Errata

zum Buch
Otto Forster: **Algorithische Zahlentheorie**, 2. Auflage
Springer Spektrum 2015, ISBN 978-3-658-06539-3

Stand: 22. Februar 2018

Seite 8, Zeile 3 von oben

`statt:` Assozitiv-Gesetz `richtig:` Assoziativ-Gesetz

Seite 13, Zeile 10 von unten

`statt:` $n_k = \sum_{i \geqslant k} b_i 2^i$ `richtig:` $n_k = \sum_{i \geqslant k} b_i 2^{i-k}$

Seite 27, Zeile 16 von oben

`statt:` $\ldots + Rx_n$ `richtig:` $\ldots + Rx_r$

Seite 27, Zeile 7 von unten

`statt:` $(y) \in (x)$ `richtig:` $(y) \subset (x)$

Seite 40, Zeile 8 von oben

`statt:` $\sum_{j=0}^{j} b_j X^j$ `richtig:` $\sum_{j=0}^{m} b_j X^j$

Seite 41, Zeile 3 von oben

`statt:` $G(X) = X^k + \sum_{\nu=1}^{k-1} b_\nu X^{k-\nu}, \quad H(X) = X^\ell + \sum_{\nu=1}^{\ell-1} c_\nu X^{\ell-\nu}$

`richtig:` $G(X) = X^k + \sum_{\nu=1}^{k} b_\nu X^{k-\nu}, \quad H(X) = X^\ell + \sum_{\nu=1}^{\ell} c_\nu X^{\ell-\nu}$

Seite 86, Zeile 16 von unten

`statt:` Piépin `richtig:` Pépin

Seite 86, Zeile 5 von unten

Die Information über die Fermatzahlen ist überholt. Die Zahl F_{24} wurde von Crandall/Mayer/Papadopoulos (Math. Comp. 72 (2002), pp. 1555 – 1572) einem Pépin-Test unterworfen, mit negativem Resultat (d.h. F_{24} ist nicht prim). Die kleinste Fermatzahl, von der man derzeit (Stand Jan. 2016) nicht weiß, ob sie prim oder zusammengesetzt ist, ist F_{33}.

Seite 116, Zeile 16 von oben

`statt:` Zahlen $p.\ q$ `richtig:` Zahlen $p,\ q$

Seite 132, Zeile 2 von oben

`statt:` $u_{i+1} := u - \ldots$ `richtig:` $u_{i+1} := u_i - \ldots$

Seite 171, Zeile 3 von unten

`statt:` `Count` `richtig:` `Count1, Count2`

Seite 172, Zeile 18 von oben

`statt:` `Count := 0;` `richtig:` `Count1 := Count2 := 0;`

Seite 182, Zeile 6 von oben

`statt:` sog subexponentielle `richtig:` sog. subexponentielle

Seite 182, Zeile 20 von oben

`statt:` $2^{1039} - 2$ `richtig:` $2^{1039} - 1$

Seite 185, Zeile 1 von oben

`statt:` $x \in G$ `richtig:` $x \in G_0$

Seite 186, Zeile 11 von oben

`statt:` Logrithmus `richtig:` Logarithmus

Seite 205, Zeile 17 von oben

`statt:` Vietàscher Wurzelsatz `richtig:` Vietascher Wurzelsatz

Seite 211, Zeile 9 von oben

Aufgabe 22.4.b) Zusätzliche Voraussetzung: $p \equiv 3 \bmod 4$.

Seite 258, Zeile 14 von oben

Der gegebene Beweis von Corollar 27.7 ist nur im Fall $c > 0$ gültig, da für die letzte Ungleichung benutzt wird, dass $v\sqrt{d} < u$.
Im Fall $c < 0$ kann man wie folgt schließen: Hier ist $u < v\sqrt{d}$. Die Ungleichung

$$|u - v\sqrt{d}| < \frac{\sqrt{d}}{u + v\sqrt{d}}$$

kann man umformen zu

$$\Big|\frac{v}{u} - \frac{1}{\sqrt{d}}\Big| < \frac{1}{u\,(u + v\sqrt{d})} < \frac{1}{2u^2}.$$

Nach Satz 27.6 ist daher v/u Näherungsbruch der Kettenbruch-Entwicklung von $1/\sqrt{d}$. Daraus folgt aber, dass u/v Näherungsbruch der Kettenbruch-Entwicklung von $\sqrt{d}$ ist. Dies ergibt sich mittels Satz 26.3 daraus, dass die Kettenbruch-Entwicklungen von $\sqrt{d}$ und $1/\sqrt{d}$ wie folgt zusammenhängen:

$$\sqrt{d} = \mathrm{cfrac}(a_0, a_1, a_2, a_3, ...) \quad \Longrightarrow \quad \frac{1}{\sqrt{d}} = \mathrm{cfrac}(0, a_0, a_1, a_2, a_3, ...).$$

Seite 281, Zeile 5 von unten

`statt:` ein ein Element `richtig:` ein Element

`statt:` Klassenruppe `richtig:` Klassengruppe

Seite 283, Zeile 21 von oben

`statt:` `cl_factorize0` `richtig:` `CLfactorize0`

Seite 304, Zeile 9 von oben

`statt:` bezeicnet `richtig:` bezeichnet

Seite 307, Zeile 12 von unten

`statt:` Samuuel `richtig:` Samuel

---

weitere Fehlermeldungen erbeten an
`forster@mathematik.uni-muenchen.de`