

Arithmétique

#	Niveau d'étude Bac +2	#	Composante Sciences Fondamentales et Appliquées	#	Volume horaire 25.0	#	Période de l'année Semestre 4
---	--------------------------	---	--	---	------------------------	---	-------------------------------------

En bref

- # **Langue(s) d'enseignement:** Français
- # **Méthode d'enseignement:** En présence
- # **Ouvert aux étudiants en échange:** Non

Présentation

Description

Il s'agit d'aborder des notions de base d'arithmétique qui ont une application directe à l'informatique :

- * arithmétique dans \mathbb{Z} : décomposition en facteurs premiers, pgcd, ppcm ;
- * algorithme d'Euclide, théorème de Bézout, lemme de Gauss ;
- * petit théorème de Fermat, congruences, valuation ;
- * calcul modulaire, l'anneau $\mathbb{Z}/n\mathbb{Z}$, le corps $\mathbb{Z}/p\mathbb{Z}$ avec p premier ;
- * théorème chinois (admis) ;
- * applications à l'informatique (par exemple : exponentiation dichotomique modulaire, RSA, etc).

Objectifs

Pour la partie arithmétique.

- * Connaître les notions de base en arithmétique.
- * Appliquer ces notions à des problèmes informatiques.

Heures d'enseignement

Arithmétique - TP	TP	3h
Arithmétique - TD	TD	12h
Arithmétique - CM	CM	10h

Compétences visées

- * Savoir manipuler les notions de bases en arithmétique.
- * Être capable d'appliquer ces notions à des problèmes informatiques.

Infos pratiques

Lieu(x)

Poitiers-Campus