



## FIȘA DISCIPLINEI (Fundamentele algebrice ale informaticii)

### 1. Date despre program

1.1 Instituția de învățământ superior	UNIVERSITATEA „OVIDIUS” DIN CONSTANȚA
1.2 Facultatea	Facultatea de Matematica si Informatica
1.3 Departamentul	Departamentul de Matematica si Informatica
1.4 Domeniul de studii	Informatica
1.5 Ciclul de studii	Licenta
1.6 Programul de studii	Informatica
1.7 Anul universitar	2025-2026

### 2. Date despre disciplină

2.1 Denumirea disciplinei	Fundamentele algebrice ale informaticii					
2.2 Cod disciplină	Info.1.2.15					
2.3 Titularul activităților de curs	Prof. univ dr. Cristina FLAUT					
2.4 Titularul activităților aplicative	Prof. univ dr. Cristina FLAUT					
2.5 Anul de studii	1	2.6 Semestrul	2	2.7 Tipul de evaluare	Ex	2.8 Regimul disciplinei DF/DOB

\* DF – disciplină fundamentală, DS – disciplină de specializare, DC – disciplină complementară

\*\* DOB – disciplină obligatorie; DOP – disciplină opțională; DFA – Disciplină facultativă

### 3. Timpul total (ore pe semestru)

3.1 Număr de ore activități directe pe săptămână	3	din care: 3.2 curs	2	3.3 aplicații***	1
3.4 Total ore activități directe pe semestru	42	din care: 3.5 curs	28	3.6 aplicații	14
3.7 Total ore de studiu individual					83
Distribuția fondului de timp					
Studiul cărților, manualelor, suportului de curs,, notițelor, bibliografie minimală recomandată					20
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren					15
Pregătire seminar / laborator / proiect, teme, referate, portofolii și eseuri					15
Pregătire pentru prezentări sau verificări					13
Pregătire pentru examinarea finală					15
Alte activități: consultații					5
3.8 Total ore pe semestru	125				
3.9 Numărul de credite	5				

\*\*\* S - seminar; L - laborator; P - proiect

### 4. Precondiții (acolo unde este cazul)

4.1 de curriculum	Liceu
4.2 de rezultate ale învățării	Notiuni de algebra la nivel de liceu



**5. Condiții necesare pentru desfășurarea optimă a activităților didactice (acolo unde este cazul)**

5.1. de desfășurare a cursului	Sala de curs disponibilă
5.2. de desfășurare a seminarului/ laboratorului / proiectului*	Sala de seminar disponibilă

\*Se alege tipul de aplicație aferent disciplinei

**6. Obiectivele disciplinei**

6.1 Obiectivul general al disciplinei	Însușirea conștințelor de bază din algebra cu aplicații în criptografie și teoria codurilor.
6.2 Obiectivele specifice	Completarea cunoștințelor de bază specifice algebrei, cu prezentarea completă și riguroasă a rezultatelor și exemplificarea aplicabilității părții teoretice în criptografie și teoria codurilor.

**7. Rezultatele învățării**

<b>Cunoștințe</b>	Studentul / Absolventul <ul style="list-style-type: none"><li>- cunoaște și explică metodele învățate utilizate pentru simularea proceselor informatice (ex. algoritmi, simulări) și nu numai</li><li>- identifică, analizează și aplică tehnici cantitative pentru a lua decizii eficiente în contexte care impun folosirea de astfel de metode</li><li>- selectează metode adecvate pentru un set de date/probleme care modelează fenomene reale</li><li>- utilizează instrumente informatice specializate pentru implementarea și testarea metodelor însușite</li></ul>
<b>Aptitudini</b>	Studentul / Absolventul <ul style="list-style-type: none"><li>- alege în mod corect algoritmul optim pentru probleme reale</li><li>- aplică algoritmi învățati în rezolvarea problemelor reale, proiectând și implementând modele simulabile</li><li>- interpretează corect și comunică concluziile analizei într-un mod clar și argumentat, adaptat publicului țintă (tehnic sau non-tehnic)</li></ul>
<b>Responsabilitate și autonomie</b>	Studentul / Absolventul: <ul style="list-style-type: none"><li>- manifestă responsabilitate în asigurarea acurateții rezultatului și timpului optim de obținere a acestuia, aplicând tehnici de validare și verificare;</li><li>- afișează disponibilitatea de a aplica metodele învățate în minicercetări în diverse domenii;</li><li>- propune și dezvoltă soluții computaționale optimizate, asumându-și responsabilitatea pentru validitatea și eficiența modelelor utilizate.</li></ul>

**8. Conținuturi**

8.1 Curs	Metode de predare	Număr ore alocate
Notiuni de logică și teoria mulțimilor.	Metode de predare-învățare interactive;	2
Relații de echivalență și de ordine. Aplicații.	Metode care implică activ studentii în învățare, punându-i în situația de a	2
Lattice. Definiție, proprietăți, exemple. Sublattice, morfism de lattice, produs de lattice. Aplicații.		12
Semigrupuri, grupuri, inele, corpuri. Definiție, exemple, proprietăți. Teoreme fundamentale de izomorfism. Inelul claselor de resturi modulo $n$ , $\mathbb{Z}_n$ . Algoritmul lui Euclid și algoritmul lui Euclid extins pentru aflarea inversului unui element modulo $n$ .		



<b>Criptografie.</b> Criptosisteme simple (cifrul lui Caesar, codificarea afina, matrice de codificare, etc.). Criptosistemul RSA. <b>Teste de primalitate si de descompunere in factori primi.</b> Testul Miller-Rabin, Metoda “rho” a lui Pollard, Metoda $p-1$ a lui Pollard, Number Field Sieve.	realiza conexiuni logice, de a produce idei și opinii proprii argumentate	8
<b>Coduri.</b> Notiuni preliminare. Coduri liniare, matrice generatoare, matrice de control, sindrom, detectare si corctare de erori. Coduri ciclice. Utilizare GAP-GUAVA.	Problematizarea; Conversatia; Metodele active Sintetiza/ esențializarea informațiilor Invățarea independentă și prin cooperare	4
<b>Bibliografie</b> [1]. Ravi P. Agarwal, <b>Cristina Flaut</b> , <i>An Introduction to Linear Algebra</i> , CRC Press-Taylor and Francis Group, Florida 33487, U.S.A., 2017, <b>ISBN 978-1-138-62670-6</b> [2]. Duncan Buell, <i>Fundamentals of Cryptography. Introducing Mathematical and Algorithmic Foundations</i> , Springer, 2021, ISBN 3030734919 [3]. Cristina Flaut, <i>Cyclic codes over some special rings</i> , Bull. Korean Math. Soc., <b>50(5)</b> (2013), 1513-1521, DOI: 10.4134/BKMS.2013.50.5.1513. [4]. Catalin Gherghe, Dorin Popescu, <i>Criptografie. Coduri. Algoritmi</i> , Editura Universitatii din Bucuresti, 2005. [5]. Neil Koblitz, <i>A Course in Number Theory and Cryptography</i> , Springer-Verlag, 1987. [6]. C. Nastasescu, C. Vraciu, <i>Bazele Algebrei</i> , Editura Didactica si Pedagogica, Bucuresti, 1986. [7]. Michael Sipser, <i>Introduction to the theory of Computation</i> , PWS PUBLISHING COMPANY, 1997, Boston. [8]. <a href="https://www.gap-system.org/Packages/guava.html">https://www.gap-system.org/Packages/guava.html</a>		
<b>8.2 Aplicații (laborator)*</b> <i>*Se alege tipul de aplicație aferent disciplinei</i>	<b>Metode de predare</b>	<b>Număr ore alocate</b>
<b>Notiuni de logica si teoria multimilor.</b> Relatii de echivalenta si de ordine. Aplicatii.	Dialogul; Problematizarea; Metodele active și interactive cu multiple; Sintetiza/ esențializarea informațiilor; Invățarea independentă și prin cooperare. Exercitiul	2
<b>Latice.</b> Definitie, proprietati, exemple. Sublatice, morfism de latice, produs de latice. Aplicatii.		2
<b>Semigrupuri, grupuri, inele, corpuri.</b> Definitie, exemple, proprietati. Teoreme fundamentale de izomorfism. Inelul claselor de resturi modulo $n$ , $\mathbb{Z}_n$ . Algoritmul lui Euclid si algoritmul lui Euclid extins pentru aflarea inversului unui element modulo $n$ .		4
<b>Criptografie.</b> Criptosisteme simple (cifrul lui Caesar, codificarea afina, matrice de codificare, etc.). Criptosistemul RSA. <b>Teste de primalitate si de descompunere in factori primi.</b> Testul Miller-Rabin, Metoda “rho” a lui Pollard, Metoda $p-1$ a lui Pollard, Number Field Sieve.		4
<b>Coduri.</b> Notiuni preliminare. Coduri liniare, matrice generatoare, matrice de control, sindrom, detectare si corctare de erori. Coduri ciclice. Utilizare GAP-GUAVA.		2
<b>Bibliografie</b> [1]. Ravi P. Agarwal, <b>Cristina Flaut</b> , <i>An Introduction to Linear Algebra</i> , CRC Press-Taylor and Francis Group, Florida 33487, U.S.A., 2017, <b>ISBN 978-1-138-62670-6</b> [2]. Duncan Buell, <i>Fundamentals of Cryptography. Introducing Mathematical and Algorithmic Foundations</i> , Springer, 2021, ISBN 3030734919 [3]. Cristina Flaut, <i>Cyclic codes over some special rings</i> , Bull. Korean Math. Soc., <b>50(5)</b> (2013), 1513-1521, DOI: 10.4134/BKMS.2013.50.5.1513. [4]. Catalin Gherghe, Dorin Popescu, <i>Criptografie. Coduri. Algoritmi</i> , Editura Universitatii din Bucuresti, 2005. [5]. Neil Koblitz, <i>A Course in Number Theory and Cryptography</i> , Springer-Verlag, 1987. [6]. C. Nastasescu, C. Vraciu, <i>Bazele Algebrei</i> , Editura Didactica si Pedagogica, Bucuresti, 1986. [7]. Michael Sipser, <i>Introduction to the theory of Computation</i> , PWS PUBLISHING COMPANY, 1997, Boston. [8]. <a href="https://www.gap-svstem.org/Packages/guava.html">https://www.gap-svstem.org/Packages/guava.html</a>		



## 9. Evaluare

Tip activitate	9.1 Criterii de evaluare	9.2 Metode de evaluare	9.3 Pondere din nota finală
9.4 Curs	Participare activa la ore	Evaluare continuă orală	10%
9.5 Aplicații <i>Laborator</i>	Referate si teme de casa, lucrari si evaluare pe parcurs	Evaluare continuă orală si scris	15%
	Interes și capacitate de lucru pentru studiu individual și în echipă	Prezentarea unui referat sau aplicarea unei metode analitice avansate ( studiu de caz)	25%
	Examen	Nota examinare	40%
Din oficiu			10%
9.6 Standard minim de performanță / Condiții de promovare			
Folosirea conostintelor de baza din algebra si aplicarea lor in criptografie si teoria codurilor. Construirea unui model matematic, pornind de la un proces real cu aplicarea algoritmului adecvat: -Sa aplice pe cazuri concrete Lema Chineza a resturilor sau sa rezolve anumite ecuatii mod $n$ . -Sa codifice si sa decodifice folosind cifrul afin.			

Data completării,

Titular activităților de curs,  
Nume/Prenume /Semnătura  
Prof. univ. dr. Cristina Flaut

12.09.2025

Titular aplicații,  
Nume/Prenume /Semnătura

Prof. univ. dr. Cristina Flaut

Data avizării în Departament,  
15.09.2025

Director de Departament,  
Conf.dr. E. Pelican

Decan,  
Conf.dr. A. Nicola