FIŞA DISCIPLINEI

1. Date despre program

1.1 Instituţia de învăţământ superior	**Universitatea “Alexandru Ioan Cuza” din Iaşi**
1.2 Facultatea	**Facultatea de Informatică**
1.3 Departamentul	**Informatică**
1.4 Domeniul de studii	**Informatică**
1.5 Ciclul de studii	**Licenţă**
1.6 Programul de studii / Calificarea	**Informatică/Licenţiat în Informatică**

2. Date despre disciplină

2.1 Denumirea disciplinei			**ASPECTE COMPUTAŢIONALE ÎN TEORIA NUMERELOR**				
2.2 Titularul activităţilor de curs			**LECT. DR. SORIN IFTENE**				
2.3 Titularul activităţilor de laborator			**LECT. DR. SORIN IFTENE**				
2.4 An de studiu	**III**	**2.5** Semestru	**II**	**2.6** Tip de evaluare	**M**	**2.7** Regimul disciplinei*	**OP**

3. Timpul total estimat (ore pe semestru şi activităţi didactice)

3.1 Număr de ore pe săptămână	**4**	din care: **3.2** curs	**2**	**3.3** laborator	**2**
3.4 Total ore din planul de învăţământ	**56**	din care: **3.5** curs	**28**	**3.6** laborator	**28**
Distribuţia fondului de timp					ore
Studiu după manual, suport de curs, bibliografie şi altele -					**14**
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren -					**14**
Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri					**28**
Tutoriat					**-**
Examinări					**4**
Alte activităţi					**-**

3.7 Total ore studiu individual	**56**
3.8 Total ore pe semestru	**116**
3.9 Număr de credite	**5**

4. Precondiţii (dacă este cazul)

4.1 De curriculum	**Discipline absolvite anterior: Fundamentele Algebrice ale Informaticii**
4.2 De competenţe	**Capacitatea de utiliza notiunile invatate la cursul de Fundamentele Algebrice ale Informaticii** **Capacitatea de a analiza complexitatea unui algoritm** **Capacitatea de a implementa un algoritm intr-un limbaj de programare la alegere**

5. Condiţii (dacă este cazul)

5.1 De desfăşurare a cursului	-
5.2 De desfăşurare a laboratorului	**-**

6. Competenţe specifice acumulate

Competenţe profesionale	**Cunoştinţe**: cei mai importanţi algoritmi pentru probleme din Teoria Numerelor şi aplicaţiile acestora **Abilităţi**: capacitatea de a proiecta/analiza/implementa algoritmi eficienţi pentru cele mai cunoscute probleme din Teoria Numerelor
Competenţe transversale	Disciplina ASPECTE COMPUTAŢIONALE ÎN TEORIA NUMERELOR combina cunostiinte din domenii diverse, precum Fundamentele Algebrice ale Informaticii şi Teoria Complexităţii, cu aplicaţii mai ales în Teoria Codurilor şi Criptografie (Securitatea Informaţiei). Studentii sunt astfel pusi in situatia de folosi/combina cunostinte din diverse domenii ale informaticii.

7. Obiectivele disciplinei

7.1 Obiectivul general	Proiectarea unor algoritmi eficienţi (şi analiza complexităţii acestora) pentru probleme specifice Teoriei Numerelor
7.2 Obiectivele specifice	La finalizarea cu succes a acestei discipline, studenţii vor fi capabili să înţeleagă, să explice, să analizeze, să utilizeze, să implementeze algoritmi eficienţi pentru cele mai cunoscute probleme din Teoria Numerelor (primalitate, factorizare, logaritmi discreti, radacini patratice)

8. Conţinut

8.1	**Curs**	**Metode de predare**	**Observaţii** (ore şi referinţe bibliografice)
1.	1.1 Prezentarea generala a cursului (motivatie, structura,organizare) 1.2 Modalitati de reprezentare ale numerelor/polinoamelor 1.3 Operaţii de bază (I) - adunare, scădere,inmultire	expunere (la tabla), dezbatere	[1], [4], [5]

2.	Operatii de baza (II) - împărţire, cel mai mare divizor comun (şi varianta extinsă), determinarea inversului, teorema Chineză a resturilor, evaluarea si interpolarea polinoamelor	expunere (la tabla), dezbatere	[1], [4], [5]
3.	Exponentiere (I) - tehnici generale, tehnici de baza fixata	expunere (la tabla), dezbatere	[4], [5]
4.	Exponentiere (II) - tehnici de exponent fixat, tehnici de multiexponentiere	expunere (la tabla), dezbatere	[4], [5]
5.	Testarea primalităţii (I) - abordari probabiliste (Fermat, Miller-Rabin, Solovay-Strassen, Lucas-Lehmer, Pocklington)	expunere (la tabla), dezbatere	[2], [5]
6.	Testarea primalităţii (II) - teste pentru numere prime de anumite forme particulare (Pépin, Proth, Lucas–Lehmer)	expunere (la tabla), dezbatere	[2], [5]
7.	Testarea primalităţii (III) - testul AKS (incluzând aici şi detecţia puterilor perfecte)	expunere (la tabla), dezbatere	[2], [5]
8.	Evaluare Partiala	test scris	-
9.	Calculul ordinului unui element şi generarea rădăcinilor primitive (şi a elementelor de un anumit ordin)	expunere (la tabla), dezbatere	[1], [5]
10.	Calculul logaritmilor discreţi	expunere (la tabla), dezbatere	[1], [5]
11.	Algoritmi de factorizare a numerelor	expunere (la tabla), dezbatere	[1], [2], [5]
12.	Factorizarea polinoamelor/generarea polinoamelor ireductibile	expunere (la tabla), dezbatere	[1], [5]
13.	Rezolvarea de ecuaţii în corpuri finite (cu accent pe determinarea radacinilor patratice)	expunere (la tabla), dezbatere	[1], [5]
14.	Aritmetica curbelor eliptice	expunere (la tabla), dezbatere	[3], [5]

Bibliografie

[1] Abhijit Das. Computational Number Theory. CRC Press, 2013
[2] Hans Riesel. Prime Numbers and Computer Methods for Factorization (2nd Edition). Birkhäuser, 2012
[3] Joseph H. Silverman. The Arithmetic of Elliptic Curves (2nd Edition). Springer, 2009
[4]F. L. Ţiplea, S. Iftene, C. Hriţcu, I. Goriac, R. Gordân, E. Erbiceanu. MpNT: A Multi-Precision Number Theory Package. Number Theoretical Algorithms (I), Technical Report TR03-02, Faculty of Computer Science, “Al. I. Cuza” University, Iaşi, 2003 (http://profs.info.uaic.ro/~tr/tr03-02.pdf)
[5] articole din conferinţe/jurnale relevante din domeniu

8.2	**Seminar / Laborator**	**Metode de predare/evaluare**	**Observaţii** (ore şi referinţe bibliografice)
1.	Lucru la prima tema (CRC, Reed-Solomon)	dezbatere/chestionarea orală	aceleiasi ca la curs
2.	Lucru la prima tema (CRC, Reed-Solomon)	dezbatere/chestionarea orală	aceleiasi ca la curs
3.	Lucru la prima tema (CRC, Reed-Solomon)	dezbatere/chestionarea orală	aceleiasi ca la curs

4.	Lucru la prima tema (CRC, Reed-Solomon)	dezbatere/chestionarea orală	aceleiasi ca la curs
5.	Lucru la a doua tema (Implementarea unui algoritm eficient de exponentiere pentru RSA)	dezbatere/chestionarea orală	aceleiasi ca la curs
6.	Lucru la a doua tema (Implementarea unui algoritm eficient de exponentiere pentru RSA)	dezbatere/chestionarea orală	aceleiasi ca la curs
7.	Lucru la a doua tema (Implementarea unui algoritm eficient de exponentiere pentru RSA)	dezbatere/chestionarea orală	aceleiasi ca la curs
8.	Evaluare Partiala	test scris	-
9.	Lucru la a treia tema (Implementarea unui algoritm de testare a primalitatii)	dezbatere/chestionarea orală	aceleiasi ca la curs
10.	Lucru la a treia tema (Implementarea unui algoritm de testare a primalitatii)	dezbatere/chestionarea orală	aceleiasi ca la curs
11.	Lucru la a treia tema (Implementarea unui algoritm de testare a primalitatii)	dezbatere/chestionarea orală	aceleiasi ca la curs
12.	Lucru la a patra tema (Implementarea unui algoritm de deteminare a logaritmului discret)	dezbatere/chestionarea orală	aceleiasi ca la curs
13.	Lucru la a patra tema (Implementarea unui algoritm de deteminare a logaritmului discret)	dezbatere/chestionarea orală	aceleiasi ca la curs
14.	Lucru la a patra tema (Implementarea unui algoritm de deteminare a logaritmului discret)	dezbatere/chestionarea orală	aceleiasi ca la curs

Bibliografie
- aceeasi ca la curs

9. Coroborarea conţinutului disciplinei cu aşteptările reprezentanţilor comunităţii, asociaţiilor profesionale şi angajatorilor reprezentativi din domeniul aferent programului

Continutul disciplinei este astfel proiectat si structurat astfel incat acopera principalele topici necesare realizarii unor implementari eficiente ale unor aplicaţii mai ales în Teoria Codurilor Detectoare si Corectoare de Erori şi Criptografie (care utilizeaza algoritmi pentru probleme specifice Teoriei Numerelor).

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere în

	[criteriile de punctare si clasificare, inclusiv cele de promovare]	[teste scrise, proiecte, teme, prezenta (sem/lab), activitate la tabla, bonusuri pentru activitati suplimentare, ...]	**nota finală (%)**
10.4 Curs	Intelegerea algoritmilor prezentati la curs, capacitatea de a le analiza complexitatea si de a-i utiliza in aplicatii	Examen Partial(EP), Examen Final (EF)	25% 25%
10.5 Seminar/ Laborator	Capacitatea de a implementa cei mai relevanti algoritmi prezentati la curs, intr-un limbaj de programare la alegere	Teme de Laborator (TL)	50%
10.6 Standard minim de performanţă			
Simultan trebuie indeplinite conditiile TL ≥ 5, EP ≥ 5, EF ≥ 5, ceea ce presupune înţelegerea şi implementarea unor algoritmi cu grad moderat de complexitate			

Data completării
22 Martie 2018

Titular de curs
LECT. DR. SORIN IFTENE

Titular de laborator
LECT. DR. SORIN IFTENE

Data avizării în departament

Director de departament