

Marcelina MOCANU

TEORIA NUMERELOR



EDITURA „ALMA MATER”
BACĂU, 2023

Cuprins

1	Divizibilitate în mulțimea numerelor întregi	1
1.1	Buna ordonare a mulțimii numerelor naturale	1
1.2	Teorema împărțirii cu rest în \mathbb{Z}	5
1.3	Relația de divizibilitate în \mathbb{N} și în \mathbb{Z}	10
2	Sisteme de numerație	13
2.1	Motivație	13
2.2	Reprezentarea numerelor naturale într-o bază de numerație b . .	16
2.3	Compararea a două numere reprezentate în baza b	22
2.4	Adunarea a două numere reprezentate în baza b	24
3	Numere prime, numere ireductibile. Descompuneri în factori primi	27
3.1	Introducere elementară	28
3.2	Elemente prime și elemente ireductibile în \mathbb{N}	31
3.3	Teorema fundamentală a aritmeticii	34
3.4	Numărul de divizori și suma divizorilor unui număr natural . . .	36
3.5	Teorema lui Legendre- exponentul unui factor prim în descom- punerea unui factorial	40
3.6	Mulțimea numerelor prime	43
3.6.1	Progresii aritmetice care conțin o infinitate de numere prime (I)	45
3.6.2	Rezultate clasice privind distribuția numerelor prime . .	47
3.6.3	Mulțimi remarcabile de numere prime. Numere Fermat, numere Mersenne	52

4	Cel mai mare divizor comun. Algoritmul lui Euclid	59
4.1	Cel mai mare divizor comun al două numere naturale	60
4.2	Algoritmul lui Euclid	63
4.3	Proprietăți ale operatorului c.m.m.d.c.	67
4.4	Cel mai mare divizor comun în \mathbb{Z} . Lema lui Bézout	72
5	Aritmetică modulară-parte I	75
5.1	Relația de congruență modulo m pe mulțimea numerelor întregi	76
5.2	Sistem complet de resturi modulo m . Mica teoremă a lui Fermat	81
5.3	Indicatorul lui Euler	86
5.4	Teorema lui Euler	91
5.5	Aplicații ale Teoremei lui Euler în algebră	94
5.5.1	Subgrupul elementelor inversabile din \mathbb{Z}_m	94
5.5.2	Rădăcinile primitive de ordin n ale unității	97
5.6	Criterii de divizibilitate	98
5.6.1	Divizibilitate cu 2 sau 5	99
5.6.2	Divizibilitate cu 3 sau 9	99
5.6.3	Cazul general	100
6	Ecuatii diofantice liniare	103
6.1	Ecuatia diofantică $ax + by = c$	104
6.1.1	Condiție necesară și suficientă de existență a soluțiilor . .	104
6.1.2	Aflarea soluției generale cunoscând o soluție particulară .	105
6.1.3	Aflarea unei soluții particulare. Algoritmul lui Euclid extins	109
6.2	Aplicații ale ecuației diofantice $ax + by = c$	112
6.2.1	Congruențe de gradul întâi	112
6.2.2	Elemente inversabile în inelul claselor de resturi modulo m	113
6.2.3	Teorema lui Wilson	115
7	Aritmetică modulară-parte a doua	117
7.1	Lema chinezească a resturilor	117
7.2	Aplicații ale aritmeticii modulare în criptografie	123
7.2.1	Introducere	123
7.2.2	Algoritmul RSA (Rivest-Shamir-Adelman)	125

8	Ecuatii diofantice de grad superior	129
8.1	Ecuatia diofantica a lui Pitagora	130
8.2	Teorema lui Fermat pentru exponentul 4	138
8.3	Teorema lui Fermat pentru exponentul 3	141
8.4	Elemente de teoria polinoamelor. Grad, radacini	144
8.5	Teorema lui Wilson-o demonstratie cu polinoame	151
9	Congruente de grad superior modulo un numar prim	155
9.1	Introducere	155
9.2	Reducerea congruentelor modulo un numar prim	156
9.3	Resturile date de puterile numerelor naturale la impartirea la m . Periodicitate	161
9.3.1	Periodicitatea resturilor $a^n \bmod m$	163
9.4	Resturile date de puterile numerelor naturale la impartirea la un numar prim	168
9.4.1	Noiunea de radacina primitiva modulo un numar prim	168
9.4.2	Existenta radacinilor primitive modulo un numar prim	176
9.5	Utilizarea radacinilor primitive modulo p in criptografie. Schimbul de chei Diffie-Hellman	179
9.6	Congruente binome modulo un numar prim	182
9.6.1	Utilizarea radacinilor primitive modulo p	182
9.6.2	Resturi patratice modulo un numar prim	185
9.6.3	Legea reciprocitatii patratice	193
9.7	Progresii aritmetice care contin o infinitate de numere prime (II)	196
10	Numere rationale. Numere irationale	201
10.1	Multimea numerelor rationale	202
10.1.1	Reprezentarea numerelor rationale sub forma de fractii ordinare	202
10.1.2	Reprezentarea numerelor rationale ca fractii zecimale.	205
10.2	Numere irationale	209
10.2.1	Radicali si numere irationale	212
10.2.2	Numerele e si π sunt irationale	214