Prof. C. P. Schnorr Sommersemester 2006

Diskrete Mathematik

Blatt 5, 19.05.2006, Abgabe 26.05.2006

Aufgabe 1. 5 Punkte. Zeige: $p = 2^{16} - 15$ ist prim.

Hinweis: $p - 1$ zerfällt in kleine Primfaktoren.

Aufgabe 2. 3 Punkte. 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. 5 Punkte. Finde eine Gauss'sche ganze Zahl $z \in \mathbf{Z}[i]$, so dass

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

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

Aufgabe 4. 6 Punkte. Sei $N \in \mathbf{N}$ ungerade mit Primfaktorzerlegung $N = \prod_{i=1}^{r} p_i^{e_i}$. Zeige

1. Jedes $a \in \mathrm{QR}_N = \{b^2 \mid b \in \mathbf{Z}_N^*\}$ hat genau 2^r Quadratwurzeln in $\mathbf{Z}_N^*$.
2. Für zufällige $x, y \in \mathbf{Z}_N^*$ mit $x^2 = y^2 \bmod N$ gilt

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