in \mathbb{N}^*$: $a \wedge 0 = a$
2. Par convention : $0 \wedge 0 = 0$

Remarque

On peut toujours supposer a et b positifs car : $a \wedge b = |a| \wedge |b|$

Théorème 1

Soient $a, b \in \mathbb{Z}$. Pour tout $k \in \mathbb{Z}$: $a \wedge b = b \wedge (a - kb)$

1 Définition du PGCD

Remarque

1. Si $a \in \mathbb{N}^*$: $a \wedge 0 = a$
2. Par convention : $0 \wedge 0 = 0$

Remarque

On peut toujours supposer a et b positifs car : $a \wedge b = |a| \wedge |b|$

Théorème 1

Soient $a, b \in \mathbb{Z}$. Pour tout $k \in \mathbb{Z}$: $a \wedge b = b \wedge (a - kb)$

Exercice 1

Etablir l'égalité pour $b \neq 0$.

Remarque

1. Si $a \in \mathbb{N}^*$: $a \wedge 0 = a$
2. Par convention : $0 \wedge 0 = 0$

Remarque

On peut toujours supposer a et b positifs car : $a \wedge b = |a| \wedge |b|$

Théorème 1

Soient $a, b \in \mathbb{Z}$. Pour tout $k \in \mathbb{Z}$: $a \wedge b = b \wedge (a - kb)$

Exemple 2

Soit $n \in \mathbb{Z}$. Montrer : $(7n - 5) \wedge (3n + 2) = (n - 9) \wedge 29$.

2 Algorithme d'Euclide pour le calcul du PGCD

Algorithme d'Euclide pour calculer $a \wedge b$

- On pose : $r_{-1} = a$ et $r_0 = b$.
- Pour $k \in \mathbb{N}$, *tant que* $r_k \neq 0$, on définit r_{k+1} comme le reste de la division euclidienne de r_{k-1} par r_k :

2 Algorithme d'Euclide pour le calcul du PGCD

Algorithme d'Euclide pour calculer $a \wedge b$

- On pose : $r_{-1} = a$ et $r_0 = b$.
- Pour $k \in \mathbb{N}$, *tant que* $r_k \neq 0$, on définit r_{k+1} comme le reste de la division euclidienne de r_{k-1} par r_k :

$$\begin{cases} r_{k-1} = q_k r_k + r_{k+1} \\ 0 \leq r_{k+1} < r_k \end{cases}$$

2 Algorithme d'Euclide pour le calcul du PGCD

Algorithme d'Euclide pour calculer $a \wedge b$

- On pose : $r_{-1} = a$ et $r_0 = b$.
- Pour $k \in \mathbb{N}$, *tant que* $r_k \neq 0$, on définit r_{k+1} comme le reste de la division euclidienne de r_{k-1} par r_k :

$$\begin{cases} r_{k-1} = q_k r_k + r_{k+1} \\ 0 \leq r_{k+1} < r_k \end{cases}$$

Théorème 2 : « pourquoi ça marche ? »

1. *L'algorithme se termine :*
2. *L'algorithme fournit le PGCD :*

2 Algorithme d'Euclide pour le calcul du PGCD

Algorithme d'Euclide pour calculer $a \wedge b$

- On pose : $r_{-1} = a$ et $r_0 = b$.
- Pour $k \in \mathbb{N}$, *tant que* $r_k \neq 0$, on définit r_{k+1} comme le reste de la division euclidienne de r_{k-1} par r_k :

$$\begin{cases} r_{k-1} = q_k r_k + r_{k+1} \\ 0 \leq r_{k+1} < r_k \end{cases}$$

Théorème 2 : « pourquoi ça marche ? »

1. *L'algorithme se termine :* il existe $n \in \mathbb{N}$ tel que $r_n > 0$ et $r_{n+1} = 0$
2. *L'algorithme fournit le PGCD :*

2 Algorithme d'Euclide pour le calcul du PGCD

Algorithme d'Euclide pour calculer $a \wedge b$

- On pose : $r_{-1} = a$ et $r_0 = b$.
- Pour $k \in \mathbb{N}$, *tant que* $r_k \neq 0$, on définit r_{k+1} comme le reste de la division euclidienne de r_{k-1} par r_k :

$$\begin{cases} r_{k-1} = q_k r_k + r_{k+1} \\ 0 \leq r_{k+1} < r_k \end{cases}$$

Théorème 2 : « pourquoi ça marche ? »

1. *L'algorithme se termine :* il existe $n \in \mathbb{N}$ tel que $r_n > 0$ et $r_{n+1} = 0$
2. *L'algorithme fournit le PGCD :* $a \wedge b = r_n$

2 Algorithme d'Euclide pour le calcul du PGCD

Algorithme d'Euclide pour calculer $a \wedge b$

- On pose : $r_{-1} = a$ et $r_0 = b$.
- Pour $k \in \mathbb{N}$, *tant que* $r_k \neq 0$, on définit r_{k+1} comme le reste de la division euclidienne de r_{k-1} par r_k :

$$\begin{cases} r_{k-1} = q_k r_k + r_{k+1} \\ 0 \leq r_{k+1} < r_k \end{cases}$$

Théorème 2 : « pourquoi ça marche ? »

1. *L'algorithme se termine :* il existe $n \in \mathbb{N}$ tel que $r_n > 0$ et $r_{n+1} = 0$
2. *L'algorithme fournit le PGCD :* $a \wedge b = r_n$

dernier reste non nul fourni par l'algorithme

2 Algorithme d'Euclide pour le calcul du PGCD

Algorithme d'Euclide pour calculer $a \wedge b$

- On pose : $r_{-1} = a$ et $r_0 = b$.
- Pour $k \in \mathbb{N}$, *tant que* $r_k \neq 0$, on définit r_{k+1} comme le reste de la division euclidienne de r_{k-1} par r_k :

$$\begin{cases} r_{k-1} = q_k r_k + r_{k+1} \\ 0 \leq r_{k+1} < r_k \end{cases}$$

Théorème 2 : « pourquoi ça marche ? »

1. *L'algorithme se termine :* il existe $n \in \mathbb{N}$ tel que $r_n > 0$ et $r_{n+1} = 0$
2. *L'algorithme fournit le PGCD :* $a \wedge b = r_n$

dernier reste non nul fourni par l'algorithme

Exercice 2

Démontrer les deux points du théorème.

2 Algorithme d'Euclide pour le calcul du PGCD

Algorithme d'Euclide pour calculer $a \wedge b$

- On pose : $r_{-1} = a$ et $r_0 = b$.
- Pour $k \in \mathbb{N}$, *tant que* $r_k \neq 0$, on définit r_{k+1} comme le reste de la division euclidienne de r_{k-1} par r_k :

$$\begin{cases} r_{k-1} = q_k r_k + r_{k+1} \\ 0 \leq r_{k+1} < r_k \end{cases}$$

Théorème 2 : « pourquoi ça marche ? »

1. *L'algorithme se termine :* il existe $n \in \mathbb{N}$ tel que $r_n > 0$ et $r_{n+1} = 0$
2. *L'algorithme fournit le PGCD :* $a \wedge b = r_n$

dernier reste non nul fourni par l'algorithme

Exemple 3

Calculer $1659 \wedge 504$.

3 Propriétés du PGCD

Théorème 3 : Relation de Bézout

Soient $a, b \in \mathbb{Z}$. Il existe $(u, v) \in \mathbb{Z}^2$ tel que :

3 Propriétés du PGCD

Théorème 3 : Relation de Bézout

Soient $a, b \in \mathbb{Z}$. Il existe $(u, v) \in \mathbb{Z}^2$ tel que : $au + bv = a \wedge b$

3 Propriétés du PGCD

Preuve par récurrence double sur k :
$au_k + bv_k = r_k$ pour certains $u_k, v_k \in \mathbb{Z}$

Théorème 3 : Relation de Bézout

Soient $a, b \in \mathbb{Z}$. Il existe $(u, v) \in \mathbb{Z}^2$ tel que : $au + bv = a \wedge b$

Exemple 4

Déterminer une relation de Bézout entre $a = 1659$ et $b = 504$.

3 Propriétés du PGCD

Preuve par récurrence double sur k :
$au_k + bv_k = r_k$ pour certains $u_k, v_k \in \mathbb{Z}$

Théorème 3 : Relation de Bézout

Soient $a, b \in \mathbb{Z}$. Il existe $(u, v) \in \mathbb{Z}^2$ tel que : $au + bv = a \wedge b$

Exemple 4

Déterminer une relation de Bézout entre $a = 1659$ et $b = 504$.

Exemple 5 : ☢ Attention ☢

Donner deux relation de Bézout entre les entiers $a = 4$ et $b = 6$.

3 Propriétés du PGCD

Théorème 4 : Lien avec les diviseurs communs

Soient $a, b \in \mathbb{Z}$.
Pour tout $d \in \mathbb{Z}$:

3 Propriétés du PGCD

Théorème 4 : Lien avec les diviseurs communs

Soient $a, b \in \mathbb{Z}$.
Pour tout $d \in \mathbb{Z}$: $d \mid a$ et $d \mid b$ ssi $d \mid a \wedge b$

3 Propriétés du PGCD

$a \wedge b$ est le plus grand des diviseurs de a et b

Théorème 4 : Lien avec les diviseurs communs

Soient $a, b \in \mathbb{Z}$.
Pour tout $d \in \mathbb{Z}$: $d \mid a$ et $d \mid b$ ssi $d \mid a \wedge b$

3 Propriétés du PGCD

$a \wedge b$ est le plus grand des diviseurs de a et b au sens de la relation de divisibilité

Théorème 4 : Lien avec les diviseurs communs

Soient $a, b \in \mathbb{Z}$.

Pour tout $d \in \mathbb{Z}$: $d \mid a$ et $d \mid b$ ssi $d \mid a \wedge b$

3 Propriétés du PGCD

$a \wedge b$ est le plus grand des diviseurs de a et b au sens de la relation de divisibilité

Théorème 4 : Lien avec les diviseurs communs

Soient $a, b \in \mathbb{Z}$.

Pour tout $d \in \mathbb{Z}$: $d \mid a$ et $d \mid b$ ssi $d \mid a \wedge b$

3 Propriétés du PGCD

$a \wedge b$ est le plus grand des diviseurs de a et b au sens de la relation de divisibilité

Théorème 4 : Lien avec les diviseurs communs

Soient $a, b \in \mathbb{Z}$.

Pour tout $d \in \mathbb{Z}$: $d \mid a$ et $d \mid b$ ssi $d \mid a \wedge b$

3 Propriétés du PGCD

$a \wedge b$ est le plus grand des diviseurs de a et b au sens de la relation de divisibilité

Théorème 4 : Lien avec les diviseurs communs

Soient $a, b \in \mathbb{Z}$.
Pour tout $d \in \mathbb{Z}$: $d \mid a$ et $d \mid b$ ssi $d \mid a \wedge b$

Exercice 3

Démontrer l'équivalence ci-dessus.

3 Propriétés du PGCD

$a \wedge b$ est le plus grand des diviseurs de a et b au sens de la relation de divisibilité

Théorème 4 : Lien avec les diviseurs communs

Soient $a, b \in \mathbb{Z}$.
Pour tout $d \in \mathbb{Z}$: $d \mid a$ et $d \mid b$ ssi $d \mid a \wedge b$

Théorème 5 : Factorisation

Soient $a, b \in \mathbb{Z}$. Pour tout $k \in \mathbb{N}^*$:

3 Propriétés du PGCD

$a \wedge b$ est le plus grand des diviseurs de a et b au sens de la relation de divisibilité

Théorème 4 : Lien avec les diviseurs communs

Soient $a, b \in \mathbb{Z}$.
Pour tout $d \in \mathbb{Z}$: $d \mid a$ et $d \mid b$ ssi $d \mid a \wedge b$

Théorème 5 : Factorisation

Soient $a, b \in \mathbb{Z}$. Pour tout $k \in \mathbb{N}^*$: $(ka) \wedge (kb) = k(a \wedge b)$

3 Propriétés du PGCD

$a \wedge b$ est le plus grand des diviseurs de a et b au sens de la relation de divisibilité

Théorème 4 : Lien avec les diviseurs communs

Soient $a, b \in \mathbb{Z}$.
Pour tout $d \in \mathbb{Z}$: $d \mid a$ et $d \mid b$ ssi $d \mid a \wedge b$

Théorème 5 : Factorisation

Soient $a, b \in \mathbb{Z}$. Pour tout $k \in \mathbb{N}^*$: $(ka) \wedge (kb) = k(a \wedge b)$

Exercice 4

Démontrer la relation ci-dessus.

PPCM

Définition 1

Soient $a, b \in \mathbb{Z}^*$. On appelle PPCM de a et b le :

PPCM

Définition 1

Soient $a, b \in \mathbb{Z}^*$. On appelle PPCM de a et b le : plus petit multiple strictement positif commun à a et b.

PPCM

Définition 1

Soient $a, b \in \mathbb{Z}^*$. On appelle PPCM de a et b le : plus petit multiple strictement positif commun à a et b.

On le note $a \vee b$

PPCM

Définition 1

Soient $a, b \in \mathbb{Z}^*$. On appelle PPCM de a et b le : plus petit multiple strictement positif commun à a et b.

On le note $a \vee b$

Remarque

Par convention, pour tout $a \in \mathbb{Z}$: $a \vee 0 = 0 \vee a = 0$

PPCM

Définition 1

Soient $a, b \in \mathbb{Z}^*$. On appelle PPCM de a et b le : plus petit multiple strictement positif commun à a et b.

On le note $a \vee b$

Remarque

Par convention, pour tout $a \in \mathbb{Z}$: $a \vee 0 = 0 \vee a = 0$

Théorème 1 : PPCM et multiples communs

Pour tout $m \in \mathbb{Z}$:

PPCM

Définition 1

Soient $a, b \in \mathbb{Z}^*$. On appelle PPCM de a et b le : plus petit multiple strictement positif commun à a et b.

On le note $a \vee b$

Remarque

Par convention, pour tout $a \in \mathbb{Z}$: $a \vee 0 = 0 \vee a = 0$

Théorème 1 : PPCM et multiples communs

Pour tout $m \in \mathbb{Z}$: $(a \mid m \quad \text{et} \quad b \mid m) \iff a \vee b \mid m$

PPCM

Définition 1

Soient $a, b \in \mathbb{Z}^*$. On appelle PPCM de a et b le : plus petit multiple strictement positif commun à a et b.

On le note $a \vee b$

Remarque

Par convention, pour tout $a \in \mathbb{Z}$: $a \vee 0 = 0 \vee a = 0$

Théorème 1 : PPCM et multiples communs

Pour tout $m \in \mathbb{Z}$: $(a \mid m \quad \text{et} \quad b \mid m) \iff a \vee b \mid m$

Théorème 2 : Factorisation

Pour tout $k \in \mathbb{N}$:

PPCM

Définition 1

Soient $a, b \in \mathbb{Z}^*$. On appelle PPCM de a et b le : plus petit multiple strictement positif commun à a et b.

On le note $a \vee b$

Remarque

Par convention, pour tout $a \in \mathbb{Z}$: $a \vee 0 = 0 \vee a = 0$

Théorème 1 : PPCM et multiples communs

Pour tout $m \in \mathbb{Z}$: $(a \mid m \quad \text{et} \quad b \mid m) \iff a \vee b \mid m$

Théorème 2 : Factorisation

Pour tout $k \in \mathbb{N}$: $(ka) \vee (kb) = k(a \vee b)$

PPCM

Définition 1

Soient $a, b \in \mathbb{Z}^*$. On appelle PPCM de a et b le : plus petit multiple strictement positif commun à a et b.

On le note $a \vee b$

Remarque

Par convention, pour tout $a \in \mathbb{Z}$: $a \vee 0 = 0 \vee a = 0$

Théorème 1 : PPCM et multiples communs

Pour tout $m \in \mathbb{Z}$: $(a \mid m \quad \text{et} \quad b \mid m) \iff a \vee b \mid m$

Théorème 2 : Factorisation

Pour tout $k \in \mathbb{N}$: $(ka) \vee (kb) = k(a \vee b)$

Théorème 3 : Relation PGCD-PPCM

Soient $a, b \in \mathbb{N}$:

PPCM

Définition 1

Soient $a, b \in \mathbb{Z}^*$. On appelle PPCM de a et b le : plus petit multiple strictement positif commun à a et b.

On le note $a \vee b$

Remarque

Par convention, pour tout $a \in \mathbb{Z}$: $a \vee 0 = 0 \vee a = 0$

Théorème 1 : PPCM et multiples communs

Pour tout $m \in \mathbb{Z}$: $(a \mid m \quad \text{et} \quad b \mid m) \iff a \vee b \mid m$

Théorème 2 : Factorisation

Pour tout $k \in \mathbb{N}$: $(ka) \vee (kb) = k(a \vee b)$

Théorème 3 : Relation PGCD-PPCM

Soient $a, b \in \mathbb{N}$: $(a \wedge b) \times (a \vee b) = ab$

III Entiers premiers entre eux

1 Définition

Définition 1

On dit que a et b sont premiers entre eux si :

Ou encore si :

1 Définition

Définition 1

On dit que a et b sont premiers entre eux si : $a \wedge b = 1$.
Ou encore si :

1 Définition

Définition 1

On dit que a et b sont premiers entre eux si : $a \wedge b = 1$.
Ou encore si : leur seul diviseur positif commun est 1.

1 Définition

Définition 1

On dit que a et b sont premiers entre eux si : $a \wedge b = 1$.
Ou encore si : leur seul diviseur positif commun est 1.

Exemple 1

9 et 14 sont premiers entre eux mais 9 et 12 ne le sont pas.

1 Définition

Définition 1

On dit que a et b sont premiers entre eux si : $a \wedge b = 1$.
Ou encore si : leur seul diviseur positif commun est 1.

☢ $a \wedge b = 1$ ne signifie pas : « b ne divise pas a » ☢

Exemple 1

9 et 14 sont premiers entre eux mais 9 et 12 ne le sont pas.

1 Définition

Définition 1

On dit que a et b sont premiers entre eux si : $a \wedge b = 1$.
Ou encore si : leur seul diviseur positif commun est 1.

☢ $a \wedge b = 1$ ne signifie pas : « b ne divise pas a » ☢

Exemple 1

9 et 14 sont premiers entre eux mais 9 et 12 ne le sont pas.

SF 8 : Résoudre une équation faisant intervenir $x \wedge y$ ou $x \vee y$

Si $a \wedge b = d$: $a = da'$ et $b = db'$ où $a' \wedge b' = 1$

1 Définition

Définition 1

On dit que a et b sont premiers entre eux si : $a \wedge b = 1$.
Ou encore si : leur seul diviseur positif commun est 1.

☢ $a \wedge b = 1$ ne signifie pas : « b ne divise pas a » ☢

Exemple 1

9 et 14 sont premiers entre eux mais 9 et 12 ne le sont pas.

SF 8 : Résoudre une équation faisant intervenir $x \wedge y$ ou $x \vee y$

Si $a \wedge b = d$: $a = da'$ et $b = db'$ où $a' \wedge b' = 1$

Exemple 2

Résoudre le système $\begin{cases} x \wedge y = 10 \\ x \vee y = 120 \end{cases}$ d'inconnue $(x, y) \in \mathbb{N}^2$

1 Définition

Définition 1

On dit que a et b sont premiers entre eux si : $a \wedge b = 1$.
Ou encore si : leur seul diviseur positif commun est 1.

☢ $a \wedge b = 1$ ne signifie pas : « b ne divise pas a » ☢

Exemple 1

9 et 14 sont premiers entre eux mais 9 et 12 ne le sont pas.

SF 8 : Résoudre une équation faisant intervenir $x \wedge y$ ou $x \vee y$

Si $a \wedge b = d$: $a = da'$ et $b = db'$ où $a' \wedge b' = 1$

Exemple 3

Résoudre l'équation $x \wedge y = x^2 - y^2 - 2$ d'inconnue $(x, y) \in \mathbb{N}^2$.

2 Théorème de Bézout et lemme de Gauss

Théorème 1 : Théorème de Bézout

Il y a équivalence entre :

i) a et b sont premiers entre eux

2 Théorème de Bézout et lemme de Gauss

Théorème 1 : Théorème de Bézout

Il y a équivalence entre :

i) a et b sont premiers entre eux

ii) Il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$.

2 Théorème de Bézout et lemme de Gauss

Théorème 1 : Théorème de Bézout

Il y a équivalence entre :

i) a et b sont premiers entre eux

ii) Il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$.

Exercice 1

Démontrer cette équivalence

Théorème 2 : Lemme de Gauss

Théorème 2 : Lemme de Gauss

Si : $a \mid bc$ et $a \wedge b = 1$ alors : $a \mid c$.

Théorème 2 : Lemme de Gauss

Si : $a \mid bc$ et $a \wedge b = 1$ alors : $a \mid c$.

☢ Attention ☢

Si $a \wedge b \neq 1$: $a \mid bc$ $\not\Longrightarrow$ $a \mid b$ ou $a \mid c$.

Par exemple :

Théorème 2 : Lemme de Gauss

Si : $a \mid bc$ et $a \wedge b = 1$ alors : $a \mid c$.

☢ Attention ☢

Si $a \wedge b \neq 1$: $a \mid bc$ $\not\Longrightarrow$ $a \mid b$ ou $a \mid c$.

Par exemple : $a = 6$, $b = 4$ et $c = 9$.

2 Théorème de Bézout et lemme de Gauss

Théorème 2 : Lemme de Gauss

Si : $a \mid bc$ et $a \wedge b = 1$ alors : $a \mid c$.

☢ Attention ☢

Si $a \wedge b \neq 1$: $a \mid bc \not\Longrightarrow a \mid b$ ou $a \mid c$.

Par exemple : $a = 6$, $b = 4$ et $c = 9$.

Exercice 2

Démontrer le lemme de Gauss à l'aide du théorème de Bézout.

Théorème 2 : Lemme de Gauss

Si : $a \mid bc$ et $a \wedge b = 1$ alors : $a \mid c$.

SF 7 : Résoudre dans $\mathbb{Z}^2$ l'équation diophantienne $ax + by = c$

Exemple 4

Trouver tous les $(x, y) \in \mathbb{Z}^2$ tels que $7x + 12y = 3$.

3 Conséquences classiques

Théorème 3 : Entier premier avec un produit

3 Conséquences classiques

Théorème 3 : Entier premier avec un produit

Si : $a \wedge b = 1$ et $a \wedge c = 1$ alors : $a \wedge bc = 1$.

Théorème 3 : Entier premier avec un produit

Si : $a \wedge b = 1$ et $a \wedge c = 1$ alors : $a \wedge bc = 1$.

Extensions

- Si : $a \wedge b_1 = 1, \ldots, a \wedge b_n = 1$ alors : $a \wedge (b_1 \ldots b_n) = 1$

Théorème 3 : Entier premier avec un produit

Si : $a \wedge b = 1$ et $a \wedge c = 1$ alors : $a \wedge bc = 1$.

Extensions

- Si : $a \wedge b_1 = 1, \ldots, a \wedge b_n = 1$ alors : $a \wedge (b_1 \ldots b_n) = 1$
- Si $a \wedge b = 1$ alors pour tous $m, n \in \mathbb{N}$: $a^n \wedge b^m = 1$

Théorème 3 : Entier premier avec un produit

Si : $a \wedge b = 1$ et $a \wedge c = 1$ alors : $a \wedge bc = 1$.

Extensions

- Si : $a \wedge b_1 = 1, \ldots, a \wedge b_n = 1$ alors : $a \wedge (b_1 \ldots b_n) = 1$
- Si $a \wedge b = 1$ alors pour tous $m, n \in \mathbb{N}$: $a^n \wedge b^m = 1$

Exercice 3 : Ex. 86.1, banque INP

Démontrer le théorème à l'aide du théorème de Bézout.

3 Conséquences classiques

Théorème 4 : Divisibilité par deux entiers premiers entre eux

Théorème 4 : Divisibilité par deux entiers premiers entre eux

Si : $a \mid c$, $b \mid c$ et $a \wedge b = 1$ alors : $ab \mid c$.

Se généralise au produit de n entiers premiers entre eux deux à deux

Théorème 4 : Divisibilité par deux entiers premiers entre eux

Si : $a \mid c$, $b \mid c$ et $a \wedge b = 1$ alors : $ab \mid c$.

Se généralise au produit de n entiers premiers entre eux deux à deux

Théorème 4 : Divisibilité par deux entiers premiers entre eux

Si : $a \mid c$, $b \mid c$ et $a \wedge b = 1$ alors : $ab \mid c$.

☢ Attention ☢

Si $a \wedge b \neq 1$: $a \mid c$ et $b \mid c$ $\not\Longrightarrow$ $ab \mid c$.

Par exemple :

Théorème 4 : Divisibilité par deux entiers premiers entre eux

Si : $a \mid c$, $b \mid c$ et $a \wedge b = 1$ alors : $ab \mid c$.

☢ Attention ☢

Si $a \wedge b \neq 1$: $a \mid c$ et $b \mid c$ $\not\Longrightarrow$ $ab \mid c$.

Par exemple : $a = 6$ $b = 10$ $c = 30$

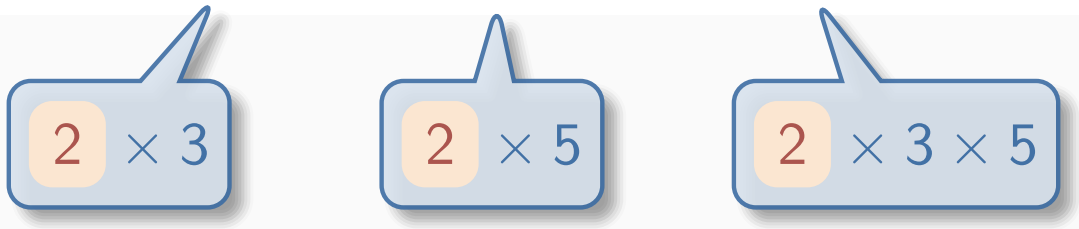
Théorème 4 : Divisibilité par deux entiers premiers entre eux

Si : $a \mid c$, $b \mid c$ et $a \wedge b = 1$ alors : $ab \mid c$.

☢ **Attention** ☢

Si $a \wedge b \neq 1$: $a \mid c$ et $b \mid c$ $\not\Longrightarrow$ $ab \mid c$.

Par exemple : $a = 6$ $b = 10$ $c = 30$



Théorème 4 : Divisibilité par deux entiers premiers entre eux

Si : $a \mid c$, $b \mid c$ et $a \wedge b = 1$ alors : $ab \mid c$.

☢ Attention ☢

Si $a \wedge b \neq 1$: $a \mid c$ et $b \mid c$ $\not\Longrightarrow$ $ab \mid c$.

Par exemple : $a = 6$ $b = 10$ $c = 30$

2×3 2×5 $2 \times 3 \times 5$

Exercice 4 : Ex. 94.2, banque INP

Démontrer ce résultat à l'aide du lemme de Gauss.

Théorème 4 : Divisibilité par deux entiers premiers entre eux

Si : $a \mid c$, $b \mid c$ et $a \wedge b = 1$ alors : $ab \mid c$.

☢ **Attention** ☢

Si $a \wedge b \neq 1$: $a \mid c$ et $b \mid c$ $\not\Longrightarrow$ $ab \mid c$.

Par exemple : $a = 6$ $b = 10$ $c = 30$

Exercice 5 : Forme irréductible d'un rationnel

Soit $r \in \mathbb{Q}$. Montrer qu'il existe un unique couple $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ pour lequel : $r = \dfrac{p}{q}$ et $p \wedge q = 1$

IV Nombres premiers

Définition 1

Soit $p \in \mathbb{N}$. On dit que p est un nombre premier si :

▸ Go to prop

Définition 1

Soit $p \in \mathbb{N}$. On dit que p est un nombre premier si : $p \geq 2$ et si ses seuls diviseurs positifs sont 1 et p.

▸ Go to prop

Définition 1

Soit $p \in \mathbb{N}$. On dit que p est un nombre premier si : $p \geq 2$ et si ses seuls diviseurs positifs sont 1 et p

diviseurs triviaux de p

▸ Go to prop

$1 \notin \mathbb{P}$

Définition 1

Soit $p \in \mathbb{N}$. On dit que p est un nombre premier si : $p \geq 2$ et si ses seuls diviseurs positifs sont 1 et p

diviseurs triviaux de p

▸ Go to prop

Ensemble noté $\mathbb{P}$

$1 \notin \mathbb{P}$

Définition 1

Soit $p \in \mathbb{N}$. On dit que p est un nombre premier si : $p \geq 2$ et si ses seuls diviseurs positifs sont 1 et p

diviseurs triviaux de p

▸ Go to prop

Ensemble noté $\mathbb{P}$

$1 \notin \mathbb{P}$

Définition 1

Soit $p \in \mathbb{N}$. On dit que p est un nombre premier si : $p \geq 2$ et si ses seuls diviseurs positifs sont 1 et p

diviseurs triviaux de p

Remarque

$n \geq 2$ n'est pas premier s'il peut s'écrire :

▸ Go to prop

Ensemble noté $\mathbb{P}$

$1 \notin \mathbb{P}$

Définition 1

Soit $p \in \mathbb{N}$. On dit que p est un nombre premier si : $p \geq 2$ et si ses seuls diviseurs positifs sont 1 et p

diviseurs triviaux de p

Remarque

$n \geq 2$ n'est pas premier s'il peut s'écrire : $n = dq$ où $2 \leq d \leq n-1$

▸ Go to prop

Ensemble noté $\mathbb{P}$

$1 \notin \mathbb{P}$

Définition 1

Soit $p \in \mathbb{N}$. On dit que p est un nombre premier si : $p \geq 2$ et si ses seuls diviseurs positifs sont 1 et p

diviseurs triviaux de p

Remarque

$n \geq 2$ n'est pas premier s'il peut s'écrire : $n = dq$ où $2 \leq d \leq n-1$

diviseur non trivial de n

▸ Go to prop

Ensemble noté $\mathbb{P}$

$1 \notin \mathbb{P}$

Définition 1

Soit $p \in \mathbb{N}$. On dit que p est un nombre premier si : $p \geq 2$ et si ses seuls diviseurs positifs sont 1 et p

diviseurs triviaux de p

Remarque

$n \geq 2$ n'est pas premier s'il peut s'écrire : $n = dq$ où $2 \leq d \leq n-1$

n est composé

diviseur non trivial de n

▸ Go to prop

Ensemble noté $\mathbb{P}$

$1 \notin \mathbb{P}$

Définition 1

Soit $p \in \mathbb{N}$. On dit que p est un nombre premier si : $p \geq 2$ et si ses seuls diviseurs positifs sont 1 et p

diviseurs triviaux de p

Remarque

$n \geq 2$ n'est pas premier s'il peut s'écrire : $n = dq$ où $2 \leq d \leq n-1$

n est composé

diviseur non trivial de n

Exemple 1 : Lemme d'Euclide

Soient $a, b \in \mathbb{Z}$ et $p \in \mathbb{P}$.
On suppose que $p \mid ab$. Montrer que : $p \mid a$ ou $p \mid b$.

▸ Go to prop

Ensemble noté $\mathbb{P}$

$1 \notin \mathbb{P}$

Définition 1

Soit $p \in \mathbb{N}$. On dit que p est un nombre premier si : $p \geq 2$ et si ses seuls diviseurs positifs sont 1 et p

diviseurs triviaux de p

Remarque

$n \geq 2$ n'est pas premier s'il peut s'écrire : $n = dq$ où $2 \leq d \leq n-1$

n est composé

diviseur non trivial de n

Exemple 2 : Nombres de Mersenne

Soit $n \in \mathbb{N}$, on pose : $M_n = 2^n - 1$.
Montrer que si M_n est premier, alors n est premier.

▸ Go to prop

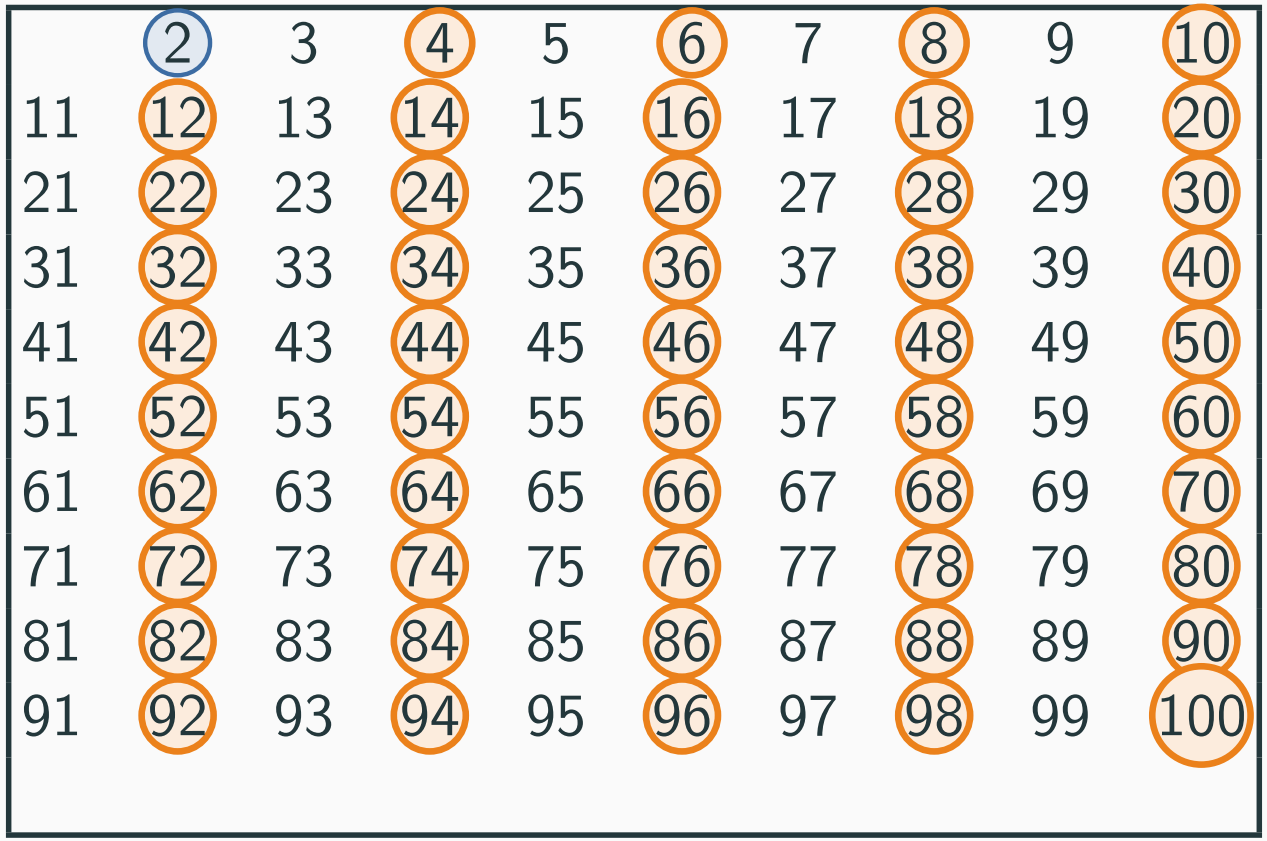
Crible d'Eratosthène

- 2 est premier

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Crible d'Eratosthène

- 2 est premier
- on raye ses multiples



	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

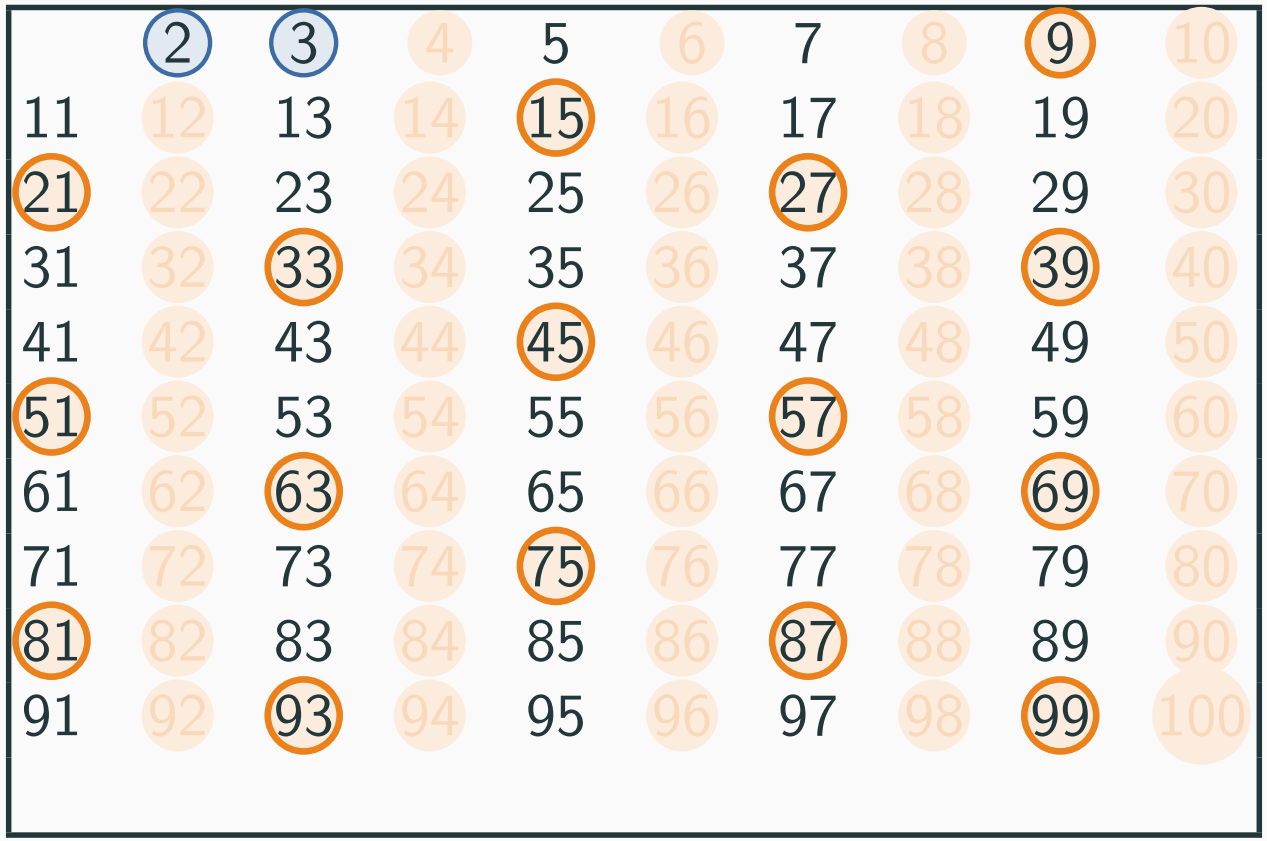
Crible d'Eratosthène

- 2 est premier
- on raye ses multiples
- 3 est premier

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Crible d'Eratosthène

- 2 est premier
- on raye ses multiples
- 3 est premier
- on raye ses multiples



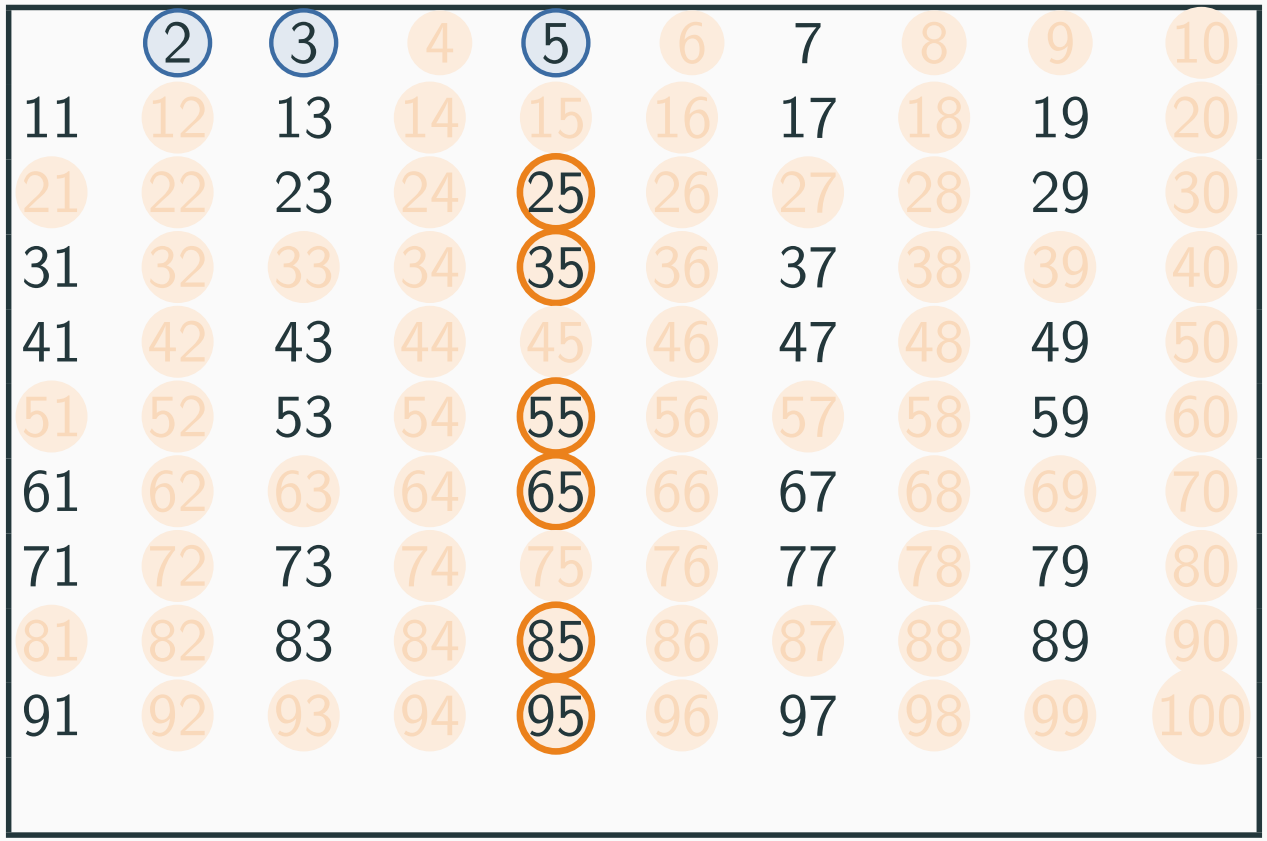
Crible d'Eratosthène

- 2 est premier
- on raye ses multiples
- 3 est premier
- on raye ses multiples
- 5 est premier

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Crible d'Eratosthène

- 2 est premier
- on raye ses multiples
- 3 est premier
- on raye ses multiples
- 5 est premier
- on raye ses multiples



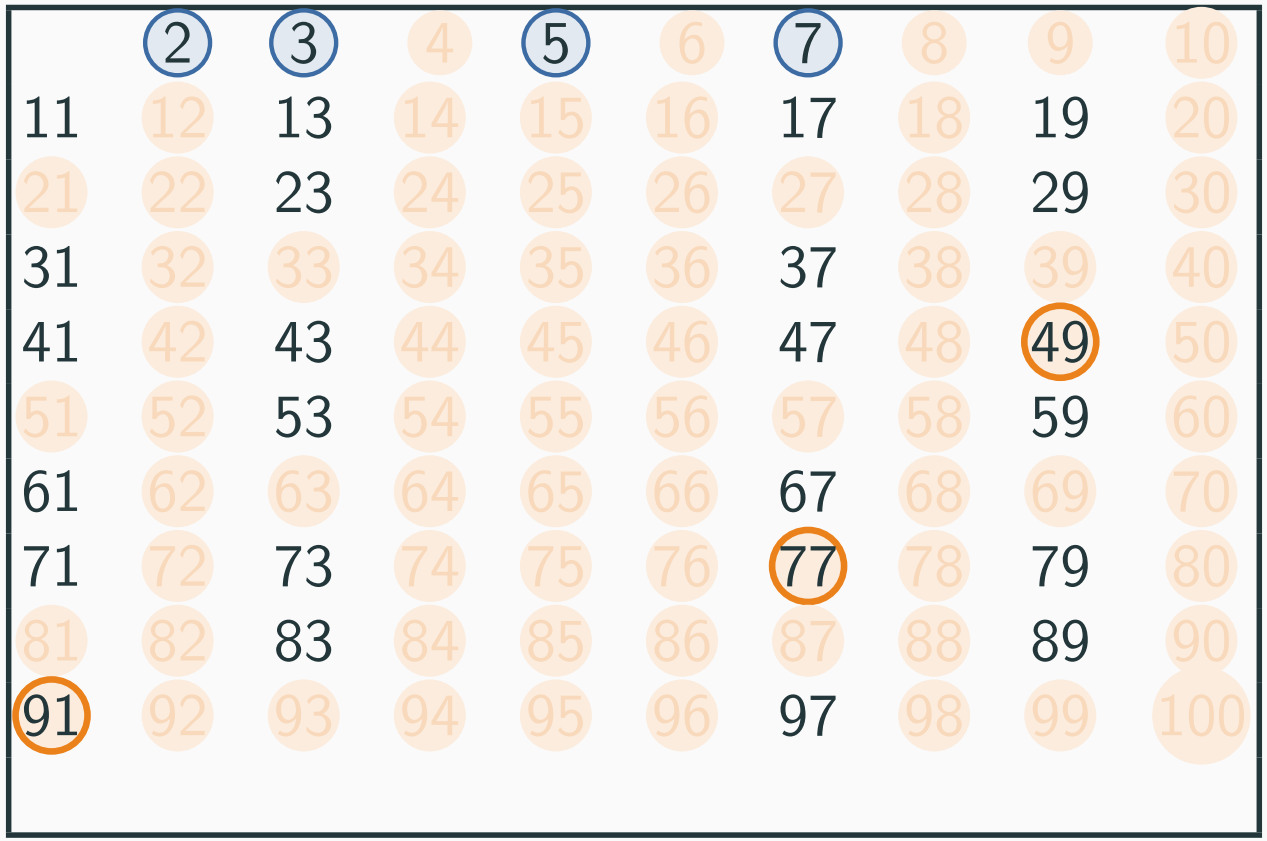
Crible d'Eratosthène

- 2 est premier
- on raye ses multiples
- 3 est premier
- on raye ses multiples
- 5 est premier
- on raye ses multiples
- 7 est premier

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

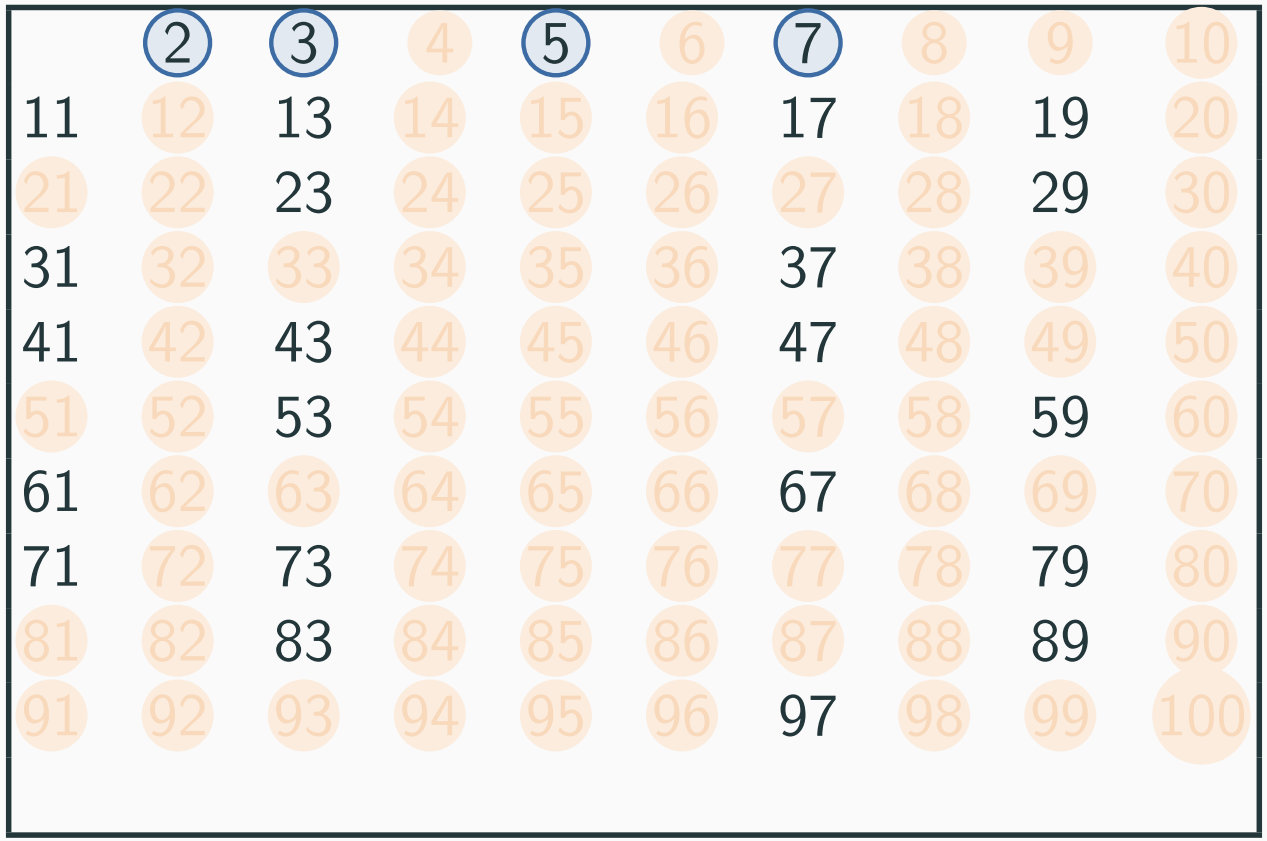
Crible d'Eratosthène

- 2 est premier
- on raye ses multiples
- 3 est premier
- on raye ses multiples
- 5 est premier
- on raye ses multiples
- 7 est premier
- on raye ses multiples



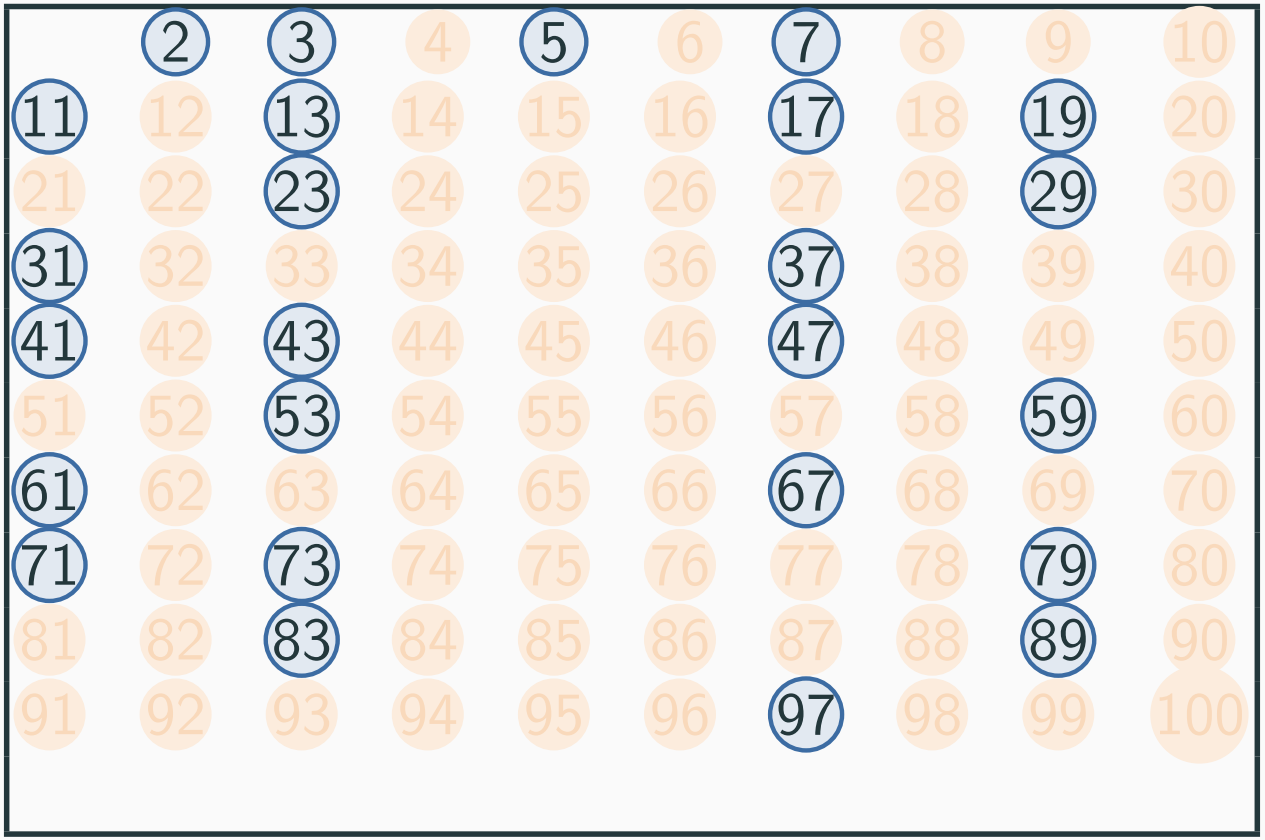
Crible d'Eratosthène

- 2 est premier
- on raye ses multiples
- 3 est premier
- on raye ses multiples
- 5 est premier
- on raye ses multiples
- 7 est premier
- on raye ses multiples
- les autres ?



Crible d'Eratosthène

- 2 est premier
- on raye ses multiples
- 3 est premier
- on raye ses multiples
- 5 est premier
- on raye ses multiples
- 7 est premier
- on raye ses multiples
- tous sont premiers



Si $m \geq 2$ n'est pas premier, il possède un diviseur premier $p \leq \sqrt{m}$

Théorème 1

Tout entier $n \geq 2$ possède au moins :

Théorème 1

Tout entier $n \geq 2$ possède au moins : un diviseur premier.

Théorème 1

Tout entier $n \geq 2$ possède au moins : un diviseur premier.

Exercice 1

Démontrer ce théorème par récurrence forte sur n.

Théorème 1

Tout entier $n \geq 2$ possède au moins : un diviseur premier.

Théorème 2

L'ensemble $\mathbb{P}$ des nombres premiers est :

Théorème 1

Tout entier $n \geq 2$ possède au moins : un diviseur premier.

Théorème 2

L'ensemble $\mathbb{P}$ des nombres premiers est : infini.

Théorème 1

Tout entier $n \geq 2$ possède au moins : un diviseur premier.

Théorème 2

L'ensemble $\mathbb{P}$ des nombres premiers est : infini.

Exercice 2

Démontrer ce théorème par l'absurde.

Exercice 3 : Ex. 86.2a), banque INP

Soit $p \in \mathbb{P}$. Montrer que pour tout $k \in [\![1\,, p-1]\!]$, p divise $\binom{p}{k}$.

Exercice 3 : Ex. 86.2a), banque INP

Soit $p \in \mathbb{P}$. Montrer que pour tout $k \in [\![1\,, p-1]\!]$, p divise $\binom{p}{k}$.

Théorème 3 : Petit théorème de Fermat

Soit $n \in \mathbb{Z}$ et soit $p \in \mathbb{P}$:

1. 2.

Exercice 3 : Ex. 86.2a), banque INP

Soit $p \in \mathbb{P}$. Montrer que pour tout $k \in [\![1\,, p-1]\!]$, p divise $\binom{p}{k}$.

Théorème 3 : Petit théorème de Fermat

Soit $n \in \mathbb{Z}$ et soit $p \in \mathbb{P}$:

1. $n^p \equiv n\ [p]$
2.

Exercice 3 : Ex. 86.2a), banque INP

Soit $p \in \mathbb{P}$. Montrer que pour tout $k \in [\![1\,, p-1]\!]$, p divise $\binom{p}{k}$.

Théorème 3 : Petit théorème de Fermat

Soit $n \in \mathbb{Z}$ et soit $p \in \mathbb{P}$:

1. $n^p \equiv n\ [p]$
2. Si p ne divise pas n : $n^{p-1} \equiv 1\ [p]$

Exercice 3 : Ex. 86.2a), banque INP

Soit $p \in \mathbb{P}$. Montrer que pour tout $k \in [\![1\,, p-1]\!]$, p divise $\binom{p}{k}$.

Théorème 3 : Petit théorème de Fermat

Soit $n \in \mathbb{Z}$ et soit $p \in \mathbb{P}$:

1. $n^p \equiv n\ [p]$
2. Si p ne divise pas n : $n^{p-1} \equiv 1\ [p]$

Exercice 4 : Ex. 86.2b) et 2c), banque INP

Démontrer ce théorème pour $n \in \mathbb{N}$.

3 Valuation p-adique

notée $v_p(a)$

Définition 2

Soient $a \in \mathbb{Z}^*$ et $p \in \mathbb{P}$. La *valuation p-adique* de a est le plus grand $k \in \mathbb{N}$ tel que p^k divise a.

3 Valuation p-adique

notée $v_p(a)$

Définition 2

Soient $a \in \mathbb{Z}^*$ et $p \in \mathbb{P}$. La *valuation p-adique* de a est le plus grand $k \in \mathbb{N}$ tel que p^k divise a. Autrement dit, $v_p(a) = k$ ssi :

-

3 Valuation p-adique

notée $v_p(a)$

Définition 2

Soient $a \in \mathbb{Z}^*$ et $p \in \mathbb{P}$. La *valuation p-adique* de a est le plus grand $k \in \mathbb{N}$ tel que p^k divise a. Autrement dit, $v_p(a) = k$ ssi :

- $p^k \mid a$ et

3 Valuation p-adique

notée $v_p(a)$

Définition 2

Soient $a \in \mathbb{Z}^*$ et $p \in \mathbb{P}$. La *valuation p-adique* de a est le plus grand $k \in \mathbb{N}$ tel que p^k divise a. Autrement dit, $v_p(a) = k$ ssi :

- $p^k \mid a \quad$ et $\quad p^{k+1} \nmid a$

3 Valuation p-adique

notée $v_p(a)$

Définition 2

Soient $a \in \mathbb{Z}^*$ et $p \in \mathbb{P}$. La *valuation p-adique* de a est le plus grand $k \in \mathbb{N}$ tel que p^k divise a. Autrement dit, $v_p(a) = k$ ssi :

- $p^k \mid a$ et $p^{k+1} \nmid a$ ou encore
- $a = p^k q$ où

3 Valuation p-adique

notée $v_p(a)$

Définition 2

Soient $a \in \mathbb{Z}^*$ et $p \in \mathbb{P}$. La *valuation p-adique* de a est le plus grand $k \in \mathbb{N}$ tel que p^k divise a. Autrement dit, $v_p(a) = k$ ssi :

- $p^k \mid a$ et $p^{k+1} \nmid a$ ou encore
- $a = p^k q$ où $p \nmid q$

3 Valuation p-adique

notée $v_p(a)$

Définition 2

Soient $a \in \mathbb{Z}^*$ et $p \in \mathbb{P}$. La *valuation p-adique* de a est le plus grand $k \in \mathbb{N}$ tel que p^k divise a. Autrement dit, $v_p(a) = k$ ssi :

- $p^k \mid a$ et $p^{k+1} \nmid a$ ou encore
- $a = p^k q$ où $p \nmid q$

Exemple 3 : pour 84

- $v_2(84) =$
- $v_3(84) =$
- $v_7(84) =$
- Si $p \notin \{2, 3, 7\}$ $v_p(84) =$

3 Valuation p-adique

notée $v_p(a)$

Définition 2

Soient $a \in \mathbb{Z}^*$ et $p \in \mathbb{P}$. La *valuation p-adique* de a est le plus grand $k \in \mathbb{N}$ tel que p^k divise a. Autrement dit, $v_p(a) = k$ ssi :

- $p^k \mid a$ et $p^{k+1} \nmid a$ ou encore
- $a = p^k q$ où $p \nmid q$

Exemple 3 : pour 84

- $v_2(84) = 2$
- $v_3(84) =$
- $v_7(84) =$
- Si $p \notin \{2, 3, 7\}$ $v_p(84) =$

3 Valuation p-adique

notée $v_p(a)$

Définition 2

Soient $a \in \mathbb{Z}^*$ et $p \in \mathbb{P}$. La *valuation p-adique* de a est le plus grand $k \in \mathbb{N}$ tel que p^k divise a. Autrement dit, $v_p(a) = k$ ssi :

- $p^k \mid a$ et $p^{k+1} \nmid a$ ou encore
- $a = p^k q$ où $p \nmid q$

Exemple 3 : pour 84

- $v_2(84) = 2$
- $v_3(84) = 1$
- $v_7(84) =$
- Si $p \notin \{2, 3, 7\}$ $v_p(84) =$

3 Valuation p-adique

notée $v_p(a)$

Définition 2

Soient $a \in \mathbb{Z}^*$ et $p \in \mathbb{P}$. La *valuation p-adique* de a est le plus grand $k \in \mathbb{N}$ tel que p^k divise a. Autrement dit, $v_p(a) = k$ ssi :

- $p^k \mid a$ et $p^{k+1} \nmid a$ ou encore
- $a = p^k q$ où $p \nmid q$

$= 2^2 \times 3^1 \times 7^1$

Exemple 3 : pour 84

- $v_2(84) = 2$
- $v_3(84) = 1$
- $v_7(84) = 1$
- Si $p \notin \{2, 3, 7\}$ $v_p(84) =$

3 Valuation p-adique

notée $v_p(a)$

Définition 2

Soient $a \in \mathbb{Z}^*$ et $p \in \mathbb{P}$. La *valuation p-adique* de a est le plus grand $k \in \mathbb{N}$ tel que p^k divise a. Autrement dit, $v_p(a) = k$ ssi :

- $p^k \mid a$ et $p^{k+1} \nmid a$ ou encore
- $a = p^k q$ où $p \nmid q$

$= 2^2 \times 3^1 \times 7^1$

$v_p(a) = 0 \Leftrightarrow p \nmid a$

Exemple 3 : pour 84

- $v_2(84) = 2$
- $v_3(84) = 1$
- $v_7(84) = 1$
- Si $p \notin \{2, 3, 7\}$ $v_p(84) = 0$

3 Valuation p-adique

notée $v_p(a)$

Définition 2

Soient $a \in \mathbb{Z}^*$ et $p \in \mathbb{P}$. La *valuation p-adique* de a est le plus grand $k \in \mathbb{N}$ tel que p^k divise a. Autrement dit, $v_p(a) = k$ ssi :

- $p^k \mid a$ et $p^{k+1} \nmid a$ ou encore
- $a = p^k q$ où $p \nmid q$

$= 2^2 \times 3^1 \times 7^1$

$v_p(a) = 0 \Leftrightarrow p \nmid a$

Exemple 3 : pour 84

- $v_2(84) = 2$
- $v_3(84) = 1$
- $v_7(84) = 1$
- Si $p \notin \{2, 3, 7\}$ $v_p(84) = 0$

Exercice 5 : Additivité des valuations p-adiques

Soit $a, b \in \mathbb{Z}^*$ et $p \in \mathbb{P}$. Montrer : $v_p(ab) =$

3 Valuation p-adique

notée $v_p(a)$

Définition 2

Soient $a \in \mathbb{Z}^*$ et $p \in \mathbb{P}$. La *valuation p-adique* de a est le plus grand $k \in \mathbb{N}$ tel que p^k divise a. Autrement dit, $v_p(a) = k$ ssi :

- $p^k \mid a$ et $p^{k+1} \nmid a$ ou encore
- $a = p^k q$ où $p \nmid q$

$= 2^2 \times 3^1 \times 7^1$

$v_p(a) = 0 \Leftrightarrow p \nmid a$

Exemple 3 : pour 84

- $v_2(84) = 2$
- $v_3(84) = 1$
- $v_7(84) = 1$
- Si $p \notin \{2, 3, 7\}$ $v_p(84) = 0$

Exercice 5 : Additivité des valuations p-adiques

Soit $a, b \in \mathbb{Z}^*$ et $p \in \mathbb{P}$. Montrer : $v_p(ab) = v_p(a) + v_p(b)$

3 Valuation p-adique

notée $v_p(a)$

Définition 2

Soient $a \in \mathbb{Z}^*$ et $p \in \mathbb{P}$. La *valuation p-adique* de a est le plus grand $k \in \mathbb{N}$ tel que p^k divise a. Autrement dit, $v_p(a) = k$ ssi :

- $p^k \mid a$ et $p^{k+1} \nmid a$ ou encore
- $a = p^k q$ où $p \nmid q$

Exercice 6 : Unicité de la décomposition en facteurs premiers

Soit $a \in \mathbb{N}^*$ et $p_1, \ldots, p_n$ les diviseurs premiers de a.
On suppose que : $a = p_1^{\alpha_1} \ldots p_n^{\alpha_n}$ pour certains $\alpha_1, \ldots, \alpha_n \in \mathbb{N}$.
Montrer que pour tout $i \in [\![1, n]\!]$: $\alpha_i = v_{p_i}(a)$.

3 Valuation p-adique

notée $v_p(a)$

Définition 2

Soient $a \in \mathbb{Z}^*$ et $p \in \mathbb{P}$. La *valuation p-adique* de a est le plus grand $k \in \mathbb{N}$ tel que p^k divise a. Autrement dit, $v_p(a) = k$ ssi :

- $p^k \mid a$ et $p^{k+1} \nmid a$ ou encore
- $a = p^k q$ où $p \nmid q$

Exercice 6 : Unicité de la décomposition en facteurs premiers

Soit $a \in \mathbb{N}^*$ et $p_1, \ldots, p_n$ les diviseurs premiers de a.
On suppose que : $a = p_1^{\alpha_1} \ldots p_n^{\alpha_n}$ pour certains $\alpha_1, \ldots, \alpha_n \in \mathbb{N}$.
Montrer que pour tout $i \in [\![1, n]\!]$: $\alpha_i = v_{p_i}(a)$.

Exposant de p_i dans la D.F.P.

4 La décomposition en facteurs premiers

Théorème 4 : Décomposition en facteurs premiers

Tout entier $a \geq 2$ s'écrit de manière unique sous la forme

$$a =$$

où : ▪ ▪ ▪

4 La décomposition en facteurs premiers

Théorème 4 : Décomposition en facteurs premiers

Tout entier $a \geq 2$ s'écrit de manière unique sous la forme

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$$

où : ▪ ▪ ▪

4 La décomposition en facteurs premiers

Théorème 4 : Décomposition en facteurs premiers

Tout entier $a \geq 2$ s'écrit de manière unique sous la forme

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$$

où : ▪ $p_1, \dots p_n \in \mathbb{P}$ ▪ ▪

4 La décomposition en facteurs premiers

Théorème 4 : Décomposition en facteurs premiers

Tout entier $a \geq 2$ s'écrit de manière unique sous la forme

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$$

où : ▪ $p_1, \dots p_n \in \mathbb{P}$ ▪ $p_1 < \dots < p_n$ ▪

Théorème 4 : Décomposition en facteurs premiers

Tout entier $a \geq 2$ s'écrit de manière unique sous la forme

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$$

où : ▪ $p_1, \dots p_n \in \mathbb{P}$ ▪ $p_1 < \dots < p_n$ ▪ $\alpha_1, \dots, \alpha_n \in \mathbb{N}^*$

4 La décomposition en facteurs premiers

ou : $a = \prod_{p \in \mathbb{P}}$

Théorème 4 : Décomposition en facteurs premiers

Tout entier $a \geq 2$ s'écrit de manière unique sous la forme

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$$

où : ▪ $p_1, \dots p_n \in \mathbb{P}$ ▪ $p_1 < \dots < p_n$ ▪ $\alpha_1, \dots, \alpha_n \in \mathbb{N}^*$

4 La décomposition en facteurs premiers

ou : $a = \prod_{p \in \mathbb{P}} p^{v_p(a)}$

Théorème 4 : Décomposition en facteurs premiers

Tout entier $a \geq 2$ s'écrit de manière unique sous la forme

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$$

où : ▪ $p_1, \dots p_n \in \mathbb{P}$ ▪ $p_1 < \dots < p_n$ ▪ $\alpha_1, \dots, \alpha_n \in \mathbb{N}^*$

4 La décomposition en facteurs premiers

ou : $a = \prod_{p \in \mathbb{P}} p^{v_p(a)}$

Théorème 4 : Décomposition en facteurs premiers

Tout entier $a \geq 2$ s'écrit de manière unique sous la forme

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$$

où : ▪ $p_1, \dots p_n \in \mathbb{P}$ ▪ $p_1 < \dots < p_n$ ▪ $\alpha_1, \dots, \alpha_n \in \mathbb{N}^*$

Exemple 4

$12 =$ $120 =$ $84 =$

4 La décomposition en facteurs premiers

ou : $a = \prod_{p \in \mathbb{P}} p^{v_p(a)}$

Théorème 4 : Décomposition en facteurs premiers

Tout entier $a \geq 2$ s'écrit de manière unique sous la forme

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$$

où : ▪ $p_1, \dots p_n \in \mathbb{P}$ ▪ $p_1 < \dots < p_n$ ▪ $\alpha_1, \dots, \alpha_n \in \mathbb{N}^*$

Exemple 4

$12 = 2^2 \times 3$ $120 =$ $84 =$

4 La décomposition en facteurs premiers

ou : $a = \prod_{p \in \mathbb{P}} p^{v_p(a)}$

Théorème 4 : Décomposition en facteurs premiers

Tout entier $a \geq 2$ s'écrit de manière unique sous la forme

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$$

où : ▪ $p_1, \dots p_n \in \mathbb{P}$ ▪ $p_1 < \dots < p_n$ ▪ $\alpha_1, \dots, \alpha_n \in \mathbb{N}^*$

Exemple 4

$12 = 2^2 \times 3$ $120 = 2^3 \times 3 \times 5$ $84 =$

4 La décomposition en facteurs premiers

ou : $a = \prod_{p \in \mathbb{P}} p^{v_p(a)}$

Théorème 4 : Décomposition en facteurs premiers

Tout entier $a \geq 2$ s'écrit de manière unique sous la forme

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$$

où : ▪ $p_1, \dots p_n \in \mathbb{P}$ ▪ $p_1 < \dots < p_n$ ▪ $\alpha_1, \dots, \alpha_n \in \mathbb{N}^*$

Exemple 4

$12 = 2^2 \times 3$ $120 = 2^3 \times 3 \times 5$ $84 = 2^2 \times 3 \times 7$

4 La décomposition en facteurs premiers

Exemple 4

$12 = 2^2 \times 3$ $\qquad$ $120 = 2^3 \times 3 \times 5$ $\qquad$ $84 = 2^2 \times 3 \times 7$

Théorème 5 : Applications à la divisibilité

Soit : $\quad a = p_1^{\alpha_1} \dots p_n^{\alpha_n} \quad$ et $\quad b = p_1^{\beta_1} \dots \ p_n^{\beta_n}$

4 La décomposition en facteurs premiers

Exemple 4

$12 = 2^2 \times 3$ $\qquad$ $120 = 2^3 \times 3 \times 5$ $\qquad$ $84 = 2^2 \times 3 \times 7$

Théorème 5 : Applications à la divisibilité

Soit : $a = p_1^{\alpha_1} \dots p_n^{\alpha_n}$ et $b = p_1^{\beta_1} \dots p_n^{\beta_n}$

1. $b \mid a$ si et seulement si les valuations p_i-adiques de b sont inférieures à celles de a :

Exemple 4

$12 = 2^2 \times 3$ $\qquad$ $120 = 2^3 \times 3 \times 5$ $\qquad$ $84 = 2^2 \times 3 \times 7$

Théorème 5 : Applications à la divisibilité

Soit : $a = p_1^{\alpha_1} \dots p_n^{\alpha_n}$ et $b = p_1^{\beta_1} \dots p_n^{\beta_n}$

1. $b \mid a$ si et seulement si les valuations p_i-adiques de b sont inférieures à celles de a : $\forall i \in [\![1\,,n]\!], \quad \beta_i \leq \alpha_i$

Exemple 4

$12 = 2^2 \times 3$ $\qquad$ $120 = 2^3 \times 3 \times 5$ $\qquad$ $84 = 2^2 \times 3 \times 7$

Théorème 5 : Applications à la divisibilité

$p_1, \ldots, p_n$: facteurs de la DFP de a ou de b

Soit : $a = p_1^{\alpha_1} \ldots p_n^{\alpha_n}$ et $b = p_1^{\beta_1} \ldots p_n^{\beta_n}$

1. $b \mid a$ si et seulement si les valuations p_i-adiques de b sont inférieures à celles de a : $\forall i \in [\![1\,,n]\!], \quad \beta_i \leq \alpha_i$

Exemple 4

$12 = 2^2 \times 3$ $\qquad$ $120 = 2^3 \times 3 \times 5$ $\qquad$ $84 = 2^2 \times 3 \times 7$

Théorème 5 : Applications à la divisibilité

$p_1, \ldots, p_n$: facteurs de la DFP de a ou de b

Soit : $a = p_1^{\alpha_1} \ldots p_n^{\alpha_n}$ et $b = p_1^{\beta_1} \ldots p_n^{\beta_n}$

1. $b \mid a$ si et seulement si les valuations p_i-adiques de b sont inférieures à celles de a : $\forall i \in [\![1\,, n]\!], \quad \beta_i \leq \alpha_i$

   ou encore ssi : $\forall p \in \mathbb{P}, \quad v_p(b) \leq v_p(a)$

Exemple 4

$12 = 2^2 \times 3$ $\qquad$ $120 = 2^3 \times 3 \times 5$ $\qquad$ $84 = 2^2 \times 3 \times 7$

Théorème 5 : Applications à la divisibilité

$p_1, \ldots, p_n$: facteurs de la DFP de a ou de b

Soit : $a = p_1^{\alpha_1} \ldots p_n^{\alpha_n}$ et $b = p_1^{\beta_1} \ldots p_n^{\beta_n}$

1. $b \mid a$ si et seulement si les valuations p_i-adiques de b sont inférieures à celles de a : $\forall i \in [\![1\,,n]\!], \quad \beta_i \leq \alpha_i$

   ou encore ssi : $\forall p \in \mathbb{P}, \quad v_p(b) \leq v_p(a)$

2. - $a \wedge b =$
   - $a \vee b =$

Exemple 4

$12 = 2^2 \times 3$ $\qquad$ $120 = 2^3 \times 3 \times 5$ $\qquad$ $84 = 2^2 \times 3 \times 7$

Théorème 5 : Applications à la divisibilité

$p_1, \dots, p_n$: facteurs de la DFP de a ou de b

Soit : $a = p_1^{\alpha_1} \dots p_n^{\alpha_n}$ et $b = p_1^{\beta_1} \dots p_n^{\beta_n}$

1. $b \mid a$ si et seulement si les valuations p_i-adiques de b sont inférieures à celles de a : $\forall i \in [\![1\,,n]\!], \quad \beta_i \leq \alpha_i$

   ou encore ssi : $\forall p \in \mathbb{P}, \quad v_p(b) \leq v_p(a)$

2. - $a \wedge b = p_1^{\min(\alpha_1,\beta_1)} \times \dots \times p_n^{\min(\alpha_n,\beta_n)}$
   - $a \vee b =$

Exemple 4

$12 = 2^2 \times 3$ $\qquad$ $120 = 2^3 \times 3 \times 5$ $\qquad$ $84 = 2^2 \times 3 \times 7$

Théorème 5 : Applications à la divisibilité

$p_1, \dots, p_n$: facteurs de la DFP de a ou de b

Soit : $a = p_1^{\alpha_1} \dots p_n^{\alpha_n}$ et $b = p_1^{\beta_1} \dots p_n^{\beta_n}$

1. $b \mid a$ si et seulement si les valuations p_i-adiques de b sont inférieures à celles de a : $\forall i \in [\![1\,,n]\!], \quad \beta_i \leq \alpha_i$

   ou encore ssi : $\forall p \in \mathbb{P}, \quad v_p(b) \leq v_p(a)$

2. - $a \wedge b = p_1^{\min(\alpha_1,\beta_1)} \times \dots \times p_n^{\min(\alpha_n,\beta_n)}$
   - $a \vee b = p_1^{\max(\alpha_1,\beta_1)} \times \dots \times p_n^{\max(\alpha_n,\beta_n)}$

Théorème 5 : Applications à la divisibilité

Soit : $a = p_1^{\alpha_1} \dots p_n^{\alpha_n}$ et $b = p_1^{\beta_1} \dots p_n^{\beta_n}$

1. $b \mid a$ si et seulement si les valuations p_i-adiques de b sont inférieures à celles de a : $\forall i \in [\![1\,,n]\!], \quad \beta_i \leq \alpha_i$

   ou encore ssi : $\forall p \in \mathbb{P}, \quad v_p(b) \leq v_p(a)$

2. - $a \wedge b = p_1^{\min(\alpha_1,\beta_1)} \times \dots \times p_n^{\min(\alpha_n,\beta_n)}$
   - $a \vee b = p_1^{\max(\alpha_1,\beta_1)} \times \dots \times p_n^{\max(\alpha_n,\beta_n)}$

Exercice 7

Calculer le PGCD de $a = 84$ et $b = 120$ selon deux méthodes.

Théorème 5 : Applications à la divisibilité

Soit : $a = p_1^{\alpha_1} \dots p_n^{\alpha_n}$ et $b = p_1^{\beta_1} \dots p_n^{\beta_n}$

1. $b \mid a$ si et seulement si les valuations p_i-adiques de b sont inférieures à celles de a : $\forall i \in [\![1\,,n]\!], \quad \beta_i \leq \alpha_i$

   ou encore ssi : $\forall p \in \mathbb{P}, \quad v_p(b) \leq v_p(a)$

2. - $a \wedge b = p_1^{\min(\alpha_1,\beta_1)} \times \dots \times p_n^{\min(\alpha_n,\beta_n)}$
   - $a \vee b = p_1^{\max(\alpha_1,\beta_1)} \times \dots \times p_n^{\max(\alpha_n,\beta_n)}$

Exemple 4

Soit $a, b \in \mathbb{N}^*$. Montrer que a divise b si et seulement si a^2 divise b^2