Projets d'algorithmique

Option maths expertes - Lycée du parc

Année 2020-2021

Organisation pratique :

Le travail proposé sera réalisé en groupe de 3 et aura pour but de produire :

— Un texte exposant le problème abordé (en le localisant dans l'histoire des mathématiques, s'il y a lieu [1]) et comportant l'énoncé des différentes définitions et propriétés utiles, éventuellement assorties de leurs démonstrations si celles-ci sont accessibles au niveau de la terminale.

— Un programme **fonctionnel** écrit en python qui résoudra le problème posé, il sera rendu sous forme informatique (envoyé par mail) et on fournira aussi une version imprimée de son code à laquelle on joindra un jeux de test montrant son fonctionnement sur quelques exemples.

Les élèves présenteront par groupe en 20 minutes leur travail. Après sa présentation, chaque groupe devra assister aux deux présentations suivantes (ou plus) et les derniers sur le planing seront le « public » des premiers sur le même principe. À l'issue de la soutenance, une note comptant pour le troisième trimestre sera attribuée.

Remarques :

Les élèves ont l'initiative des groupes **sauf si ça se passe mal.**

La rédaction devra être entièrement originale, tout plagiat sera sanctionné par la note 0.

La liste des sujets

Pour chaque sujet on donne :

— Une courte introduction à la question abordée,

— une liste de références utiles,

— une description aussi claire que possible de la production demandée.

Remarque : Un groupe peut proposer un sujet hors de la liste mais il sera refusé s'il est jugé inadapté.

1. Exponentiation rapide et implémentation du système de cryptographie RSA. $(***)$

   On exposera l'algorithme d'exponentiation rapide ainsi que les principes du système RSA. La partie mathématique devra comporter des démonstrations.

   Le programme réalisé devra permettre de coder (respectivement décoder) un texte à l'aide de clefs publiques (respectivement privées) données par l'utilisateur, on ne cherchera pas à faire intervenir des nombres premiers particulièrement grands.

   Références : Exercice 135 page 91 de votre livre.

   Michel Demazure : Cours d'algèbre (disponible au CDI sous la cote 512 DEM).

   Pierre Wassef : Arithmétique (disponible au CDI sous la cote 512 WAS).

   Sujet très documenté sur Internet.

1. Attention à éviter les trop longs développements dans cette direction, ce travail n'est pas de nature biographique ou historique.

2. Test de primalité et décomposition en facteurs premiers. (∗)

   L'objet principal de ce sujet est de programmer au moins une procédure permettant de tester si un nombre est premier et de l'utiliser ensuite pour une seconde procédure récursive permettant de calculer la décomposition en facteurs premiers d'un entier donné.

   On ajoutera une fonction permettant d'analyser, de manière empirique, la vitesse d'exécution en fonction de la taille de l'entier à factoriser.

   Référence : Sujet documenté sur Internet.

   Michel Demazure : Cours d'algèbre (disponible au CDI sous la cote 512 DEM).

3. Résolution automatique des équations diophantiennes du type $ax + by = c$. (∗∗)

   On explicitera un procédé de résolution de l'équation diophantienne $ax + by = c$ qui envisagera toutes les éventualités pour les nombres a, b et c. Cette partie devra comporter des démonstrations.

   On réalisera ensuite un programme qui prend en entrée les valeurs de a, b et c et qui donnent en sortie l'ensemble des couples solutions de l'équation diophantienne $ax + by = c$. La principale difficulté consiste à n'oublier aucun des différents cas qui peuvent se présenter.

   Référence : Votre cours.

4. Codage par code affine et cryptanalyse fréquentielle. (∗∗)

   On exposera les bases théoriques du procédé de codage affine.

   Un premier programme permettra de coder et décoder un texte relativement court écrit avec 26 lettres par le procédé de codage affine associé à l'application $n \mapsto an + b$ où a et b sont deux nombres choisis par l'utilisateur.

   Un second programme permettra de casser le code sans connaitre la clef de codage par une analyse fréquentielle d'apparition des lettres dans le message codé.

   Références : Exercice 133 page 90 de votre livre.

   Sujet documenté sur Internet.

5. Théorème des nombres premiers, comptage des nombres premiers et « vérification » asymptotique du théorème. (∗∗)

   On exposera le théorème des nombres premiers.

   Le programme réalisé permettra de compter les nombres premiers et ainsi de vérifier le comportement asymptotique de la fonction π. On pourra présenter plusieurs versions du programme mettant en oeuvre différents algorithmes.

   Références : Jean-Paul Delahaye, *Merveilleux nombres premiers*, au CDI sous la cote 510 DEL.

6. Conjecture de Goldbach. (∗)

   On exposera la conjecture de Goldbach.

   Un premier programme permettra de décomposer en somme de deux nombres premiers un nombre pair entré par l'utilisateur.

   Un second programme vérifiera la conjecture de Goldbach aussi loin qu'il fonctionne. On pourra en proposer plusieurs versions.

   Références : Jean-Paul Delahaye, *Merveilleux nombres premiers*, au CDI sous la cote 510 DEL.

   Apostolos Doxiadis, *Oncle Petros et la conjecture de Goldbach* (Roman), cote CDI : 820 DOX.

   Sujet documenté sur Internet.

7. Nombres parfaits et nombres premiers de Mersenne. (∗∗)

On donnera la définition des nombres parfaits et on montrera le théorème d'Euclide sur les nombres parfaits pairs et sa réciproque due à Euler. On indiquera aussi ce qu'il en est du cas des nombres parfaits impairs.

Plusieurs programme sont possibles comme par exemple un programme qui recherche les nombres premiers de Mersenne et un autre qui « vérifierait » aussi loin qu'il fonctionne que les nombres impairs ne sont pas parfaits.

Références : Exercices 3.11 et 3.12 dans *Arithmétique*, Pierre Wassef au CDI sous la cote 512 WAS.

Sujet documenté sur Internet.

8. Postulat de Bertrand et conjecture de Legendre. $(***)$

   On exposera le résultat connu sous l'appellation de postulat de Bertrand. Si on choisit d'en exposer une démonstration celle-ci devra être maitrisée. On exposera la conjecture de Legendre.

   Un premier programme permettra de donner une solution effective au postulat de Bertrand pour des valeurs raisonnables de n. Un second programme fera de même pour la conjecture de Legendre et un troisième pourra vérifier la conjecture de Legendre aussi loin qu'il fonctionne.

   Références : Martin Aigner et Günter M. Ziegler *Raisonnements divins* au CDI sous la cote 510 AIG.

   Sujet documenté sur Internet, (une preuve « facile » au postulat de Bertrand sur Wikipédia.)

9. Système de numération. Conversion automatique d'un système dans un autre. $(*)$

   On exposera le principe des systèmes de numération.

   Le programme réalisé permettra de convertir d'un système de numération vers un autre après avoir défini la base et la valeurs des symboles pris dans $\{0, 1, \ldots, 9, A, B, \ldots, Z\}$.

   On pourra par exemple déterminer la valeur en décimal de son prénom dans le système de numération de base 26 correspondant à l'alphabet.

   Références : Exercice 58 page 21 de votre livre.

   Sujet documenté sur Internet.

10. Test de primalité de Fermat et nombre de Carmichael $(**)$

    On exposera le test de non-primalité de Fermat, son utilisation comme test probabiliste de primalité et le cas des nombres de Carmichael. Si on veux creuser ce dernier sujet on parlera du théorème de Korselt avec éventuellement une démonstration.

    On programmera le test de Fermat que l'on utilisera pour produire des nombres probablement premier.

    Références : Michel Demazure : *Cours d'algèbre* (disponible au CDI sous la cote 512 DEM).

    Sujet documenté sur Internet.

11. Inversion des matrices par la méthode du pivot de Gauss $(**)$

    On définira les matrices de manipulation élémentaire en explicitant leur action sur une matrice lors d'un produit à droite ou à gauche. On exposera ensuite la méthode du pivot de Gauss pour obtenir l'inverse d'une matrice.

    Un programme permettra d'obtenir l'inverse d'une matrice suivant cette méthode de manière automatique.

    Remarque : Pour éviter des problèmes numériques on travaillera avec des fractions.

12. Diagonalisation des matrices 2x2

    Sujet très mathématique.