Hochschule für
Technik und Wirtschaft
des Saarlandes
University of Applied Sciences

Studiengang Kommunikationsinformatik (Master)
Prof. Dr.–Ing. Damian Weber

Sicherheit und Kryptographie – Übung 3

Aufgabe 1 (Erweiterter ggT)

a) Benutzen Sie den erweiterten Euklidischen Algorithmus, um $\frac{1}{30}$ in $\mathbf{F}_{167}$ auszurechnen. Überprüfen Sie das Resultat durch geschicktes Multiplizieren ohne Taschenrechner.

b) Benutzen Sie den erweiterten Euklidischen Algorithmus, um $\frac{1}{X^2+1}$ in

$$\mathbf{F}_{5^3} = \mathbf{F}_5[X]/(X^3 + X + 1)$$

zu bestimmen.

Aufgabe 2 (Teilbarkeit)

Für zwei Elemente a, b eines Rings R bedeutet a *teilt* b $(a|b)$, dass $c \in R$ existiert mit $a \cdot c = b$.

a) Zeigen Sie: Teilbarkeit ist eine Relation, die reflexiv und transitiv ist.

b) Wenn $a|1$ so heißt a eine Einheit von R. Die Menge der Einheiten eines Rings R wird mit R^* bezeichnet.

i) Finden Sie alle Einheiten von $\mathbf{Z}$.

ii) Zeigen Sie, daß $3 + 2\sqrt{2}$ eine Einheit des Rings

$$\mathbf{Z}[\sqrt{2}] = \{c + d\sqrt{2} \mid c, d \in \mathbf{Z}\}$$

ist. Finden Sie unendlich viele Einheiten des Rings $\mathbf{Z}[\sqrt{2}]$.