

Andreas Bartholor...

Josef Rung

Hans Kern



dandelion.com

© 2008 [AGI-Information Management Consultants](#)  
May be used for personal purposes only or by  
libraries associated to [dandelion.com](#) network.

# Zahlentheorie für Einsteiger

Mit einem Geleitwort  
von Jürgen Neukirch



vieweg

# Inhaltsverzeichnis

<b>1</b>	<b>Vollständige Induktion</b>	<b>1</b>
1.1	Das kleinste Element . . . . .	1
1.2	Das Prinzip vom Maximum . . . . .	7
1.3	Das Induktionsprinzip. . . . .	8
1.4	Zusammenfassung . . . . .	21
<b>2</b>	<b>Euklidischer Algorithmus</b>	<b>24</b>
2.1	Teilen mit Rest. . . . .	24
2.2	Zahlen benennen. Stellenwertsysteme. . . . .	28
2.3	Rechnen mit langen Zahlen. . . . .	36
2.4	Der größte gemeinsame Teiler. . . . .	46
2.5	Das Rechnen mit Kongruenzen. . . . .	54
2.6	Ein wenig Geheimniskrämerei. . . . .	61
2.7	Primzahlen. . . . .	66
2.8	Ein kleiner Spaziergang zum Primzahlsatz . . . . .	79
2.9	Der chinesische Restsatz . . . . .	81
2.10	Die Euler-Funktion. . . . .	101
<b>3</b>	<b>Der kleine Fermatsche Satz</b>	<b>106</b>
3.1	Kleiner Fermat. . . . .	106
3.2	Die Ordnung einer Zahl modulo einer Primzahl. . . . .	113
3.3	Primitivwurzeln. . . . .	115
3.4	S. Germain's Beitrag zum Problem von Fermat . . . . .	127
3.5	Verschlüsseln mit dem Kleinen Fermat . . . . .	133
3.6	Logarithmieren modulo $p$ . . . . .	136
3.7	Einheiten in Primpotenzmoduln. . . . .	139
<b>4</b>	<b>Die Jagd nach großen Primzahlen</b>	<b>145</b>
4.1	Der negative Fermat-Test . . . . .	145
4.2	Pseudoprimzahlen. . . . .	153
4.3	Pseudoprimzahlen zur Basis $a$ und Carmichael-Zahlen . . . . .	160
4.4	Ein probabilistischer Primzahltest . . . . .	162

4.5	Primzahltest von Miller und Rabin - Starke Pseudoprimzahlen . . . . .	.164
4.6	RSA-Verschlüsselung . . . . .	.172
	Stichwortverzeichnis	<b>174</b>
	Literaturverzeichnis	<b>177</b>