Prof. C. P. Schnorr Sommersemester 2004

Kryptographische Algorithmen

Blatt 8 02.07.2004, Abgabe 09.07.2004

Aufgabe 1. 1. Löse $x^2 + y^2 = 221 = 13 \cdot 17$ über $\mathbf{Z}$.

2. Berechne $U, U^{-1} \in \mathrm{GL}_3(\mathbf{Z})$ mit

$$U^t \begin{bmatrix} 1 & & \\ & 1 & \\ & & -N \end{bmatrix} U = \begin{bmatrix} & 1 & \\ 1 & d & \\ & & N \end{bmatrix}, \ d \in \{0, 1\}.$$

3. Löse $x^2 + y^2 - 221z^2 = 10$ mittels U^{-1}.

Aufgabe 2. Ersetze im Signaturschema die Gleichung $x^2 + y^2 - Nz^2 = 0$ durch $x^2 - y^2 + Nz^2 = 0$.

Beschreibe den geheimen Schlüssel, die Schlüsselaufbereitung, Berechnung von $U \in \mathrm{GL}_2(\mathbf{Z})$ und die Signaturerzeugung.

Aufgabe 3. Ersetze in Aufgabe 1 $x^2 + y^2 = 221z^2$ durch $x^2 - y^2 + 221z^2$.