UNIVERSITATEA DIN CRAIOVA Aprobat din anul univ.
Facultatea de matematică şi informatică 2008-2009
Departamentul de matematică
Domeniul fundamental : MATEMATICĂ
Specializarea: MATEMATICĂ INFORMATICĂ
Forma de învăţământ: cursuri de zi
Durata studiilor : 3 ani

FIŞA DISCIPLINEI

Algoritmi în teoria numerelor

Titular curs: Lector.dr. Christina-Theresia Dan

Cod: Mi3506
Ciclul I: LICENŢĂ
Anul III, Semestrul V, Curs 28 ore, Seminar 28 ore
Nr. credite : 5
Domeniul : Matematică
Tip de disciplină : opţională
Categoria formativă : disciplină de specialitate
Obiective : Cunoaşterea proprietăţilor de bază ale congruenţelor şi a posibilităţii lor de aplicare; aplicarea noţiunilor prezentate în rezolvarea unor probleme cu caracter aplicativ; cunoaşterea principalelor probleme dificile din punct de vedere computational şi algoritmii folosiţi în prezent pentru soluţionarea lor; posibilitatea realizării de programe comparative care să permită studierea în paralel a mai multor algoritmi prezentaţi.
Discipline anterioare cerute: Cursurile de: teoria elementară a numerelor, algebră (I, II şi III), programarea calculatoarelor.
Forma de evaluare: Colocviu (C): două probe scrise şi realizarea unui număr de minim 3 programe folosind algoritmii prezentaţi.

Conţinut:

C_1 : *Divizibilitate pe* $\mathbb{N}$ **(**recapitularea principalilor algoritmi**)**: algoritmul lui Euclid de determinare a c.m.m.d.c.-ului a două numere; teorema lui Lamé; algoritmul lui Euclid extins; algoritmul de rezolvare a ecuaţiilor diofantice liniare.

C_2 : *Congruenţe*. Proprietăţi generale. Exponenţiere modulară (metoda ridicării successive la pătrat şi reducerii mod n). Algoritm de rezolvare a congruenţelor liniare şi de determinare a inversului mod n.

C_3 : *Sisteme de congruenţe*. Algoritmul lui Gauss de rezolvare a sistemelor de congruenţe (teorema chinezească a resturilor). Inversa modulo n a unei matrice. Aplicaţii în rezolvarea de sisteme de congruenţe.

C_4 : *Aplicaţii ale congruenţelor*. Factorizarea unor numere de formă particulară. Teste de divizibilitate. Calendarul. Programarea unui turneu.

C_5 : *Index aritmetic*. Definiţie. Proprietăţi. *Exponenţi universali*. Exponent universal minimal $\lambda(n)$ şi ± 1 exponent maximal $\lambda_0(n)$. Definiţii, algoritmi de calcul şi de determinare a unui element de ordin $\lambda(n)$ sau $\lambda_0(n)$. Aplicaţii (metode de generare de numere pseudo-aleatoare, îmbinarea cablurilor telefonice).

C_6 : *Teste de primalitate deterministice*. Căutare de divizori primi prin încercări. Teste $n-1$. Test Pepin. Teste $n+1$. Test Lucas-Lehmer. Algoritmul AKS.

C_7 : *Teste de primalitate probabilistice*. Test Fermat. Algoritm de calcul al simbolului Jacobi. Test Solovay-Strassen. Test Miller-Rabin.

$C_8 – C_9$: *Problema factorizării*. Generalități. Factorizare prin căutare directă . Metoda Fermat. Metoda Pollard-rho. Metoda Pollard p-1. Metoda bazei factor. Metoda fracțiilor continue. Metoda filtrului pătratic. Metoda curbelor eliptice. Filtrul corpului de numere.

$C_{10} – C_{11}$: *Problema logaritmului discret* (DLP). Generalități. Algoritmul Shanks (baby-step giant-step). Algoritmul Silver-Pohlig-Hellman. Algoritmul Pollard-rho. Algoritmul index-calculus (pentru determinarea log discret în corpuri finite).

C_{12} : *Problema rădăcinilor pătrate mod n*. Algoritm de determinare a unei rădăcini pătrate modulo p, un număr prim. Variante pentru cazurile particulare: $p \equiv 3 (\mathrm{mod}\ 4)$, $p \equiv 5 (\mathrm{mod}\ 8)$ şi $p-1 = 2^s t$, cu s număr mare. Rădăcini pătrate modulo $n = pq$, cu p şi q numere prime distincte. Metodă flip coin.

$C_{13} – C_{14}$: *Problema sumei unei submulțimi* (*subset-sum problem*) *şi problema rucsac* (*knapsack problem*). Noțiuni introductive. Algoritmi pentru rezolvarea computațională a problemei. Algoritm de determinare a unei baze reduse cunoscând o bază a unei lattice $L \subseteq \mathbb{R}^n$. Aplicarea algoritmului anterior la rezolvarea problemei subset-sum de densitate scăzută şi la aproximarea simultană diofantică (metodă folosită în atacuri asupra criptosistemelor).

Bibliografie:

1. Buşneag, D., Boboc, F., Piciu, D., *Aritmetică şi teoria numerelor*, Editura Universitaria, Craiova, 1999.
2. Dan, C., *Algoritmi în teoria numerelor*, Editura Universitaria, Craiova, 2005.
3. Dincă, Al., *Introducere în teoria algebrică a numerelor,* Editura Universitaria, Craiova, 2006.
4. Koblitz, N., *A Course in Number Theory and Cryptography*, Springer-Verlag, Berlin, 1994.
5. Knut, D.E., *The Art of Computer Programming*, vol. I, ed. a II-a, Addison-Wesley, 1973.
6. Rosen, K. H., *Elementary Number Theory and Cryptography*, Addison-Wesley, 1993.