

Cuprins

Introducere	11
1 Teoria numerelor	13
1.1 Fundamente teoretice	13
1.1.1 Cel mai mare divizor comun. Algoritmul lui Euclid extins	16
1.1.2 Numere prime. Teorema fundamentală a aritmeticii	22
1.1.3 Inelul întregilor lui Gauss	28
1.1.4 Șiruri recurente. Numerele lui Fibonacci	34
1.1.5 Congruențe. Teorema chinezească a resturilor	38
1.1.6 Teorema lui Fermat, Wilson, și Euler	46
1.1.7 Resturi pătratice	62
1.1.8 Curbe eliptice	74
1.2 Teste de primalitate	91
1.2.1 Testul Fermat	91
1.2.2 Testul Miller-Rabin	101
1.2.3 Testul Agrawal-Kayal-Saxena	103
1.2.4 Teste bazate pe curbe eliptice	105
1.3 Factorizarea numerelor	107
1.3.1 Metoda ρ a lui Pollard	107
1.3.2 Metoda $p - 1$ a lui Pollard	110
1.3.3 Algoritmul ECM al lui Lenstra	112
1.4 Probleme propuse	122
2 Criptografie	123
2.1 Criptare RSA	124
2.2 Criptare ElGamal	128
2.3 Probleme propuse	129
3 Teoria singularităților	131
3.1 Introducere	132
3.2 Topologia lui (X, x)	134

3.2.1	Nodul lui (X, x)	134
3.2.2	Clasificarea topologică a fibrărilor de drepte complexe peste suprafețe compacte Riemanniene	136
3.2.3	Preliminarii analitice	138
3.3	Singularități complexe	140
3.3.1	Singularități cât	143
3.4	Rezoluția singularităților	145
3.4.1	Graful de rezoluție	147
3.5	Rezoluția lui $f : (X, x) \rightarrow (\mathbf{C}, 0)$	148
3.5.1	Graful de rezoluție scufundată al $f : (X, x) \rightarrow (\mathbf{C}, 0)$. .	149
3.5.2	Proprietățile topologice ale lui \mathcal{Y}	150
3.6	Comentarii și exemple	153
3.7	Matricea de intersecție	156
3.8	Singularități ale curbelor	157
3.9	Construcția tubulară	158
3.9.1	Fibratul de disc tubular	158
3.9.2	Invarianți topologici ai lui L_X via graful de rezoluție . .	160
3.9.3	Exemple	161
3.10	Graful lui $(f(x, y) - z^n = 0, 0)$	163
3.10.1	Proprietăți ale grafului de rezoluție al lui $(f(x, y) - z^n = 0, 0)$	164
3.10.2	Exemple	165
3.11	Aplicații	174
3.12	Probleme propuse	177
Bibliografie		178
Listă de figuri		186
Glosar		189

cel mai mic număr prim cu 1000 de cifre.

Dacă descoperim însă că un număr nu este prim, – există metode care certifică acest fapt, fără a arăta concret un factor al numărului – atunci poate urma problema mai grea: cum arată descompunerea numărului respectiv în factori?

Poate părea din nou paradoxal, dar această problemă este mult mai grea. Iată aici spre exemplu un număr cu "doar" 92 de cifre:

4345558902424423758570790549406988302398763614902127610737883607737
1874875390720546716755309

Ei bine, știm precis că acest număr este compus, are divizori proprii, dar nu suntem în stare să-i aflăm pe aceștia. Problema descompunerii în factori este mult mai grea. Atât de grea încât o putem folosi – paradoxal, cum și neștiința poate fi utilă uneori – în construirea unor "lacăte" care ascund bine informația pe care dorim să o protejăm, pentru a fi inteligibilă doar celui căruia i se adresează...

Considerăm, că aceste puține exemple sunt suficiente pentru a motiva continuarea studiului paginilor ce urmează.