

Préparation des oraux

Présentation générale des leçons d'arithmétique

Jean-François Culus

14 avril 2016

- 12. Multiples, diviseurs, division euclidienne
- 13. PGCD, égalité de Bézout
- 14. Nombres premiers, décomposition d'un entier en produit de facteurs premiers
- 15. Congruences dans $\mathbb{Z}$

L'enseignement de spécialité prend appui sur la résolution de problèmes. Cette approche permet une introduction motivée des notions mentionnées dans le programme. Plusieurs exemples de problèmes sont donnés à titre indicatif. L'étude des situations envisagées dans le cadre de cet enseignement conduit à un travail de modélisation et place les élèves en position de recherche. Les thèmes abordés sont particulièrement propices à l'utilisation des outils informatiques (logiciels de calcul, tableur) et à la mise en oeuvre d'algorithmes. Le niveau d'approfondissement des notions est guidé par les besoins rencontrés dans la résolution des problèmes traités.

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

Distinction Outil numérique vs. Algorithmique / Programmation

Deux points de vue de l'informatique : outil ou objet d'étude.

- **Outils** Utilisation de logiciel pour conjecturer, illustrer, représenter, modéliser ...
- **Objet d'étude** Production d'algorithme pour résoudre un problème.

Exemple : Faire un algorithme qui en entrée : Somme, en sortie : Nombre minimum de pièces (euros) pour atteindre cette somme.

Changement de paradigme maths / info : passage de résolution d'un problème vers trouver une méthode de résolution de ce type de problème.

Exemples de problèmes

Problèmes de codage (codes barres, code ISBN, clé du RIB, code INSEE)

Problème 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, Carmichael)

Sensibilisation au système cryptographique RSA.

Contenus

- Divisibilité dans $\mathbb{Z}$
- Division euclidienne
- Congruence dans $\mathbb{Z}$
- 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.

- **Codage (Larousse)** Action de coder un texte, des données informatiques ; chiffrement, encodage
- **Codage (informatique)** Ensemble de règles définissant une correspondance biunivoque entre des informations et leur représentation par des caractères, des symboles ou des éléments de signal.
- **Chiffrement (Larousse)** Opération qui consiste à transformer un message à transmettre, dit *message clair*, en un autre message, inintelligible pour un tiers, dit *message chiffré*, en vue d'assurer le secret de sa transmission
- **Cryptographie (Wikipedia)** discipline s'attachant à protéger des messages (assurant confidentialité, authenticité et intégrité) en s'aidant souvent de secrets ou clés.

- **Algorithme (Wikipedia)** Un algorithme est une suite finie et non ambiguë d'opérations ou d'instructions permettant de résoudre un problème ou d'obtenir un résultat.

Le mot algorithme vient du nom latinisé du mathématicien perse Al-Khawarizmi. On retrouve aujourd'hui des algorithmes dans de nombreuses applications telles que le fonctionnement des ordinateurs, la cryptographie, la planification et l'utilisation optimale des ressources, le traitement d'images, ...

- **Dans les programmes (TS)**

Suite majorée, minorée, bornée. Des activités algorithmiques sont menées dans ce cadre. Approx de Π , e , ...

T.V.I : Des activités algorithmiques sont réalisées dans le cadre de la recherche de solutions de $f(x) = k$.

Conditionnement et indépendance : Des activités algorithmiques sont réalisées dans le cadre, notamment pour simuler une marche aléatoire

Le programme de Spécialité TS

- résolution de problème
- travail de modélisation et place les élèves en position de recherche
- propices à l'utilisation des outils informatiques (logiciels de calcul, tableur) et à la mise en oeuvre d'algorithmes.
- motiver les notions via des problèmes concrets (modélisation)
- problèmes ouverts & avec prise d'initiative
- aspect algorithmiques / programmation

Les notions :

- ① Multiples / diviseurs
- ② division euclidienne dans $\mathbb{N}$, dans $\mathbb{Z}$,
- ③ Congruence
- ④ Pgcd, nombres premiers entre eux, Bézout
- ⑤ Nombres premiers, décomposition d'un entier en produit de facteurs premiers

Attention : Distinguer entiers (naturels $\neq$ relatifs).

L'algorithmique dans le programme de TS

En seconde, les élèves ont conçu et mis en oeuvre quelques algorithmes. Cette formation se poursuit tout au long du cycle terminal. Dans le cadre de cette activité algorithmique, les élèves sont entraînés à :

- décrire certains algorithmes en langage naturel ou dans un langage symbolique ;
- en réaliser quelques-uns à l'aide d'un tableur ou d'un programme sur calculatrice ou avec un logiciel adapté ;

L'algorithmique dans le programme de TS

Aucun langage, aucun logiciel n'est imposé. L'algorithmique a une place naturelle dans tous les champs des mathématiques et les problèmes posés doivent être en relation avec les autres parties du programme (analyse, géométrie, statistiques et probabilités, logique) mais aussi avec les autres disciplines ou le traitement de problèmes concrets. À l'occasion de l'écriture d'algorithmes et de programmes, il convient de donner aux élèves de bonnes habitudes de rigueur et de les entraîner aux pratiques systématiques de vérification et de contrôle.