PROGRAMME DES COURS FONDAMENTAUX

ALGORITHME ET CRYPTOGRAPHIE
(G. ROBIN) :

Algorithme en Théorie des Nombres :
Complexité d'un algorithme, Nombre au hasard, Algorithme de réduction dans un réseau , Factorisation dans Z [X], Evaluation de la fonction ζ et recherche des zéros.

Cryptographie :
Cryptographie à clé secrète : méthodes de susbtitution, de transposition, D.E.S...; Cryptographie à clé publique : méthodes du logarithme discret, R.S.A., sac à dos,...; Authentification de la signature.

PRIMALITE ET FACTORISATION
(J.L. NICOLAS) :

Introduction à la théorie des Nombres :
Approximation rationnelle, symbole de Legendre et de Jacobi, formes quadratiques, fractions continues, courbes elliptiques.

Tests de primalité :
Nombre de Carmichael, suites de Lucas,tests probabilistes.

Algorithmes de factorisation :
Fermat, Lehman, Shanks, des fractions continues, crible quadratique, Schnorr, Lenstra.

OTIMISATION
(S. DOLECKI) :

Programmation différentiable :
Conditions d'optimalité (1er et 2ème ordre), qualification des contraintes, multiplicateurs de Lagrange.

Elèments de programmation non différentiable:
Dérivées unilatérales, conditions d'optimalité du 1er ordre.

Optimisation convexe et convexe généralisée :
Conditions d'optimalité, Lagrangiens augmentés, pénalisation.

Stabilité et existence des solutions :
Semi-continuités, convergences, stabilité (contraintes, optima, valeurs optimales).

Application au calcul des variations et au contrôle optimal :
Fonctionnnelles intégrales, conditions de Euler-Lagrange, principe bang-bang.

OPTIMISATION NUMERIQUE
(C. LEMARECHAL et Ch. MALIVERT) :

Méthodes du 1er et 2ème ordre :

(Gradient, gradient conjugué, quasi-Newton) mise en oeuvre sur ordinateur.

Introduction aux problèmes non différentiables. Méthodes de sous-gradients et de faisceaux. Introduction aux problèmes avec contraintes.

COURS SPECIALISES -

Calcul formel (G. ROBIN, J.P. MASSIAS)

Cartes à mémoire

Programmation discrète (M. VOLLE)

Automates (J.P. BOREL)

Commande optimale (J. BLOT)

Complémentarité (M. THERA)

Schémas multivoques et synthèse des algorithmes
(P. HUARD, Direction des Etudes et Recherche, E.D.F.)

Problèmes d'optimisation numérique de grande taille
(V.H. NGUYEN, F.N.D.P. Namur)

Economie Mathématique
(B. CORNET, Paris 1 ,Panthéon Sorbonne)

UNIVERSITE
DE LIMOGES
Département de
Mathématiques

Cryptographie & Optimisation

D.E.A.

D'INGENIERIE
MATHEMATIQUE

Responsable: J.L. Nicolas
U.F.R. des Sciences
123, Av. A.Thomas
87060 Limoges
Secrétariat : M^me Guerletin
tél: 55 79 46 22