Übungsblatt 3

Kryptographie und Kodierungstheorie
WiSe 16/17

Aufgabe 3.1. Zeigen Sie, dass die Faktorgruppe $\mathbb{Q}/\mathbb{Z}$ nicht endlich erzeugt ist.

Aufgabe 3.2. Beweisen Sie den Elementarteilersatz, d.h. zu jeder Matrix $N \in \mathbb{Z}^{r\times n}$ mit $r \leq n$ und $\operatorname{rank}(N) = r$ existieren positive ganze Zahlen $e_1 \mid e_2 \mid \cdots \mid e_r$ und Matrizen $R \in \mathrm{GL}(r,\mathbb{Z}), S \in \mathrm{SL}(n,\mathbb{Z})$, sodass

$$N = R \left(\begin{array}{ccc|ccc} e_1 & & & 0 & \cdots & 0 \\ & \ddots & & \vdots & \ddots & \vdots \\ & & e_r & 0 & \cdots & 0 \end{array}\right) S.$$

Hinweis: Euklidischer Algorithmus von links und von rechts.

Aufgabe 3.3. Sei

$$0 \longrightarrow A \longrightarrow B \xrightarrow{p} C \longrightarrow 0$$

eine exakte Sequenz abelscher Gruppen und es gelte $B \cong A \oplus C$. Zeigen Sie, dass dann ein Schnitt $s : C \longrightarrow B$ existiert, d.h. es ein solches s gibt mit $p \circ s = \mathrm{id}_C$.

Aufgabe 3.4. Beschreiben Sie die Dechiffrierung einer im CFB-Modus verschlüsselten Nachricht.

Aufgabe 3.5. Eine Nachricht über dem Alphabet $\Sigma = \{\_, A, B, \ldots, Z\} = \mathbb{Z}/27\mathbb{Z}$, wobei _ für das Leerzeichen steht, wird mit der Hill-Chiffre ($n = 5$) im CFB-Modus mit Blocklänge 3 chiffriert. Das Resultat ist

```
DNKXUQMCXYBATIPRXOMZZXBMOFRAUTVOPKGNZBZQVPYM
AXRCMIMRXPJMOJIZOWGLNEAODTRSMNVTUJRNYULGZS Q
W WSSBHMNRKIPTXIJGSDJGCOAOCQRXRMQRJLRHPJIQKC
KAFQIXYXOOZTQLGCFHGNNBIAKUCXAK JWGDOFBR IEHJ
SE ULYXLOUSCLEVYHOTVHRATLHQRKJTXCT EYEGIQK P
IEGHWRXWPLCQCUSVKH GBBSKEUWDAIQDTZAWU VJRQJA
EWP HTPZQ WGFTFAIWMNNRESOBXQIZSKXGPLHALTWBRH
ZPGEPWX BJHHNXZHKYTQBDZMASSFIPWVHNAQYDVP
```

Wie lautet die Nachricht?
Hinweis: Sie sollten einen Computer benutzen. Der Initialisierungsvektor ist genau die erste Zeile der Schlüsselmatrix, welche die Gestalt

$$\begin{pmatrix} 3 & 8 & * & 1 & 0 \\ 0 & 0 & 2 & 24 & 5 \\ 6 & 0 & 0 & 15 & 22 \\ 21 & 17 & 11 & 0 & 1 \\ 8 & 15 & 26 & 13 & 9 \end{pmatrix}$$

hat.