

---

# Inhaltsverzeichnis

<b>1</b>	<b>Vier spannende Probleme</b>	1
1.1	Natürliche Zahlen als Summe zweier Primzahlen	1
1.2	Primzahlen als Differenz zweier Quadratzahlen	2
1.3	Freitag, der 13. – ein Unglückstag?	5
1.4	Welche Fehler erkennt die IBAN?	7
<b>2</b>	<b>Teiler, Vielfache, Reste</b>	15
2.1	Definition	15
2.2	Teilbarkeits- und Vielfachenrelation als Ordnungsrelationen	18
2.2.1	Veranschaulichung durch Pfeildiagramme	18
2.2.2	Ordnungsrelation	21
2.3	Summen- und Produktregel	22
2.3.1	Summenregel	22
2.3.2	Differenzregel	23
2.3.3	Produktregeln	24
2.4	Division mit Rest	26
2.5	Kongruenzrelation/Restgleichheitsrelation	29
2.5.1	Seitenweise Addition von Kongruenzen	30
2.5.2	Seitenweise Multiplikation von Kongruenzen	31
2.5.3	Einsatzgebiete der Kongruenzrelation	33
2.6	Aufgaben	33
<b>3</b>	<b>Primzahlen</b>	37
3.1	Primzahlen – unterschiedliche Gesichter	37
3.2	Bestimmung von Primzahlen – Sieb des Eratosthenes	39
3.3	Verteilung der Primzahlen	44
3.3.1	Primzahlzwillinge	44
3.3.2	Primzahltrillinge/Primzahlvierlinge	45
3.3.3	Primzahlücken	46
3.4	Wie viele Primzahlen gibt es?	48
3.5	Primzahlformeln	50

3.6	Primzahlsatz	52
3.7	Jagd nach Primzahlrekorden	53
3.8	Vollkommene Zahlen	55
3.9	Einige offene Primzahlprobleme	60
3.10	Aufgaben	62
<b>4</b>	<b>Primzahlen – Bausteine der natürlichen Zahlen</b>	<b>65</b>
4.1	Problematisierung	65
4.2	Existenz der Primfaktorzerlegungen	67
4.3	Eindeutigkeit der Primfaktorzerlegungen	68
4.4	Folgerungen	71
4.4.1	Primzahlkriterium	71
4.4.2	Lemma von Euklid	73
4.4.3	Teilmengen	73
4.4.4	Weiterer Ausblick	75
4.5	Aufgaben	75
<b>5</b>	<b>Größter gemeinsamer Teiler und kleinstes gemeinsames Vielfaches</b>	<b>79</b>
5.1	$ggT$ und Teilmengen	80
5.2	$ggT$ und Primfaktorzerlegung	83
5.2.1	Ein Beispiel	83
5.2.2	Allgemeine Vorgehensweise	84
5.3	$ggT$ und Euklidischer Algorithmus	85
5.3.1	Ein Beispiel	86
5.3.2	Verallgemeinerung der zentralen Beweisidee	88
5.3.3	Euklidischer Algorithmus	88
5.4	$kgV$ und Vielfachenmengen	91
5.5	$kgV$ und Primfaktorzerlegung	95
5.6	Zusammenhang zwischen $ggT$ und $kgV$	96
5.7	Linearkombinationen natürlicher Zahlen	98
5.8	Lineare diophantische Gleichungen	103
5.9	Die Fermat'sche Vermutung – eine abenteuerliche Geschichte	106
5.10	Aufgaben	108
<b>6</b>	<b>Kongruenzen, Restklassenmengen und klassische Sätze</b>	<b>113</b>
6.1	Die Kongruenzrelation <i>modulo</i> $m$	113
6.1.1	Rechnen mit Resten	113
6.1.2	Alternative Definition der Kongruenzrelation	116
6.1.3	Rechnen mit Kongruenzen	119
6.1.4	Die Kongruenzrelation als Äquivalenzrelation	120
6.2	Restklassenmengen <i>modulo</i> $m$	121
6.2.1	Restklassen als Äquivalenzklassen	122

6.2.2	Rechnen mit Restklassen . . . . .	123
6.2.3	Restklassengleichungen . . . . .	126
6.2.4	Sprachebenen der Zahlentheorie . . . . .	127
6.2.5	Restklassenmengen als Beispiele für algebraische Strukturen . . .	129
6.3	Klassische Sätze der Elementaren Zahlentheorie . . . . .	135
6.3.1	Sätze von Euler und Fermat . . . . .	135
6.3.2	Chinesischer Restsatz . . . . .	138
6.3.3	Satz von Wilson . . . . .	142
6.4	Aufgaben . . . . .	143
<b>7</b>	<b>Stellenwertsysteme und Teilbarkeitsregeln . . . . .</b>	<b>147</b>
7.1	Stellenwertsysteme – einige Bemerkungen . . . . .	148
7.1.1	Dezimales Stellenwertsystem . . . . .	148
7.1.2	Nichtdezimale Stellenwertsysteme . . . . .	149
7.1.3	Notation einer Zahl in verschiedenen Basen . . . . .	149
7.1.4	Anforderungen an eine Basis . . . . .	150
7.1.5	Mögliche Basen von Stellenwertsystemen . . . . .	150
7.2	Ausgewählte Eigenschaften der Kongruenzrelation . . . . .	153
7.3	Endstellenregeln . . . . .	153
7.3.1	Dezimales Stellenwertsystem . . . . .	154
7.3.2	Nichtdezimale Stellenwertsysteme . . . . .	158
7.4	Quersummenregeln . . . . .	160
7.4.1	Dezimales Stellenwertsystem . . . . .	160
7.4.2	Nichtdezimale Stellenwertsysteme . . . . .	162
7.5	Alternierende Quersummenregeln . . . . .	164
7.5.1	Dezimales Stellenwertsystem . . . . .	164
7.5.2	Nichtdezimale Stellenwertsysteme . . . . .	168
7.6	Vorteile des Zugangsweges über die Kongruenzrelation . . . . .	170
7.7	Aufgaben . . . . .	171
<b>8</b>	<b>Dezimalbrüche/Systembrüche . . . . .</b>	<b>175</b>
8.1	Darstellungsformen von rationalen Zahlen . . . . .	176
8.1.1	Größenvergleich von gemeinen Brüchen als Herausforderung . . .	176
8.1.2	Vorteile der unterschiedlichen Darstellungsformen . . . . .	177
8.1.3	Erste einfache Darstellungswechsel . . . . .	177
8.2	Dezimalbruchentwicklungen als Erweiterung des Dezimalsystems . . . .	178
8.2.1	Erweiterung des Dezimalsystems und des Divisionsalgorithmus .	178
8.2.2	Erste Erkundungen . . . . .	182
8.2.3	Erste Systematisierungen . . . . .	183
8.3	Endliche Dezimalbruchentwicklungen . . . . .	184
8.4	Periodische Dezimalbruchentwicklungen . . . . .	186
8.4.1	Reinperiodische Dezimalbruchentwicklungen . . . . .	187

8.4.2	Gemischtperiodische Dezimalbruchentwicklungen . . . . .	191
8.5	Andere Stellenwertsysteme – andere Systembruchentwicklungen . . . . .	192
8.5.1	Erste Beispiele . . . . .	192
8.5.2	Divisionsalgorithmus in anderen Stellenwertsystemen . . . . .	194
8.5.3	Verallgemeinerung der Resultate aus dem Dezimalsystem . . . . .	196
8.6	Aufgaben . . . . .	198
<b>9</b>	<b>Fehler erkennen, Fehler korrigieren – Prüfziffern &amp; Co.</b> . . . . .	<b>201</b>
9.1	GTIN und EAN . . . . .	203
9.1.1	Aufbau und Zielsetzung . . . . .	203
9.1.2	Die Prüfziffer . . . . .	205
9.1.3	Sicherheit des Prüfziffernsystems . . . . .	207
9.1.4	Zusammenfassung . . . . .	213
9.2	Die Internationale Standardbuchnummer ISBN-13 . . . . .	213
9.2.1	Einige Bemerkungen zur Einführung . . . . .	213
9.2.2	Aufbau der ISBN-13 . . . . .	213
9.2.3	Sicherheit des ISBN-13-Prüfziffernsystems . . . . .	214
9.2.4	Zusammenhang von ISBN-10 und ISBN-13 . . . . .	215
9.3	Die Internationale Standardbuchnummer ISBN-10 . . . . .	215
9.3.1	Berechnung der ISBN-10-Prüfziffer . . . . .	215
9.3.2	Sicherheit des ISBN-10-Prüfziffernverfahrens . . . . .	216
9.3.3	Zusammenfassung . . . . .	220
9.4	Die Pharmazentralnummer PZN . . . . .	221
9.4.1	Aufbau der PZN und Berechnung der Prüfziffer . . . . .	222
9.4.2	Sicherheit der PZN . . . . .	222
9.5	Die Internationale Bankkontonummer IBAN . . . . .	223
9.5.1	Sicherheit des IBAN-Prüfziffernverfahrens . . . . .	223
9.5.2	Zusammenfassung . . . . .	228
9.6	Quick-Response-Code & Co. – eine Skizze . . . . .	229
9.6.1	Entwicklung, Zielsetzung und Aufbau des QR-Codes . . . . .	230
9.6.2	Grundidee der Fehlerkorrektur . . . . .	231
9.6.3	Verwandte Codes . . . . .	232
9.7	Aufgaben . . . . .	233
<b>10</b>	<b>Verschlüsselung und digitale Signaturen – RSA &amp; Co.</b> . . . . .	<b>237</b>
10.1	Grundsituationen der Kryptologie . . . . .	237
10.2	Symmetrische und asymmetrische Verschlüsselung . . . . .	239
10.2.1	Symmetrische Verfahren . . . . .	239
10.2.2	Asymmetrische Verfahren . . . . .	240
10.2.3	Vor- und Nachteile der beiden Verfahren & hybride Verfahren . . . . .	242
10.3	Beispiele für symmetrische Verfahren – Cäsar-Chiffren & Co. . . . .	243
10.3.1	Monoalphabetische Substitution . . . . .	243

---

10.3.2 Polyalphabetische Substitution . . . . .	246
10.4 Ein Beispiel für asymmetrische Verschlüsselung – das RSA-Verfahren . . . . .	247
10.4.1 Grundidee des RSA-Verfahrens . . . . .	247
10.4.2 Wahl des Moduls und Generierung der Schlüssel . . . . .	251
10.4.3 Effektivität und Effizienz des Verfahrens . . . . .	253
10.5 Aufgaben . . . . .	255
<b>11 Ausblick: Quadratische Reste . . . . .</b>	<b>257</b>
11.1 Erste Begriffe und Erkundungen . . . . .	258
11.2 Erste Aussagen über quadratische Reste . . . . .	260
11.3 Das Legendre-Symbol und weitere Aussagen . . . . .	262
11.4 Das Quadratische Reziprozitätsgesetz . . . . .	263
<b>Lösungshinweise zu ausgewählten Aufgaben . . . . .</b>	<b>265</b>
<b>Liste der wichtigsten Symbole und Bezeichnungen . . . . .</b>	<b>273</b>
<b>Bisher erschienene Bände der Reihe Mathematik Primarstufe und     Sekundarstufe I + II . . . . .</b>	<b>277</b>
<b>Literatur . . . . .</b>	<b>279</b>
<b>Sachverzeichnis . . . . .</b>	<b>281</b>