Chapitre 10 : anneau des entiers, arithmétique

Table des matières

1 PGCD et PPCM

1.1 Rappels

Définition 1 On rappelle que l'ensemble $\mathbb{Z}$ muni des LCI $+$ et $\times$ forme un anneau commutatif, d'élément nul 0 et d'élément unité 1. On rappelle également que les sous groupes de $(\mathbb{Z},+)$ sont exactement les ensembles $a\cdot\mathbb{Z}=\{a\cdot p\in\mathbb{Z}\mid p\in\mathbb{Z}\}$, où a est un entier. On rappelle enfin que pour tous entiers a et b, on dit que a ***divise*** b ou que b ***est un multiple de*** a si $b\in a\cdot\mathbb{Z}$ ($\Longleftrightarrow \exists p\in\mathbb{Z},\, b=a\cdot p$).

Exemple 1 Quels sont tous les diviseurs de 0 ? Quels sont les inversibles de l'anneau $\mathbb{Z}$?

1.2 Division euclidienne

Théoréme 1 Soient a et b deux entiers avec $b\neq 0$. Alors, il existe un unique couple (q,r) d'entiers tel que :
- $a=b\cdot q+r$
- $0\leqslant r<|b|$.

Remarque 1 • L'entier q est le ***quotient*** dans la division euclidienne de a par b et l'entier r est le ***reste*** dans cette division euclidienne.
- On note parfois $a=r[b]$ pour signifier que b divise $a-r$.

1.3 Pgcd et ppcm

Proposition 1 Soient a et b deux entiers. L'ensemble $a\cdot\mathbb{Z}+b\cdot\mathbb{Z}=\{a\cdot p+b\cdot p'\mid (p,p')\in\mathbb{Z}^2\}$ forme un sous-groupe de $(\mathbb{Z},+)$. Il existe un unique entier d positif tel que $a\cdot\mathbb{Z}+b\cdot\mathbb{Z}=d\cdot\mathbb{Z}$. Cet entier est appelé ***pgcd des nombres*** a ***et*** b et noté $d=a\wedge b$.
De même, l'ensemble $a\cdot\mathbb{Z}\cap b\cdot\mathbb{Z}$ forme un sous-groupe de $(\mathbb{Z},+)$. Il existe un unique entier m positif tel que $a\cdot\mathbb{Z}\cap b\cdot\mathbb{Z}=m\cdot\mathbb{Z}$. Cet entier est appelé ***ppcm des nombres*** a ***et*** b et noté $m=a\vee b$.

Exemple 2 Pour tout entier a, on a : $0\wedge a=|a|$ et $0\vee a=0$. Pour tout entier a, on a : $1\wedge a=1$ et $1\vee a=|a|$.

Proposition 2 Soient a et b deux entiers non nuls.
- Soit α un diviseur commun à a et à b. Alors $\alpha|(a\wedge b)$ et donc le pgcd $a\wedge b$ est le plus grand commun diviseur à a et à b.
- Soit β un multiple commun à a et à b. Alors $(a\vee b)|\beta$ et donc le ppcm $a\vee b$ est le plus petit commun multiple à a et à b.

2 Nombres premiers entre eux

2.1 Définition

Définition 2 Soient a et b deux entiers. On dit que les nombres a et b sont ***premiers entre eux*** si $a\wedge b=1$.

2.2 Caractérisation : relation de Bezout

Théoréme 2 Soient a et b deux entiers. Les nombres a et b sont premiers entre eux si et seulement si il existe un couple d'entiers (u, v) tel que :

$$a \cdot u + b \cdot v = 1.$$

Une telle relation est appelée ***relation de Bezout***.

Proposition 3 Soient a et b deux entiers non tous nuls. Alors le pgcd $d = a \wedge b$ est non nul et en posant $a' = \frac{a}{d}$ et $b' = \frac{b}{d}$, les nombres a' et b' sont deux entiers premiers entre eux.

Méthode : Comment trouver une relation de Bezout entre deux entiers ?

Soient a et b deux entiers non nuls. Pour trouver u et v deux entiers tels que $a \cdot u + b \cdot v = a \wedge b$:

- faire la division euclidienne de $q_0 = a$ par $q_1 = b$
- faire la division euclidienne de q_n par q_{n+1} et poser q_{n+2} le reste obtenu
- recommencer jusqu'à tomber sur un reste nul $q_s = 0$
- donner le pgcd : le dernier reste non nul q_{s-1} [algorithme d'Euclide]
- exprimer q_{s-1} en fonction de q_{s-2} et q_{s-3}, ainsi de suite en remontant les calculs
- aboutir à une formule de q_{s-1} en fonction de $q_0 = a$ et $q_1 = b$.

Exemple 3 • Voici un script PYTHON pour l'implémentation de la division euclidienne :

```
def Div_Eucl(a,b) :
    r,q=abs(a),0
    while r>=abs(b) :
        r-=abs(b)
        q+=1
    if a<0 :
        r,q=-r,-q
    if r<0:
        r+=abs(b)
        q-=1
    if b<0 :
        q=-q
    return [q,r]
```

Par exemple :

```
a,b=89,-35
print(Div_Eucl(a,b))
>>> [-2, 19]
```

• Voici un script PYTHON pour l'implémentation d'une combinaison linéaire entière de $a \wedge b$ en fonction de a et b :

```
def Bezout(a,b) :
    L=[]
    A,B=a,b
    while B!= 0 :
        q,r=Div_Eucl(A,B)
        L.append(q)
        A,B=B,r
    # le pgcd de A et B vaut A
    # on remonte les calculs
```

```
    Res=[1,-L[-2]]
    for k in range(len(L)-2) :
        u,v=Res
        Res=[v,u-v*L[-3-k]]
    return Res
```

Par exemple :

```
a,b=133,-17
print(Bezout(a,b))
>>> [-6, -47]
```

Exemple 4 • Existe-t-il une relation de Bezout entre 459 et 612 ?
- Déterminer une relation de Bezout entre 17 et 235.

2.3 Théorème de Gauss

Théoréme 3 Soient a, b et c trois entiers. Alors :
- si $a|(b \cdot c)$ et si $a \wedge b = 1$, alors $a|c$
- si $a \wedge c = 1$ et $b \wedge c = 1$, alors $(a \cdot b) \wedge c = 1$
- si $a|c$, $b|c$ et $a \wedge b = 1$, alors $(a \cdot b)|c$.

2.4 Équations diophantiennes

Définition 3 On appelle ***équation diophantienne***, toute équation à inconnues entières.

Méthode : Comment résoudre une équation diophantienne $a \cdot x + b \cdot y = c$?

Pour résoudre, regarder d'abord si c est multiple de $a \wedge b$:

▶ si c non multiple, aucune solution

▶ si c multiple de $a \wedge b$:
- diviser l'équation par $a \wedge b$: $a' \cdot x + b' \cdot y = c'$ avec $a' \wedge b' = 1$
- trouver une solution particulière (x_0, y_0) par l'algorithme d'Euclide
- utiliser le théorème de Gauss dans $a'(x - x_0) = -b'(y - y_0)$ pour écrire : $x = x_0 - kb'$ et $y = y_0 + ka'$, avec k un entier
- vérifier que ces solutions marchent.

Exemple 5 Résoudre les équations d'inconnue $(x, y) \in \mathbb{Z}^2$:
- $23x - 57y = 100$
- $21x + 98y = 14$.

3 Nombres premiers

3.1 Définition, première caractérisation

Définition 4 On appelle ***nombre premier***, tout entier supérieur ou égal à 2 irréductible dans l'anneau $(\mathbb{Z}, +, \times)$. Autrement dit, un nombre premier est un entier $p \geqslant 2$ vérifiant la condition suivante :

$$\forall (a, b) \in \mathbb{Z}^2, \quad p = a \cdot b \Longrightarrow \Big[a = \pm 1 \text{ ou } b = \pm 1\Big].$$

Un nombre entier p est premier si ses seuls diviseurs positifs sont 1 et p.

Méthode : Comment montrer qu'un nombre est premier ?

Pour montrer que n est premier :

- ▶ tester si aucun entier entre 2 et $\sqrt{n}$ ne divise n
- ▶ tester la parité, la preuve par 3, 5, 11

Exemple 6 Parmi les nombres suivants, y a-t-il des nombres premiers ? 2, -5, 1, 119, 123456789, 235415, 2912356547177.

Proposition 4 Soit n un entier supérieur ou égal à 2. Alors, il existe un nombre premier p divisant n.

Proposition 5 Soit p un nombre premier. Alors, pour tout $n \in \mathbb{Z}$, le nombre p ne divise pas n si et seulement si $p \wedge n = 1$.

Proposition 6 • Soit p un nombre premier divisant un produit d'entiers $a_1 \times \cdots \times a_n$. Alors, l'entier p divise au moins l'un des termes $a_1, \cdots, a_n$.
• Soit p un nombre premier divisant un produit $p_1 \times \cdots \times p_n$ de nombres premiers. Alors, le nombre premier p est égal à l'un des nombres premiers $p_1, \cdots, p_n$.

3.2 Infinité des nombres premiers

Proposition 7 L'ensemble des nombres premiers est infini.

Remarque 2 Le nombre $2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 59 \times 509$ n'est pas premier.

3.3 Décomposition en facteurs premiers

Théoréme 4 Pour tout entier $n \geqslant 2$, il existe une liste de nombres premiers, unique à ordre près $(p_1, p_2, \cdots, p_r)$ telle que :

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

Cette décomposition s'appelle la ***décomposition en facteurs premiers*** de l'entier n.
En rangeant les facteurs premiers égaux, on peut écrire la factorisation comme suit :

$$n = \pi_1^{\alpha_1} \cdots \pi_s^{\alpha_s},$$

avec les nombres premiers $\pi_1, \cdots, \pi_s$ tous différents et les exposants $\alpha_1, \cdots, \alpha_s$ dans $\mathbb{N}^*$.

Définition 5 • On dit qu'une famille de complexes $(\lambda_i)_{i\in I}$ est ***à support fini*** ou est une ***famille presque nulle*** si l'ensemble $J = \left\{i \in I \mid \lambda_i \neq 0\right\}$ est fini.
• Soit $n \in \mathbb{N}^*$. En notant $\mathscr{P}$ l'ensemble infini des nombres premiers, il existe une seule famille $(\alpha_p)_{p\in\mathscr{P}}$ à support fini telle que

$$n = \prod_{p\in\mathscr{P}} p^{\alpha_p}.$$

Pour tout nombre premier p, on appelle ***p-valuation de*** n, l'exposant $\alpha_p \in \mathbb{N}$. Cette p-valuation est notée $\nu_p(n)$. Cette p-valuation est nulle si et seulement si p ne divise pas n, si et seulement si $p \wedge n = 1$.

Exemple 7 • Si n et m sont deux entiers dans $\mathbb{N}^*$, comment exprimer à l'aide des valuations le fait qu'ils soient premiers entier eux ? le fait que n divise m ? le fait que n soit un carré parfait ?
- Proposer une nouvelle démonstration pour le théorème de Gauss.
- Le nombre $\sqrt{54}$ est-il rationnel ?

Méthode : Comment calculer facilement le pgcd ou ppcm de deux nombres ?

Si a et b sont deux entiers donnés sous forme factorisée, pour calculer le pgcd
- ▶ prendre un premier dans la liste des diviseurs premiers de a ou de b
- ▶ prendre le minimum des deux exposants dans les deux listes (si le premier n'apparaît pas dans une liste, l'exposant est nul).
- ▶ refaire la même chose avec tous les nombres premiers des deux listes de diviseurs
- ▶ faire le produit de ces premiers portés à l'exposant minimum : on obtient le pgcd. Pour le ppcm, refaire la même chose en remplaçant « *minimum* » par « *maximum* ».

  Pour savoir si a et b sont premiers entre eux, regarder si les deux listes de diviseurs n'ont aucun premier commun.

Exemple 8 Si a et b sont dans $\mathbb{N}^*$, simplifier $(a \wedge b) \times (a \vee b)$.

4 Anneaux $\mathbb{Z}/n\mathbb{Z}$

4.1 Construction d'une relation d'équivalence

Proposition 8 Soit $n \geqslant 2$ un entier. On définit sur $\mathbb{Z}$ la relation de congurence modulo n :

$$\forall (p,q) \in \mathbb{Z}^2,\ p\mathscr{R}q \Longleftrightarrow n \text{ divise } p-q.$$

La relation $\mathscr{R}$ ainsi définie est une relation d'équivalence et pour tout $p \in \mathbb{Z}$, la classe d'équivalence $\overline{p}$ de l'entier p modulo $\mathscr{R}$ est :

$$\overline{p} = p + n\mathbb{Z}.$$

On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble quotient des classes d'équivalence.
On a l'égalité :

$$\mathbb{Z}/n\mathbb{Z} = \left\{\overline{0}, \overline{1}, \cdots, \overline{n-1}\right\}$$

et l'ensemble $\mathbb{Z}/n\mathbb{Z}$ compte exactement n classes d'équivalence.

4.2 Structure d'anneau

Proposition 9 Soit $n \geqslant 2$ un entier. On définit deux lois de composition interne sur l'ensemble $\mathbb{Z}/n\mathbb{Z}$:

- une addition :
$$\forall(\overline{p},\overline{q}) \in (\mathbb{Z}/n\mathbb{Z})^2,\ \overline{p}+\overline{q} = \overline{p+q}$$
- une multiplication :
$$\forall(\overline{p},\overline{q}) \in (\mathbb{Z}/n\mathbb{Z})^2,\ \overline{p}\times\overline{q} = \overline{p\times q}.$$

L'ensemble $\mathbb{Z}/n\mathbb{Z}$ muni de ces deux lois $+$ et $\times$ forme un anneau commutatif.

4.3 Propriétés de l'anneau $\mathbb{Z}/n\mathbb{Z}$

Proposition 10 Soit $n \geqslant 2$ un entier. Les trois assertions suivantes sont équivalentes :

- l'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps
- l'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre
- l'entier n est un nombre premier.

Exemple 9 • Déterminer tous les inverses des éléments de $(\mathbb{Z}/7\mathbb{Z})^*$.

- [petit théorème de Fermat] Soit n un nombre premier. Pour tout entier a,
$$a \wedge n = 1 \Longrightarrow a^{n-1} \equiv 1\ [n].$$