

Tous les énoncés du cours (définitions et théorèmes) sont exigibles. En revanche, les seules démonstrations exigibles sont celles des résultats mentionnés au paragraphe « Questions de cours ».

## Chapitre 13 - Arithmétique dans $\mathbb{Z}$

- Diviseurs, multiples, entiers associés. Propriétés de la relation de divisibilité :
  - × caractérisation des entiers associés ;
  - × relation d'ordre sur  $\mathbb{N}$  ;
  - × compatibilité avec les combinaisons linéaires, produits, puissances.
- Relation de congruence modulo un entier, propriétés :
  - × relation d'équivalence sur  $\mathbb{Z}$  ;
  - × compatibilité avec les sommes, produits, puissances ;
  - × multiplication/division par un entier non nul.
- Division euclidienne.
- PGCD, PPCM de deux entiers.
  - × Définitions en lien avec l'ordre usuel sur  $\mathbb{N}$  ;
  - × Algorithme d'Euclide, les diviseurs communs de deux entiers sont ceux de son PGCD ;
  - × Algorithme d'Euclide étendu, relations de Bézout ;
  - × Propriétés du PGCD (associativité et factorisation par un diviseur commun).
- Extension à une famille finie d'entiers de la notion de PGCD et de ses propriétés.
- Entiers premiers entre eux dans leur ensemble/deux à deux.
  - × Théorème de Bézout, théorème de Gauss, division dans les congruences.
  - × Forme irréductible d'un rationnel.
- Propriétés du PPCM.
- Nombres premiers, lemme d'Euclide, infinité de l'ensemble des nombres premiers.
- Crible d'Ératosthène.
- Valuation  $p$ -adique d'un entier non nul :
  - × additivité ;
  - × théorème de décomposition primaire ;
  - × caractérisation de la divisibilité via les valuations  $p$ -adiques ;
  - × expressions alternatives du PGCD et du PPCM.
- Petit théorème de Fermat.

## Questions de cours

- Exposer les énoncés relatifs à n'importe quelle notion du programme de colle.

Les preuves des énoncés suivants sont exigibles.

- La divisibilité est une relation d'ordre sur  $\mathbb{N}$ .
- La relation de congruence modulo un entier est une relation d'équivalence sur  $\mathbb{Z}$ .
- Théorème de division euclidienne.
- Présentation de l'algorithme d'Euclide étendu.
- Expressions alternatives du PGCD et du PPCM via les valuations  $p$ -adiques.
- Petit théorème de Fermat.