

Marcelina MOCANU

**TEORIA NUMERELOR
EXERCITII ȘI PROBLEME**



Editura „Alma Mater” Bacău

2021

Cuprins

1	Teorema împărțirii cu rest. Aplicații	1
1.1	Introducere	1
1.2	Resturile date de numerele întregi la împărțirea cu m . Principiul cutiei	3
1.3	Resturile pătratelor perfecte la împărțirea la un număr natural dat	7
1.4	Numărul multiplilor unui număr dat dintr-un interval	10
1.5	Exponentul unui factor prim din descompunerea unui factorial	12
2	Divizibilitatea expresiilor. Metoda descompunerii	17
2.1	Divizibilitatea unor numere de formă dată scrise în baza 10	19
2.2	Aplicații ale descompunerii diferențelor de puteri cu același exponent	20
2.3	Sume de puteri cu exponent impar ale primelor numere naturale	22
2.4	Numerele Mersenne	23
2.5	Divizibilitatea unor produse de numere naturale	25
3	Sisteme de numerație	31
3.1	Introducere	31
3.2	Transformarea unui număr din baza 10 în baza b	33
3.3	Divizibilitatea unor numere scrise în bază 10	36
3.4	Divizibilitatea unor numere scrise în bază b	37
3.5	Aplicații ale scrierii binare	38
4	Aplicații ale descompunerii în factori primi	41
4.1	Introducere	41
4.2	Mulțimea numerelor prime este infinită	45

4.3	Numere prime de formă dată	46
4.4	Radicali iraționali din numere naturale	47
4.5	Numărul divizorilor și suma divizorilor unui număr natural . . .	49
4.6	Descompuneri ale unui număr ca produs de doi factori relativ primi	54
5	Cel mai mare divizor comun și cel mai mic multiplu comun	57
5.1	Introducere	57
5.2	Proprietăți ale operatorului c.m.m.d.c.	59
5.3	Puterile a două numere relativ prime sunt relativ prime	64
5.4	Aflarea unui număr pentru care se cunosc c.m.m.d.c. și c.m.m.m.c.	65
6	Algoritmul lui Euclid	71
6.1	Introducere	71
6.2	Aplicații numerice ale algoritmului lui Euclid	75
6.3	C.m.m.d.c. al două numere Mersenne	76
6.4	Algoritmul lui Euclid extins	78
7	Mica teoremă a lui Fermat. Teorema lui Euler	83
7.1	Introducere	83
7.2	Divizibilitatea cu numere prime a unor expresii polinomiale . . .	87
7.3	Resturile date de puterile unui număr întreg la împărțirea la un număr prim	92
7.4	Indicatorul lui Euler	99
7.5	Teorema lui Euler. Aplicații imediate	106
7.6	Teorema lui Euler. Aplicații la studiul fracțiilor zecimale periodice	112
7.7	Criterii de divizibilitate cu $k \in \{2^m, 5^m, 3, 9, 11, 7\}$	114
8	Teorema lui Wilson	119
8.1	Introducere	119
8.2	Demonstrație cu polinoame a Teoremei lui Wilson	121
8.3	Unificarea teoremelor Fermat și Wilson	123
8.4	Resturile date de (produse de) factoriale la împărțiri	124
9	Ecuatii diofantice liniare	127
9.1	Introducere	127

9.2	Aflarea soluției generale a unei ecuații diofantice liniare cunoscând o soluție particulară	128
9.3	Interpretarea geometrică a ecuațiilor diofantice liniare	131
9.4	Aflarea unei soluții particulare a ecuației diofantice liniare folosind Algoritmul lui Euclid extins	135
9.5	Ecuații diofantice liniare în Matematica distractivă	141
9.6	Elemente inversabile în inelul claselor de resturi modulo m . . .	143
10	Congruențe de gradul întâi	151
10.1	Introducere	151
10.2	Congruențe de gradul întâi. Două metode de rezolvare	155
10.3	Proprietăți ale congruențelor de gradul întâi. Simplificare, amplificare	158
10.4	Numărul de soluții ale unei ecuații de gradul întâi în \mathbb{Z}_m	159
10.5	Lema chinezească a resturilor	161
10.5.1	Introducere	161
10.5.2	Aplicarea algoritmului legat de Lema chinezească a resturilor	163
11	Ecuații diofantice de grad superior	171
11.1	Ecuația lui Pitagora	171
11.1.1	Generarea soluțiilor ecuației lui Pitagora	171
11.1.2	Triplete pitagorice particulare	173
11.1.3	Triunghiuri pitagorice. Divizibilitatea lungimilor unor laturi cu 3, 4 sau 5	175
11.1.4	Triunghiuri pitagorice și funcții trigonometrice	178
11.1.5	Aplicație a ecuației lui Pitagora la rezolvarea unei ecuații diofantice de gradul IV	179
11.2	Alte ecuații diofantice de grad superior	180
11.2.1	O sumă de trei cuburi perfecte care este cub perfect	180
11.2.2	Aflarea a două numere întregi având dată suma inverselor. Metoda parametrică	183
11.2.3	Metoda descompunerii. Rezolvarea unei ecuații de gradul al treilea cu 3 necunoscute	189
11.2.4	Sistem simetric de ecuații diofantice de gradul III cu 3 necunoscute	191

12	Congruențe de grad superior. Polinoame cu coeficienți întregi	195
12.1	Condiție suficientă pentru ca funcția polinomială asociată în $\mathbb{Z}_m[X]$ să fie identic nulă	195
12.2	Rădăcini raționale ale polinoamelor cu coeficienți întregi	197
12.3	Mica teoremă a lui Fermat și divizibilitatea cu un număr prim a unor coeficienți binomiali	202
12.4	Formulele Faulhaber	205
13	Congruențe de grad superior. Rădăcini primitive modulo un număr prim	213
13.1	Perioada principală a șirului resturilor date de puterile numerelor întregi la împărțirea la un număr natural	213
13.1.1	Introducere	213
13.1.2	Ordinul modulo m al unui număr întreg	216
13.1.3	Rădăcini primitive modulo un număr prim	217
13.2	Congruențe binome. Resturi pătratice	227
13.2.1	Congruențe binome modulo un număr prim	227
13.2.2	Gradul unei congruențe binome modulo un număr prim- condiție suficientă de existență a soluțiilor	230
13.2.3	Numărul valorilor $a \pmod{p}$ pentru care congruența $x^k \equiv a \pmod{p}$ are soluții	231
13.2.4	Resturi pătratice modulo un număr prim	232
14	Aplicații ale teoriei numerelor	237
14.1	Aplicație în criptografie: Algoritmul RSA	237
14.2	Probleme de matematică distractivă	241
14.2.1	Problema vaselor cu apă	241
14.2.2	Problema nucilor de cocos	244
14.2.3	Problema lui Bachet	245
14.2.4	Marea teoremă a lui Fermat în cultura populară	251
15	Teste grilă de verificare a cunoștințelor	257