Leçon 44 - Divisibilité et congruence sur $\mathbb{Z}$. PGCD et PPCM

⇒ Divisibilité dans $\mathbb{Z}$

⇒ Arithmétique modulaire

⇒ Divisibilité dans $\mathbb{Z}$

⇒ Arithmétique modulaire

1. Problèmes

2. Divisibilité dans $\mathbb{Z}$
   - 2.1. Intégrité de $\mathbb{Z}$ et régularité
   - 2.2. Diviseurs, multiples
   - 2.3. Division euclidienne de a par b
   - 2.4. Arithmétique modulaire

⇒ Divisibilité dans $\mathbb{Z}$

⇒ Arithmétique modulaire

Problèmes

Problème Pairs, impairs. . .

Problèmes

Problème Pairs, impairs. . .

Problème Table de multiplication modulo n

$\times_{[5]}$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$\times_{[6]}$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

Problèmes

Problème Représentation sous (sur ?) un treilli

Problèmes

Problème Représentation sous (sur ?) un treilli

Problème Division euclidienne et PGCD

Problèmes

Problème Représentation sous (sur ?) un treilli

Problème Division euclidienne et PGCD

Problème Monde fictif

⇒ Divisibilité dans $\mathbb{Z}$

⇒ Arithmétique modulaire

Intégrité

Proposition - Intégrité de l'anneau $\mathbb{Z}$

$\mathbb{Z}$ est un anneau intègre.

Formellement :

$$\forall\, a, b \in \mathbb{Z}, \qquad a \times b = 0 \Longrightarrow a = 0 \text{ ou } b = 0$$

Intégrité

Proposition - Intégrité de l'anneau $\mathbb{Z}$

$\mathbb{Z}$ est un anneau intègre.

Formellement :

$$\forall\, a, b \in \mathbb{Z}, \qquad a \times b = 0 \Longrightarrow a = 0 \text{ ou } b = 0$$

Démonstration

Régularité

Comme pour tout anneau intègre,

Proposition - Régularité de l'anneau $\mathbb{Z}$

Les éléments non nuls de $\mathbb{Z}$ sont réguliers. Formellement :

$$\forall\ a \in \mathbb{Z}, a \neq 0, \qquad \forall\ b, c \in \mathbb{Z}, a \times b = a \times c \Longrightarrow b = c$$

Régularité

Comme pour tout anneau intègre,

Proposition - Régularité de l'anneau $\mathbb{Z}$

Les éléments non nuls de $\mathbb{Z}$ sont réguliers. Formellement :

$$\forall\ a \in \mathbb{Z}, a \neq 0, \qquad \forall\ b, c \in \mathbb{Z}, a \times b = a \times c \Longrightarrow b = c$$

Démonstration

Régularité

Comme pour tout anneau intègre,

Proposition - Régularité de l'anneau $\mathbb{Z}$

Les éléments non nuls de $\mathbb{Z}$ sont réguliers. Formellement :

$$\forall\ a \in \mathbb{Z}, a \neq 0, \qquad \forall\ b, c \in \mathbb{Z}, a \times b = a \times c \Longrightarrow b = c$$

Démonstration

Remarque. A quoi sert cette propriété ?

⇒ Divisibilité dans $\mathbb{Z}$

⇒ Arithmétique modulaire

1. Problèmes

2. Divisibilité dans $\mathbb{Z}$

- 2.1. Intégrité de $\mathbb{Z}$ et régularité
- 2.2. Diviseurs, multiples
- 2.3. Division euclidienne de a par b
- 2.4. Arithmétique modulaire

Diviseurs et ensemble des diviseurs

Définition - Diviseur, multiple

Soit $(a,b) \in \mathbb{Z}^2$. On dit que b *divise* a s'il existe $k \in \mathbb{Z}$ tel que $a = kb$ et on note $b|a$.

On dit aussi que b est un *diviseur* de a, ou que a est un *multiple* de b.

On note $b\mathbb{Z} = \{b \times k; k \in \mathbb{Z}\}$ l'ensemble des multiples de b.

Diviseurs et ensemble des diviseurs

Définition - Diviseur, multiple

Soit $(a,b) \in \mathbb{Z}^2$. On dit que b *divise* a s'il existe $k \in \mathbb{Z}$ tel que $a = kb$ et on note $b|a$.
On dit aussi que b est un *diviseur* de a, ou que a est un *multiple* de b.
On note $b\mathbb{Z} = \{b \times k; k \in \mathbb{Z}\}$ l'ensemble des multiples de b.

Savoir-faire. Montrer que b divise a

(Sous-entendu : dans $\mathbb{Z}$). Le plus important n'est pas de montrer l'existence de k tel que $k \times b = a$ mais bien de montrer que $k \in \mathbb{Z}$

Diviseurs et ensemble des diviseurs

Définition - Diviseur, multiple

Soit $(a,b) \in \mathbb{Z}^2$. On dit que b *divise* a s'il existe $k \in \mathbb{Z}$ tel que $a = kb$ et on note $b|a$.
On dit aussi que b est un *diviseur* de a, ou que a est un *multiple* de b.
On note $b\mathbb{Z} = \{b \times k; k \in \mathbb{Z}\}$ l'ensemble des multiples de b.

Savoir-faire. Montrer que b divise a

(Sous-entendu : dans $\mathbb{Z}$). Le plus important n'est pas de montrer l'existence de k tel que $k \times b = a$ mais bien de montrer que $k \in \mathbb{Z}$

Définition - Ensemble des diviseurs

On notera par la suite $\mathscr{D}(a)$ l'ensemble des diviseurs de a. Pour $a \neq 0$, cet ensemble ne contient qu'un nombre fini d'éléments puisque : $d|a \Rightarrow |d| \leqslant |a|$.

Remarques

Application Majoration du cardinal

Remarques

Application Majoration du cardinal

Remarque Le cas de 0 et 1

Remarques

Application Majoration du cardinal

Remarque Le cas de 0 et 1

Définition - Nombres associés

Soit $(a,b) \in \mathbb{Z}^2$. on dit que a et b sont associés si $a|b$ et $b|a$. On a la caractérisation suivante :

$$(a|b \text{ et } b|a) \Leftrightarrow |a| = |b| \Leftrightarrow \exists\, \epsilon \in \{-1,1\} = \mathbb{Z}^\times : a = \epsilon b$$

Division et combinaison linéaire

Proposition - Division de combinaison linéaire

Soit $(a,b) \in \mathbb{Z}^2$. Pour $(u,v) \in \mathbb{Z}^2$, $n \in \mathbb{Z}$, $n \neq 0$ on a :

$$(d|a \text{ et } d|b) \Longrightarrow d|au+bv$$

$$an|bn \Longleftrightarrow a|b$$

Division et combinaison linéaire

Proposition - Division de combinaison linéaire

Soit $(a,b) \in \mathbb{Z}^2$. Pour $(u,v) \in \mathbb{Z}^2$, $n \in \mathbb{Z}$, $n \neq 0$ on a :

$$(d|a \text{ et } d|b) \Longrightarrow d|au+bv$$

$$an|bn \Longleftrightarrow a|b$$

Démonstration

Division et combinaison linéaire

Proposition - Division de combinaison linéaire

Soit $(a,b) \in \mathbb{Z}^2$. Pour $(u,v) \in \mathbb{Z}^2$, $n \in \mathbb{Z}$, $n \neq 0$ on a :

$$(d|a \text{ et } d|b) \Longrightarrow d|au+bv$$

$$an|bn \Longleftrightarrow a|b$$

Démonstration

Exercice

Montrer que la relation « divise » est une relation d'ordre

⇒ Divisibilité dans $\mathbb{Z}$

⇒ Arithmétique modulaire

1. Problèmes

2. Divisibilité dans $\mathbb{Z}$

- 2.1. Intégrité de $\mathbb{Z}$ et régularité
- 2.2. Diviseurs, multiples
- 2.3. Division euclidienne de a par b
- 2.4. Arithmétique modulaire

Théorie

Heuristique - La division euclidienne : des soustractions !

Il est souvent beaucoup plus efficace de considérer la division euclidienne comme une succession de soustraction de a par b (ou d'addition de b à a si $a < 0$).
(De même pour l'algorithme d'Euclide).

Théorie

Heuristique - La division euclidienne : des soustractions !

Il est souvent beaucoup plus efficace de considérer la division euclidienne comme une succession de soustraction de a par b (ou d'addition de b à a si $a < 0$).
(De même pour l'algorithme d'Euclide).

Théorème - Division euclidienne

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

$$a = bq + r \text{ et } 0 \leqslant r < b.$$

q et r sont appelés respectivement *quotient* et *reste* de la division euclidienne de a par b.
Dans ce cours, nous noterons comme en Python : $a//b$ pour désigner q et $a\%b$ pour désigner r.

Théorie

Heuristique - La division euclidienne : des soustractions !

Il est souvent beaucoup plus efficace de considérer la division euclidienne comme une succession de soustraction de a par b (ou d'addition de b à a si $a < 0$).
(De même pour l'algorithme d'Euclide).

Théorème - Division euclidienne

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

$$a = bq + r \text{ et } 0 \leqslant r < b.$$

q et r sont appelés respectivement *quotient* et *reste* de la division euclidienne de a par b.
Dans ce cours, nous noterons comme en Python : $a//b$ pour désigner q et $a\%b$ pour désigner r.

Démonstration

Critère de divisibilité

Proposition - Critère de divisibilité et division euclidienne

Soient $a \in \mathbb{Z}$, $b \in \mathbb{N}^*$.
$b|a$ si et seulement si le reste de la division euclidienne de a par b vaut 0.

Critère de divisibilité

Proposition - Critère de divisibilité et division euclidienne

Soient $a \in \mathbb{Z}$, $b \in \mathbb{N}^*$.
$b|a$ si et seulement si le reste de la division euclidienne de a par b vaut 0.

Démonstration

Algorithme

Python - Division euclidienne

```
1  def div_eucl(a,b):
2      """division euclidienne de a par b"""
3      #Principe : on soustrait b autant que necessaire a a
4      d,k=a,0
5      if a<0 :
6          c,eps=-b,-1 # si a<0, il faudra additionner b
7      else :
8          c,eps=b,1
9      while d>=b or d<0:
10         d=d-c
11         k=k+eps #k = nbre de soustractions = quotient
12     return(k,d)
```

Algorithme

Python - Division euclidienne

```
1  def div_eucl(a,b):
2      """division euclidienne de a par b"""
3      #Principe : on soustrait b autant que necessaire a a
4      d,k=a,0
5      if a<0 :
6          c,eps=-b,-1 # si a<0, il faudra additionner b
7      else :
8          c,eps=b,1
9      while d>=b or d<0:
10         d=d-c
11         k=k+eps #k = nbre de soustractions = quotient
12     return(k,d)
```

Application `div_eucl(12,5)` et `div_eucl(-12,5)`

Algorithme

Une autre idée est d'exploiter la récursivité :

Python - Division euclidienne

```
1  def div_eucl_rec(a,b):
2      """calcul de la division euclidienne de a par b, par recu
3      if a<b and a>-1:
4          return(0,a)
5      elif a>b :
6          m,n=div_eucl_rec(a-b,b)
7          return(m+1,n)
8      else :
9          m,n=div_eucl_rec(a+b,b)
10         return(m-1,n)
```

⇒ Divisibilité dans $\mathbb{Z}$

⇒ Arithmétique modulaire

1. Problèmes

2. Divisibilité dans $\mathbb{Z}$

- 2.1. Intégrité de $\mathbb{Z}$ et régularité
- 2.2. Diviseurs, multiples
- 2.3. Division euclidienne de a par b
- 2.4. Arithmétique modulaire

Relation d'équivalence

Définition - a congru à b modulo n

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

On dit que a *est congru à* b *modulo* n si n divise $a - b$

$(\Longleftrightarrow a - b \in n\mathbb{Z})$,

c'est-à-dire s'il existe $k \in \mathbb{Z}$ tel que $a = b + kn$.

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

Relation d'équivalence

Définition - a congru à b modulo n

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

On dit que a *est congru à* b *modulo* n si n divise $a - b$

$(\Longleftrightarrow a - b \in n\mathbb{Z})$,

c'est-à-dire s'il existe $k \in \mathbb{Z}$ tel que $a = b + kn$.

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

Pour tout $n \in \mathbb{N}^*$, la relation de congruence modulo n est une relation d'équivalence (nous l'avons déjà vu).

Relation d'équivalence

Définition - a congru à b modulo n

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

On dit que a *est congru à* b *modulo* n si n divise $a - b$

$(\Longleftrightarrow a - b \in n\mathbb{Z})$,

c'est-à-dire s'il existe $k \in \mathbb{Z}$ tel que $a = b + kn$.

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

Pour tout $n \in \mathbb{N}^*$, la relation de congruence modulo n est une relation d'équivalence (nous l'avons déjà vu).

Remarque $\mathbb{U}_n$

Système de représentants

La proposition suivante donne un système de représentant naturel (et donc le nombre de classe d'équivalence)

Proposition - Reste

Soit $n \in \mathbb{N}^*$. Pour tout $a, b \in \mathbb{Z}$

$$a \equiv b[n] \iff a\%n = b\%n.$$

Ainsi, $[\![0, n-1]\!]$ est un système de représentant de $\dfrac{\mathbb{Z}}{\cdot \equiv \cdot [n]}$, ensemble possédant donc n éléments

Système de représentants

La proposition suivante donne un système de représentant naturel (et donc le nombre de classe d'équivalence)

Proposition - Reste

Soit $n \in \mathbb{N}^*$. Pour tout $a, b \in \mathbb{Z}$

$$a \equiv b[n] \iff a\%n = b\%n.$$

Ainsi, $[\![0, n-1]\!]$ est un système de représentant de $\dfrac{\mathbb{Z}}{\cdot \equiv \cdot [n]}$, ensemble possédant donc n éléments

Démonstration

Arithmétique modulaire

Proposition - Opérations : arithmétique modulaire

Soit $n \in \mathbb{N}$. La congruence modulo n est compatible avec l'addition et la multiplication :
Pour a, a', b, b' entiers relatifs on a

$$\begin{cases} a \equiv a'[n] \\ b \equiv b'[n] \end{cases} \Longrightarrow \begin{cases} a+b \equiv a'+b'[n] \\ a \times b \equiv a' \times b'[n] \end{cases}$$

Arithmétique modulaire

Proposition - Opérations : arithmétique modulaire

Soit $n \in \mathbb{N}$. La congruence modulo n est compatible avec l'addition et la multiplication :
Pour a, a', b, b' entiers relatifs on a

$$\begin{cases} a \equiv a'[n] \\ b \equiv b'[n] \end{cases} \Longrightarrow \begin{cases} a+b \equiv a'+b'[n] \\ a \times b \equiv a' \times b'[n] \end{cases}$$

Démonstration

Applications

Truc &Astuce pour le calcul. Réduction modulo n

La réduction modulo n réduit les calculs : les nombres ne dépassent pas la valeur n.
En revanche, on perd des informations ou bien parfois, on supprime les informations inutiles (à quoi sert de connaître exactement un nombre, alors que seul son dernier chiffre est demandé ?)

Applications

Truc &Astuce pour le calcul. Réduction modulo n

La réduction modulo n réduit les calculs : les nombres ne dépassent pas la valeur n.
En revanche, on perd des informations ou bien parfois, on supprime les informations inutiles (à quoi sert de connaître exactement un nombre, alors que seul son dernier chiffre est demandé ?)

Remarque Vérifier un calcul

Applications

Truc &Astuce pour le calcul. Réduction modulo n

La réduction modulo n réduit les calculs : les nombres ne dépassent pas la valeur n.
En revanche, on perd des informations ou bien parfois, on supprime les informations inutiles (à quoi sert de connaître exactement un nombre, alors que seul son dernier chiffre est demandé ?)

Remarque Vérifier un calcul

Exercice

Avons-nous l'équivalence $a \equiv b[n] \iff ca \equiv cb[n]$?
Quelle est l'implication. Donner un contre-exemple de l'implication réciproque. Une condition pour l'équivalence ?

Applications

Truc &Astuce pour le calcul. Réduction modulo n

La réduction modulo n réduit les calculs : les nombres ne dépassent pas la valeur n.
En revanche, on perd des informations ou bien parfois, on supprime les informations inutiles (à quoi sert de connaître exactement un nombre, alors que seul son dernier chiffre est demandé ?)

Remarque Vérifier un calcul

Exercice

Avons-nous l'équivalence $a \equiv b[n] \iff ca \equiv cb[n]$?
Quelle est l'implication. Donner un contre-exemple de l'implication réciproque. Une condition pour l'équivalence ?

Remarque Réduction modulo p, $p \in \mathscr{P}$

Conclusion

Objectifs

⇒ Divisibilité dans $\mathbb{Z}$

⇒ Arithmétique modulaire

Conclusion

Objectifs

⇒ Divisibilité dans $\mathbb{Z}$

- On dit que $a|b$ ssi $\exists\ q \in \mathbb{Z}$ tel que $b = aq$.

Conclusion

Objectifs

⇒ Divisibilité dans $\mathbb{Z}$

- On dit que $a|b$ ssi $\exists\ q \in \mathbb{Z}$ tel que $b = aq$.
- Critère équivalent : $a|b$ ssi $b\%a == 0$ (notation Python).

Conclusion

Objectifs

⇒ Divisibilité dans $\mathbb{Z}$

- On dit que $a|b$ ssi $\exists\ q \in \mathbb{Z}$ tel que $b = aq$.
- Critère équivalent : $a|b$ ssi $b\%a == 0$ (notation Python).
- Dans ce cas, il faut voir la division euclidienne de b par a comme une suite (finie) de soustraction de a dans b...

Conclusion

Objectifs

⇒ Divisibilité dans $\mathbb{Z}$

⇒ Arithmétique modulaire

Conclusion

Objectifs

⇒ Divisibilité dans $\mathbb{Z}$

⇒ Arithmétique modulaire

- Relation de congruence

Conclusion

Objectifs

⇒ Divisibilité dans $\mathbb{Z}$

⇒ Arithmétique modulaire

- Relation de congruence
- Un représentant de chaque classe modulo n : le reste de la division euclidienne

Conclusion

Objectifs

⇒ Divisibilité dans $\mathbb{Z}$

⇒ Arithmétique modulaire

- Relation de congruence
- Un représentant de chaque classe modulo n : le reste de la division euclidienne
- Transfert des propriétés algébriques (addition, multiplication. Division ?)

Conclusion

Objectifs

⇒ Divisibilité dans $\mathbb{Z}$

⇒ Arithmétique modulaire

Pour la prochaine fois

- Lecture du cours : chapitre 15 : Arithmétique dans $\mathbb{Z}$
  3. PGCD
- Exercice n° 306, 315 & 317
- TD de jeudi :
  8h-10h : N° 388, 398, 307, 310, 316
  10h-12h : N° 397, 314, 312, 319, 321