Leçon 45 - Divisibilité et congruence sur $\mathbb{Z}$. PGCD et PPCM

⇒ Algorithme d'Euclide et couple de Bézout

⇒ Deux caractérisations du PGCD et factorisation (premiers entre eux)

⇒ Algorithme d'Euclide et couple de Bézout

⇒ Deux caractérisations du PGCD et factorisation (premiers entre eux)

Définition « naturelle »

SI il s'agit du plus grand pour la relation d'ordre classique : $\leqslant$.
Analyse Construction du $PGCD$

Définition « naturelle »

SI il s'agit du plus grand pour la relation d'ordre classique : $\leqslant$.
Analyse Construction du $PGCD$

Définition - $PGCD$ de a et b

Soient a et b deux entiers relatifs non nuls.
On appelle $PGCD$ (Plus Grand Commun Diviseur) de a et b, le nombre

$$PGCD(a,b) = \max\left(\mathscr{D}(a) \cap \mathscr{D}(b) \cap \mathbb{N}\right).$$

On le note également $a \wedge b$.
On a clairement $b \wedge a = a \wedge b = |a| \wedge |b|$.
Par convention on pose pour $a \in \mathbb{Z}$, $a \wedge 0 = |a|$ (y compris si $a = 0$).

Exemple et remarques

Exemple $a = 36$, $b = 30$

Exemple et remarques

Exemple $a = 36$, $b = 30$

Remarque Divisibilité des nombres de $\mathscr{D}(30) \cap \mathscr{D}(36)$

Exemple et remarques

Exemple $a = 36$, $b = 30$
Remarque Divisibilité des nombres de $\mathscr{D}(30) \cap \mathscr{D}(36)$
Remarque Algorithme des facteurs premiers

⇒ Algorithme d'Euclide et couple de Bézout

⇒ Deux caractérisations du PGCD et factorisation (premiers entre eux)

Algorithme des divisions successives pour obtenir le $PGCD$

Lemme - Stabilité par division euclidienne

Soit $(a,b) \in \mathbb{Z} \times \mathbb{N}^*$.
Si $a = bq + r$, alors $\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(r) \cap \mathscr{D}(b)$ et donc $a \wedge b = b \wedge r$.

Algorithme des divisions successives pour obtenir le $PGCD$

Lemme - Stabilité par division euclidienne

Soit $(a,b) \in \mathbb{Z} \times \mathbb{N}^*$.
Si $a = bq + r$, alors $\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(r) \cap \mathscr{D}(b)$ et donc $a \wedge b = b \wedge r$.

Démonstration

Algorithme des divisions successives pour obtenir le $PGCD$

Lemme - Stabilité par division euclidienne

Soit $(a,b) \in \mathbb{Z} \times \mathbb{N}^*$.
Si $a = bq + r$, alors $\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(r) \cap \mathscr{D}(b)$ et donc $a \wedge b = b \wedge r$.

Démonstration

Heuristique - Algorithme pour obtenir le $PGCD$ de deux nombres

La proposition donne un algorithme qui exploite une suite de division euclidienne pour trouver le $PGCD(a,b)$.
Il permet également d'obtenir les coefficients de Bézout de a et b.
On notera qu'il s'applique à deux nombres a et b : $0 < b < a$.
Toute recherche de $PGCD(a,b)$ se ramène à ce cas là, en effet :

- Si $b = 0$ alors $PGCD(a,b) = |a|$
- Si $b \neq 0$, alors $PGCD(a,b) = PGCD(|a|,|b|) = PGCD(|b|,|a|)$

Algorithme d'Euclide

Proposition - Algorithme d'Euclide

Soient $a, b \in \mathbb{N}^*$. Supposons que $0 < b < a$. L'algorithme d'Euclide consiste en un succession de division euclidienne :

- On commence par poser $r_0 = a$ et $r_1 = b$;
- ensuite, k désignant un entier naturel non nul (étape de l'algorithme),
  tant que $r_{k+1} \neq 0$,
  on note r_{k+2} le reste de la division euclidienne de r_k par r_{k+1}
  (on a donc $r_{k+2} < r_{k+1}$).

Il existe $N \in \mathbb{N}^*$ tel que $r_N = 0$,
r_{N-1} est alors le dernier reste non nul de (r_k), et :
$a \wedge b = r_{N-1}$

Algorithme d'Euclide

Proposition - Algorithme d'Euclide

Soient $a, b \in \mathbb{N}^*$. Supposons que $0 < b < a$. L'algorithme d'Euclide consiste en un succession de division euclidienne :

- On commence par poser $r_0 = a$ et $r_1 = b$;
- ensuite, k désignant un entier naturel non nul (étape de l'algorithme),
  tant que $r_{k+1} \neq 0$,
  on note r_{k+2} le reste de la division euclidienne de r_k par r_{k+1}
  (on a donc $r_{k+2} < r_{k+1}$).

Il existe $N \in \mathbb{N}^*$ tel que $r_N = 0$,
r_{N-1} est alors le dernier reste non nul de (r_k), et :
$a \wedge b = r_{N-1}$

Démonstration

Applications

Application $PGCD(1542, 58) = 2$

Applications

Application $PGCD(1542,58)=2$

Savoir-faire. Exploiter la division euclidienne (théorie)

Si $f:\mathbb{Z}^2\to E$ (E quelconque) tel que $f(a,b)=f(b,a\%b)$, alors $f(a,b)=f(a\wedge b,0)$

Applications

Application $PGCD(1542,58) = 2$

Savoir-faire. Exploiter la division euclidienne (théorie)

Si $f : \mathbb{Z}^2 \to E$ (E quelconque) tel que $f(a,b) = f(b, a\%b)$, alors $f(a,b) = f(a \wedge b, 0)$

Truc & Astuce pour le calcul. Trouver son erreur dans un algorithme d'Euclide

Une fois l'algorithme terminé, il est important de vérifier que le dernier reste non nul est bien un diviseur de a et de b.
Si ce n'est pas le cas, il faut revenir à la ligne de calcul où le reste obtenu n'est pas divisible par le PGCD-candidat.

Python

Python - Division euclidienne

On peut écrire l'algorithme d'Euclide sous Python. Remarquons que dans le programme ainsi écrit, on tient compte des cas $b = 0$ et a ou b négatif.

```
def alg_eucl(a,b):
    """pgcd(a,b) par algorithme d'Euclide"""
    if b==0:
        return(a)
    a1,a2=max(abs(a),abs(b)),min(abs(a),abs(b))
    ra,rb=a1,a2
    while rb!=0:
        rc=div_eucl(ra,rb)[1]
        ra,rb=rb,rc
    return(ra)
```

⇒ Algorithme d'Euclide et couple de Bézout

⇒ Deux caractérisations du PGCD et factorisation (premiers entre eux)

Coefficient de (Bachet-)Bézout

Analyse Exploitation plus approfondie encore de l'algorithme d'Euclide

Coefficient de (Bachet-)Bézout

Analyse Exploitation plus approfondie encore de l'algorithme d'Euclide

Théorème - Coefficients de Bézout

Soit $(a,b) \in \mathbb{Z}^2$. Il existe des entiers u et v tels que $au + bv = a \wedge b$.
Un tel couple (u,v) est appelé un couple de coefficients de Bézout de a et b.

Coefficient de (Bachet-)Bézout

Analyse Exploitation plus approfondie encore de l'algorithme d'Euclide

Théorème - Coefficients de Bézout

Soit $(a,b) \in \mathbb{Z}^2$. Il existe des entiers u et v tels que $au + bv = a \wedge b$.
Un tel couple (u,v) est appelé un couple de coefficients de Bézout de a et b.

Savoir-faire. Pas unicité du couple de Bézout. Les obtenir tous

Il n'y a pas unicité du couple (u,v) :
si (u_0,v_0) est un couple de Bezout, en divisant par $\delta = a \wedge b$:

$$ua + bv = u_0 a + v_0 b \Rightarrow \frac{a}{\delta}(u-u_0) = \frac{b}{\delta}(v-v_0) \underbrace{\Rightarrow}_{\text{Gauss}} a|\delta(v-v_0)\dots$$

alors pour tout $n \in \mathbb{Z}$, $(u_0 + n\frac{b}{\delta}, v_0 - n\frac{a}{\delta})$ en est aussi un.

Coefficient de (Bachet-)Bézout

Python. Division euclidienne

```python
def Bezout(a,b):
    """pgcd(a,b)+coefficient de Bezout"""
    if b==0:
        return(a)
    a1,a2=max(abs(a),abs(b)),min(abs(a),abs(b))
    u,uu=1,0
    v,vv=0,1
    ra,rb=a1,a2
    while rb!=0:
        q,rc=div_eucl(ra,rb)
        ra,rb=rb,rc
        u,uu=uu,u-q*uu
        v,vv=vv,v-q*vv
    return(ra,u,v)
```

Coefficient de (Bachet-)Bézout

Truc & Astuce pour la calcul. Obtenir un couple de Bézout

En pratique, on trouve (u,v) en EN REMONTANT l'algorithme d'Euclide.

(à la main, il vaut mieux partir des valeurs numériques, elles n'arrivent qu'en fin d'algorithme).

Par exemple pour 1542 et 58 on a (en remontant les division euclidienne) :

$$2 = 10-2\times4 = 10-2(24-2\times10) = -2\times24+5\times10 = -2\times24+5\times(34-24)$$

$$= 5\times34-7\times24 = 5\times34-7\times(58-34) = -7\times58+12\times34$$

$$= -7\times58+12\times(1542-26\times58) = 12\times1542-319\times58.$$

Donc $1542u+58v=2$, avec (par exemple) : $u=12$ et $v=-319$.

Algorithme d'Euclide, arithmétique modulaire et carrelage

Analyse Relation de Bézout modulaire

Algorithme d'Euclide, arithmétique modulaire et carrelage

Analyse Relation de Bézout modulaire

Exercice

Donner une représentation théorique de la recherche du PGCD de a et de b, par algorithme d'Euclide dans un carrelage.

On pourra appliquer la méthode pour donner le $PGCD$ et les coefficient de Bézout pour les couples $(13, 7)$ et $(12, 6)$

⇒ Algorithme d'Euclide et couple de Bézout

⇒ Deux caractérisations du PGCD et factorisation (premiers entre eux)

Caractérisation par divisibilité

En fait la définition, du plus grand pour la relation d'ordre « est un diviseur de »coincide.

Caractérisation par divisibilité

En fait la définition, du plus grand pour la relation d'ordre « est un diviseur de »coincide.

Remarque Relation binaire

Caractérisation par divisibilité

En fait la définition, du plus grand pour la relation d'ordre « est un diviseur de »coincide.

Remarque Relation binaire

Proposition - Caractérisation essentielle du $PGCD$

Soit $(a,b) \in \mathbb{Z}^2$.

Alors $a \wedge b$ est le seul entier naturel dont les diviseurs sont exactement les diviseurs communs à a et b :

$$\mathscr{D}(a \wedge b) = \mathscr{D}(a) \cap \mathscr{D}(b)$$

autre façon de l'écrire :

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

Caractérisation par divisibilité

En fait la définition, du plus grand pour la relation d'ordre « est un diviseur de »coincide.

Remarque Relation binaire

Proposition - Caractérisation essentielle du $PGCD$

Soit $(a,b) \in \mathbb{Z}^2$.

Alors $a \wedge b$ est le seul entier naturel dont les diviseurs sont exactement les diviseurs communs à a et b :

$$\mathscr{D}(a \wedge b) = \mathscr{D}(a) \cap \mathscr{D}(b)$$

autre façon de l'écrire :

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

Remarque Force de cette propriété

Caractérisation par divisibilité

En fait la définition, du plus grand pour la relation d'ordre « est un diviseur de »coincide.

Remarque Relation binaire

Proposition - Caractérisation essentielle du $PGCD$

Soit $(a,b) \in \mathbb{Z}^2$.

Alors $a \wedge b$ est le seul entier naturel dont les diviseurs sont exactement les diviseurs communs à a et b :

$$\mathscr{D}(a \wedge b) = \mathscr{D}(a) \cap \mathscr{D}(b)$$

autre façon de l'écrire :

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

Remarque Force de cette propriété

Démonstration

Exploiter/Démontrer un PGCD

Savoir-faire. Trouver un PGCD. Exploiter un PGCD

On note $\delta = a \wedge b$.
Pour trouver le PGCD de a et de b :
on démontrer que si $m|a$ et $m|b$, alors nécessairement $m|\delta$.
Puis, on cherche m, le plus grand possible (si $m = 1$, alors $a \wedge b = 1$).
Pour exploiter le PGCD de a et de b :
On exploite le fait que si $m|\delta$, alors $m|a$ et $m|b$.
Et on travaille sur cette co-divisibilité

Exploiter/Démontrer un PGCD

Savoir-faire. Trouver un PGCD. Exploiter un PGCD

On note $\delta = a \wedge b$.
Pour trouver le PGCD de a et de b :

on démontrer que si $m|a$ et $m|b$, alors nécessairement $m|\delta$.

Puis, on cherche m, le plus grand possible (si $m = 1$, alors $a \wedge b = 1$).

Pour exploiter le PGCD de a et de b :

On exploite le fait que si $m|\delta$, alors $m|a$ et $m|b$.

Et on travaille sur cette co-divisibilité

Application - $\lambda a \wedge \lambda b = \lambda(a \wedge b)$

Combinaison linéaire entière

Proposition - Combinaison linéaire

Soient $a, b \in \mathbb{Z}$.
On note $a\mathbb{Z} + b\mathbb{Z} = \{ua + vb, u, v \in \mathbb{Z}\}$, ensemble des combinaisons linéaires de a et de b.
Alors
$$a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$$

Combinaison linéaire entière

Proposition - Combinaison linéaire

Soient $a, b \in \mathbb{Z}$.
On note $a\mathbb{Z} + b\mathbb{Z} = \{ua + vb, u, v \in \mathbb{Z}\}$, ensemble des combinaisons linéaires de a et de b.
Alors
$$a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$$

Démonstration

Combinaison linéaire entière

Proposition - Combinaison linéaire

Soient $a, b \in \mathbb{Z}$.
On note $a\mathbb{Z} + b\mathbb{Z} = \{ua + vb, u, v \in \mathbb{Z}\}$, ensemble des combinaisons linéaires de a et de b.
Alors

$$a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$$

Démonstration

Combinaisons linéaires (entières)

Dès que l'on a des combinaisons linéaires d'entiers (on appelle cela un réseau d'entiers), il faut penser que la maille élémentaire est donné par le PGCD des nombres. C'est pas exemple le cas du problème « monde ficitf »

⇒ Algorithme d'Euclide et couple de Bézout

⇒ Deux caractérisations du PGCD et factorisation (premiers entre eux)

Identité de Bézout

Définition - Couple d'entiers premiers entre eux

a et b sont dits *premiers entre eux* si $a \wedge b = 1$.

Identité de Bézout

Définition - Couple d'entiers premiers entre eux

a et b sont dits *premiers entre eux* si $a \wedge b = 1$.

On a bien une équivalence :

Théorème (ou identité) de Bézout

Soient a et b deux entiers relatifs non nuls. Alors

$$a \wedge b = 1 \Longleftrightarrow \exists (u,v) \in \mathbb{Z}^2 \text{ tel que } au + bv = 1$$

Identité de Bézout

Définition - Couple d'entiers premiers entre eux

a et b sont dits *premiers entre eux* si $a \wedge b = 1$.

On a bien une équivalence :

Théorème (ou identité) de Bézout

Soient a et b deux entiers relatifs non nuls. Alors

$$a \wedge b = 1 \iff \exists (u,v) \in \mathbb{Z}^2 \text{ tel que } au + bv = 1$$

Démonstration

Usage

Comme il est plus simple de travailler avec des nombres premiers entre eux, on exploite souvent le savoir-faire suivant :

Savoir-faire. Usage fréquent

Soient $a, b \in \mathbb{Z}$. On note $\delta = a \wedge b$.
Alors, $a = \delta a'$ et $b = \delta b'$, avec $a' \wedge b' = 1$.
Puis on travaille avec les a' et b'

⇒ Algorithme d'Euclide et couple de Bézout

⇒ Deux caractérisations du PGCD et factorisation (premiers entre eux)

Lemme de Gauss

Théorème - Lemme de Gauss

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

$$(a \wedge b = 1 \text{ et } a|bc) \Longrightarrow a|c.$$

Lemme de Gauss

Théorème - Lemme de Gauss

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

$$(a \wedge b = 1 \text{ et } a|bc) \Longrightarrow a|c.$$

Démonstration

Lemme de Gauss

Théorème - Lemme de Gauss

Soient $a, b, c \in \mathbb{Z}$. Alors
$$(a \wedge b = 1 \text{ et } a|bc) \Longrightarrow a|c.$$

Démonstration

Proposition - Facteur relativement premier

Soient $a, b, c \in \mathbb{Z}$. Alors
$$(a \wedge b = 1 \text{ et } a \wedge c = 1) \Longrightarrow a \wedge bc = 1 \text{ (réciproque vraie)}$$
$$(a \wedge b = 1, a|c, b|c) \Longrightarrow ab|c$$

Lemme de Gauss

Théorème - Lemme de Gauss

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

$$(a \wedge b = 1 \text{ et } a | bc) \Longrightarrow a | c.$$

Démonstration

Proposition - Facteur relativement premier

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

$$(a \wedge b = 1 \text{ et } a \wedge c = 1) \Longrightarrow a \wedge bc = 1 \text{ (réciproque vraie)}$$

$$(a \wedge b = 1, a | c, b | c) \Longrightarrow ab | c$$

Démonstration

Lemme de Gauss

Théorème - Lemme de Gauss

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

$$(a \wedge b = 1 \text{ et } a | bc) \Longrightarrow a | c.$$

Démonstration

Proposition - Facteur relativement premier

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

$$(a \wedge b = 1 \text{ et } a \wedge c = 1) \Longrightarrow a \wedge bc = 1 \text{ (réciproque vraie)}$$

$$(a \wedge b = 1, a|c, b|c) \Longrightarrow ab|c$$

Démonstration

<u>Exercice</u>

On note $\mathscr{P}_a = \{b \mid a \wedge b = 1\}$ et $a\mathbb{Z} = \{ak, k \in \mathbb{Z}\}$.

Exprimer les propositions précédentes avec ces ensembles.

Décomposition en facteurs relativement premiers

Corollaire - Facteurs premiers

Soient $a, c, b_1, \ldots, b_n$ des entiers relatifs.

$$(\forall i \in [\![1, n]\!], a \wedge b_i = 1) \Longrightarrow a \wedge \prod_{i=1}^{n} b_i = 1$$

$$(i \neq j \Rightarrow b_i \wedge b_j = 1 \text{ et } \forall i \in [\![1, n]\!], b_i | c) \Longrightarrow \prod_{i=1}^{n} b_i \Big| c$$

Décomposition en facteurs relativement premiers

Corollaire - Facteurs premiers

Soient $a, c, b_1, \ldots, b_n$ des entiers relatifs.

$$(\forall i \in [\![1,n]\!], a \wedge b_i = 1) \Longrightarrow a \wedge \prod_{i=1}^{n} b_i = 1$$

$$(i \neq j \Rightarrow b_i \wedge b_j = 1 \text{ et } \forall i \in [\![1,n]\!], b_i | c) \Longrightarrow \prod_{i=1}^{n} b_i \Big| c$$

Démonstration

Décomposition en facteurs relativement premiers

Corollaire - Facteurs premiers

Soient $a, c, b_1, \dots, b_n$ des entiers relatifs.

$$(\forall i \in [\![1,n]\!], a \wedge b_i = 1) \Longrightarrow a \wedge \prod_{i=1}^n b_i = 1$$

$$(i \neq j \Rightarrow b_i \wedge b_j = 1 \text{ et } \forall i \in [\![1,n]\!], b_i | c) \Longrightarrow \prod_{i=1}^n b_i \Big| c$$

Démonstration

Corollaire - Forme irréductible d'un rationnel

Soit $r \in \mathbb{Q}$. Il existe un unique couple $(p,q) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $r = \dfrac{p}{q}$ et tel que p et q soient premiers entre eux.

Cette écriture est appelée la forme irréductible de r.

Les autres écritures fractionnaires sont de la forme $r = \dfrac{\lambda p}{\lambda q}$ avec $\lambda \in \mathbb{Z}^*$.

Décomposition en facteurs relativement premiers

Corollaire - Facteurs premiers

Soient $a, c, b_1, \ldots, b_n$ des entiers relatifs.

$$(\forall i \in [\![1,n]\!], a \wedge b_i = 1) \Longrightarrow a \wedge \prod_{i=1}^n b_i = 1$$

$$(i \neq j \Rightarrow b_i \wedge b_j = 1 \text{ et } \forall i \in [\![1,n]\!], b_i | c) \Longrightarrow \prod_{i=1}^n b_i \Big| c$$

Démonstration

Corollaire - Forme irréductible d'un rationnel

Soit $r \in \mathbb{Q}$. Il existe un unique couple $(p,q) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $r = \dfrac{p}{q}$ et tel que p et q soient premiers entre eux.

Cette écriture est appelée la forme irréductible de r.

Les autres écritures fractionnaires sont de la forme $r = \dfrac{\lambda p}{\lambda q}$ avec $\lambda \in \mathbb{Z}^*$.

Démonstration

Conclusion

Objectifs

⇒ Algorithme d'Euclide et couple de Bézout

⇒ Deux caractérisations du PGCD et factorisation (premiers entre eux)

Conclusion

Objectifs

$\Rightarrow$ Algorithme d'Euclide et couple de Bézout

- Plus grand des diviseurs, mais pour quelle relation d'ordre : $\leqslant$ ou $|$?

Conclusion

Objectifs

$\Rightarrow$ Algorithme d'Euclide et couple de Bézout

- Plus grand des diviseurs, mais pour quelle relation d'ordre : $\leqslant$ ou $|$?
  Les deux ! !

Conclusion

Objectifs

$\Rightarrow$ Algorithme d'Euclide et couple de Bézout

- Plus grand des diviseurs, mais pour quelle relation d'ordre : $\leqslant$ ou $|$?
  Les deux !!
- Algorithme d'Euclide qui s'appuie sur la conservation du $PGCD$ en exploitant la suite des restes.

Conclusion

Objectifs

$\Rightarrow$ Algorithme d'Euclide et couple de Bézout

- Plus grand des diviseurs, mais pour quelle relation d'ordre : $\leqslant$ ou $|$?
  Les deux !!
- Algorithme d'Euclide qui s'appuie sur la conservation du $PGCD$ en exploitant la suite des restes.
- Coefficients de Bézout.

Conclusion

Objectifs

⇒ Algorithme d'Euclide et couple de Bézout

⇒ Deux caractérisations du PGCD et factorisation (premiers entre eux)

Conclusion

Objectifs

⇒ Algorithme d'Euclide et couple de Bézout

⇒ Deux caractérisations du PGCD et factorisation (premiers entre eux)

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

Conclusion

Objectifs

⇒ Algorithme d'Euclide et couple de Bézout

⇒ Deux caractérisations du PGCD et factorisation (premiers entre eux)

Conclusion

Objectifs

$\Rightarrow$ Algorithme d'Euclide et couple de Bézout

$\Rightarrow$ Deux caractérisations du PGCD et factorisation (premiers entre eux)

Conclusion

Objectifs

⇒ Algorithme d'Euclide et couple de Bézout

⇒ Deux caractérisations du PGCD et factorisation (premiers entre eux)

- $u|a$ 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

⇒ Algorithme d'Euclide et couple de Bézout

⇒ Deux caractérisations du PGCD et factorisation (premiers entre eux)

Pour la prochaine fois

- Lecture du cours : chapitre 17 : Arithmétique dans $\mathbb{Z}$
  5. Entiers premiers entre eux ⇒ 7. PPCM
- Exercice n° 308 & 309