



# Arithmétique et dénombrement



## Présentation

### Description

Cette UE vise à présenter les concepts élémentaires d'arithmétique et de dénombrement utiles pour le début de la licence en mathématiques.

### Objectifs

#### Dénombrement élémentaire

- \* Cardinal d'un ensemble fini. Cardinal et opérations ensemblistes. Cardinal et applications injectives, surjectives, bijectives. Cardinal d'un ensemble d'applications. Nombre de parties d'un ensemble. Fonction indicatrice.
- \* Introduction aux cardinaux infinis. Bijection entre ensembles. Dénombrabilité. Argument diagonal de Cantor.  $X$  et  $P(X)$  n'ont pas le même cardinal.  $\mathbf{R}$  est indénombrable.
- \* Arrangements, permutations, combinaisons (coefficients binomiaux), triangle de Pascal, formule du binôme.
- \* Formule du crible générale (application au dénombrement des dérangements, des surjections, etc.).
- \* Relation binaire sur un ensemble. Relation d'équivalence, partition en classes d'équivalence, quotient d'un ensemble par une relation d'équivalence (exemples sur des ensembles déjà connus). Relation d'ordre, partiel, total, exemples.
- \* Applications à des exemples de probabilités élémentaires finies (nombre de cas favorables/nombre de cas total)

#### Arithmétique élémentaire dans $\mathbf{Z}$

- \* Nombres entiers, écriture dans une base.
- \* Divisibilité, nombres premiers (infinitude, algorithme du crible). Division euclidienne (algorithme d'Euclide).
- \* PGCD et PPCM. Théorème de Bézout (et algorithme d'Euclide étendu), nombres premiers entre eux, lemme d'Euclide, lemme de Gauss. Équations diophantiennes  $ax + by = c$ . Décomposition en produit de nombres premiers. Application : pour  $n \notin \mathbf{N}$ , est soit un entier soit irrationnel.
- \* Arithmétique modulaire (congruences). Petit théorème de Fermat. Théorème chinois des restes.
- \* Étude de  $\mathbf{Z}/n\mathbf{Z}$ , vu comme anneau. Inversibles,  $\mathbf{Z}/n\mathbf{Z}$  est un corps si et seulement si  $n$  est premier. Réinterprétation du théorème de Bézout. Réinterprétation du petit théorème de Fermat (définition de l'indicatrice d'Euler, théorème d'Euler). Réinterprétation du théorème chinois des restes.
- \* Illustration par la cryptographie.

### Pré-requis nécessaires

Programme de mathématiques du S1 (principalement Raisonnement et théorie des ensembles) et programmes de mathématiques du lycée (à minima spécialité mathématiques de première)

Pré-requis recommandés :

Programme de mathématiques du S1 (principalement Raisonnement et théorie des ensembles) et programmes de mathématiques du lycée (idéalement spécialité



mathématiques de terminale, voire option mathématiques expertes.)

---

## Informations complémentaires

Volumes horaires\* :

CM : 30 h

TD : 30 h

TP : 0

Terrain : 0

## Infos pratiques

---

### Contacts

Responsable pédagogique

Simon MODESTE

☎ 04 67 14 35 80

✉ [simon.modeste@umontpellier.fr](mailto:simon.modeste@umontpellier.fr)