

1 Arithmétique dans \mathbb{Z}

- a) Divisibilité dans \mathbb{Z} , congruences. Division euclidienne dans \mathbb{Z} , classes de congruence modulo n .
- b) Bases de numérations.
- c) Pgcd de deux entiers : définition, calcul par l'algorithme d'Euclide. Coefficients de Bézout, calcul par l'algorithme d'Euclide amélioré.
- d) Entiers premiers entre eux. Divers résultats classiques, dont le th. de Gauss. Résolution des équations du type $ax + by = c$, d'inconnue $(x, y) \in \mathbb{Z}^2$. Forme irréductible d'un rationnel. Inverse modulo n , condition d'existence.
- e) Ppcm de deux entiers. Lien avec le pgcd.
- f) Généralisation du pgcd, ppcm à plusieurs entiers, entiers premiers entre eux dans leur ensemble, premiers entre eux 2 à 2.
- g) Nombres premiers, l'ensemble des nombres premiers est infini. Décomposition en facteurs premiers. Valuations p -adiques, condition de divisibilité et calcul du pgcd, ppcm à l'aide des décompositions en facteurs premiers.
- h) Petit théorème de Fermat.

Démonstrations à connaître :

- résolution de l'équation $ax + by = c$ d'inconnue $(x, y) \in \mathbb{Z}^2$
- existence de la décomposition primaire d'un entier
- unicité de la décomposition primaire
- petit théorème de Fermat