

## 2.1 Der Primzahlsatz

Sei  $\pi(x)$  die Anzahl aller Primzahlen  $p \leq x$ . Etwas allgemeiner sei  $\pi_{a,b}(x)$  die Anzahl der Primzahlen  $p \leq x$  der Form  $p = ak + b$ . Der Primzahlsatz ist die asymptotische Relation

$$\pi_{a,b}(x) \sim \frac{1}{\varphi(a)} \cdot \frac{x}{\ln(x)}$$

unter der Voraussetzung, daß  $a$  und  $b$  teilerfremd sind. Speziell für  $a = 1$  und  $b = 0$  wird asymptotisch geschätzt:

$$\pi(x) \sim \frac{x}{\ln(x)}.$$

Über die Qualität dieser Approximation gibt es viele theoretische und empirische Ergebnisse, zum Beispiel eine Formel von ROSSER und SCHOENFELD

$$\frac{x}{\ln(x)} \cdot \left(1 + \frac{1}{2 \ln(x)}\right) < \pi(x) < \frac{x}{\ln(x)} \cdot \left(1 + \frac{3}{2 \ln(x)}\right) \text{ für } x \geq 59.$$

Mit Hilfe des Primzahlsatzes kann man, wenn auch nicht völlig exakt, folgende Fragen beantworten:

**Wieviele Primzahlen  $< 2^k$  gibt es?**

Ungefähr

$$\frac{2^k}{k \cdot \ln(2)}$$

Stück, mindestens (für  $k \geq 6$ )

$$\frac{2^k}{k \cdot \ln(2)} \cdot \left(1 + \frac{1}{2k \ln(2)}\right).$$

Für  $k = 128$  sind das ungefähr  $3.8 \cdot 10^{36}$ , für  $k = 255$  ungefähr  $3.3 \cdot 10^{74}$ , für  $k = 256$  ungefähr  $6.5 \cdot 10^{74}$ .

**Wieviele  $k$ -Bit-Primzahlen gibt es?**

$\pi(2^k) - \pi(2^{k-1})$ , also ungefähr

$$\frac{2^k}{k \cdot \ln(2)} - \frac{2^{k-1}}{(k-1) \cdot \ln(2)} = \frac{2^{k-1}}{\ln(2)} \cdot \frac{k-2}{k(k-1)}$$

Stück. Für  $k = 128$  sind das ungefähr  $1.9 \cdot 10^{36}$ , für  $k = 255$  ungefähr  $1.6 \cdot 10^{74}$ , für  $k = 256$  ungefähr  $3.2 \cdot 10^{74}$ . Anders ausgedrückt ist eine zufällig gewählte  $k$ -Bit-Zahl mit der Wahrscheinlichkeit

$$\frac{\pi(2^k) - \pi(2^{k-1})}{2^{k-1}} \approx \frac{2}{k \cdot \ln(2)} - \frac{1}{(k-1) \ln(2)} = \frac{1}{\ln(2)} \cdot \frac{k-2}{k(k-1)}$$

Primzahl; für  $k = 256$  ist das ungefähr 0.0056.

Eine zuverlässige untere Schranke erhält man aus der Abschätzung

$$\pi(2^k) - \pi(2^{k-1}) > 0.71867 \cdot \frac{2^k}{k} \quad \text{für } k \geq 21.$$

Auf jeden Fall gibt es in den für das RSA-Verfahren relevanten Größenbereichen so viele Primzahlen, daß ein Exhaustionsangriff völlig wirkungslos bleiben müsste.