ARITHMÉTIQUE

Le programme concerne les notions les plus utiles à l'informatique. La numération est indispensable aux langages de bas niveau. L'arithmétique modulaire est utile à la cryptographie, aux corrections d'erreurs et plus généralement à de nombreux algorithmes.

CONTENUS	CAPACITÉS ATTENDUES	COMMENTAIRES
Systèmes de numération		
Numération en bases 10, 2 et 16 des entiers et des réels. Conversions entre ces bases.	• Passer de l'écriture d'un nombre dans une base à une autre.	Les nombres négatifs sont précédés du signe moins (–), quelle que soit la base utilisée. On fait le lien entre le calcul binaire et le calcul booléen : les booléens sont alors 1 et 0, interprétés comme signifiant « il y en a, ou pas ».
Notions d'arrondi et de précision.	• Arrondir un entier ou un réel (par défaut, par excès, au plus près…). • Se conformer à un nombre de chiffres significatifs.	On se limite à des cas simples en base 10 et en base 2. On ne fait aucune théorie sur les calculs d'incertitude.
Addition, soustraction, multiplication et division des entiers naturels.	• Calculer à la main : – des additions en bases 2 et 16 ; – des multiplications et des divisions par une puissance de deux, en base 2.	
Arithmétique modulaire		On évite tout excès de technicité en s'efforçant d'utiliser des présentations concrètes.
Division euclidienne : quotient, reste, existence, unicité.		On se limite aux entiers naturels.
Nombres premiers, décomposition en produit de facteurs premiers, entiers premiers entre eux, PGCD de deux entiers.	• Décomposer un entier naturel en produit de facteurs premiers et déterminer tous ses diviseurs. • Mettre en œuvre un algorithme : – de recherche de nombres premiers ; – de décomposition en produit de facteurs premiers.	Aucune technique n'est censée être connue.

Congruences. Compatibilité avec l'addition et la multiplication. Propriété : modulo n, les multiples de a sont les multiples de PGCD(a, n).	• Mener un calcul de congruence modulo n. • Parcourir une liste circulaire par sauts d'amplitude constante	On montre l'efficacité du langage des congruences. On note que le parcours n'est exhaustif que quand la longueur du saut et la taille de la liste sont des entiers premiers entre eux.