J.W. Goethe-Universität, Frankfurt am Main

Sommersemester 2008

Prof. Dr. C.P. Schnorr, Antoine Scemama

Diskrete Mathematik, Übung 5

Aufgabe 1. Finde eine Gauss'sche ganze Zahl $z \in \mathbb{Z}[i]$, so dass

$$z = 2 \bmod 3, \quad z = 1 \mod (1+2i), \; z = 0 \bmod 2 \; .$$

Dabei bedeute $z = c \mod m$, dass $\exists t \in \mathbb{Z}[i]$: $z = c + tm$.

Aufgabe 2. Gegeben seien drei RSA–Moduln $N_1 < N_2 < N_3$ und $x^3 \bmod N_i$ für $i = 1, 2, 3$ für ein $x \in [0, N_1[$.

Zeige, dass $x \in [0, N_1[$ in pol. Zeit berechenbar ist.

(Somit darf beim RSA-Schema mit Kodierexponent e dieselbe Nachricht x nicht mit e verschiedenen Moduln N_i kodiert werden.)

Aufgabe 3.
Ordne den Buchstaben $A, \ldots, Z$ die ersten 26 zu $7 \cdot 19 = 133$ teilerfremden Zahlen > 1 zu.
Verschlüssele die Nachricht `GEHEIM` im RSA–Schema mit $N = 133$ und $e = 5$.
Bestimme $\varphi(N)$, $\lambda(N)$, $e^{-1} \bmod \varphi(N)$, $e^{-1} \bmod \lambda(N)$.

Aufgabe 4. Sei $N \in \mathbb{N}$ ungerade mit Primfaktorzerlegung $N = \prod_{i=1}^{r} p_i^{e_i}$. Zeige
1. Jedes $a \in \mathrm{QR}_N = \{b^2 \mid b \in \mathbb{Z}_N^*\}$ hat genau 2^r Quadratwurzeln in $\mathbb{Z}_N^*$.
2. Für zufällige $x, y \in \mathbb{Z}_N^*$ mit $x^2 = y^2 \bmod N$ gilt

$$\mathrm{Ws}[\mathrm{ggT}(x \pm y, N) \neq 1] = 1 - 2^{-r+1} \; .$$

Hinweis:
$$\mathbb{Z}_N^* \cong \mathbb{Z}_{p_1^{e_1}}^* \times \cdots \times \mathbb{Z}_{p_r^{e_r}}^*$$
$$\#\{x \in \mathbb{Z}_N^* \mid x^2 = z \mod N\} = 2^r \text{ gilt für alle } z \in QR_N.$$

Abgabetermin dieses Blattes: Donnerstag 15. Mai 2008, 12.10 Uhr

Übungsblätter im Internet:

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