TECHNISCHE UNIVERSITÄT BERLIN SS 2008
Fakultät II – Institut für Mathematik
Dozent: Prof. Dr. Michael Pohst
Assistent: Osmanbey Uzunkol Abgabe:26.06.2008
`www.math.tu-berlin.de/~kant/algebra1-ss2008` in der Übung

10. Übung Algebra I

(Primideale, noethersche Ringe, Teilbarkeit in Ringen)

---

1. Aufgabe

Bestimmen Sie den Durchschnitt sämtlicher Primideale von $\mathbb{Z}/n\mathbb{Z}$ für $n \in \mathbb{N}$.

(4 Punkte)

2. Aufgabe

Ein Ring R mit 1 heißt **Boolescher** Ring, falls für alle $x \in R$ die Gleichung $x^2 = x$ gilt.

(a) Zeigen Sie, dass nicht trivialle Booleschen Ringe die Charakteristik 2 besitzen.

(b) $\mathcal{A} \neq \{0\}$ sei ein echtes Ideal eines Booleschen Ringes R. Zeigen Sie, dass $\mathcal{A}$ genau dann ein Primideal ist, falls $\mathcal{A}$ ein maximales Ideal ist.

(3 Punkte)

3. Aufgabe

Es seien R ein noetherscher Ring und P ein Primideal von R. Zeigen Sie, dass die Lokalisierung von R bei P auch noethersch ist.

(3 Punkte)

4. Aufgabe

(a) Es sei R ein Integritätsring mit 1. Wir definieren die folgende Relation:

$$a \sim b :\Leftrightarrow \text{es existiert eine Einheit } \epsilon \text{ mit } a = \epsilon b.$$

Zeigen Sie, dass $\sim$ eine Äquivalenzrelation ist. Bestimmen Sie die Äquivalenzklassen, falls R zusätzlich ein Boolescher Ring ist.

(b) Es sei R ein Integritätsring mit 1 und $a_1, \cdots, a_n \in R$. Zeigen Sie:
Ist $p \in R$ ein Primelement und $p | a_1 \cdots a_n$, dann existiert ein j mit $p | a_j$.

(c) R sei ein Intergitätsring mit $a_1, \cdots, a_n \in R$. Zeigen Sie, dass die folgende Relation gilt:

$$\mathrm{ggT}(a_1, \cdots, a_n) \sim \mathrm{ggT}((a_1, \cdots, a_{n-1}), a_n),$$

wobei $\sim$ die im Teil (a) definierte Äquivalenzrelation ist.

(4 Punkte)

5. Aufgabe*

Zeigen Sie, dass jedes Primideal P in einem kommutativen Ring R mit 1 genau dann ein Hauptideal ist, falls jedes Ideal I in R ein Hauptideal ist.

(3+2 Punkte)

6. Aufgabe

Implementieren die das in der Übung erwähnte RSA Verfahren in `KASH3`. Betrachten Sie dafür das Alphabet

$$\{A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z\},$$

wobei A die Position 0 hat, B die Position 1 usw. Worte werden wie folgt verschlüsselt:

Ist ein Wort gegeben, z.B. "HALLO", so wird zuerst eine Liste L der Positionen der Buchstaben des gegeben Wortes im Alphabet erstellt. Hier wäre das $[7, 0, 11, 11, 14]$, d.h. also $H \leftrightarrow 7$, $A \leftrightarrow 0$ usw. Dann wird daraus eine Zahl $k \in \mathbb{N}$ berechnet wie folgt:

$$k = 7 \cdot 26^4 + 0 \cdot 26^3 + 11 \cdot 26^2 + 11 \cdot 26 + 14,$$

also eine 26-adische Darstellung. Dann benutzen Sie die Zahl, die Sie von oben genantem Verschlüsselungsverfahren erhalten haben, um die Nachrichten mittels RSA zu ver- und entschlüsseln.

(3+2 Punkte)

Hinweis: Die 6. Aufgabe kann bis 03.07.2008 abgegeben werden.