MPSI1 – Programme de colles
Semaine 11 – du 11 au 15 décembre 2023

Arithmétique dans l'ensemble des entiers relatifs

L'objectif de cette section est d'étudier les propriétés de la divisibilité des entiers et des congruences. L'approche préconisée reste élémentaire en ce qu'elle ne fait pas appel au langage des structures algébriques.

CONTENUS	CAPACITÉS & COMMENTAIRES
a) Divisibilité et division euclidienne	
Divisibilité dans $\mathbb{Z}$, diviseurs, multiples. Théorème de la division euclidienne.	Caractérisation des couples d'entiers associés.
b) PGCD et algorithme d'Euclide	
PGCD de deux entiers naturels dont l'un au moins est non nul.	Notation $a \wedge b$. Le PGCD de a et b est défini comme étant le plus grand élément (pour l'ordre naturel dans $\mathbb{N}$) de l'ensemble des diviseurs communs à a et b.
Algorithme d'Euclide.	L'ensemble des diviseurs communs à a et b est égal à l'ensemble des diviseurs de $a \wedge b$. $a \wedge b$ est le plus grand élément (au sens de la divisibilité) de l'ensemble des diviseurs communs à a et b. Pour $k \in \mathbb{N}^*$, PGCD de ka et kb.
Extension au cas de deux entiers relatifs.	
Relation de Bézout.	Détermination d'un couple de Bézout par l'algorithme d'Euclide étendu.
PPCM.	Notation $a \vee b$.
c) Entiers premiers entre eux	
Couple d'entiers premiers entre eux. Théorème de Bézout. Lemme de Gauss. Si a et b sont premiers entre eux et divisent n, alors ab divise n. Si a et b sont premiers à n, alors ab est premier à n. PGCD d'un nombre fini d'entiers, relation de Bézout. Entiers premiers entre eux dans leur ensemble, premiers entre eux deux à deux.	Forme irréductible d'un rationnel.
d) Nombres premiers	
Nombre premier. L'ensemble des nombres premiers est infini. Existence et unicité de la décomposition d'un entier naturel non nul en produit de nombres premiers.	Crible d'Ératosthène.
Pour p premier, valuation p-adique. Valuation p-adique d'un produit.	Notation $v_p(n)$. Caractérisation de la divisibilité en termes de valuations p-adiques. Expressions du PGCD et du PPCM à l'aide des valuations p-adiques.
e) Congruences	
Relation de congruence modulo un entier sur $\mathbb{Z}$. Opérations sur les congruences : somme, produit. Utilisation d'un inverse modulo n pour résoudre une congruence modulo n. Petit théorème de Fermat.	Notation $a \equiv b\ [n]$. Les anneaux $\mathbb{Z}/n\mathbb{Z}$ sont hors programme.

Programme de cette colle :

— cours d'arithmétique.

— exercices d'arithmétique.

Exemples de questions de cours

1. Théorème de la division euclidienne (dans $\mathbb{N}$).
2. Relation de Bézout.
3. Théorème de Bézout.
4. Existence/unicité de la forme irréductible d'un rationnel.
5. Algorithme d'Euclide.
6. Théorème(s) de Gauss.
7. L'ensemble des nombres premiers est infini.
8. Définition et caractérisation de la valuation p-adique.
9. Existence de la décomposition en facteurs premiers. L'unicité est + pénible à écrire.
10. Petit théorème de Fermat.