Inhaltsverzeichnis

1 **Motivation und Einführung** 1
Literatur 3

Teil I Numerik

2 **Einführung in die Numerische Mathematik** 7
Literatur 8

3 **Zahldarstellungen und Fehleranalyse** 9
3.1 Zahldarstellungen und Maschinenzahlen 9
3.2 Aufgaben mit Lösungen 15
3.3 Fehlerarten und ihre Kontrolle 16
3.4 Aufgaben mit Lösungen 20
Literatur 22

4 **Numerische Näherungsverfahren in $\mathbb{R}$** 23
4.1 Banachscher Fixpunktsatz in $\mathbb{R}$ 27
4.2 Aufgaben mit Lösungen 32
4.3 Newton-Verfahren 33
4.4 Aufgaben mit Lösungen 35
4.5 Heron-Verfahren 36
4.6 Aufgaben mit Lösungen 40
4.7 Sekanten-Verfahren 41
4.8 Aufgaben mit Lösungen 44
4.9 Abstieg-Verfahren 46
4.10 Aufgaben mit Lösungen 51
4.11 Dividierte-Differenzen-Verfahren 54
4.12 Aufgaben mit Lösungen 59
4.13 Trapez- und Simpson-Regel 62
4.14 Aufgaben mit Lösungen 66

Bibliografische Informationen
http://d-nb.info/1206808527

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

4.15 Iterierte Trapez- und Simpson-Regel 67
4.16 Aufgaben mit Lösungen 70
Literatur 72

5 Numerische Näherungsverfahren in $\mathbb{R}^n$ 73
5.1 Normen und Folgen in $\mathbb{R}^n$ 73
5.2 Banachscher Fixpunktsatz in $\mathbb{R}^n$ 77
5.3 Gesamtschritt-Verfahren 79
5.4 Aufgaben mit Lösungen 84
5.5 Einzelschritt-Verfahren 86
5.6 Aufgaben mit Lösungen 89
5.7 SOR-Verfahren 91
5.8 Von-Mises-Geiringer-Verfahren 92
5.9 Aufgaben mit Lösungen 95
Literatur 96

Teil II Grafik

6 Einführung in die Computer-Grafik 99
Literatur 103

7 Klassische polynomiale Interpolationsmethoden 105
7.1 Einfache polynomiale Strategien 105
7.2 Aufgaben mit Lösungen 109
7.3 Polynomiale Interpolation nach Lagrange 110
7.4 Aufgaben mit Lösungen 114
7.5 Polynomiale Interpolation nach Newton 116
7.6 Aufgaben mit Lösungen 122
7.7 Polynomiale Interpolation nach Aitken-Neville 125
7.8 Aufgaben mit Lösungen 128
Literatur 129

8 Klassische Subdivision-Techniken 131
8.1 Interpolierende Subdivision nach Dubuc 131
8.2 Aufgaben mit Lösungen 136
8.3 Approximierende Subdivision nach Chaikin 137
8.4 Aufgaben mit Lösungen 141
Literatur 142

9 Klassische Strategien über Rechtecken 143
9.1 Bilineare Interpolation über Rechtecken 143
9.2 Aufgaben mit Lösungen 144

9.3 Gouraud-Schattierung über Rechtecken 145
9.4 Aufgaben mit Lösungen 147
9.5 Phong-Schattierung über Rechtecken 148
9.6 Aufgaben mit Lösungen 151
9.7 Transfinite Interpolation über Rechtecken 151
9.8 Aufgaben mit Lösungen 155
9.9 Polynomiale Approximation über Rechtecken 156
9.10 Aufgaben mit Lösungen 159
Literatur 160

10 Klassische Strategien über Dreiecken 161
10.1 Lineare Interpolation über Dreiecken 161
10.2 Aufgaben mit Lösungen 163
10.3 Gouraud-Schattierung über Dreiecken 164
10.4 Aufgaben mit Lösungen 166
10.5 Phong-Schattierung über Dreiecken 166
10.6 Aufgaben mit Lösungen 168
10.7 Transfinite Interpolation über Dreiecken 169
10.8 Aufgaben mit Lösungen 173
10.9 Polynomiale Approximation über Dreiecken 174
10.10 Aufgaben mit Lösungen 177
Literatur 177

Teil III Kryptik

11 Einführung in die Kryptografie 181
Literatur 184

12 Grundlagen der Zahlentheorie 187
12.1 Grundlegende Begriffe 187
12.2 Satz von Fermat und Euler 189
12.3 Aufgaben mit Lösungen 192
12.4 Euklidischer Algorithmus 193
12.5 Aufgaben mit Lösungen 199
12.6 Der chinesische Restsatz 201
12.7 Aufgaben mit Lösungen 206
12.8 Polynome über beliebigen Körpern 209
12.9 Aufgaben mit Lösungen 215
12.10 Euklidischer Algorithmus für Polynome 216
12.11 Aufgaben mit Lösungen 223
Literatur 225

13 Spezielle Galois-Felder 227
13.1 Galois-Feld $GF(2) = \mathbb{Z}_2$ 227
13.2 Aufgaben mit Lösungen 229
13.3 Galois-Feld $GF(4)$ 232
13.4 Aufgaben mit Lösungen 237
13.5 Galois-Feld $GF(8)$ 238
13.6 Aufgaben mit Lösungen 241
13.7 Galois-Feld $GF(16)$ 242
13.8 Aufgaben mit Lösungen 248

14 Einwegfunktionen 253
14.1 Einwegfunktionen ohne Falltür 253
14.2 Aufgaben mit Lösungen 256
14.3 Einwegfunktionen mit Falltür 257
14.4 Aufgaben mit Lösungen 260
Literatur 261

15 Asymmetrische Verschlüsselungsverfahren 263
15.1 Diffie-Hellman-Verfahren 263
15.2 Aufgaben mit Lösungen 265
15.3 RSA-Verfahren 266
15.4 Aufgaben mit Lösungen 270
15.5 Anwendungs- und Sicherheitsaspekte asymmetrischer Verfahren . . . 271
15.6 Aufgaben mit Lösungen 291
Literatur 294

16 Symmetrische Verschlüsselungsverfahren 295
16.1 Vernam-Verfahren 295
16.2 Aufgaben mit Lösungen 297
16.3 DES-Verfahren 298
16.4 Aufgaben mit Lösungen 302
16.5 AES-Verfahren 304
16.6 Aufgaben mit Lösungen 313
16.7 Anwendungs- und Sicherheitsaspekte symmetrischer Verfahren 316
Literatur 317

17 Elliptische Kurven 319
17.1 Elliptische Kurven (char $\mathbf{K} > 3$) 320
17.2 Aufgaben mit Lösungen 326
17.3 EC-Diffie-Hellman-Verfahren (char $\mathbf{K} > 3$) 328
17.4 Aufgaben mit Lösungen 331
17.5 Elliptische Kurven (char $\mathbf{K} = 2$) 332
17.6 Aufgaben mit Lösungen 336

17.7 EC-Diffie-Hellman-Verfahren (char $\mathbf{K} = 2$) 338
17.8 Aufgaben mit Lösungen 340
17.9 Anwendungs- und Sicherheitsaspekte von ECC-Verfahren 341
17.10 Aufgaben mit Lösungen 346
17.11 Verschlüsseln, Hashen, Signieren: Das Zusammenspiel 348
Literatur 349

18 Post-Quanten-Kryptografie 351
18.1 NTRU-Verfahren 355
18.2 Aufgaben mit Lösungen 364
18.3 RLWE-Verfahren 367
18.4 Aufgaben mit Lösungen 373
Literatur 375

Sach-Index 377

Namen-Index 381

Mathe-Index 383