Prof. C. P. Schnorr Sommersemester 2004

Kryptographische Algorithmen

Blatt 6 02.06.2004, Abgabe 09.06.2004

Aufgabe 1. $n \in \mathbf{N}$ habe $t \geq 2$ verschiedene Primteiler. Zeige, dass man n zu gegebenem $\lambda(n)$ in $O(\log_2(n))$ arithmetischen Schritten mit Ws $\geq \frac{1}{2}$ zerlegen kann.

Hinweis: Berechne eine zufällige Quadratwurzel von 1 mod n.

Aufgabe 2. Sei $n = \Pi_{i=1}^{t} p_i^{e_i}$ ungerade, $n-1 = q2^k, q$ ungerade
und $a \in_R \{z \in \mathbf{Z}_n^* \mid z^{n-1} = 1 \bmod n\}$. Zeige:
Mit $\mathrm{Ws}_a \geq 1 - 2^{-t+1}$ gilt $\mathrm{ggT}(a^{q2^i} - 1, n) \notin \{1, n\}$ für ein i, $0 \leq i < k$.

Motivation: Für $t \geq 2$ bedeutet $z^{n-1} = 1 \bmod n$, dass der Fermat-Test die Nicht-Primheit von n mit z nicht erkennt.

Miller-Rabin Primzahltest. Sei $n = \prod_{i=1}^{t} p_i^{e_i}$, $n-1 = 2^k q$, q ungerade.

$$\mathrm{MR}(n) =_{\mathrm{def}} \{a \in \mathbf{Z}_n^* \mid a^q \neq 1 \bmod n, \quad \begin{array}{l} a^{q2^i} \neq -1 \bmod n \\ \text{für } i = 0, \ldots, k-1 \end{array} \}$$

Aufgabe 3. Zeige: $\mathrm{MR}(n) = \emptyset$ für $t = 1$.

Aufgabe 4. Zeige: $\#\ \mathrm{MR}(n)/\varphi(n) = \Omega(1)$ für $t \geq 2$.

Hinweis: o.B.d.A. $\lambda(n) \nmid n-1$, d.h. n ist keine Carmichaelzahl.
Es gilt sogar $\#\ \mathrm{MR}(n)/\varphi(n) \geq \frac{3}{4}$.