Colle 14

Les questions "★ " sont avec un développement (démonstration, exemple, exercice).

Extrait du programme

1. 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.

a. Divisibilité et division euclidienne

Divisibilité dans $\mathbb{Z}$, diviseurs, multiples.	Caractérisation des couples d'entiers associés.
Théorème de la division euclidienne.	

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.	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 premiers 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.	Crible d'Eratosthène.
L'ensemble des nombres premiers est infini.	
Existence et unicité de la décomposition d'un entier naturel non nul en produit de nombres premiers.	
Pour p premier, valuation p-adique.	Notation $v_p(n)$.
Valuation p-adique d'une produit.	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 $\mathbb{Z}$.	Notation $a \equiv b [n]$.
Opérations sur les congruences : somme, produit.	Les anneaux $\mathbb{Z}/n\mathbb{Z}$ sont hors programme.
Utilisation d'un inverse modulo n pour résoudre une congruence modulo n.	
Petit théorème de Fermat.	

Méthodes et savoir-faire

- Calculer un PGCD, un PPCM, une relation de Bezout
- Travailler avec des congruences
- Travailler avec les valuations p-adiques

Questions de cours

➜ Relation de divisibilité, relation de congruence, propriétés (spécifier l'implication qui est un corollaire de théorème de Gauss - cas d'un facteur inversible modulo n)

★ Nombres premiers. Établir que $\mathbb{P}$ est infini.
Décrire le crible d'Eratosthène et préciser la propriété fondatrice.

➜ PGCD (pour deux entiers, pour une famille d'entiers). Propriétés.
Division euclidienne. Algorithme d'Euclide.

★ Définir une relation de Bezout pour deux entiers. Décrire l'algorithme d'Euclide étendu.
Résoudre le lemme chinois suivant :

$$\begin{cases} x \equiv 3\ [15] \\ x \equiv 7\ [23] \end{cases}$$

★ Montrer que les diviseurs communs de a et b sont les diviseurs de $a \wedge b$:

$$\mathrm{Div}(a) \cap \mathrm{Div}(b) = \mathrm{Div}(a \wedge b)$$

➜ Entiers premiers entre eux (dans leur ensemble, deux à deux).
Théorème de Bézout. Théorème de Gauss. Corollaires sur la congruence, la divisibilité et le produit.

★ Énoncer le théorème de Gauss. Établir l'unicité de la forme irréductible d'un rationnel.

➜ PPCM. Propriétés.

★ Montrer que $a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z} = \left(\dfrac{|ab|}{a \wedge b}\right)\mathbb{Z}$

➜ Valuation p-adique et ses propriétés : additivité, factorisation première, divisibilité, PGCD, PPCM.

★ Petit théorème de Fermat (avec son lemme).

★ Énoncer le petit théorème de Fermat (avec son lemme) et montrer que :

(i) pour tout $n \in \mathbb{N}^*$, les diviseurs premiers impairs de $n^2 + 1$ sont congrus à 1 modulo 4 ;

(ii) il existe une infinity de nombre premiers congrus à 1 modulo 4.