TECHNISCHE UNIVERSITÄT BERLIN Wintersemester 2004/ 2005
Fakultät II – Institut für Mathematik
Dozent: Prof. Dr. F. HESS
WM: M. WAGNER
www.math.tu-berlin.de/~hess/krypto2

1. Übung Kryptographie II

1. Aufgabe Smith-Normalform (6 Punkte)

Berechnen Sie die Smith-Normalform $S(A)$ der Matrix $A \in \mathbb{Z}^{5\times 4}$ mit

$$A = \begin{pmatrix} 12 & 6 & 21 & 9 \\ 19 & 6 & 0 & 21 \\ 2 & 5 & 1 & 17 \\ 1 & 1 & 0 & 13 \\ 63 & 22 & 11 & 15 \end{pmatrix}.$$

Schreiben Sie dabei jeden Schritt auf (d.h. die Berechnung der einzelnen unimodularen Matrizen). Wie sehen die unimodularen Matrizen $U \in \mathbb{Z}^{5\times 5}$ und $V \in \mathbb{Z}^{4\times 4}$ mit $S(A) = UAV$ aus?

2. Aufgabe Homomorphie-Satz f¨ur Moduln (4 Punkte)

Beweisen Sie den Homomorphiesatz für unitäre R-Moduln N, M, wobei R ein kommutativer Ring mit 1 und nullteilerfrei ist.

3. Aufgabe Hermite-Normalform (6 Punkte)

Gegeben seien die Matrizen $B, A \in \mathbb{Z}^{4\times 3}$ mit

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 0 & 1 \\ 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix} \text{ und } B = \begin{pmatrix} 1 & 2 & 13 \\ 0 & 10 & 1 \\ 2 & 5 & 2 \\ 1 & 22 & 13 \end{pmatrix}.$$

Zeigen Sie, daß durch die Spalten der Matrix A ein $\mathbb{Z}$-Modul gegeben und daß der Kern von A ein $\mathbb{Z}$-Modul ist. Berechnen Sie den Kern von A. Berechnen Sie den Schnitt der $\mathbb{Z}$-Moduln, die durch die Matrizen A und B erzeugt werden. Welche Information erhält man immer aus der Hermite-Normalform von A über das von A erzeugte $\mathbb{Z}$-Modul?

Gesamt: 16 Punkte