

INDHOLD

Forord	v
I Tal og modulo-regning	
1 Indledning	3
Opgaver til Kapitel 1	5
2 De naturlige tal – Induktion	7
2.1 Dedekind–Peanos aksiomer og induktion	7
Opgaver til Kapitel 2	15
3 Divisibilitet og største fælles divisor	19
3.1 Største fælles divisor – Euklids algoritme	19
3.2 Mindste fælles multiplum	23
Opgaver til Kapitel 3	24
4 Primtal og heltalsdeling	29
4.1 Primtalsfaktoriserings	30
Opgaver til Kapitel 4	33
5 Uendelig mange primtal – tre beviser	37
5.1 Euklids bevis	37
5.2 Bevis baseret på Fermat-tal	37
5.3 Eulers bevis	38
6 Optælling af primtal – primtalssætningen	41
6.1 Chebyshevs sætning	42
6.2 En nedre grænse for antallet af primtal op til en vis størrelse	43
7 Landaus primtalsproblemer	45
7.1 Goldbachs formodning	45
7.2 Formodningen om primtalstvillinger	46
7.3 Hardy-Littlewood-formodningen	46
7.4 $(N^2 + 1)$ -formodningen	47
7.5 Legendres formodning	47
8 Mersenne-primtal – de største kendte primtal	49
8.1 Mersenne-primtal og perfekte tal	49

9	Kongruenser og potenser	51
9.1	Kongruensklasser og modulær regning	51
9.2	Fermats lille sætning	58
9.3	Eulers sætning og roduddragning modulo m	59
	Opgaver til Kapitel 9	64
10	Primalstest	67
10.1	Rabin–Millers probabilistiske primalstest	67
10.2	Konstruktion af store (sandsynlige) primtal	69
	Opgaver til Kapitel 10	70
11	Relationer	71
11.1	Ækvivalensrelationer	71
	Opgaver til Kapitel 11	75
 II Ringe – Polynomiumsringe – Kvotientringe		
12	Ringe – faktorisering	79
12.1	Faktorisering af primtal i $\mathbb{Z}[i]$ og Diofantiske ligninger	81
	Opgaver til Kapitel 12	82
13	Polynomier	87
13.1	Polynomiumsringe	87
13.2	Faktorisering af et polynomium i $K[X] - K$ et legeme	88
13.3	Polynomiers division	89
13.4	Rødder i et polynomium med koefficienter i et legeme K	91
13.5	Interpolation med polynomier	92
13.6	Euklids algoritme for polynomier	93
13.7	Bezouts identitet for polynomier	94
13.8	Entydig faktorisering i $K[X] - K$ et legeme	96
13.9	Polynomier med koefficienter i \mathbb{Z} og i \mathbb{Q}	97
13.10	Polynomier med koefficienter i \mathbb{R} og i \mathbb{C}	101
	Opgaver til Kapitel 13	107
14	Kongruensringe og legemer	111
14.1	Kongruensklasser og modulær regning i $K[X]$	111
	Opgaver til Kapitel 14	117
15	Primitivt element i \mathbb{Z}_p – diskret logaritme	119
15.1	Primitivt element	119
15.2	Det diskrete logaritmeproblem	121
15.3	Diskret logaritme med Pollards ρ -metode	121
	Opgaver til Kapitel 15	125

III	Kryptografi og Kodning: RSA, ElGamal, Shamir Secret Sharing, Reed–Solomon-fejlkorrektion	
16	Hemmelig kommunikation og digital underskrift	129
16.1	Offentlig-nøgle-kryptosystemet RSA	130
16.2	ElGamal-offentlig-nøgle-kryptosystem	131
	Opgaver til Kapitel 16	132
17	Shamir Secret Sharing	133
	Opgaver til Kapitel 17	136
18	Reed–Solomon-koder	137
18.1	Introduktion	137
18.2	Lineære koder, Hamming-afstand	138
18.3	Konstruktion af Reed–Solomon-koder	139
18.4	Afkodning af Reed–Solomon-koder	140
	Opgaver til Kapitel 18	145
 Appendikser		
A	COCALC–SAGE	149
A.1	Vedr. Divisibilitet og største fælles divisor, jf. Kapitel 3	149
A.2	Vedr. Primaltal, faktorisering og optælling af primaltal, jf. Kapitel 4 og Kapitel 6	150
A.3	Vedr. Kongruenser og potenser, jf. Kapitel 9	151
A.4	Primaltest, jf. Kapitel 10	152
A.5	Vedr. Polynomier, jf. Kapitel 13	153
A.6	Vedr. Kongruensringe og legemer, jf. Kapitel 14	154
A.7	Vedr. Primitivt element i \mathbb{Z}_p – diskret logaritme, jf. Kapitel 15	156
A.8	Vedr. Reed–Solomon-koder, jf. Kapitel 18	156
B	Gentagen kvadrering	159
C	Ligningssystemer	161
	Opgaver til Appendiks C	173
	Navne	177
	Litteratur	181
	Indeks	185