Goethe-Universität, Frankfurt am Main
Sommersemester 2008
Prof. Dr. C.P. Schnorr, Antoine Scemama

Diskrete Mathematik, Übung 6

Aufgabe 1. Zeige, dass im Miller-Rabin Test mindestens die Hälfte der $a \in \mathbb{Z}_N^*$ Zeugen für die Nicht-Primheit eines nicht primen N sind.
Hinweis: Knuth, Vol. 2 Aufgabe 4.5.4 (22), Crandall, Pomerance (2001), Thm. 3.4.4.

Aufgabe 2. Zeige: N ist Carmichael-Zahl gdw $N = p_1 \cdots p_r$ Produkt von $r \geq 3$ verschiedene Primzahlen $p_1, \ldots, p_r$ ist, so dass $(p_j - 1) \mid (\frac{N}{p_j} - 1)$ für $j = 1, \ldots, r$.
Hinweis: Satz 4.12 (Skript)

Eine **Blum-Zahl** ist ein RSA–Modul $N = pq$ mit p, q prim und $p, q = 3 \bmod 4$.

Aufgabe 3. Zeige, dass für Blum-Zahlen N gilt
1. $-1 \notin \mathrm{QR}_N = (\mathbf{Z}_N^*)^2$,
2. Jedes $x \in \mathrm{QR}_N$ hat genau eine Quadratwurzel in QR_N
3. $|\mathrm{QR}_N| = \varphi(N)/4 = 1 \bmod 2$.

Hinweis: $-1 \in \mathrm{QR}_N$ impliziert $-1 \in \mathrm{QR}_p$ und $-1^{(p-1)/2} = 1 \mod p$.

Rabin-Schema öffentl. Blum-Zahl N, geheim $\varphi(N)$

$$E : \mathrm{QR}_N \to \mathrm{QR}_N, \quad E(x) = x^2 \bmod N$$
$$D : \mathrm{QR}_N \to \mathrm{QR}_N, \quad D(x) = x^{2^{-1} \bmod (\varphi(N)/4)} \bmod N.$$

Aufgabe 4. Zeige
1. $E \circ D = D \circ E = \mathrm{id}_{\mathrm{QR}_N}$
2. Jeder Algorithmus zu D liefert die Zerlegung von N
3. Für $x \in_R \mathbf{Z}_N^*$ liefert $D(x^2)$ mit $\mathrm{Ws}_x = \frac{1}{2}$ die Zerlegung von N.

Abgabetermin dieses Blattes: Montag 26. Mai 2008, 10.10 Uhr

Übungsblätter im Internet:
www.mi.informatik.uni-frankfurt.de:
Teaching, Diskrete Mathematik.