Contenus

- Divisibilité dans $\mathbb{Z}$.
- Division euclidienne d'un élément de $\mathbb{Z}$ par un élément de $\mathbb{N}^*$.
- Congruences dans $\mathbb{Z}$. Compatibilité des congruences avec les opérations.
- PGCD de deux entiers. Algorithme d'Euclide.
- Couples d'entiers premiers entre eux.
- Théorème de Bézout.
- Théorème de Gauss.
- Nombres premiers. Leur ensemble est infini.
- Existence et unicité de la décomposition d'un entier en produit de facteurs premiers.
- Petit théorème de Fermat.

Capacités attendues

- Déterminer les diviseurs d'un entier, le PGCD de deux entiers.
- Résoudre une congruence $ax \equiv b\ [n]$. Déterminer un inverse de a modulo n lorsque a et n sont premiers entre eux.
- Établir et utiliser des tests de divisibilité, étudier la primalité de certains nombres, étudier des problèmes de chiffrement.
- Résoudre des équations diophantiennes simples.

Démonstrations

- Écriture du PGCD de a et b sous la forme $ax + by$, $(x,y) \in \mathbb{Z}^2$.
- Théorème de Gauss.
- L'ensemble des nombres premiers est infini.

Exemples d'algorithmes

- Algorithme d'Euclide de calcul du PGCD de deux nombres et calcul d'un couple de Bézout.
- Crible d'Ératosthène.
- Décomposition en facteurs premiers.

Problèmes possibles

- Détermination des racines rationnelles d'un polynôme à coefficients entiers.
- Lemme chinois et applications à des situations concrètes.
- Démonstrations du petit théorème de Fermat.
- Problèmes de codage (codes barres, code ISBN, clé du Rib, code Insee).
- Étude de tests de primalité : notion de témoin, nombres de Carmichaël.
- Problèmes de chiffrement (affine, Vigenère, Hill, RSA).
- Recherche de nombres premiers particuliers (Mersenne, Fermat).
- Exemples simples de codes correcteurs.
- Étude du système cryptographique RSA.
- Détermination des triplets pythagoriciens.
- Étude des sommes de deux carrés par les entiers de Gauss.
- Étude de l'équation de Pell-Fermat.