# Mathematische Grundlagen der Kryptografie (1321) SS 06

**Nachklausur am 30.9.2006:**

**Aufgabenstellungen**

**I. Die Lösungen der folgenden Aufgaben brauchen Sie nicht zu begründen.**

### Aufgabe I.1

(Eine Umrechnungstabelle zwischen Buchstaben und Elementen aus $\mathbb{Z}/26\mathbb{Z}$ befindet sich am Ende der Klausur.)

(a) Der folgende Geheimtext ist mit dem Verschiebe-Kryptosystem und dem Schlüssel 18 verschlüsselt:

NAWD

Wie lautet der Klartext?

(b) Der folgende Geheimtext ist mit dem affinen Kryptosystem und dem Schlüssel $(9, 2)$ verschlüsselt:

MZVYXE

Wie lautet der Klartext?

(c) Der folgende Geheimtext ist mit dem Permutationskryptosystem mit dem Schlüsselwort VIGENERE und dem Schlüsselbuchstaben X verschlüsselt:

CXBT

Wie lautet der Klartext?

(d) Der folgende Geheimtext ist mit dem Selbstschlüssel-Kryptosystem und dem Schlüssel 5 verschlüsselt:

ILM

Wie lautet der Klartext?

(e) Der folgende Geheimtext ist mit dem Vigenère-Kryptosystem und dem Schlüsselwort EUKLID verschlüsselt.

OFKFAXV

Wie lautet der Klartext?

[*2 + 2 + 2 + 2 + 2 = 10 Punkte*]

**Aufgabe I.2**

Gegeben sei $\mathbb{F}_{19}^{\times}$.

(a) Wieviele erzeugende Elemente gibt es in $\mathbb{F}_{19}^{\times}$?

(b) Bestimmen Sie ein erzeugendes Element.

(c) Bestimmen Sie alle erzeugenden Elemente.

(d) Wieviele Elemente der Ordnung 6 gibt es?

[*2 + 4 + 2 + 2 = 10 Punkte*]

**Aufgabe I.3**

Bestimmen Sie das Minimalpolynom von $\sqrt{3+i}$ über $\mathbb{Q}$ (dabei ist $i$ die komplexe Zahl mit $i^2 = -1$).

[*4 Punkte*]

**Aufgabe I.4**

Was besagt der kleine Satz von Fermat?

[*4 Punkte*]

**Aufgabe I.5**

Geben Sie jeweils ein Beispiel für einen Ring $R$, der kein Körper ist, und zwei Elemente $r, s \in R$, so dass $r$ und $s$ Einheiten sind und

(a) $r + s$ ist ebenfalls eine Einheit in $R$.

(b) $r + s$ ist keine Einheit in $R$.

*[2 + 2 = 4 Punkte]*

**II. Die Lösungen der folgenden Aufgaben sollen begründet werden.**

### Aufgabe II.1

Sei $p$ eine Primzahl und $n \in \mathbb{N}$. Zeigen Sie, dass es für jedes $x \in \mathbb{F}_{p^n}$ genau eine $p$-te Wurzel gibt, das heißt, genau ein $y \in \mathbb{F}_{p^n}$ mit $y^p = x$.

[*8 Punkte*]

### Aufgabe II.2

Seien $p$ und $q$ verschiedene Primzahlen mit $p \equiv q \equiv 3(\mathrm{mod}4)$. Zeigen Sie: Hat die Gleichung $x^2 \equiv q(\mathrm{mod}p)$ keine Lösung, dann hat die Gleichung $x^2 \equiv p(\mathrm{mod}q)$ genau zwei Lösungen in $\mathbb{Z}/q\mathbb{Z}$.

[*8 Punkte*]

### Aufgabe II.3

Zeigen Sie, dass $L = \{x \in \mathbb{Z}^3 \mid \begin{pmatrix} 1 & 2 & 2 \\ 0 & 1 & 2 \\ 1 & 1 & 2 \end{pmatrix} x \equiv 0(\mathrm{mod}2)\}$ ein Gitter ist und bestimmen Sie $\det L$.

[*10 Punkte*]

### Aufgabe II.4

Beschreiben Sie den Primzahltest von Solovay-Strassen (jeweils in wenigen Sätzen).

(a) Auf welcher mathematischen Aussage beruht der Test?

(b) Was sind Eingabe und Ausgabe des Tests?

(c) Wie geht man vor?

(d) Warum ist der Test ein so genannter probabilistischer Algorithmus?

[*2 + 2 + 4 + 4 = 12 Punkte*]

**Aufgabe II.5**

Sei $M = \{z^5 - z \mid z \in \mathbb{Z}\}$ und sei $I$ das kleinste Ideal in $\mathbb{Z}$, das $M$ enthält. Dann gilt $I = n\mathbb{Z}$ für ein $n \in \mathbb{N}$. Bestimmen Sie $n$.

[*10 Punkte*]

**Hinweis:** Die Buchstaben A,..,Z entsprechen folgenden Elementen aus $\mathbb{Z}/26\mathbb{Z}$:

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 |

| S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|
| 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |