

# Inhoud

---

<i>Dankwoord</i>	15
<b>Hoofdstuk 1 · Instapwiskunde</b>	<b><u>17</u></b>
1.1 <i>Letterrekenen</i>	18
Reële getallen	18
Reële veeltermen	23
1.2 <i>Vergelijkingen met één onbekende</i>	25
Lineaire vergelijkingen	25
Kwadratische vergelijkingen	26
1.3 <i>Reflectie</i>	32
<b>Hoofdstuk 2 · Logaritmen</b>	<b><u>35</u></b>
2.1 <i>Begripsvorming</i>	36
Definitie	36
Eigenschap	37
Bestaansvoorwaarden	37
Soorten logaritmen	38
2.2 <i>Rekenregels</i>	40
Hoofdbewerkingen	40
Veranderen van grondtal	42
Een notatiekwestie	43
2.3 <i>Logaritmische vergelijkingen</i>	43
Via de definitie	43
Eenzelfde grondtal	43
Gemengde grondtallen	44
2.4 <i>Reflectie</i>	46
<b>Hoofdstuk 3 · Functies</b>	<b><u>49</u></b>
3.1 <i>Begrippen uit de reële analyse</i>	50
3.2 <i>Veeltermfuncties</i>	51
Lineaire functies	51
Kwadratische functies	53
Krommen	54
Hogere graadsfuncties	54
3.3 <i>Snijpunten tussen functies</i>	56

3.4	<i>Logaritmische functies</i>	57
3.5	<i>Exponentiële functies</i>	58
3.6	<i>De absolute waarde-functie</i>	60
3.7	<i>Discrete functies</i>	60
	De functie 'floor'	61
	De functie 'ceiling'	61
3.8	<i>Reflectie</i>	62
<b>Hoofdstuk 4 · Getalformaten</b>		<b><u>65</u></b>
4.1	<i>Soorten getallen</i>	66
	Begrippen uit de rekenkunde	66
	Tiendelige getallen	69
	Tweedelige getallen	70
	Achtdelige getallen	74
	Zestiendelige getallen	76
4.2	<i>Converteren tussen getalformaten</i>	78
	Converteren naar decimaal formaat	78
	Modulorekenen	79
	Converteren van tiendelige naar vreemde getalbases	80
	Hoekformaten	82
	Converteren tussen getalbases die een macht van 2 zijn	83
4.3	<i>Reflectie</i>	85
<b>Hoofdstuk 5 · Getallen in computers</b>		<b><u>87</u></b>
5.1	<i>De moderne computer</i>	88
5.2	<i>Getalopslag van natuurlijke getallen</i>	90
	Opslagformaten	91
	Natuurlijke overflow	91
5.3	<i>Getalopslag van gehele getallen</i>	92
	Keuze voor het 2-komplement	93
	Converteren tussen decimale en 2-komplementweergave	95
	2-komplementformaten	96
	Gehele overflow	96
5.4	<i>Getalopslag van reële getallen</i>	98
	Reële opslagfouten	99
	De reële getalopslag als idee	104
	Visualisering van de reële getalopslag	106
	IEEE opslagstandaarden voor $\mathbb{R}$	113
	Foutvoortplanting	118
5.5	<i>Reflectie</i>	125

<b>Hoofdstuk 6 · Booleaanse wiskunde</b>	<b><u>127</u></b>
6.1 <i>Uitsprakenlogica</i>	128
Uitspraken	129
Verbindingen	129
Samengestelde uitspraken en redeneerwetten	131
Bewijsvoering	137
Structuur	138
Paradoxen	138
6.2 <i>Schakelalgebra</i>	140
Schakelaarcircuits	140
Combinatorische circuits	142
6.3 <i>Booleaanse algebra</i>	147
Structuur	147
Axioma's van Huntington	148
Booleaanse rekenregels	149
Booleaanse functies	151
6.4 <i>Karnaughkaarten</i>	156
Begrippen	157
Normaliseren van functies	159
Vereenvoudigen van functies	161
6.5 <i>IT-toepassingen</i>	167
Programmeren	167
RAID4/5	168
Subnetting	170
Nand-technologie	171
6.6 <i>Reflectie</i>	172
<b>Hoofdstuk 7 · Inleiding tot de cryptografie</b>	<b><u>175</u></b>
7.1 <i>Begrippen omtrent cryptografie</i>	176
7.2 <i>Het schema van de cryptografie</i>	176
7.3 <i>Soorten cryptografie</i>	177
Indeling naar invoer	177
Indeling naar symmetrie	178
Indeling naar algoritme	179
7.4 <i>Kraakpogingen</i>	179
De kracht van de sleutel	179
De kwaliteit van het algoritme	180
Kraaktechnieken	180
7.5 <i>Cryptografische rekenomgevingen</i>	181
Associatietabellen	181

Restsystemen	183
Oplossen van lineaire vergelijkingen	190
Structuren met één bewerking	192
Structuren met twee bewerkingen	198
7.6 <i>Reflectie</i>	199
<b>Hoofdstuk 8 · Lineaire cijfers</b>	<b><u>201</u></b>
8.1 <i>Rekenomgeving</i>	202
De ringstructuur met twee bewerkingen	202
Tweede vuistregel voor modulorekenen	205
8.2 <i>Lineaire cijfers</i>	205
De publieke rekenomgeving	205
De vercijfering	206
De ontcijfering	207
Het algoritme	208
De kraakpoging	209
8.3 <i>Soorten lineaire cijfers</i>	210
Het caesarcijfer	210
Het multiplicatiecijfer	210
Een bijzondere kraakpoging	211
8.4 <i>Reflectie</i>	213
<b>Hoofdstuk 9 · Klutsfuncties</b>	<b><u>215</u></b>
9.1 <i>Eenrichtingsfuncties</i>	216
9.2 <i>Klutsfuncties</i>	216
Toepassingen	218
Kwaliteiten van een klutsfunctie	218
9.3 <i>Parallellisatie</i>	219
Restvectoren	220
Chinese reststelling	220
Parallelliseren van hoofdbewerkingen	224
9.4 <i>Uitgebreide grootste gemene deler</i>	225
Het algoritme ‘uggd’	225
Invers element in een reststelsel	226
Bewijs van de chinese reststelling	227
Lineaire vergelijkingen in een reststelsel	228
9.5 <i>Reflectie</i>	234

<b>Hoofdstuk 10 · RSA</b>	<b><u>237</u></b>
10.1 <i>Rekenomgeving</i>	238
10.2 <i>Getaltheorie</i>	238
De totiëntfunctie	238
De stelling van Euler	240
Het gemengd modularekenen	240
10.3 <i>Rivest Shamir Adleman</i>	241
De publieke rekenomgeving	241
De versleuteling	241
De ontsleuteling	242
Het algoritme	242
Voorbeeld	243
De kraakpoging	245
10.4 <i>Handtekenen met RSA</i>	246
De handtekening	246
De authenticatie	246
Het algoritme	247
Een gelaagde toepassing	247
10.5 <i>Parallelliseren van RSA</i>	249
10.6 <i>Reflectie</i>	253
<b>Hoofdstuk 11 · DSA</b>	<b><u>255</u></b>
11.1 <i>Rekenomgeving</i>	256
De veldstructuur met twee bewerkingen	256
Generatoren	258
11.2 <i>Discrete functies</i>	260
Discrete logaritmen	260
Discrete logaritmische functie	260
Discrete exponentiële functie	261
11.3 <i>Diffie-Hellman-sleuteluitwisseling</i>	262
De publieke rekenomgeving	262
De uitwisseling	262
Het algoritme	263
De kraakpoging	264
11.4 <i>Digital Signature Algorithm</i>	266
De publieke rekenomgeving	266
De handtekening	267
De authenticatie	268
Het algoritme	269
De kraakpoging	270
11.5 <i>Reflectie</i>	272

<b>Hoofdstuk 12 · Elliptische krommenversleuteling</b>	<b><u>275</u></b>
12.1 <i>Rekenomgeving</i>	276
12.2 <i>Reële elliptische krommen</i>	276
De reële elliptische krommengroep	277
Analytische aspecten	280
12.3 <i>Discrete elliptische krommen</i>	281
Kwadratische residu's	281
Priemkrommen $\mathbb{E}_p(b, c)$	282
De priemkrommengroep	285
Generatorpunten	285
12.4 <i>Priemkrommencriptografie</i>	289
De publieke rekenomgeving	289
De versleuteling	290
De ontsleuteling	292
Het priemkrommenalgoritme	293
De kraakpoging	294
12.5 <i>Priemkrommensleuteluitwisseling</i>	294
De uitwisseling	295
Het uitwisselingsalgoritme	295
De kraakpoging	296
12.6 <i>Priemkrommenhandtekening</i>	297
De handtekening	297
De authenticatie	298
12.7 <i>Reflectie</i>	299
<b>Hoofdstuk 13 · AES</b>	<b><u>301</u></b>
13.1 <i>Rekenomgeving</i>	302
Het binair priemveld $\mathbb{Z}_2$	302
De binaire quotiëntingen	303
De binaire galoisvelden	309
13.2 <i>Advanced Encryption Standard</i>	311
De publieke rekenomgeving	311
Het AES-versleutelingsalgoritme	313
De versleuteling als functie	319
Het ontsleutelingsalgoritme	321
De ontsleuteling als omgekeerde functie	326
Herbruikbaarheid van het algoritme	326
Implementeren van het algoritme	328
13.3 <i>De kraakpoging</i>	328
De brute kracht aanval	328
De AES-eenrichtingsfunctie	329
13.4 <i>Reflectie</i>	333

<b>Hoofdstuk 14 · Inleiding tot codes</b>	<b><u>335</u></b>
14.1 <i>Begrippen omtrent codes</i>	336
14.2 <i>Het schema van de codeertheorie</i>	337
14.3 <i>Soorten codes</i>	338
Indeling naar doelstelling	338
Indeling naar afstand	339
Indeling naar algoritme	339
14.4 <i>Rekenomgevingen van codes</i>	340
14.5 <i>Constructie van codes</i>	341
De ‘codering’ zonder extra bits	341
Coderingen met één extra bit	342
Een codering met twee overtallige bits	342
Een 3-bit overtallige codering	342
Een 4-bit overtallige codering	343
14.6 <i>Parameters van codes</i>	343
14.7 <i>Foutafhandeling bij algemene codes</i>	346
De ‘codering’ zonder extra bits	346
Coderingen met één extra bit	346
Een codering met twee overtallige bits	347
Een 3-bit overtallige codering	347
Een 4-bit overtallige codering	348
De muisknoppen-codering $C(5,4,3)$	348
Een spoorwegsein-codering	349
Dichtste buur-corrigering	351
14.8 <i>Reflectie</i>	353
<b>Hoofdstuk 15 · Lineaire codes</b>	<b><u>355</u></b>
15.1 <i>Rekenomgeving</i>	356
Vectorruimten	356
Interne allocatie	358
15.2 <i>Constructie van lineaire codes</i>	358
Het nulcodewoord	359
Hamming gewicht	360
Basiscodewoorden	360
Notatie	361
15.3 <i>Matrixweergave van lineaire codes</i>	362
Generatormatrix $G$	362
Pariteitstester $H$	364
15.4 <i>Foutafhandeling bij lineaire codes</i>	366
Syndromen	366

Schema van lineaire codes	374
15.5 <i>Hamming codes</i>	375
Het ontstaan	375
De constructie van hamming codes	375
De foutafhandeling bij hamming codes	376
15.6 <i>Reflectie</i>	377
<b>Hoofdstuk 16 · Cyclische tests</b>	<b><u>379</u></b>
16.1 <i>Rekenomgeving</i>	380
16.2 <i>Constructie van cyclische tests</i>	381
Cyclisch testen in $\mathbb{Z}$	381
Het CRC-algoritme met binaire veeltermen	382
16.3 <i>Cyclische tests versus klutsfuncties</i>	388
Geen integriteitsgarantie	388
Geen eenrichtingsfunctie	389
16.4 <i>Foutafhandeling bij cyclische tests</i>	389
Samenstelling van de CRC-veelterm	390
Illustraties en uitzonderingen	391
De troeven van cyclische tests	393
16.5 <i>Reflectie</i>	395
<b>Hoofdstuk A · Notatie-afspraken</b>	<b><u>397</u></b>
A.1 <i>Sleutels</i>	397
A.2 <i>Alfabetten</i>	398
Latijns alfabet	398
Grieks alfabet	398
A.3 <i>Wiskundige symboliek</i>	399
Verzamelingen	399
Wiskundige symbolen	400
Wiskundige sleutelwoorden	401
Getallen	401
<b>Hoofdstuk B · (Windows)ANSI ASCII</b>	<b><u>403</u></b>
<b>Hoofdstuk C · Wegwijzers</b>	<b><u>407</u></b>
C.1 <i>Didactische wegwijzer</i>	407
C.2 <i>Antwoorden wegwijzer</i>	407
<i>Bronvermelding</i>	408
<i>Index</i>	411