MPSI1 – Programme de colles
Semaine 10 – du 1$^{\text{er}}$ au 5 décembre 2025

Arithmétique dans l'ensemble des entiers relatifs

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. Algorithme d'Euclide.	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. 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.	Forme irréductible d'un rationnel.
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.	
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 sur l'arithmétique.
- exercices sur l'arithmétique. Éventuellement, si vous le souhaitez, des révisions sur les suites en dernière partie de colle.

Exemples de questions de cours

1. Théorème de la division euclidienne dans $\mathbb{N}$.
2. Relation de Bézout.
3. Théorèmes de Bézout et de Gauss (en admettant la relation).
4. Si $(a, b) \in (\mathbb{N}^*)^2$, alors $ab = (a \wedge b)(a \vee b)$.
5. L'ensemble des nombres premiers est infini.
6. Valuation p-adique : bonne définition, et valuation d'un produit.
7. $a \wedge b = \prod_{p \in \mathbb{P}} p^{\min(v_p(a), v_p(b))}$
8. Petit théorème de Fermat.