

Anmerkung zu S. 89

Auf Seite 89 oben wird die Wahrscheinlichkeit abgeschätzt, bei der zufälligen Wahl von s den Wert 0 oder einen zu r nicht teilerfremden Wert zu erhalten. Dies ist wie folgt zu ergänzen:

Die Anzahl der Primfaktoren von r ist höchstens $\log r$, da jeder Primfaktor mindestens den Wert 2 hat. Die Anzahl der Werte für s , die ungleich 0 und zu r teilerfremd sind, ist mindestens die Anzahl der Primzahlen im Bereich von 2 bis r abzüglich der Primfaktoren von r , also mindestens $r/(2 \log r) - \log r$. Die Wahrscheinlichkeit, ein „gutes“ s zu erhalten beträgt somit mindestens

$$\frac{(r/(2 \log r)) - \log r}{r}.$$

Für $r \geq 256$ ist dies mindestens $1/(4 \log r) \geq 1/(4 \log N)$. Für $r \in \{2, \dots, 255\}$ kann man vorab abtesten, ob r die gesuchte Ordnung ist, sodass wir diesen Fall vernachlässigen können. In den im Skript folgenden Abschätzungen sollte also die untere Schranke $1/(4 \log N)$ für die Erfolgswahrscheinlichkeit benutzt werden.