

MPSI 2  
Programme des colles de mathématiques.  
Semaine 5 : du lundi 4 novembre au vendredi 8.

**Liste des questions de cours**

- 1°) Présenter la construction de  $\mathbb{Z}$  en tant qu'ensemble quotient de  $\mathbb{N}^2$  par une certaine relation d'équivalence. Expliquer comment on définit l'addition.
- 2°) Décrire les sous-groupes de  $\mathbb{Z}$ , en justifiant.
- 3°) Lorsque  $B$  est une partie de  $\mathbb{Z}$ , préciser quels sont les éléments de  $Gr(B)$ , le groupe engendré par  $B$ , en justifiant.
- 4°) Montrer que  $p$  est premier ssi  $p$  est premier avec tout nombre premier contenu dans  $\llbracket 2, \sqrt{p} \rrbracket$ . Présenter le crible d'Ératosthène (sans justifications supplémentaires).
- 5°) Montrer que  $\mathbb{P}$  est de cardinal infini.
- 6°) Donner la définition du PGCD  $a \wedge b$  de deux entiers relatifs, puis montrer que  $a \wedge b = \inf_{\{ |a|, |b| \}}$ .
- 7°) Démontrer l'associativité du PGCD et la distributivité de la multiplication par rapport au PGCD.
- 8°) Démontrer les théorèmes de Bézout et de Gauss.
- 9°) Montrer que, pour tout  $a, b \in \mathbb{Z}$ ,  $|ab| = (a \wedge b)(a \vee b)$ .
- 10°) Énoncer et démontrer le théorème fondamental de l'arithmétique.
- 11°) Présenter l'algorithme d'Euclide pour le calcul du PGCD et pour le calcul de coefficients de Bézout de deux entiers premiers entre eux.
- 12°) Résoudre l'équation de Bézout  $au + bv = c$  en l'inconnue  $(u, v) \in \mathbb{Z}^2$ .

**Les thèmes de la semaine**

**Remarque.** L'arithmétique est pour le moment présentée sans  $\mathbb{Z}/n\mathbb{Z}$ . On admet (temporairement) le petit théorème de Fermat.

**1 Relations d'ordre, relations d'équivalence**

En révision.

## 2 Les entiers relatifs

### 2.1 Construction de $\mathbb{Z}$

Addition et multiplication, ordre sur  $\mathbb{Z}$ , valeur absolue, inégalité triangulaire.

**Propriété.** Toute partie non vide majorée de  $\mathbb{Z}$  possède un maximum.  
Toute partie non vide minorée de  $\mathbb{Z}$  possède un minimum.

**Propriété.**  $\mathbb{Z}$  est un anneau intègre.  
Exemple d'anneau non intègre.

### 2.2 Les sous-groupes de $\mathbb{Z}$

Division euclidienne dans  $\mathbb{Z}$ .

Définition d'un sous-groupe de  $\mathbb{Z}$ .

Les sous-groupes de  $(\mathbb{Z}, +)$  sont exactement les  $n\mathbb{Z}$ , où  $n \in \mathbb{N}$ .

Intersection de sous-groupes de  $\mathbb{Z}$ .

Définition du sous-groupe engendré par une partie de  $\mathbb{Z}$ .

$$Gr(B) = \left\{ \sum_{i=1}^n a_i b_i / n \in \mathbb{N}, (a_1, \dots, a_n) \in \mathbb{Z}^n, (b_1, \dots, b_n) \in B^n \right\}.$$

### 2.3 Divisibilité

Si pour tout  $i \in \{1, \dots, p\}$ ,  $b \mid a_i$ , alors  $b \mid \sum_{i=1}^p c_i a_i$ . Si  $b \mid a$  et  $d \mid c$ , alors  $bd \mid ac$ .

Pour tout  $(a, b) \in \mathbb{Z}^2$ ,  $a \mid b \iff b\mathbb{Z} \subseteq a\mathbb{Z}$ .

$a$  et  $b$  sont premiers entre eux si et seulement si les seuls diviseurs communs de  $a$  et  $b$  sont 1 et  $-1$ .  
Famille de  $n$  entiers deux à deux premiers entre eux ou bien globalement premiers entre eux.

Si  $p \in \mathbb{P}$  et  $a \in \mathbb{Z}$ , alors ou bien  $p \mid a$ , ou bien  $p$  et  $a$  sont premiers entre eux.

$p$  est premier ssi  $p$  est premier avec tout nombre premier contenu dans  $\llbracket 2, \sqrt{p} \rrbracket$ .

Crible d'Ératosthène.

$\mathbb{P}$  est de cardinal infini.

### 2.4 Congruence

Relation de congruence modulo  $k$ , lien avec la division euclidienne par  $k$ .

Compatibilités de la congruence avec l'addition et la multiplication.

Petit théorème de Fermat (admis pour le moment).

### 2.5 PGCD

Soit  $(a, b) \in \mathbb{Z}^2$ . le PGCD de  $a$  et  $b$  (noté  $a \wedge b$ ) est l'unique  $d \in \mathbb{N}$  tel que  $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ .  
Pour la relation d'ordre de divisibilité dans  $\mathbb{N}$ ,  $a \wedge b = \inf_{\mid} \{|a|, |b|\}$ .

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

Généralisation au PGCD d'une famille de  $n$  entiers relatifs, au PGCD d'une partie de  $\mathbb{Z}$ .

**Propriété.** Soit  $k \in \mathbb{N}$ ,  $a_1, \dots, a_k \in \mathbb{Z}$  et  $h \in \{1, \dots, k\}$ .

— Commutativité du PGCD :

$PGCD(a_1, \dots, a_k)$  ne dépend pas de l'ordre de  $a_1, \dots, a_k$ .

- Associativité du PGCD :  
 $PGCD(a_1, \dots, a_k) = PGCD(a_1, \dots, a_h) \wedge PGCD(a_{h+1}, \dots, a_k)$ .
- Distributivité de la multiplication par rapport au PGCD : pour tout  $\alpha \in \mathbb{Z}$ ,  
 $PGCD(\alpha a_1, \dots, \alpha a_k) = |\alpha| PGCD(a_1, \dots, a_k)$ .

## 2.6 PPCM

Soit  $(a, b) \in \mathbb{Z}^2$ . Le PPCM de  $a$  et  $b$  (noté  $a \vee b$ ) est l'unique entier naturel  $m$  tel que  $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$ .  
 Alors  $a \vee b = \sup\{|a|, |b|\}$ .

Généralisation au PPCM d'une famille de  $n$  entiers relatifs, au PPCM d'une partie de  $\mathbb{Z}$ .

**Propriété.** Soit  $k \in \mathbb{N}$ ,  $a_1, \dots, a_k \in \mathbb{Z}$  et  $h \in \{1, \dots, k\}$ .

- Commutativité du PPCM :  
 $PPCM(a_1, \dots, a_k)$  ne dépend pas de l'ordre de  $a_1, \dots, a_k$ .
- Associativité du PPCM :  
 $PPCM(a_1, \dots, a_k) = PPCM(a_1, \dots, a_h) \vee PPCM(a_{h+1}, \dots, a_k)$ .
- Distributivité de la multiplication par rapport au PPCM :  
 pour tout  $\alpha \in \mathbb{Z}$ ,  $PPCM(\alpha a_1, \dots, \alpha a_k) = |\alpha| PPCM(a_1, \dots, a_k)$ .

## 2.7 Les théorèmes de l'arithmétique

Théorème de Bézout.

Si  $(a, b) \in \mathbb{Z}^2$ , il existe  $(a', b') \in \mathbb{Z}^2$ , avec  $a'$  et  $b'$  premiers entre eux, tel que  $a = a'd$  et  $b = b'd$ .

Théorème de Gauss.

Si  $p \mid ab$  et si  $p$  est premier, alors  $p \mid a$  ou  $p \mid b$ .

**Propriété.** Soit  $(a, b, c) \in \mathbb{Z}^3$ ,  $n \in \mathbb{N}^*$  et  $a_1, \dots, a_n \in \mathbb{Z}$ .

- ◇ Si  $a \wedge b = a \wedge c = 1$ , alors  $a \wedge bc = 1$ .
- ◇ Si  $a \mid b$ ,  $c \mid b$  et  $a \wedge c = 1$  alors  $ac \mid b$ .
- ◇  $|ab| = (a \wedge b)(a \vee b)$ .

**Théorème fondamental de l'arithmétique.** Pour tout  $a \in \mathbb{N}^*$ , il existe une unique famille presque nulle d'entiers naturels  $(\nu_p)_{p \in \mathbb{P}} \in \mathbb{N}^{(\mathbb{P})}$  telle que  $a = \prod_{p \in \mathbb{P}} p^{\nu_p}$ .

Si  $a = \prod_{p \in \mathbb{P}} p^{\nu_p}$  et  $b = \prod_{p \in \mathbb{P}} p^{\mu_p}$ , Alors  $a \mid b \iff [\forall p \in \mathbb{P}, \nu_p \leq \mu_p]$ .

De plus,  $a \wedge b = \prod_{p \in \mathbb{P}} p^{\min(\nu_p, \mu_p)}$  et  $a \vee b = \prod_{p \in \mathbb{P}} p^{\max(\nu_p, \mu_p)}$ .

**Lemme d'Euclide :** Si  $r$  est le reste de la division euclidienne de  $a$  par  $b$ , alors  $a \wedge b = b \wedge r$ .

**Algorithme d'Euclide** pour le calcul du PGCD et pour le calcul de coefficients de Bézout de deux entiers premiers entre eux.

**Exercice.** Équation de Bézout  $au + bv = c$  en l'inconnue  $(u, v) \in \mathbb{Z}^2$ .

## Prévisions pour la semaine prochaine :

$\mathbb{Q}$  et  $\mathbb{R}$ .