RUHR UNIVERSITÄT BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Gottfried Herold

Hausübungen zur Vorlesung

Zahlentheorie

SS 2013

Blatt 5 / 3. Mai 2013 / Abgabe bis spätestens 13. Mai 2013, 12:00 Uhr in dem Kasten auf NA 02 oder am Anfang der Vorlesung

Geben Sie bitte die Aufgaben zur Vereinfachung der Korrektur folgendermassen nach Aufgaben getrennt ab:

- Aufgaben 1,2 in Kasten A
- Aufgaben 3,4 in Kasten B
- Aufgabe 5 in Kasten C

Die Kästen auf NA 02 sind entsprechend beschriftet. Wenn Sie in der Vorlesung abgeben, machen sie einfach 3 getrennte Stapel. Schreiben Sie auf alle 3 Abgaben jeweils Ihre(n) Namen und/oder Matrikelnummer(n).
Bitte schreiben Sie auf Ihre Abgaben eine Sollrückgabestelle (Übungsgruppe, Zentralübung, persönlich in NA5/74).

AUFGABE 1 (4 Punkte)**:**
Seien $n, m \in \mathbb{Z}, n, m > 0$ beliebig, nicht notwendig teilerfremd. Zeigen Sie:

(a) $\phi(n) \cdot \phi(m) = \phi(\text{ggT}(n, m)) \cdot \phi(\text{kgV}(n, m))$

(b) $\phi(nm) = \phi(n) \cdot \phi(m) \cdot \frac{\text{ggT}(n,m)}{\phi(\text{ggT}(n,m))}$

AUFGABE 2 (3 Punkte)**:**
Sei $N > 1$ quadratfrei, d.h. in der Primfaktorzerlegung von N kommt kein Primfaktor mehrfach vor. Sei weiterhin e teilerfremd zu $\phi(N)$ und d so gewählt, dass $de \equiv 1 \mod \phi(N)$.
Zeigen Sie, dass dann für alle $a \in \mathbb{Z}$ gilt: $a^{ed} \equiv a \mod N$.
Beachten Sie, dass wir nicht fordern, dass a teilerfremd zu N ist.

— bitte wenden —

AUFGABE 3 (4 Punkte)**:**

(a) Zeigen Sie, dass $X^2 + 1 \in \mathbb{F}_7[X]$ irreduzibel ist.

Betrachten Sie nun den Körper $\mathbb{F}_{49} = \mathbb{F}_7[X]/(X^2 + 1)$.

(b) Bestimmen Sie die Lösungsmenge folgenden linearen Gleichungsystems über $\mathbb{F}_{49}$ in den Unbekannten $v_1, v_2 \in \mathbb{F}_{49}$:

$$\begin{aligned} \overline{2X} \cdot v_1 + \overline{3X + 5} \cdot v_2 &= \overline{1} \\ \overline{3X + 5} \cdot v_1 + \overline{2X + 5} \cdot v_2 &= \overline{4X + 1} \end{aligned}$$

AUFGABE 4 (3 Punkte)**:**
Welche der folgenden abelschen Gruppen (=$\mathbb{Z}$-Moduln) sind endlich erzeugt? Begründen Sie jeweils ihre Antwort.

(a) $(\mathbb{Q}, +)$

(b) $U_n = ((\mathbb{Z}/n\mathbb{Z})^*, \cdot)$

(c) $(\mathbb{F}_p[X]/(f), +)$, wobei p Primzahl und $f \in \mathbb{F}_p[X]$ normiertes Polynom (nicht notwendig irreduzibel).

AUFGABE 5 (6 Punkte)**:**
Wir haben Körper bislang als Restklassen von Polynomen konstruiert. In dieser Aufgabe wollen wir sehen, dass wir diese Körper auch als Unterringe des Matrizenrings konstruieren können.
Sei K ein beliebiger Körper und q ein beliebiges Polynom in $K[X]$ von Grad $n > 0$. Wir betrachten $L := K[X]/(q)$, was für irreduzible q ein Körper ist. Wie in der Vorlesung ist ein vollständiges Repräsentantensystem R für L gegeben durch die Polynome von Grad $< n$ $R = \{\hat{f} = \hat{f}_0 + \hat{f}_1 X + \ldots + \hat{f}_{n-1} X^{n-1} \mid \hat{f}_i \in K\}$. Der eindeutige Repräsentant $\hat{f} \in R$ von $f \in L$ ist dabei der Rest der Polynomdivision von f durch q. Für $f \in L$ sei f_{coo} der (Spalten-) Koordinatenvektor $(\hat{f}_0, \hat{f}_1, \ldots, \hat{f}_{n-1})^T \in K^n$ des eindeutigen Repräsentanten $\hat{f} = \sum_{i=0}^{n-1} \hat{f}_i X^i \in R$ von f.
Sei $\Psi : L \to K^{n \times n}$ gegeben durch

$$\Psi(f) = \left(f_{\text{coo}}, (Xf)_{\text{coo}}, (X^2 f)_{\text{coo}}, \ldots, (X^{n-1} f)_{\text{coo}}\right),$$

wobei $(f_{\text{coo}}, \ldots, (X^{n-1} f)_{\text{coo}})$ eine $n \times n$-Matrix ist.
Zeigen Sie:

(a) Für alle $f, g \in L$ gilt $\Psi(f) \cdot g_{\text{coo}} = (f \cdot g)_{\text{coo}}$, wobei das Produkt auf der linken Seite Matrix-Vektor-Multiplikation ist und auf der rechten Seite die Multiplikation in L.

(b) Ψ ist ein injektiver Ringhomomorphismus.

(c) Geben Sie einen Unterring von $\mathbb{R}^{2\times 2}$ an, der isomorph zu $\mathbb{C}$ ist.

Hinweise/Bemerkungen: Teil (a) besagt, dass $\Psi(f)$ ist die darstellende Matrix der Abbildung $L \ni g \mapsto fg \in L$ bzgl. der K-Basis $1, X, \ldots, X^{n-1}$ von L ist.
Vermeiden Sie es, in Teil (b) das Produkt zweier Matrizen zu berechnen. Benutzen Sie stattdessen das Ergebnis von (a) sowie die Tatsache, dass zwei Matrizen $A, B \in K^{n \times n}$ gleich sind, genau dann wenn $Av = Bv$ für alle Vektoren $v \in K^n$.