Leçon 46 - Divisibilité et congruence sur $\mathbb{Z}$. PGCD et PPCM

⇒ Deux caractérisations du PGCD et factorisation

⇒ Généralisations

⇒ Deux caractérisations du PGCD et factorisation

⇒ Généralisations

$PGCD$ d'un nombre fini d'entiers relatifs

Heuristique. Définition

Au lieu de construire le $PGCD$ de k nombres en prenant :

$$\delta = \max\left(\mathscr{D}(a_1) \cap \mathscr{D}(a_2) \cdots \mathscr{D}(a_k) \cap \mathbb{N})\right)$$

on préfère prendre la caractéristique vue par la suite :

$$d|a \text{ et } d|b \Longrightarrow d|\delta$$

Dans ce cas le terme « plus grand »ne doit pas être pris pour la relation d'ordre $n \leqslant m$, mais pour la relation d'ordre $n|m$.

Définition 1

Définition par récurrence

Soient $k \in \mathbb{N}^*$, $k \geqslant 2$ et $(a_1, a_2, \ldots a_k) \in \mathbb{Z}^k$. Alors

$$\bigwedge_{i=1}^{k} a_i := \left(\bigwedge_{i=1}^{k-1} a_i\right) \wedge a_k$$

On (aur)a $\bigwedge_{i=1}^{k} a_i = \max\left(\mathscr{D}(a_1) \cap \mathscr{D}(a_2) \cdots \mathscr{D}(a_k) \cap \mathbb{N}\right)$.

Définition 1

Définition par récurrence

Soient $k \in \mathbb{N}^*$, $k \geqslant 2$ et $(a_1, a_2, \dots a_k) \in \mathbb{Z}^k$. Alors

$\bigwedge_{i=1}^{k} a_i := \left(\bigwedge_{i=1}^{k-1} a_i\right) \wedge a_k$

On (aur)a $\bigwedge_{i=1}^{k} a_i = \max\left(\mathscr{D}(a_1) \cap \mathscr{D}(a_2) \cdots \mathscr{D}(a_k) \cap \mathbb{N}\right)$.

L'identité de Bézout se généralise également :

Proposition - Décomposition de Bézout

Soient $k \in \mathbb{N}^*$, $k \geqslant 2$, et $(a_1, a_2, \dots, a_k) \in \mathbb{Z}^k$.

$$\exists (u_1, \dots, u_k) \in \mathbb{Z}^k \quad \Big| \quad \bigwedge_{i=1}^{k} a_i = \sum_{i=1}^{k} u_i a_i.$$

Définition 1

Définition par récurrence

Soient $k \in \mathbb{N}^*$, $k \geqslant 2$ et $(a_1, a_2, \ldots a_k) \in \mathbb{Z}^k$. Alors

$\bigwedge_{i=1}^{k} a_i := \left(\bigwedge_{i=1}^{k-1} a_i\right) \wedge a_k$

On (aur)a $\bigwedge_{i=1}^{k} a_i = \max\left(\mathscr{D}(a_1) \cap \mathscr{D}(a_2) \cdots \mathscr{D}(a_k) \cap \mathbb{N}\right)$.

L'identité de Bézout se généralise également :

Proposition - Décomposition de Bézout

Soient $k \in \mathbb{N}^*$, $k \geqslant 2$, et $(a_1, a_2, \ldots, a_k) \in \mathbb{Z}^k$.

$$\exists (u_1, \ldots, u_k) \in \mathbb{Z}^k \quad | \quad \bigwedge_{i=1}^{k} a_i = \sum_{i=1}^{k} u_i a_i.$$

Démonstration

Caractérisation par les diviseurs<

Proposition - Proposition avec l'ensemble des diviseurs

Pour tout $j \in \mathbb{N}_k$, $\bigwedge_{i=1}^k a_i$ est un diviseur de a_j.
Mieux : $\bigwedge_{i=1}^k a_i = \max\left(\mathscr{D}(a_1) \cap \mathscr{D}(a_2) \cdots \mathscr{D}(a_k) \cap \mathbb{N}\right)$ au sens de la relation d'ordre | ou $\leqslant$.

On a $\mathscr{D}(\bigwedge_{i=1}^k a_i) = \bigcap_{j=1}^{k} \mathscr{D}(a_j)$.

Caractérisation par les diviseurs<

Proposition - Proposition avec l'ensemble des diviseurs

Pour tout $j \in \mathbb{N}_k$, $\bigwedge_{i=1}^k a_i$ est un diviseur de a_j.
Mieux : $\bigwedge_{i=1}^k a_i = \max\left(\mathscr{D}(a_1) \cap \mathscr{D}(a_2) \cdots \mathscr{D}(a_k) \cap \mathbb{N}\right)$ au sens de la relation d'ordre | ou $\leqslant$.

On a $\mathscr{D}(\bigwedge_{i=1}^k a_i) = \bigcap_{j=1}^{k} \mathscr{D}(a_j)$.

Démonstration

⇒ Deux caractérisations du PGCD et factorisation

⇒ Généralisations

$PGCD$ d'un nombre fini d'entiers relatifs

Proposition - Critère caractéristique du $PGCD(a_1, a_2, \ldots a_k)$

Soient $k \in \mathbb{N}^*$, $k \geqslant 2$, et $(a_1, a_2, \ldots, a_k) \in \mathbb{Z}^k$.
$\bigwedge_{i=1}^{k} a_i$ est l'unique entier naturel d dont les diviseurs sont exactement les diviseurs communs à tous les a_i, c'est-à-dire tel que

$$\forall n \in \mathbb{Z}, \qquad (\forall i \in [\![1, k]\!], n | a_i) \Longleftrightarrow n | d.$$

$PGCD$ d'un nombre fini d'entiers relatifs

Proposition - Critère caractéristique du $PGCD(a_1, a_2, \dots a_k)$

Soient $k \in \mathbb{N}^*$, $k \geqslant 2$, et $(a_1, a_2, \dots, a_k) \in \mathbb{Z}^k$.
$\bigwedge_{i=1}^{k} a_i$ est l'unique entier naturel d dont les diviseurs sont exactement les diviseurs communs à tous les a_i, c'est-à-dire tel que

$$\forall n \in \mathbb{Z}, \qquad (\forall i \in [\![1, k]\!], n | a_i) \Longleftrightarrow n | d.$$

Démonstration

$PGCD$ d'un nombre fini d'entiers relatifs

Proposition - Critère caractéristique du $PGCD(a_1, a_2, \ldots a_k)$

Soient $k \in \mathbb{N}^*$, $k \geqslant 2$, et $(a_1, a_2, \ldots, a_k) \in \mathbb{Z}^k$.
$\bigwedge_{i=1}^{k} a_i$ est l'unique entier naturel d dont les diviseurs sont exactement les diviseurs communs à tous les a_i, c'est-à-dire tel que

$$\forall n \in \mathbb{Z}, \qquad (\forall i \in [\![1, k]\!], n | a_i) \Longleftrightarrow n | d.$$

Démonstration

Savoir-faire. Démonter/utiliser le PGCD de $(a_1, a_2, \ldots a_k)$

Tout diviseur du PGCD, divise chaque a_i.
Toute diviseur de tous les a_i est un diviseur de leur PGCD.
Et le PGCD est le plus grand de tous les diviseurs au sens de la relation d'ordre de la division (c'est une borne inférieure).

Factorisation

Proposition - Linéarité absolue

Soit $x \in \mathbb{Z}$. Le PGCD de $(a_1 x, a_2 x, \dots a_k x)$ est $|x| \times \wedge_{i=1}^{k} a_i$.

Factorisation

Proposition - Linéarité absolue

Soit $x \in \mathbb{Z}$. Le PGCD de $(a_1 x, a_2 x, \ldots a_k x)$ est $|x| \times \wedge_{i=1}^{k} a_i$.

Démonstration

Combinaison linéaire

Proposition - Sous-groupe $a_1\mathbb{Z} + a_2\mathbb{Z} + \cdots + a_k\mathbb{Z}$

Soient $a_1, a_2, \ldots a_k \in \mathbb{N}$.
Alors $a_1\mathbb{Z} + a_2\mathbb{Z} + \cdots + a_k\mathbb{Z}$ est exactement le sous-groupe de $(\mathbb{Z}, +)$: $\left(\bigwedge_{i=1}^k a_i\right)\mathbb{Z}$.
Autrement écrit, le groupe engendré par $\{a_1, a_2, \ldots a_k\}$ est le groupe $\left(\bigwedge_{i=1}^k a_i\right)\mathbb{Z}$.

$$< a_1, a_2, \ldots a_k >_{\mathbb{Z}} = \left(\bigwedge_{i=1}^k a_i\right) \cdot \mathbb{Z}$$

Combinaison linéaire

Proposition - Sous-groupe $a_1\mathbb{Z} + a_2\mathbb{Z} + \cdots + a_k\mathbb{Z}$

Soient $a_1, a_2, \dots a_k \in \mathbb{N}$.
Alors $a_1\mathbb{Z} + a_2\mathbb{Z} + \cdots + a_k\mathbb{Z}$ est exactement le sous-groupe de $(\mathbb{Z}, +)$: $\left(\bigwedge_{i=1}^k a_i\right)\mathbb{Z}$.
Autrement écrit, le groupe engendré par $\{a_1, a_2, \dots a_k\}$ est le groupe $\left(\bigwedge_{i=1}^k a_i\right)\mathbb{Z}$.

$$< a_1, a_2, \dots a_k >_{\mathbb{Z}} = \left(\bigwedge_{i=1}^k a_i\right) \cdot \mathbb{Z}$$

Démonstration

⇒ Deux caractérisations du PGCD et factorisation

⇒ Généralisations

Entiers premiers entre eux dans leur ensemble

Définition - Entiers premiers entre eux dans leur ensemble

Les entiers $a_1, \dots, a_k$ sont dits *premiers entre eux dans leur ensemble* si leur PGCD vaut 1.

Entiers premiers entre eux dans leur ensemble

Définition - Entiers premiers entre eux dans leur ensemble

Les entiers $a_1, \ldots, a_k$ sont dits *premiers entre eux dans leur ensemble* si leur PGCD vaut 1.

Attention. Ne pas confondre « premiers entre eux dans leur ensemble »et « premiers deux à deux »

Il ne faut pas confondre « premiers entre eux dans leur ensemble » et « premiers deux à deux ».
Par exemple $a =$, $b =$ et $c =$
sont
mais ne sont pas .

Entiers premiers entre eux dans leur ensemble

Définition - Entiers premiers entre eux dans leur ensemble

Les entiers $a_1,\ldots,a_k$ sont dits *premiers entre eux dans leur ensemble* si leur PGCD vaut 1.

Attention. Ne pas confondre « premiers entre eux dans leur ensemble »et « premiers deux à deux »

Il ne faut pas confondre « premiers entre eux dans leur ensemble » et « premiers deux à deux ».
Par exemple $a=6$, $b=15$ et $c=10$
sont
mais ne sont pas .

Entiers premiers entre eux dans leur ensemble

Définition - Entiers premiers entre eux dans leur ensemble

Les entiers $a_1, \ldots, a_k$ sont dits *premiers entre eux dans leur ensemble* si leur PGCD vaut 1.

Attention. Ne pas confondre « premiers entre eux dans leur ensemble »et « premiers deux à deux »

Il ne faut pas confondre « premiers entre eux dans leur ensemble » et « premiers deux à deux ».
Par exemple $a = 6$, $b = 15$ et $c = 10$
sont premiers entre eux dans leur ensemble
mais ne sont pas premiers entre eux 2 à 2.

Entiers premiers entre eux dans leur ensemble

Tous les savoir-faire donnés précédemment sur les PGCD se généralisent à plusieurs nombres. Nous ne les ré-écrirons pas mais il faudra savoir y penser. Voici un exemple

Entiers premiers entre eux dans leur ensemble

Tous les savoir-faire donnés précédemment sur les PGCD se généralisent à plusieurs nombres. Nous ne les ré-écrirons pas mais il faudra savoir y penser. Voici un exemple

Savoir-faire. Réduction à des entiers premiers entre eux (2)

Soient $a_1, a_2, \dots a_k \in \mathbb{Z}$. On note $\delta = \bigwedge_{i=1}^{k} a_i = 1$.
Alors pour tout $i \in [\![1, k]\!]$, $a_i = \delta a'_i$, avec $(a'_1, a'_2, \dots, a'_k)$ premiers entre eux dans leur ensemble.
Puis on travaille avec les a'_i

Identité de Bézout

Proposition - Théorème (identité) de Bézout

Soient $a_1,\ldots,a_k$ des entiers relatifs. Alors

$$\bigwedge_{i=1}^k a_i = 1 \iff \exists (u_1,\ldots,u_k) \in \mathbb{Z}^k \mid \sum_{i=1}^k u_i a_i = 1$$

Identité de Bézout

Proposition - Théorème (identité) de Bézout

Soient $a_1,\dots,a_k$ des entiers relatifs. Alors

$$\bigwedge_{i=1}^{k} a_i = 1 \Longleftrightarrow \exists (u_1,\dots,u_k) \in \mathbb{Z}^k \mid \sum_{i=1}^{k} u_i a_i = 1$$

Démonstration

Identité de Bézout

Proposition - Théorème (identité) de Bézout

Soient $a_1,\dots,a_k$ des entiers relatifs. Alors

$$\bigwedge_{i=1}^k a_i = 1 \Longleftrightarrow \exists (u_1,\dots,u_k)\in\mathbb{Z}^k \mid \sum_{i=1}^k u_i a_i = 1$$

Démonstration

Savoir-faire. Exploiter l'identité de Bézout

Pour montrer que $(a_1,\dots a_n)$ sont premiers entre eux, ils arrivent, qu'on montre :

$$\exists\ u_1,u_2,\dots u_n \in \mathbb{Z} \text{ tels que } \sum_{i=1}^n u_i a_i = 1$$

Quand, on sait que $(a_1,\dots a_n)$ sont premiers entre eux, on génère alors $u_1,u_2,\dots u_n\in\mathbb{Z}$ tels que $\sum_{i=1}^n u_i a_i = 1$ et on exploite ces (u_i).

⇒ Deux caractérisations du PGCD et factorisation

⇒ Généralisations

Construction du $PPCM$

Analyse Construction du $PPCM$

Construction du $PPCM$

Analyse Construction du $PPCM$

Définition - $PPCM$ de a et de b

Soient a et b deux entiers relatifs non nuls.
On appelle $PPCM$ (Plus Petit Commun Multiple) de a et b, le nombre

$$PPCM(a,b) = \min\left(a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^*\right)$$

On le note également $a \vee b$.
On a clairement $b \vee a = a \vee b = |a| \vee |b|$.

Caractérisations

Proposition - Caractérisation essentielle du $PPCM$

Soit $(a,b) \in \mathbb{Z}^2$. Alors $a \vee b$ est le seul entier naturel dont les multiples sont exactement les multiples communs à a et b

$$a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$$

c'est-à-dire tel que

$$\forall m \in \mathbb{Z}, (a|m \text{ et } b|m) \Longleftrightarrow a \vee b|m$$

Caractérisations

Proposition - Caractérisation essentielle du $PPCM$

Soit $(a,b) \in \mathbb{Z}^2$. Alors $a \vee b$ est le seul entier naturel dont les multiples sont exactement les multiples communs à a et b

$$a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$$

c'est-à-dire tel que

$$\forall m \in \mathbb{Z}, (a|m \text{ et } b|m) \Longleftrightarrow a \vee b|m$$

Démonstration

Caractérisations

Proposition - Caractérisation essentielle du $PPCM$

Soit $(a,b)\in\mathbb{Z}^2$. Alors $a\vee b$ est le seul entier naturel dont les multiples sont exactement les multiples communs à a et b

$$a\mathbb{Z}\cap b\mathbb{Z}=(a\vee b)\mathbb{Z}$$

c'est-à-dire tel que

$$\forall m\in\mathbb{Z}, (a|m \text{ et } b|m) \Longleftrightarrow a\vee b|m$$

Démonstration

Savoir-faire. Trouver un PPCM. Exploiter un PPCM

On note $\mu=a\vee b$.

Pour trouver le PPCM ,

on démontre que si $a|m$ et $b|m$, alors nécessairement $\mu|m$.

Puis on cherche le m le plus petit possible.

Pour exploiter le PPCM,

on exploite le fait que si $\mu|m$, alors $a|m$ et $b|m$.

Et on travaille sur cette co-divisibilité.

Linéarité

Proposition - Linéarité

Soient $a, b, \lambda \in \mathbb{Z}$ alors $\lambda a \vee \lambda b = |\lambda| \times (a \vee b)$.

Linéarité

Proposition - Linéarité

Soient $a, b, \lambda \in \mathbb{Z}$ alors $\lambda a \vee \lambda b = |\lambda| \times (a \vee b)$.

Démonstration

⇒ Deux caractérisations du PGCD et factorisation

⇒ Généralisations

Relation $PPCM$ et $PGCD$

Proposition - Relation $PPCM$ et $PGCD$

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

- si $a \wedge b = 1$ alors $|ab| = (a \vee b)$.
- dans le cas général, $|ab| = (a \wedge b) \times (a \vee b)$.

Relation $PPCM$ et $PGCD$

Proposition - Relation $PPCM$ et $PGCD$

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

- si $a \wedge b = 1$ alors $|ab| = (a \vee b)$.
- dans le cas général, $|ab| = (a \wedge b) \times (a \vee b)$.

Démonstration

Relation $PPCM$ et $PGCD$

Proposition - Relation $PPCM$ et $PGCD$

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

- si $a \wedge b = 1$ alors $|ab| = (a \vee b)$.
- dans le cas général, $|ab| = (a \wedge b) \times (a \vee b)$.

Démonstration

Remarque Généralisation à un nombre fini d'entiers

Conclusion

Objectifs

⇒ Deux caractérisations du PGCD et factorisation

⇒ Généralisations

Conclusion

Objectifs

⇒ Deux caractérisations du PGCD et factorisation

- $u|a$ et $u|b$ ssi $u|(a \wedge b)$

Conclusion

Objectifs

⇒ Deux caractérisations du PGCD et factorisation

Conclusion

Objectifs

⇒ Deux caractérisations du PGCD et factorisation

Conclusion

Objectifs

$\Rightarrow$ Deux caractérisations du PGCD et factorisation

- $u|a$ et $u|b$ ssi $u|(a \wedge b)$
- $a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$
- Identité de Bézout (CNS)
- Lemme(s) de Gauss

Conclusion

Objectifs

⇒ Deux caractérisations du PGCD et factorisation

⇒ Généralisations

Conclusion

Objectifs

⇒ Deux caractérisations du PGCD et factorisation

⇒ Généralisations

- PGCD de plusieurs nombres

Conclusion

Objectifs

⇒ Deux caractérisations du PGCD et factorisation

⇒ Généralisations

- PGCD de plusieurs nombres
- Calcul du PPCM (comme borne inférieure)

Conclusion

Objectifs

⇒ Deux caractérisations du PGCD et factorisation

⇒ Généralisations

Pour la prochaine fois

- Lecture du cours : chapitre 16 : Nombres premiers
- Exercice n°318 & 320