ARITHMETIQUE

Dr. Mathias K. KOUAKOU

MAÎTRE DE CONFERENCES

Université F.H.B de Cocody Abidjan (Côte d'Ivoire)

15 janvier 2023

Un peu d'histoire des nombres

Un peu d'histoire des nombres

D'abord étaient connus les entiers 1, 2, 3,.... Ces entiers sont connus aussi dans les **langues africaines**. Puis furent créés 0 et ensuite -1, -2, -3,....grâce aux paris faits dans des jeux (courses de chevaux, combats,...), par les arabes vers le $V^{ème}$ siècle **après J-C**.

Un peu d'histoire des nombres

D'abord étaient connus les entiers 1, 2, 3,.... Ces entiers sont connus aussi dans les **langues africaines**. Puis furent créés 0 et ensuite -1, -2, -3,....grâce aux paris faits dans des jeux (courses de chevaux, combats,...), par les arabes vers le $V^{ème}$ siècle **après J-C**.

Remarque : Au départ, bien avant le $V^{ème}$-siècle, zéro comme chiffre n'était pas toujours représenté. Par exemple :

305 était écrit 3 5 pour ne pas être confondu à 35.

Les ensembles $\mathbb{N}$ et $\mathbb{Z}$

Les ensembles $\mathbb{N}$ et $\mathbb{Z}$

- $\mathbb{N} = \{0, 1, 2, 3, ...\}$
  est l'ensemble des entiers naturels.

Les ensembles $\mathbb{N}$ et $\mathbb{Z}$

- $\mathbb{N} = \{0, 1, 2, 3, ...\}$
  est l'ensemble des entiers naturels.

- $\mathbb{Z} = \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
  est l'ensemble des entiers relatifs.

Les ensembles $\mathbb{N}$ et $\mathbb{Z}$

- $\mathbb{N} = \{0, 1, 2, 3, ...\}$
  est l'ensemble des entiers naturels.

- $\mathbb{Z} = \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
  est l'ensemble des entiers relatifs.

Les ensembles $\mathbb{N}$ et $\mathbb{Z}$

- $\mathbb{N} = \{0, 1, 2, 3, ...\}$
  est l'ensemble des entiers naturels.

- $\mathbb{Z} = \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
  est l'ensemble des entiers relatifs.

Remarque

Il y a deux types d'entiers : les pairs et les impairs (en anglais : the odd numbers and the even numbers). Les nombres pairs $\ldots, -4, -2, 0, 2, \ldots$ sont de la forme : $2n$.

Diviseurs et multiples dans $\mathbb{Z}$

Diviseurs et multiples dans $\mathbb{Z}$

Définition

Soient a et b deux entiers. On dira que a divise b, s'il existe un entier k tel que $b = k \cdot a$. On note $a|b$. On dit également que a est **un diviseur** de b ou que b est **un multiple** de a.

Diviseurs et multiples dans $\mathbb{Z}$

Définition

Soient a et b deux entiers. On dira que a divise b, s'il existe un entier k tel que $b = k \cdot a$. On note $a|b$. On dit également que a est **un diviseur** de b ou que b est **un multiple** de a.

Nombres premiers

Un entier $n \geq 2$ est dit premier, si ses seuls diviseurs positifs sont 1 et lui-même n.

Diviseurs et multiples dans $\mathbb{Z}$

Définition

Soient a et b deux entiers. On dira que a divise b, s'il existe un entier k tel que $b = k \cdot a$. On note $a|b$. On dit également que a est **un diviseur** de b ou que b est **un multiple** de a.

Nombres premiers

Un entier $n \geq 2$ est dit premier, si ses seuls diviseurs positifs sont 1 et lui-même n.

Exemples de nombres premiers

2, 3, 5, 7, 11,...

Diviseurs et multiples dans $\mathbb{Z}$

Définition

Soient a et b deux entiers. On dira que a divise b, s'il existe un entier k tel que $b = k \cdot a$. On note $a|b$. On dit également que a est **un diviseur** de b ou que b est **un multiple** de a.

Nombres premiers

Un entier $n \geq 2$ est dit premier, si ses seuls diviseurs positifs sont 1 et lui-même n.

Exemples de nombres premiers

2, 3, 5, 7, 11,...

Remarque

Il y a une infinité de nombres premiers !

Propriétés

Propriétés

Soient a, b et c des entiers relatifs.

Propriétés

Soient a, b et c des entiers relatifs.

1) Si $b \neq 0$ et a divise b alors $|a| \leq |b|$. Cela montre en particulier que b n'a qu'un nombre fini de diviseurs.

Propriétés

Soient a, b et c des entiers relatifs.

1) Si $b \neq 0$ et a divise b alors $|a| \leq |b|$. Cela montre en particulier que b n'a qu'un nombre fini de diviseurs.

Propriétés

Soient a, b et c des entiers relatifs.

1) Si $b \neq 0$ et a divise b alors $|a| \leq |b|$. Cela montre en particulier que b n'a qu'un nombre fini de diviseurs.

2) Si a divise b et que b divise a, alors $|a| = |b|$.

Propriétés

Soient a, b et c des entiers relatifs.

1) Si $b \neq 0$ et a divise b alors $|a| \leq |b|$. Cela montre en particulier que b n'a qu'un nombre fini de diviseurs.

2) Si a divise b et que b divise a, alors $|a| = |b|$.

Propriétés

Soient a, b et c des entiers relatifs.

1) Si $b \neq 0$ et a divise b alors $|a| \leq |b|$. Cela montre en particulier que b n'a qu'un nombre fini de diviseurs.

2) Si a divise b et que b divise a, alors $|a| = |b|$.

3) Si a divise b et b divise c, alors a divise c.

Propriétés

Soient a, b et c des entiers relatifs.

1) Si $b \neq 0$ et a divise b alors $|a| \leq |b|$. Cela montre en particulier que b n'a qu'un nombre fini de diviseurs.

2) Si a divise b et que b divise a, alors $|a| = |b|$.

3) Si a divise b et b divise c, alors a divise c.

Propriétés

Soient a, b et c des entiers relatifs.

1) Si $b \neq 0$ et a divise b alors $|a| \leq |b|$. Cela montre en particulier que b n'a qu'un nombre fini de diviseurs.

2) Si a divise b et que b divise a, alors $|a| = |b|$.

3) Si a divise b et b divise c, alors a divise c.

4) Si a divise b et c, alors pour tous entiers n et m, a divise $nb + mc$.

PGCD

PGCD

Définition

Soient a et b deux entiers non nuls. Le plus grand entier naturel qui divive à la fois a et b est appelé **le plus grand commun diviseur** de a et b. On le note $pgcd(a, b)$.

PGCD

Définition

Soient a et b deux entiers non nuls. Le plus grand entier naturel qui divive à la fois a et b est appelé **le plus grand commun diviseur** de a et b. On le note $pgcd(a, b)$.

Remarque

Si a divise b, alors $pgcd(a, b) = a$.

PGCD

Définition

Soient a et b deux entiers non nuls. Le plus grand entier naturel qui divive à la fois a et b est appelé **le plus grand commun diviseur** de a et b. On le note $pgcd(a, b)$.

Remarque

Si a divise b, alors $pgcd(a, b) = a$.

Lemme :La division euclidienne dans $\mathbb{Z}$

Soient $b \in \mathbb{Z}$ et $a \in \mathbb{N}^*$. Il existe un unique couple $(s, r) \in \mathbb{Z} \times \mathbb{N}$ tel que

- $0 \leq r < a$
- $b = sa + r$

Sur la division euclidienne

Sur la division euclidienne

Définition

s et r sont appelés respectivement **quotient** et **reste** de la division euclidienne de b par a.

Sur la division euclidienne

Définition

s et r sont appelés respectivement **quotient** et **reste** de la division euclidienne de b par a.

Remarque

a divise b si et seulement si $r = 0$.

Algorithme d'Euclide

Naissance : Inconnue
Actif vers 300 av J.C.

Algorithme d'Euclide

Naissance : Inconnue
Actif vers 300 av J.C.

Lemme d'Euclide

Soient a et b deux entiers non nuls. S'il existent un entier non nul r et un entier k tels que $a = kb + s$, alors les diviseurs communs à a et b sont exactement les diviseurs commun à b et s. En particulier on a :

$$pgcd(a, b) = pgcd(b, s)$$

Algorithme d'Euclide

Algorithme d'Euclide

Soient a un entier non nul, b un entier naturel non nul. Comment trouver $d = pgcd(a, b)$? On pose $r_0 = b$, et on effectue les divisions euclidiennes successives suivantes **tant que le reste n'est pas nul** :

$$a = s_1 r_0 + r_1, \quad r_0 = s_2 r_1 + r_2, \quad r_1 = s_3 r_2 + r_3, \quad r_2 = s_4 r_3 + r_4, \ldots$$

$$r_{n-1} = s_{n+1} r_n + r_{n+1}, \forall n \in \mathbb{N}^*.$$

Algorithme d'Euclide

Algorithme d'Euclide

Soient a un entier non nul, b un entier naturel non nul. Comment trouver $d = pgcd(a, b)$? On pose $r_0 = b$, et on effectue les divisions euclidiennes successives suivantes **tant que le reste n'est pas nul** :

$$a = s_1 r_0 + r_1, \quad r_0 = s_2 r_1 + r_2, \quad r_1 = s_3 r_2 + r_3, \quad r_2 = s_4 r_3 + r_4, \ldots$$

$$r_{n-1} = s_{n+1} r_n + r_{n+1}, \forall n \in \mathbb{N}^*.$$

Théorème

Le $pgcd(a, b)$ est le dernier reste non nul obtenu par l'algorithme d'Euclide.

Nombres premiers entre eux

Nombres premiers entre eux

Définition

Deux entiers non nuls a et b sont dits premiers entre eux, si

$$pgcd(a, b) = 1$$

Nombres premiers entre eux

Définition

Deux entiers non nuls a et b sont dits premiers entre eux, si

$$pgcd(a, b) = 1$$

Remarque

Si $d = pgcd(a, b)$, alors $\frac{a}{d}$ et $\frac{b}{d}$ sont premiers entre eux.

PPCM de deux entiers

PPCM de deux entiers

Définition

Soient a et b deux entiers non nuls. Le plus petit entier naturel non nul qui est multiple à la fois a et b est appelé **le plus petit commun diviseur** de a et b. On le note $ppcm(a, b)$.

PPCM de deux entiers

Définition

Soient a et b deux entiers non nuls. Le plus petit entier naturel non nul qui est multiple à la fois a et b est appelé **le plus petit commun diviseur** de a et b. On le note $ppcm(a, b)$.

Propriétés Remarquables

Soient a, b deux entiers non nuls.

1. Si $c \in \mathbb{Z}$ est un multiple de a et b, alors c est un multiple de $ppcm(a, b)$.
2. On a :

$$pgcd(a, b) \cdot ppcm(a, b) = a \cdot b.$$

Théorèmes de Bézout et de Gauss

Etienne Bézout

Nationnalité : Française
Naissance : 31 mars 1730 à Nemours (Royaume de France)
Décès : 27 septembre 1783 à Avon (Royaume de France)

Johann Carl Friedrich Gauss

Nationnalité : Allemande
Naissance : 30 avril 1777 à Brunswick (Allemagne)
Décès : 23 février 1855 à Göttingen (Allemagne)

Théorèmes de Bézout et de Gauss

Théorèmes de Bézout et de Gauss

Théorème de Bézout

1. Soient $a, b \in \mathbb{Z}$ et $d = pgcd(a, b)$. Alors
$$\exists (u, v) \in \mathbb{Z}^2 \text{ tel que } au + bv = d \quad (d > 0).$$
2. a et b deux entiers sont premiers entre eux si et seulement si
$$\exists (u, v) \in \mathbb{Z}^2 \text{ tel que } au + bv = 1.$$

Théorèmes de Bézout et de Gauss

Preuve

1) On considère l'ensemble $\{am + bn, (m, n) \in \mathbb{Z}^2\}$ qu'on note $a\mathbb{Z} + b\mathbb{Z}$.
Il est clair que $a\mathbb{Z} + b\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$, donc

$$\exists c \in \mathbb{N} \text{ tel que } a\mathbb{Z} + b\mathbb{Z} = c\mathbb{Z}.$$

Par ailleurs, $a\mathbb{Z} \subset d\mathbb{Z}$ et $b\mathbb{Z} \subset d\mathbb{Z}$ donc $c\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} \subset d\mathbb{Z}$. En particulier c est un multiple de d et alors $c \geq d$.
L'égalité $a\mathbb{Z} + b\mathbb{Z} = c\mathbb{Z}$ montre que c divise à la fois a et b, donc $pgcd(a, b) = d \geq c$. Finalement, on a $c = d$.

2) $(\Rightarrow)$ est clair.

$(\Leftarrow)$ si $au + bv = 1$, alors tout diviseur de a et b divise $au + bv$, donc divise 1.

Théorèmes de Bézout et de Gauss

Remarque

On a

$$a\mathbb{Z} + b\mathbb{Z} = pgcd(a, b)\mathbb{Z} \text{ et } a\mathbb{Z} \cap b\mathbb{Z} = ppcm(a, b)\mathbb{Z}.$$

Théorèmes de Bézout et de Gauss

Remarque

On a

$$a\mathbb{Z} + b\mathbb{Z} = pgcd(a, b)\mathbb{Z} \text{ et } a\mathbb{Z} \cap b\mathbb{Z} = ppcm(a, b)\mathbb{Z}.$$

Comment trouver une relation de Bézout ?

Théorèmes de Bézout et de Gauss

Remarque

On a

$$a\mathbb{Z} + b\mathbb{Z} = pgcd(a, b)\mathbb{Z} \text{ et } a\mathbb{Z} \cap b\mathbb{Z} = ppcm(a, b)\mathbb{Z}.$$

Comment trouver une relation de Bézout ?

Pour a et b donnés, on trouve une relation de Bézout $au + bv = pgcd(a, b)$ en utilisant encore l'algorithme d'Euclide.

Théorèmes de Bézout et de Gauss

Théorème de Gauss

Soient a, b et c trois entiers non nuls.

1) Si a divise le produit bc et a est premier avec b, alors a divise c.
2) Si a et b sont premiers entre eux et chacun divise c, alors le produit ab divise c.

Nombres premiers

Nombres premiers

Définition

Un entier $n \geq 2$ est dit premier si ses seuls diviveurs positifs sont 1 et n lui même.

Nombres premiers

Définition

Un entier $n \geq 2$ est dit premier si ses seuls diviveurs positifs sont 1 et n lui même.

Théorème

Il y a une infinité de nombres premiers.

Nombres premiers

Définition

Un entier $n \geq 2$ est dit premier si ses seuls diviveurs positifs sont 1 et n lui même.

Théorème

Il y a une infinité de nombres premiers.

Preuve

Soit $\mathcal{P} = \{2, 3, 5, 7, \ldots\}$ l'ensemble des nombres premiers. Par l'absurde supposons que $\mathcal{P}$ soit fini, et p_n son plus grand élément. Alors l'entier naturel $q = 2 \cdot 3 \cdot 5 \cdot 7 \cdot \cdots \cdot p_n + 1$ n'est pas premier, et serait donc divisible par un élément de $\mathcal{P}$. Mais aucun nombre premier ne pourrait diviser q car il divise déjà le facteur produit de q, et donc diviserait 1. Cela est absurde, et donc $\mathcal{P}$ ne peut être fini.

Nombres premiers

Théorème fondamental de l'arithmétique

Tout entier $n \geq 2$ peut s'écrire de façon unique comme produit

$$n = p_1 \cdot p_2 \cdot p_3 \cdots p_r$$

où $r \in \mathbb{N}^\star$, les p_i sont des nombres premiers tels que $p_1 \leq p_2 \cdot \cdots \leq p_r$.

Nombres premiers

Théorème fondamental de l'arithmétique

Tout entier $n \geq 2$ peut s'écrire de façon unique comme produit

$$n = p_1 \cdot p_2 \cdot p_3 \cdots p_r$$

où $r \in \mathbb{N}^\star$, les p_i sont des nombres premiers tels que $p_1 \leq p_2 \cdot \cdots \leq p_r$.

Preuve

Soit $n \in \mathbb{N}^\star$ et $n \geq 2$.

Existence de la décomposition : Par récurrence sur n, on obtient facilement que soit n est lui-même premier, soit il est produit d'un nombre avec un autre entier n'. On alors $n = pn'$, et forcement $n' < n$ donc n' s'écrit comme produit de nombres premiers selons l'hypothèse de récurrence et par suite n aussi.

Nombres premiers

Preuve (Suite)

Unicité : Si pour un entier $n \geq 2$, on a

$$n = p_1 \cdot \cdot p_s = p'_1 \cdot \cdot p'_{s'} \ ,$$

grâce aux théorèmes de **Bézout** et **Gauss**, on aura

1. $s = s'$,
2. $p_i = p'_i$

Nombres premiers

Définition

Soient p un nombre premier et n un entier naturel non nul.

- Si p divise n, on dit que p est un **facteur premier** de n.
- Le plus grand entier naturel k tel que p^k divise n s'appelle **l'exposant** de p dans n.

Dans le théorème de la décomposition, en regroupant les nombres premiers identiques, on obtient :

Tout entier $n \geq 2$ peut s'écrire de façon unique comme produit

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

où $r \in \mathbb{N}^\star$, les p_i sont des nombres premiers distincts tels que $p_1 < p_2 < \cdots < p_r$.

Nombres premiers

Remarque

Si un nombre premier p n'apparaît pas dans la décomposition de n, son exposant dans n est **zéro**.

Nombres premiers

Remarque

Si un nombre premier p n'apparaît pas dans la décomposition de n, son exposant dans n est **zéro**.

Théorème

Soient a et b deux entiers naturels non nuls. Pour tout nombre premier p, on note $\alpha(p)$ et $\beta(p)$ respectivement l'exposant de p dans a et l'exposant de p dans b. On a l'équivalence suivante :

Nombres premiers

Remarque

Si un nombre premier p n'apparaît pas dans la décomposition de n, son exposant dans n est **zéro**.

Théorème

Soient a et b deux entiers naturels non nuls. Pour tout nombre premier p, on note $\alpha(p)$ et $\beta(p)$ respectivement l'exposant de p dans a et l'exposant de p dans b. On a l'équivalence suivante :

a divise b **si et seulement si** pour tout nombre premier p, $\alpha(p) \leq \beta(p)$.

Congruence modulo un entier

Définition

Soient $n \in \mathbb{N}^\star$ et $a, b \in \mathbb{Z}$. On dira que a est congru à b modulo n et on notera $a \equiv b[n]$, si $a - b \in n\mathbb{Z}$, c'est-à-dire $a - b$ est un multiple de n.

La congruence modulo n définit une relation binaire sur $\mathbb{Z}$. Cette relation est clairement une relation d'équivalence.

L'anneau quotient $\frac{\mathbb{Z}}{n\mathbb{Z}}$ où $n \geq 2$

On rappelle que l'ensemble quotient $\frac{\mathbb{Z}}{n\mathbb{Z}}$ a exactement n éléments, qui sont les n classes d'équivalence des entiers 0,1,2,..., $n-1$, modulo n. On a

$$\frac{\mathbb{Z}}{n\mathbb{Z}} = \{\overline{0}, \overline{1}, .., \overline{n-1}\}$$

$\frac{\mathbb{Z}}{n\mathbb{Z}}$ est un anneau avec les deux lois de composition internes :
l'addition $+$: $\quad \overline{a} + \overline{b} = \overline{a+b}$
la multiplication $\times$: $\quad \overline{a} \times \overline{b} = \overline{a}$.

L'anneau quotient $\frac{\mathbb{Z}}{n\mathbb{Z}}$ où $n \geq 2$

Le groupe multiplicatif de l'anneau $\frac{\mathbb{Z}}{n\mathbb{Z}}$ est

$$\mathcal{U}\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right) = \left\{\overline{x} \in \frac{\mathbb{Z}}{n\mathbb{Z}} : \ pgcd(x, n) = 1\right\}.$$

L'anneau quotient $\frac{\mathbb{Z}}{n\mathbb{Z}}$ où $n \geq 2$

Le groupe multiplicatif de l'anneau $\frac{\mathbb{Z}}{n\mathbb{Z}}$ est

$$\mathcal{U}\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right) = \left\{\overline{x} \in \frac{\mathbb{Z}}{n\mathbb{Z}} : \ pgcd(x, n) = 1\right\}.$$

Proposition

Pour un entier premier p, l'anneau $\frac{\mathbb{Z}}{p\mathbb{Z}}$ est **un corps**.

Précisement, toutes les classes non nulles sont inversibles.

Nombre d'EULER $\varphi(n)$, $n \in \mathbb{N}^*$

Définition

Pour tout entier $n \in \mathbb{N}^*$, l'entier $\varphi(n) = card\left(\mathcal{U}\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)\right)$ est appelé nombre d'Euler.

Nombre d'EULER $\varphi(n)$, $n \in \mathbb{N}^*$

Définition

Pour tout entier $n \in \mathbb{N}^*$, l'entier $\varphi(n) = card\left(\mathcal{U}\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)\right)$ est appelé nombre d'Euler.

Remarque

Rappelons que :

$$\mathcal{U}\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right) = \left\{\bar{a} \in \frac{\mathbb{Z}}{n\mathbb{Z}} : pgcd(a, n) = 1\right\}.$$

On a alors : $\varphi(1) = 1$; $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$.

Nombre d'EULER $\varphi(n)$, $n \in \mathbb{N}^*$

Propriétés

1) Si $n, m \in \mathbb{N}^*$ et $pgcd(n, m) = 1$, alors

$$\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$$

2) Pour tout entier $n \geq 2$, on a

$$n = \sum_{k/n} \varphi(k).$$

3) Pour tout nombre premier p et pour tout entier m non nul, on a :

$$\varphi(p^m) = p^m - p^{m-1}.$$

Nombre d'EULER $\varphi(n)$, $n \in \mathbb{N}^*$

Exercice

Calculer $\varphi(51000)$ et $\varphi(121)$.

Nombre d'EULER $\varphi(n)$, $n \in \mathbb{N}^*$

Théorème d'EULER

Soient deux entiers $n > 1$ et $x \geq 1$. Si x est premier avec n, alors

$$x^{\varphi(n)} \equiv 1 mod(n).$$

Nombre d'EULER $\varphi(n)$, $n \in \mathbb{N}^*$

Théorème d'EULER

Soient deux entiers $n > 1$ et $x \geq 1$. Si x est premier avec n, alors

$$x^{\varphi(n)} \equiv 1 mod(n).$$

Comme corollaire, on a le théorème suivant.

Nombre d'EULER $\varphi(n)$, $n \in \mathbb{N}^*$

Théorème d'EULER

Soient deux entiers $n > 1$ et $x \geq 1$. Si x est premier avec n, alors

$$x^{\varphi(n)} \equiv 1 mod(n).$$

Comme corollaire, on a le théorème suivant.

Corollaire (Petit théorème de FERMAT)

Soient p un nombre premier et $x \in \mathbb{Z}$. On a

1. si $x \notin p\mathbb{Z}$, alors $x^{p-1} \equiv 1 \mod (p)$.
2. pour tout $x \in \mathbb{Z}$, on a $x^p \equiv x \mod (p)$.

Systèmes de congruences

On a le théorème suivant :

Théorème des restes chinois

Si n_1, n_2,....,n_k sont des entiers positifs deux à deux premiers entre eux, alors pour tous a_1, a_2,.....,$a_k \in \mathbb{Z}$, le système suivant, appelé système de congruences,

$$\begin{cases} x & \equiv & a_1 & \mod (n_1) \\ x & \equiv & a_2 & \mod (n_2) \\ \cdot & \equiv & \cdot & \\ \cdot & \equiv & \cdot & \\ x & \equiv & a_k & \mod (n_k) \end{cases}$$

a des solutions et, si x_0 est une solution particulière, alors l'ensemble des solutions s'écrit :

$$\{x_0 + (n_1 \cdot n_2 \cdots n_k) \cdot a,\ a \in \mathbb{Z}\}.$$