Arithmétique

Les problèmes étudiés peuvent notamment être issus de la cryptographie ou relever directement de questions mathématiques, par exemple à propos des nombres premiers.

Exemples de problèmes	Contenus
Problèmes de codage (codes barres, code ISBN, clé du Rib, code Insee Problèmes de chiffrement (chiffrement affine, chiffrement de Vigenère, chiffrement de Hill). Questionnement sur les nombres premiers : infinitude, répartition, tests de primalité, nombres premiers particuliers (Fermat, Mersenne, Carmichaël). Sensibilisation au système cryptographique RSA.	• Divisibilité dans Z. • Division euclidienne. • Congruences dans Z. • PGCD de deux entiers. • Entiers premiers entre eux. • Théorème de Bézout. • Théorème de Gauss. • Nombres premiers. • Existence et unicité de la décomposition en produit de facteurs premiers.

Matrices et suites

Il s'agit d'étudier des exemples de processus discrets, déterministes ou stochastiques, à l'aide de suites ou de matrices. On introduit le calcul matriciel sur des matrices d'ordre 2. Les calculs sur des matrices d'ordre 3 ou plus sont essentiellement effectués à l'aide d'une calculatrice ou d'un logiciel.

Exemples de problèmes	Contenus
Marche aléatoire simple sur un graphe à deux ou trois sommets. Marche aléatoire sur un tétraèdre ou sur un graphe à N sommets avec saut direct possible d'un sommet à un autre : à chaque instant, le mobile peut suivre les arêtes du graphe probabiliste ou aller directement sur n'importe quel sommet avec une probabilité constante p. Etude du principe du calcul de la pertinence d'une page web. Modèle de diffusion d'Ehrenfest : N particules sont réparties dans deux récipients ; à chaque instant, une particule choisie au hasard change de récipient. Modèle proie prédateur discrétisé : - évolution couplée de deux suites récurrentes ; - étude du problème linéarisé au voisinage du point d'équilibre.	• Matrices carrées, matrices colonnes : opérations. • Matrice inverse d'une matrice carrée. • Exemples de calcul de la puissance n-ième d'une matrice carrée d'ordre 2 ou 3. • Écriture matricielle d'un système linéaire. • Suite de matrices colonnes (U_n) vérifiant une relation de récurrence du type $U_{n+1} = AU_n + C$: - recherche d'une suite constante vérifiant la relation de récurrence ; - étude de la convergence. • Étude asymptotique d'une marche aléatoire.

Activités découvertes	Thèmes étudiés	Chapitres associés	TP ou devoir en temps libre	compléments
Codes barres	division par 10, division euclidienne, divisibilité, (apll : numération en différentes bases)	1) Divisibilité dans Z 2) Division euclidienne et congruences	Clés de contrôle (ISBN, INSEE, codes barres, RIB) Ruban de pascal	Numération Code sécurité sociale Métiers de la cryptographie Générateur de nombres aléatoires (GLC)
Calendriers (transmath p8,p18)	congruence et critère de divisibilité (apl : n° insee, preuve par 9, puissance d'un entier modulo n, chiffrement affine et de Hill)		Triplets pythagoriciens, calendriers, Chiffrement (affine, Vigenère)	
Vacances de la Toussaint				
Découverte des tableaux de nombres (fichier : mat_act1) Matrices et coordonnées	Graphes et matrices (lectures et écritures)	3) Matrices carrées, évolution de processus (1)	Marches aléatoires, matrices de transition, graphes	Traitement de l'image
Marche aléatoire sur un segment (	somme, produit et puissance de matrices		Transformation géométriques de figures	
Vacances de Noël				
pb d'optimisation	pgcd	4) PGCD, 5) th. de Bézout, Th. de Gauss	Algorithme d'Euclide Pixellisation	Pixellisation
Sablier Points a coordonées entières Chiffrement affine	nombres premiers entre eux, th de Bachet de Méziriac Th de Gauss		Recherche des coefficients de Bézout Algorithme d'Euclide (dé)chiffrement (affine, Vigenère) Chiffrement de Hill	Equations diophantiennes
Vacances d'hiver				
Etude d'une page web, traitement de l'image	Matrices, inverse et systèmes	5) Matrices carrées, évolution de processus(2)	Interprétation géométrique de la résolution de systèmes Chiffrement de Hill	
Nombre de Matyasevich (hyp p64) :nombre de diviseurs d'un entier, nombres de Fermat, nombres premiers	Nombres premiers Décomposition en produit de facteurs premiers	6) Nombres premiers	Primalité d'un entier (algo) Infinitude,répartition, test Nombres premiers particuliers (Fermat, Mersenne, Carmichaël) Système RSA	

<table>
<tr><td colspan="5">Vacances de printemps</td></tr>
<tr><td>étude asymptotique d'une marche aléatoire</td><td>Puissance n-ième d'une matrice carrée
Convergence vers un état stable</td><td rowspan="2">7) Matrices et études asymptotiques de processus discrets.</td><td>Système proies/prédateurs
population de rongeurs</td><td>Notion de bouchons</td></tr>
<tr><td>Part de marché</td><td>Suite de matrices colonnes</td><td>Urnes d'Ehrenfest</td><td></td></tr>
</table>

Soit 28 semaines de cours et 2 semaines réservées aux BB.