

MOTIVATIA PROGRAMULUI DE MASTER „CRIPTOGRAFIE ȘI TEORIA CODURILOR” (Context general, Misiune si Obiective strategice)

Criptografia și teoria codurilor sunt domenii relativ noi pentru cercetarea fundamentală de la noi din facultate. Este prima oară când se propune organizarea unui asemenea master. Pe de altă parte, domeniile aceste, deși făcând parte din matematica aplicată, utilizează, pe lângă noțiuni și tehnici specifice informaticii și statisticii, foarte multe noțiuni și tehnici de algebră, teoria numerelor și geometrie algebrică. Or, Facultatea de Matematică și Informatică a Universității din București are eminenți specialiști în toate aceste domenii, cercetători renumiți, cu rezultate remarcabile publicate în reviste de top (de exemplu *Inventiones Mathematicae*, *Mathematische Annalen*, *Advances in Mathematics*, *Journal of Algebra*, *Fundamenta Informaticae*, *Acta Informatica* etc.) Specialiștii în aceste domenii au îndrumat doctorate remarcabile, derulează constant granturi naționale și participă la contracte și colaborări internaționale.

Cursurile vor fi ținute de specialiști din 3 catedre, anume: Algebră; Geometrie Complexă, Topologie și Geometrie computațională; Fundamentele informaticii.

În vara lui 2008, Catedra de Geometrie Complexă, Topologie și Geometrie computațională va fi principala organizatoare a celei de-a doua școli de vară internaționale de Teoria codurilor de la Vatra Dornei. De asemenea, specialiști ai acestei catedre (prof.dr. D.Popescu și conf.dr. C.Gherghe) au ținut în anii din urmă cursuri opționale de criptografie foarte apreciate de studenți și au publicat la Editura Universității un curs în acest domeniu. Prof.dr. A.Atanasiu, din Catedra de Fundamentele Informaticii, ține, la rândul său, de mai mulți ani cursuri de criptografie aplicată pentru informaticieni și are numeroase contribuții publicate în reviste de specialitate.

Toate acestea justifică din plin acreditarea unui master de Criptografie și Teoria codurilor.

Masterul de Criptografie si Teoria Codurilor dorește să demonstreze că matematica pură de înaltă valoare (geometria algebrică, teoria curbelor eliptice, geometria proiectivă, teoria numerelor) poate fi folosită atât în cercetare cât și în practica de zi cu zi.

Obiectivul general al masterului este ca studenții să-si însușească unele concepte fundamentale, necesare atât în formarea celor care vor urma “latura aplicată”, de exemplu criptografie sau teoria codurilor, cât și a celor care intenționează să se specializeze în unele domenii ale matematicii pure: algebră, geometrie algebrică si diferențială, teoria numerelor.

6. PLAN DE ÎNVĂȚĂMÂNT
Anul I (2008-2009)

Nr. crt.	Disciplina	Semestrul I				Semestrul II			
		Nr. ore curs	Nr. ore sem	Evaluare	Nr. credite	Nr. ore curs	Nr. ore sem	Evaluare	Nr. credite
1	Algebra Comutativa	2	2	E	7,5	-	-	-	-
2	Topologie	2	2	E	7,5	-	-	-	-
3	Geometrie Riemanniana	2	2	E	7,5	-	-	-	-
4	Inele si categorii de module	2	2	E	7,5	-	-	-	-
5	Curbe Algebrice	-	-	-	-	2	2	E	7,5
6	Introducere in teoria fasciculelor	-	-	-	-	2	2	E	7,5
7	Grupuri si Reprezentari	-	-	-	-	2	2	E	7,5
8	Algebra omologica	-	-	-	-	2	2	E	7,5

Anul II (2009-2010)

Nr. crt.	Disciplina	Semestrul I				Semestrul II			
		Nr. ore curs	Nr. ore sem	Evaluare	Nr. credite	Nr. ore curs	Nr. ore sem	Evaluare	Nr. credite
1	Criptografie Computationala	2	2	E	7,5	-	-	-	-
2	Curbe Eliptice	2	2	E	7,5	-	-	-	-
3	Geometrie Algebrica	2	2	E	7,5	-	-	-	-
4	Teoria Numerelor	2	2	E	7,5	-	-	-	-
5	Introducere in Teoria Codurilor	-	-	-	-	2	2	E	7,5
6	Criptografie Aplicata	-	-	-	-	2	2	E	7,5
7	Securitatea Fluxului Informational	-	-	-	-	2	2	E	7,5
8	Algebra Computationala	-	-	-	-	2	2	E	7,5

7.1. FIȘA UNITĂȚII DE CURS

TITLUL: ALGEBRA COMUTATIVA

SEMESTRUL: An I, Semestrul I

STATUTUL: obligatoriu

NR.ORE / SAPTAMANA: Curs 2, Seminar 2

FORMA DE EXAMINARE: examen scris

CREDITE: 7,5

OBIECTIVE: Acest curs isi propune completarea conceptelor de algebra comutativa studiate in timpul facultatii si totodata invatarea unor concepte mai dificile in vederea cercetarii in algebra comutativa.

PROGRAMA ANALITICA

- Inele de polinoame, inele de fractii.
- Ideale prime si maximale.
- Inele Noetheriene si Artiniene.
- Module graduate, functii Hilbert si serii Hilbert.
- Ideale monomiale si complexe simpliciale.
- Ideale prime asociate si descompuneri primare.
- Dimensiune Krull.
- Inele locale regulate.

BIBLIOGRAFIE

1. M. F. Atiyah si I. G. Macdonald, Introduction to commutative algebra, Addison-Wesley, 1969.
2. W. Bruns si J. Herzog, Cohen-Macaulay Rings, Cambridge, 1998.
3. H. Matsumura, Commutative ring theory, Cambridge, University Press, 1986.
4. R. H. Villarreal, Monomial algebras, Marcel Dekker, Inc. 2001.

7.2. FIȘA UNITĂȚII DE CURS

TITLUL: TOPOLOGIE

SEMESTRUL: An I, Semestrul I

STATUTUL: obligatoriu

NR.ORE / SAPTAMANA: Curs 2, Seminar 2

FORMA DE EXAMINARE: examen scris

CREDITE: 7,5

OBIECTIVE: Cursul isi propune consolidarea, sistematizarea si completarea unor notiuni fundamentale de topologie generala si de topologie algebrica cu aplicatii in diverse teorii moderne. Sunt prezentate si demonstrate cateva teoreme importante.

PROGRAMA ANALITICA

- Spatii topologice. Functii continue
- Spatii topologice separate. Spatii topologice compacte. Teorema lui Tihonov
- Spatii topologice regulate. Spatii topologice normale
- Partitie continua a unitatii
- Omotopie
- Grup fundamental
- Proiectii de acoperire
- Complexe simpliciale. Complexe simpliciale geometrice
- Complexe de lanturi
- Omologie
- Omologie simpliciala
- Omologie singulara
- Siruri Mayer-Vietoris
- Coomologie
- Aplicatii

BIBLIOGRAFIE

1. N. Bourbaki : Topologie générale, Hermann, Paris, 1960
2. E. Spanier : Algebraic Topology, Springer-Verlag. XIV, 1982
3. C. Teleman: Elemente de topologie si varietati diferentiabile, Ed. Did. Pedagogica (1964)

7.3. FIȘA UNITĂȚII DE CURS

TITLUL: GEOMETRIE RIEMANNIANA

SEMESTRUL: An I, Semestrul I

STATUTUL: obligatoriu

NR.ORE / SAPTAMANA: Curs 2, Seminar 2

FORMA DE EXAMINARE: examen scris

CREDITE: 7,5

OBIECTIVE: Cursul reprezinta o introducere in Geometria diferentiaza globala si teoria geometrica a grupurilor Lie. Se studiaza legatura intre invariantii geometrici si topologici ai unei varietati riemanniene, demonstrandu-se unele teoreme de comparatie (care dau conditii suficiente pentru ca o varietate riemanniana sa fie homeomorfa, difeomorfa sau izometrica cu o varietate etalon, de obicei cu o forma spatiala).

PROGRAMA ANALITICA

- Elemente introductive de grupuri si de algebre Lie.
- Conexiuni invariante pe grupuri Lie
- Metrici semi-riemanniene invariante pe grupuri Lie
- Proprietati globale ale geodezicelor
- Aplicatia exponentiala. Campuri Jacobi.
- Legatura intre curbura si comportarea geodezicelor
- Completitudine pe varietati riemanniene. Teorema Hopf-Rinow
- Teorema lui Hadamard
- Clasificarea varietatilor cu curbura constanta
- Teoreme de comparatie

BIBLIOGRAFIE

1. M. Berger, A Panoramic View of Riemannian Geometry, Springer, 2003
2. M. Do Carmo, Riemannian Geometry, Birkhauser, 1992
3. L. Nicolescu – Grupuri Lie, Ed. Univ. Bucuresti, 1994
4. L. Nicolescu, G. Pripoe, C. Zara – Teoreme si probleme de grupuri Lie, Ed. Univ. Bucuresti, 1996

7.4. FIȘA UNITĂȚII DE CURS

TITLUL: INELE SI CATEGORII DE MODULE

SEMESTRUL: An I, Semestrul I

STATUTUL: obligatoriu

NR.ORE / SAPTAMANA: Curs 2, Seminar 2

FORMA DE EXAMINARE: examen scris

CREDITE: 7,5

OBIECTIVE: Inele si module reprezinta notiuni oferă fundamentale pentru numeroase domenii din matematica modernă (algebră, geometrie, analiza matematica, informatica etc.). Cursul își propune să prezinte in detaliu proprietatile acestor obiecte, precum si sa faca o introducere in teoria categoriilor.

PROGRAMA ANALITICA

- **Module:** module, morfisme de module, submodule, module factor, morfisme de module, bimodule, inele de endomorfisme.
- **Sume si produse directe:** definitii si proprietati, descompunerea inelului, module libere, inele IBN (cu proprietatea de invarianta a numarului de elemente ale bazei).
- **Module proiective si injective:** definitii, exemple, Teorema Baer, Teorema Eckmann-Schopf.
- **Conditii de finitudine:** module simple si semisimple, module (inele) noetheriene, module (inele) artiniene, module de lungime finita, module indecompozabile. Teoremele Jordan-Holder, Azumaya, Krull-Schmidt.
- **Produs tensorial:** produs tensorial de module, bimodule si algebre, proprietatea de adjunctie, module plate.
- **Concepte de baza in teoria categoriilor:** categorii, functori, transformari naturale, echivalenta si dualitate de categorii, functori reprezentabili, functori adjuncti, produse si coproduse.
- **Inele de matrice si echivalenta categoriilor de module peste un inel si peste inele de matrice.**

BIBLIOGRAFIE

1. F. W. Anderson, K. R. Fuller, Rings and categories of modules, Second Edition, Graduate Texts in Math., Vol. 13, Springer Verlag, Berlin-Heidelberg-New York, 1992.
2. T. Y. Lam, Lectures on modules and rings, Graduate Texts in Math., Vol. 189, Springer Verlag, Berlin-Heidelberg-New York, 1998.
3. C. Nastasescu, Inele. Module. Categorii, Editura Academiei, 1976.
4. S. Mac Lane, Categories for the working mathematician, 2nd edition, Graduate Texts in Math., Vol. 5, Springer Verlag, Berlin-Heidelberg-New York, 1998.
5. I. D. Ion, C. Nita, S. Buzeteanu, Capitole speciale de algebra moderna, Tipografia Univ. Bucuresti, 1984.
6. I. D. Ion, N. Radu, Algebra, Ed. Didactica si pedagogica, Bucuresti, 1981.
7. J. J. Rotman, Advanced modern algebra, Prentice Hall, 2002.

7.5. FIȘA UNITĂȚII DE CURS

TITLUL: CURBE ALGEBRICE

SEMESTRUL: An I, Semestrul I

STATUTUL: obligatoriu

NR.ORE / SAPTAMANA: Curs 2, Seminar 2

FORMA DE EXAMINARE: examen scris

CREDITE: 7,5

OBIECTIVE: La sfarsitul cursului, studentii vor fi capabili:

1. sa identifice invarianti ai curbelor algebrice si sa decida daca doua curbe date sunt izomorfe (biregulat sau birational)
2. sa utilizeze sisteme liniare de divizori pentru a determina morfisme ale curbelor proiective netede
3. sa caracterizeze diverse clase de curbe algebrice
4. sa aplice metodele geometriei algebrice in rezolvarea unor probleme clasice

PROGRAMA ANALITICA

- Inele de polinoame si module peste inele de polinoame: teorema bazei, teorema zerourilor, polinomul Hilbert. Lema de normalizare. Baze Groebner.
- Curbe afine plane: functii regulate, inelul de coordonate, functii rationale, inelul local al unui punct, spatiul tangent, puncte netede si puncte singulare, conul tangent. Probleme de clasificare a curbelor afine plane.
- Curbe proiective plane: functii rationale, spatiul tangent. Teorema lui Bezout.
- Curbe proiective netede: divizori, genul unei curbe. Teorema Riemann-Roch. Scufundari ale curbelor netede. Curbe hipereliptice. Teorema Clifford. Inegalitatea Castelnuovo. Probleme de clasificare.
- Modele nesingulare ale curbelor: normalizare, unicitatea modelului proiectiv neted.

BIBLIOGRAFIE

1. Fulton, W., Algebraic curves. An introduction to Algebraic Geometry, W.A. Benjamin Inc., 1969.
2. Hartshorne, R., Algebraic Geometry, Springer-Verlag, New York, 1977.
3. Hulek, K., Elementary Algebraic Geometry, Student Math Library, vol.20, 2000.
4. G. Kempf, Algebraic Varieties, Cambridge, 1993.
5. I. Shafarevich, Bazele Geometriei Algebrice, Springer 1977.
6. Walker, R.J., Algebraic Curves, Princeton Univ., 1950.

7.6. FIȘA UNITĂȚII DE CURS

TITLUL: INTRODUCERE IN TEORIA FASCICOLELOR

SEMESTRUL: An I, Semestrul II

STATUTUL: obligatoriu

NR.ORE / SAPTAMANA: Curs 2, Seminar 2

FORMA DE EXAMINARE: examen scris

CREDITE: 7,5

OBIECTIVE: Scopul cursului este sa ofere o introducere elementara in teoria fascicolelor peste spatii topologice si, mai ales, penste varietati. In particular, se va introduce coomologia cu coeficienti in fascicole si se va schita demonstratia teoremei lui de Rham abstracte. Asemenea notiuni sint fundamentale pentru cursurile mai avansate de topologie, de functii de mai multe variabile complexe, de geometrie algebrica si de geometrie diferentiaala.

PROGRAMA ANALITICA

- Spații topologice. Generalități (conexiune, separare, compacitate, paracompacitate).
- Varietăți reale și complexe. Generalități (definiții, morfisme, exemple).
- Partiția unității pe spații topologice și varietăți diferențiabile.
- Prefascicole. Morfisme de prefascicole. Secțiuni.
- Fascicole. Legătura cu prefascicolele.
- Rezoluții de fascicole.
- Șiruri exacte de fascicole.
- Fascicole moi și fascicole flasce.
- Coomologie cu coeficienți într-un fascicol.
- Coomologie Čech. Clasificarea fibraților vectoriali de rang 1.
- Teorema lui de Rham abstractă.

BIBLIOGRAFIE

1. R. Godement, Topologie algébrique et théorie des faisceaux. Hermann, Paris, 1973.
2. R.O. Wells, Differential analysis on complex manifolds, Springer, 1979.
3. G.E. Bredon, Sheaf theory, Springer, 1997.

7.7. FIȘA UNITĂȚII DE CURS

TITLUL: GRUPURI ȘI REPREZENTARI

SEMESTRUL: An I, Semestrul II

STATUTUL: obligatoriu

NR.ORE / SAPTAMANA: Curs 2, Seminar 2

FORMA DE EXAMINARE: examen scris

CREDITE: 7,5

OBIECTIVE: Cursul prezinta concepte si rezultate importante din teoria grupurilor legate de actiuni ale grupurilor pe multimi, p-grupuri, grupuri simple. Sunt demonstrate mai multe rezultate de clasificare, totodata fiind prezentate tehnici folosite la clasificarea grupurilor finite. Este prezentata o introducere in teoria reprezentarilor de grupuri, demonstrandu-se cateva rezultate importante legate de reprezentari complet reductibile si grupuri rezolubile.

PROGRAMA ANALITICA

- Actiuni ale grupurilor pe multimi.
- p-grupuri si teoremele lui Sylow.
- Produse semidirecte.
- Rezultate de clasificare pentru grupuri finite: ordin p^2 , p^3 , pq (p si q prime).
- Grupuri simple.
- Teorema Schur-Zassenhaus.
- Serii de compozitie: teorema Jordan-Holder.
- Grupuri nilpotente si rezolubile.
- Categoria reprezentarilor liniare ale unui grup.
- Reprezentari complet reductibile: teorema Maschke.
- Teoria caracterelor grupurilor finite.
- Teorema $p^a q^b$ a lui Burnside.

BIBLIOGRAFIE

1. T. Albu, N. Manolache, 19 lectii de teoria grupurilor, Editura Universitatii Bucuresti, 1987.
2. Alperin, J.L., Bell, Rowen B., Groups and representations, [Graduate Texts in Mathematics](#), Vol. 162, Springer Verlag, 1995.
3. J. J. Rotman, An Introduction to the Theory of Groups, [Graduate Texts in Mathematics](#), Vol. 148, Springer Verlag, 1999.
4. C. Nastasescu, C. Nita, C. Vraciu, Bazele algebrei, Editura Academiei, 1986.
5. D. Popescu, C. Vraciu, Elemente de teoria grupurilor finite, Editura Stiintifica si enciclopedica, 1986.

7.8. FIȘA UNITĂȚII DE CURS

Titlul: Algebra omologica

Statutul: obligatoriu

Nr.ore/sapt.: 2 curs; 2 seminar

Anul/Semestrul: Anul I, Semestrul II

Forma de examinare: examen

Credite: 7,5

OBIECTIVE Algebra omologică oferă instrumente și tehnici de lucru fundamentale pentru numeroase domenii din matematica modernă (algebră, geometrie algebrică și diferențială, topologie algebrică, analiză complexă, teoria operatorilor, etc.). Cursul își propune să realizeze o introducere în algebra omologică, prezentând noțiunile și rezultatele de bază: complexe de (co)lanțuri și (co)omologia complexelor, rezoluții proiective și injective, construcția functorilor derivați, precum și aplicații ale acestora la studiul grupurilor, și algebrelor asociative.

PROGRAMA

- **Categorii și functori:** Definiții, exemple, functori aditivi, functori exacti.
- **Complexe de lanțuri și colanțuri:** Definiții și proprietăți elementare. Categoria complexelor de (co)lanțuri. Operații cu complexe, șiruri exacte de complexe. Morfisme omotope. Exemple din alte domenii ale matematicii.
- **(Co)omologia complexelor:** Definiție și proprietăți elementare. Șirul exact lung în (co)omologie și aplicații ale acestuia la calculul (co)omologiei.
- **Module proiective și injective:** Caracterizări echivalente. În categoriile de module există suficiente obiecte injective și proiective.
- **Rezoluții proiective și injective:** Existența rezoluțiilor proiective și injective în categorii de module. Teorema de comparare a rezoluțiilor. Exemple.
- **Functori derivați:** Construcție. Proprietăți ale functorilor derivați.
- **Functorii Tor și Ext:** Caracterizări ale modulelor proiective, injective și plate folosind Tor și Ext. Dimensiune proiectivă, injectivă, plată și globală. Inele de dimensiune mică. Functorul Ext și extensiile de module.
- **Aplicații ale functorilor derivați la studiul grupurilor:** Definiția (co)omologiei grupurilor. Rezoluția Bar. Complexul standard. Clasificarea extensiilor cu nucleu abelian. Calculul (co)omologiei grupurilor ciclice.
- **Aplicații ale functorilor derivați la studiul algebrelor asociative:** (Co)omologiei Hochschild. Rezoluția și complexul standard. Calculul primului grup de coomologie Hochschild. Clasificarea extinderilor de algebre. Algebre de dimensiune Hochschild cel mult.

BIBLIOGRAFIE

1. *Joseph J. Rotman, An Introduction to Homological Algebra*, Pure and Applied Mathematics, Academic Press, 1979.
2. *L. Vermani, An Elementary Approach to Homological Algebra*, CRC Press, 2003.
3. *Charles Weibel, An introduction to homological algebra*, Cambridge Studies in Advanced Mathematics **38**, Cambridge University Press, 1994.

7.9. FIȘA UNITĂȚII DE CURS

TITLUL: CRIPTOGRAFIE COMPUTATIONALA

SEMESTRUL: An II, Semestrul III

STATUTUL: obligatoriu

NR.ORE / SAPTAMANA: Curs 2, Seminar 2

FORMA DE EXAMINARE: examen scris

CREDITE: 7,5

OBIECTIVE: Studentii vor cunoaste functionarea principalelor criptosisteme simetrice si cu cheie publica precum si cateva metode de atac ale acestora. Vor fi prezentate directiile moderne ale criptografiei (criptosisteme cu curbe eliptice si criptografia cuantica).

PROGRAMA ANALITICA

- Criptografie Clasica. (Criptosisteme clasice si criptanaliza lor, Modele de comunicare sigura, Atacuri ale criptosistemelor).
- Criptosisteme simetrice (Data Eryption Standard, Advanced Encryption Standard).
- Metode de criptanaliza.
- Criptosisteme perfect sigure (Teorema lui Shannon, criptosistemul One Time Pad).
- Criptografie cu cheie publica: Protocolul Diffie-Hellman, Criptosistemul RSA (Descriere, metode de atac), Criptosistemul Rabin, Criptosistemul El Gamal, Criptosistemul Knapsack, Functii Hash, Autentificarea mesajelor, Signaturi digitale si protocoale de autentificare)
- Criptosisteme cu curbe eliptice
 - RSA
 - ElGamal
 - Menezes-Vansone
- Criptografie cuantica (protocoalele BB)

BIBLIOGRAFIE

1. Menezes, A. J., Van Oorschot, P. C., Vanstone, S. A: Handbook of Applied Cryptography (CRC Press).
2. Stinson, D. R.: Cryptography: Theory and Practice, (Chapman and Hall)
3. C. Ghergh, D. Popescu: Criptografie, Coduri, Algoritmi, (Ed. Univ. Bucuresti)

7.10. FIȘA UNITĂȚII DE CURS

TITLUL: CURBE ELIPTICE

SEMESTRUL: An II, Semestrul III

STATUTUL: obligatoriu

NR.ORE / SAPTAMANA: Curs 2, Seminar 2

FORMA DE EXAMINARE: examen scris

CREDITE: 7,5

OBIECTIVE: Prezentarea bazelor teoretice necesare pentru intelegerea si utilizarea algoritmilor criptografici ce folosesc curbe eliptice. Prezentarea catorva astfel de algoritmi si a unor aspecte legate de implementarea lor.

PROGRAMA ANALITICA

- Curbe algebrice: functii regulate, functii ratiionale, divizori, teorema Riemann-Roch.
- Geometria curbelor eliptice: ecuatiia Weierstrass, legea grupala, izogenii.
- Curbe eliptice peste corpul numerelor complexe: parametrizare Weierstrass, polinom modular.
- Invarianti ai curbelor eliptice: Modulul Tate, pairing-ul Weil. Grupul formal al unei curbe eliptice.
- Curbe eliptice peste corpuri finite: Teorema Hasse, inelul de endomorfisme, curbe supersingulare.
- Aplicatii: calculul numarului de puncte al unei curbe eliptice peste un corp finit; curbe eliptice peste inele comutative finite.

BIBLIOGRAFIE

1. Silverman, J. , The arithmetic of elliptic curves. GTM 106, Springer-Verlag, New York, 1992.
2. Washington, L., Elliptic curves. Number theory and cryptography. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2003. .
3. Husemoller, D., Elliptic curves. Second edition. With appendices by Otto Forster, Ruth Lawrence and Stefan Theisen. GTM 111, Springer-Verlag, New York, 2004

7.11. FIȘA UNITĂȚII DE CURS

TITLUL: GEOMETRIE ALGEBRICA

SEMESTRUL: An II, Semestrul III

STATUTUL: obligatoriu

NR.ORE / SAPTAMANA: Curs 2, Seminar 2

FORMA DE EXAMINARE: examen scris

CREDITE: 7,5

OBIECTIVE: La sfarsitul cursului, studentii vor fi capabili:sa identifice invarianti ai varietatilor algebrice, sa utilizeze scufundari sau morfisme ale varietatilor algebrice pentru a justifica proprietati, sa foloseasca metode specifice de demonstratie sau de calcul in probleme diverse.

PROGRAMA ANALITICA

- Varietati afine si cuasi-afine: functii regulate, functii rationale, punctul de vedere birational.
- Teoria locala: dimensiune Krull, nesingularitate, consecinte ale factorialitatii inelelor locale regulate.
- Varietati proiective: scufundari Segre si Veronese, varietatile proiective sunt proprii.
- Proiectii si corespondente.
- Divizori si sisteme liniare. Clasa canonica.
- Fascicule coerente si cuasi-coerente. Coomologia varietatilor proiective.
- Teoria intersectiei pe suprafete: teorema Riemann-Roch, eclatare, forma de intersectie a eclatatei.
- Limbajul schemelor. Varietati peste corpuri finite.

BIBLIOGRAFIE

1. J. Harris, Algebraic Geometry, Springer, 1992.
2. G. Kempf, Algebraic Varieties, Cambridge, 1993.
3. D. Mumford, Complex projective varieties, Springer 1975.
4. I. Shafarevich, Bazele Geometriei Algebrice, Springer 1977

7.12. FIȘA UNITĂȚII DE CURS

TITLUL: TEORIA NUMERELOR

SEMESTRUL: An II, Semestrul III

STATUTUL: obligatoriu

NR.ORE / SAPTAMANA: Curs 2, Seminar 2

FORMA DE EXAMINARE: examen scris

CREDITE: 7,5

OBIECTIVE: Cursul își propune să dezvolte acele ramuri ale teoriei numerelor necesare studiului criptografiei. Întrucât cea mai importantă metodă de criptare se bazează pe numere prime mari, un accent special va fi pus pe teoria numerelor prime.

Vor fi descrise metode care permit găsirea unor numere prime mari. Problema este interesantă în sine dar are și o componentă practică extrem de importantă (de exemplu, centrul de cercetări de proiectare și producție Cray investește extrem de mult în găsirea numerelor prime mari iar fabricantul de microprocesoare Intel folosește un program de găsire a numerelor prime Mersenne pentru a testa fiecare Pentium pus în comerț). O altă direcție a cursului se referă la metodele de factorizare. Importanța lor este covârșitoare în criptografia de azi. Se face o trecere în revistă a celor mai importante metode de factorizare de la cele mai simple la cele mai sofisticate (cum ar fi NFS care a permis descompunerea unor numere Fermat). Prezentarea acestor metode de factorizare furnizează și o panoramă inedită a teoriei numerelor

PROGRAMA ANALITICA

- Congruențe, resturi pătratice, simbolul Legendre, reciprocitate pătratică.
- Corpuri finite, logaritm discret.
- Numere prime. Distribuția numerelor prime.
- Prime Fermat și prime Mersenne. Testul Lucas-Lehmer.
- Numere pseudoprime. Numere Carmichael. Pseudoprime Fibonacci.
- Metode de factorizare. Metoda lui Fermat și cea a bazei de factori. Metoda fracțiilor continue. Metodele rho și p-1 ale lui Pollard. Algoritmii lui Lenstra.
- Forme pătratice. Metoda de factorizare bazată pe forme pătratice. Corpuri de numere algebrice. Ciurul corpurilor de numere algebrice (NFS).
- Dezvoltări recente. Metoda de factorizare a lui Agrawal-Kayal-Saxena

BIBLIOGRAFIE

1. R. Crandall, C. Pomerance, Prime Numbers. A computational perspective, Springer 2005 (ediția a doua).
2. G. Everest, T. Ward, An Introduction to Number Theory, Springer 2006.
3. C. Gherghe, D. Popescu, Criptografie.Coduri.Algoritmi, Editura Universității București, 2005.
4. A. Gica, L. Panaitopol, O Introducere în Aritmetică și Teoria Numerelor, Editura Universității București, 2001.
5. N. Koblitz, A Course in Number Theory and Cryptography, Springer 1987.
6. P. Ribenboim, The New Book of Prime Number Records, Springer 1996.
7. J. H. Silverman, J. Tate, Rational Points on Elliptic Curves, Springer 1994 (ediția a doua).

7.13. FIȘA UNITĂȚII DE CURS

TITLUL: TEORIA CODURILOR

SEMESTRUL: An II, Semestrul IV

STATUTUL: obligatoriu

NR.ORE / SAPTAMANA: Curs 2, Seminar 2

FORMA DE EXAMINARE: examen scris

CREDITE: 7,5

OBIECTIVE: Studentii vor cunoaste mecanismele matematice ce stau in spatele functionarii mijloacelor moderne de comunicare. Vor sti principalele tipuri de coduri (liniare cat si neliniare). Vor putea codifica, detecta si corecta erori cu codurile studiate.

PROGRAMA ANALITICA

- 1.Detectarea erorilor, corectarea si decodificarea (Principii generale, distanta Hamming, distanta unui cod).
- 2.Coduri liniare (Pondere Hamming, Matrice generatoare si matricea de control, codificarea si decodificarea cu coduri liniare, Sintromul)
- 3.Margini in teoria codurilor (Lower bounds, Gilbert-Varhamov bound, Hamming bound and perfect codes, Singleton bound, Plotkin bound).
- Coduri Hamming (Codificare si decodificare).
- Coduri Reed -Muler.
- 6 Coduri ciclice (Definitie, polinomul generator, algoritmi de decodificare)
- Coduri BCH.
- Coduri Reed-Solomon.
- Coduri retea.
- Coduri de resturi patratice.
- 11.Coduri Goppa
- Coduri provenind din geometria algebrica
- Elemente de teoria informatiei a lui Shannon.

BIBLIOGRAFIE

1. T.Hoboldt, H.V.Lindt: Algebraic Geometry Codes.
2. C. Gherghel, D. Popescu: Criptografie, Coduri, Algoritmi, (Ed. Univ. Bucuresti) 2005.
3. Coding Theory: S.Ling, C.Xing, Cambridge University Press 2004.

7.14. FIȘA UNITĂȚII DE CURS

TITLUL: CRIPTOGRAFIE APLICATA

SEMESTRUL: An II, Semestrul IV

STATUTUL: obligatoriu

NR.ORE / SAPTAMANA: Curs 2, Seminar 2

FORMA DE EXAMINARE: examen scris

CREDITE: 7,5

OBIECTIVE: O prezentare a celor mai importante protocoale criptografice legate de câteva domenii în care securitatea informației este foarte solicitată: autentificari de mesaje si semnături electronice, comerț electronic, vot electronic, securitatea poștei electronice. Noțiunile prezentate sunt o continuare naturală a construcției sistemelor de criptare, completând o componentă aplicativă suplimentară.

PROGRAMA ANALITICA

- Semnături digitale (Definiții, proprietăți generale, Scheme generale de semnătură, Standarde de semnătură electronică, Protocoale de semnătură incontestabilă, Protocoale de semnătură fără eșec, Semnături de grup, Semnături blind, Semnături cu mandat/arbitru, Semnături proxy, Semnături de tip fail-stop)
- Elemente de comerț electronic (Proprietăți generale; arhitectura unui sistem de comerț electronic, Sisteme electronice de plăți – Sistemul Brands, Sisteme bazate pe modelul provocare – răspuns: Schnorr, Sisteme electronice de plată; protocolul “Digital Cash”, Portofele electronice, Securitatea tranzacțiilor electronice - Protocolul SET; Smart carduri)
- Elemente de vot electronic (Protocoale bazate pe scheme de partajare a secretelor, Protocoale de tip provocare – răspuns, Securitatea votului electronic)
- Securitatea poștei electronice.

BIBLIOGRAFIE

1. A. Bruen, M. Forcinito, Cryptography, Information Theory, and Error - Correction, Wiley Interscience 2005.
2. A. Konheim - Computer Security and Cryptography, Wiley Interscience, 2007.
4. Menezes A., Oorschot P., Vanstone S. - Handbook of Applied Cryptography
5. D. Salmon - Data Privacy and Security, Springer Professional Computing, 2003
6. Schneier B. - Applied Cryptography, John Wiley and Sons, 1995
7. Stinton D. - Cryptography, Theory and Practice, Chapman& Hall CRC, 2002
8. Digital signature standard; National Bureau of Standards, FIPS Publications 186, 1994

7.15. FIȘA UNITĂȚII DE CURS

TITLUL: SECURITATEA FLUXULUI INFORMATIONAL

SEMESTRUL: An II, Semestrul IV

STATUTUL: obligatoriu

NR.ORE / SAPTAMANA: Curs 2, Seminar 2

FORMA DE EXAMINARE: examen scris

CREDITE: 7,5

OBIECTIVE: Cursul completeaza informatiile din cursurile anterioare legate de securitatea informatiei, construind modele teoretice de securitate a fluxului de informatii (verificarea protocoalelor de securitate protocoale de partajare a secretelor), precum și module importante de definire a transmiterii securizate a informatiei pe canale nesigure (gestiunea cheilor de sesiune).

PROGRAMA ANALITICA

- Verificarea protocoalelor de securitate (Proprietăți generale de securitate, Compunerea și verificarea proprietăților generale de securitate, Modelul Abadi – Rogaway)
- Protocoale de partajare a secretelor (Structuri de acces și modele generale, Scheme de partajare de tip majoritar, ierarhice, ponderate, Scheme generale de partajare, Posibilități de extensie a schemelor de partajare, Criptografie vizuală)
- Gestiunea cheilor de sesiune (Definiții, proprietăți generale, clasificări, Modele standard, Protocolul Neeham – Schroder, Protocolul Kerberos, Protocoale bazate pe problema Diffie – Hellmann, Datate)
- Generatori de numere pseudoaleatoare (Generatori bazați pe probleme criptografice, Generatori bazați pe LFSR, Standarde de evaluare a generatorilor de numere pseudoaleatoare)

BIBLIOGRAFIE

1. Atanasiu A. – Secret Sharing Schemes, capitol in Informatics Security Handbook, vol 2 (Ivan I., C. Toma eds), Editura ASE, 2007.
2. Atanasiu, A. – Securitatea informației, vol. 1 (Criptografie), Ed. Infodata, Cluj, 2007.
3. A. Konheim - Computer Security and Cryptography, Wiley Interscience, 2007.
4. Menezes A., Oorschot P., Vanstome S. - Handbook of Applied Cryptography.
5. D. Salmon - Data Privacy and Security, Springer Professional Computing, 2003.
6. Schneier B. - Applied Cryptography, John Wiley and Sons, 1995.
7. Stinton D. - Cryptography, Theory and Practice, Chapman& Hall CRC, 2002.

7.16. FIȘA UNITĂȚII DE CURS

TITLUL: ALGEBRA COMPUTATIONALA

SEMESTRUL: An II, Semestrul IV

STATUTUL: obligatoriu

NR.ORE / SAPTAMANA: Curs 2, Seminar 2

FORMA DE EXAMINARE: examen scris

CREDITE: 7,5

OBIECTIVE: Acest curs isi propune introducerea studentilor in domeniul combinatoricii in algebra comutativa. Sunt studiate totodata proprietati ale grafurilor cu ajutorul unor concepte noi din algebra commutative, oferindu-se posibilitatea de a studia probleme actuale in acest domeniu.

PROGRAMA ANALITICA

- Baze Grobner: Lema lui Dickson, Teorema Hilbert a bazei, ordini monomiale, criteriul lui Buchberger, algoritmul lui Buchberger de calcul a unei baze Groebner, baze Grobner reduse, ideale initiale.
- Clase de ideale monomiale: ideale initiale generice, ideale monomiale stabile, ideale cu caturi liniare, trecerea de la ideale omogene la idealele lor initiale, polarizare.
- Dualitate Alexander si rezolutii: teorema Eagon-Reiner, formula lui Hochster, criteriul lui Reisner.
- Ideale muchii: grafuri, grafuri Cohen-Macaulay, grafuri bipartite Cohen-Macaulay, grafuri cordale, teorema lui Dirac despre grafurile cordale.

BIBLIOGRAFIE

1. D. Cox, J. Little, D. O'Shea, Ideals, Varieties and Algorithms, Springer-Verlag New York, 2nd edition, 1997.
2. G.M. Greuel, G. Pfister, A Singular Introduction to Commutative Algebra, Springer-Verlag New York, 2002.
3. M. Kreuzer, L. Robbiano, Computational Commutative Algebra 1, Springer- Verlag New York, 2000.
4. M. Kreuzer, L. Robbiano, Computational Commutative Algebra 2, Springer- Verlag New York, 2005.
5. R. Villarreal, Monomial Algebras, Marcel Dekker, 2001.

9. PROGRAMA ANALITICA pentru concursul de admitere

Prima probă – examen scris

A doua probă – examen oral

Pentru examenul oral candidatii vor prezenta 3 subiecte alese din programa examenului.

PROGRAMA ANALITICA

1. Elemente de algebra liniara (spatii vectoriale, aplicatii liniare, forme biliniare, spatii vectoriale euclidiene)
2. Geometrie afina (spatii afine, subspatii afine, ecuatiile varietatilor afine)
3. Geometrie euclidiană (spatii euclidiene, izometrii)
4. Geometrie proiectiva (spatii proiective, subspatii proiective)
5. Grupuri si morfisme de grupuri: definitii si proprietati, subgrupuri, teorema lui Lagrange, ordinul unui element, subgrupuri normale, grupuri factor, teoreme de izomorfism, grupuri de permutari, grupuri rezolubile.
6. Inele si corpuri: definitii si proprietati, ideale, inele factor, ideale prime si ideale maximale, inele de polinoame, proprietati de universalitate si teoreme de izomorfism, proprietati aritmetice ale inelelor de polinoame, corpul de fractii al unui inel integru, extinderi algebrice de corpuri.

BIBLIOGRAFIE

1. L.Ornea, A.Turtoi, O introducere in geometrie, Ed.Theta, Bucuresti, 2000.
2. I.Ion, N.Radu, Algebra, EDP 1991
3. C.Nastasescu, C.Nita, C.Vraciu, Bazele algebrei, Ed.Academiei, 1986