Mathematische Grundlagen der Kryptografie (1321)SoSe 06

Nachklausur am 30.9.2006:

Lösungsvorschläge zu den Aufgaben

zu Aufgabe I.1

(a) Der Geheimtext als Folge von Elementen aus $\mathbb{Z}/26\mathbb{Z}$ ist $[13, 0, 22, 3]$. Zum Entschlüsseln muss nun der Schlüssel 18 in $\mathbb{Z}/26\mathbb{Z}$ jeweils subtrahiert werden. Dies ergibt $[21, 8, 4, 11]$ oder VIEL.

(b) In $\mathbb{Z}/26\mathbb{Z}$ gilt $9^{-1} = 3$, also ist die Entschlüsselungsabbildung $y \mapsto 3(y - 2) \bmod 26$. Der Geheimtext als Folge von Elementen aus $\mathbb{Z}/26\mathbb{Z}$ ist $[12, 25, 21, 24, 23, 4]$. Mit der Entschlüsselungsabbildung wird daraus $[4, 17, 5, 14, 11, 6]$ oder ERFOLG.

(c) Das Permutationskryptosystem mit dem Schlüsselwort VIGENERE und dem Schlüsselbuchstaben X liefert folgende Verschlüsselungsabbildung:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
E	N	R	A	B	C	D	F	H	J	K	L	M	O	P	Q	S	T

S	T	U	V	W	X	Y	Z
U	W	X	Y	Z	V	I	G

Der Klartext ist also FUER.

(d) Der Geheimtext als Folge von Elementen aus $\mathbb{Z}/26\mathbb{Z}$ ist $[8, 11, 12]$. Beim Selbstschlüssel-Kryptosystem mit Schlüssel 5 ist also das erste Element des Klartextes $8 - 5 = 3$. Das zweite Element ist nun $11 - 3 = 8$ und das dritte ist $12 - 8 = 4$. Der Klartext ist also DIE.

(e) Das Schlüsselwort Euklid ist $[4, 20, 10, 11, 8, 3]$ als Folge von Elementen aus $\mathbb{Z}/26\mathbb{Z}$. Diese Folge wird nun vom Geheimtext $[14, 5, 10, 5, 0, 23, 21]$ subtrahiert. Das ergibt $[10, 11, 0, 20, 18, 20, 17]$ oder KLAUSUR.

zu Aufgabe I.2

(a) $\mathbb{F}_{19}^{\times}$ ist eine zyklische Gruppe mit 18 Elementen. Es gibt also mit Proposition 4.8.5 genau $\varphi(18) = 6$ erzeugende Elemente.

(b) Wir versuchen 2 als erzeugendes Element. Es ist $2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 16, 2^5 = 13, 2^6 = 7, 2^7 = 14, 2^8 = 9, 2^9 = 18, 2^{10} = 17, 2^{11} = 15, 2^{12} = 11, 2^{13} = 3, 2^{14} = 6, 2^{15} = 12, 2^{16} = 5, 2^{17} = 10, 2^{18} = 1$ in $\mathbb{F}_{19}$. Also ist 2 ein erzeugendes Element.

(c) Mit Proposition 4.8.5 sind die erzeugenden Elemente nun von der Form 2^k mit $\mathrm{ggT}(k, 18) = 1$. Also sind $2^1 = 2$, $2^5 = 13$, $2^7 = 14$, $2^{11} = 15$, $2^{13} = 3$ und $2^{17} = 10$ die erzeugenden Elemente von $\mathbb{F}_{19}^\times$.

(d) Da 6 ein Teiler von 18, der Gruppenordnung ist, gibt es mit Proposition 4.8.5 gerade $\varphi(6) = 2$ Elemente der Ordnung 6. (Diese sind 8 und 12.)

zu Aufgabe I.3

Sei $x = \sqrt{3+i}$. Dann gilt $x^2 = 3+i$ und $x^2-3 = i$, also $(x^2-3)^2 = x^4-6x^2+9 = -1$. Es folgt $x^4-6x^2+10 = 0$. Auf jeden Fall ist also $\sqrt{3+i}$ eine Nullstelle des Polynoms $T^4-6T^2+10 \in \mathbb{Q}[T]$, und damit ist das Minimalpolynom ein Teiler dieses Polynoms. Die Nullstellen dieses Polynoms über $\mathbb{C}$ sind $\sqrt{3+i}, -\sqrt{3+i}, \sqrt{3-i}$ und $-\sqrt{3-i}$. Also gilt $T^4 - 6T^2 + 10 = (T - \sqrt{3+i})(T + \sqrt{3+i})(T - \sqrt{3-i})(T + \sqrt{3-i})$. Ein echter Faktor des Polynoms in $\mathbb{Q}[T]$ müsste den Grad zwei haben, denn ein Faktor vom Grad eins ist ein Linearfaktor, und die liegen nicht in $\mathbb{Q}[T]$ und bei einem Faktor vom Grad drei bleibt ein Linearfaktor über, der nicht in $\mathbb{Q}[T]$ liegt, und das kann auch nicht sein. Nun kann man aber leicht ausrechnen, dass weder $(T - \sqrt{3+i})(T + \sqrt{3+i})$ noch $(T - \sqrt{3+i})(T - \sqrt{3-i})$ noch $(T - \sqrt{3+i})(T + \sqrt{3-i})$ in $\mathbb{Q}[T]$ liegen. Damit ist $T^4 - 6T^2 + 10$ irreduzibel über $\mathbb{Q}$, es ist normiert und hat $\sqrt{3+i}$ als Nullstelle, also ist es das Minimalpolynom von $\sqrt{3+i}$ über $\mathbb{Q}$.

zu Aufgabe I.4

Der kleine Satz von Fermat besagt, dass für eine Primzahl p und ein $a \in \mathbb{N}$ mit $\mathrm{ggT}(a, p) = 1$ immer $a^{p-1} \equiv 1 (\mathrm{mod} p)$ gilt.

zu Aufgabe I.5

(a) Sei $R = \mathrm{M}_{22}(\mathbb{R})$, die Menge aller 2×2-Matrizen über $\mathbb{R}$. Sei $r = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Dann ist r eine Einheit in R, denn $\det(r) = 1$. Sei $s = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$. Dann ist s ebenfalls

invertierbar mit $\det(s) = 1$. Es gilt $r + s = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$. Also ist $\det(r + s) = 3$ und $r + s$ ist invertierbar.

(b) In $\mathbb{Z}$ sind $r = 1$ und $s = -1$ Einheiten, aber $r + s = 0$ ist keine Einheit.

zu Aufgabe II.1

Sei p eine Primzahl und $n \in \mathbb{N}$.

Behauptung Für jedes $x \in \mathbb{F}_{p^n}$ gibt es genau eine p-te Wurzel, das heißt, genau ein $y \in \mathbb{F}_{p^n}$ mit $y^p = x$.

Beweis Sei $x \in \mathbb{F}_{p^n}$. Dann gilt $x^{p^n} = x$, wie wir in Lemma 8.3.1 gesehen haben. Es folgt $x = (x^{p^{n-1}})^p$, also ist $y = x^{p^{n-1}}$ eine p-te Wurzel aus x. Angenommen, $y^p = z^p = x$. Dann ist $0 = y^p - z^p = (y - z)^p$, denn in Körpern mit Charakteristik p gilt $(a + b)^p = a^p + b^p$ für alle a, b. Aus $(y - z)^p = 0$ folgt aber $y - z = 0$, also $y = z$. Damit ist gezeigt, dass jedes Element aus $\mathbb{F}_{p^n}$ genau eine p-te Wurzel besitzt. □

zu Aufgabe II.2

Seien p und q verschiedene Primzahlen mit $p \equiv q \equiv 3 (\mathrm{mod} 4)$.

Behauptung 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 $\mathbb{Z}/q\mathbb{Z}$.

Beweis Wenn die Gleichung $x^2 \equiv q (\mathrm{mod} p)$ keine Lösung besitzt, dann bedeutet das, dass q ein quadratischer Nichtrest mod$p$ ist. Also ist $(\frac{q}{p}) = -1$. Mit dem Reziprozitätssatz und weil $p \equiv q \equiv 3 (\mathrm{mod} 4)$ gilt, folgt $(\frac{p}{q}) = 1$. Das heißt, p ist ein quadratischer Rest mod$q$. Also besitzt die Gleichung $x^2 \equiv p (\mathrm{mod} q)$ eine Lösung. Ist aber x eine Lösung dieser Gleichung, dann auch $-x$, denn dann ist auch $(-x)^2 \equiv x^2 \equiv p (\mathrm{mod} q)$. Außerdem ist $x \not\equiv -x (\mathrm{mod} q)$, denn angenommen $x \equiv -x (\mathrm{mod} q)$, dann folgt $2x \equiv 0 (\mathrm{mod} q)$, also $q \mid 2x$. Da $q \equiv 3 (\mathrm{mod} 4)$ gilt, ist q ungerade, also folgt $q \mid x$ und $x \equiv 0 (\mathrm{mod} q)$ und damit auch $p \equiv 0 (\mathrm{mod} q)$. Das kann aber nicht sein, weil p und q zwei verschiedene Primzahlen und damit teilerfremd sind.

Mehr als zwei Lösungen kann die Gleichung $x^2 \equiv p (\mathrm{mod} q)$ auch nicht besitzen, denn Lösungen dieser Gleichung sind Nullstellen des Polynoms $T^2 - p \in \mathbb{F}_q[T]$, und dieses Polynom hat höchstens zwei Nullstellen. □

zu Aufgabe II.3

Behauptung $L = \{x \in \mathbb{Z}^3 \mid \begin{pmatrix} 1 & 2 & 2 \\ 0 & 1 & 2 \\ 1 & 1 & 2 \end{pmatrix} x \equiv 0(\mathrm{mod}2)\}$ ist ein Gitter mit $\det L = 4$.

Beweis Sei $A = \begin{pmatrix} 1 & 2 & 2 \\ 0 & 1 & 2 \\ 1 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix} \in \mathrm{M}_{33}(\mathbb{F}_2)$. Man sieht sofort, dass die Treppennormalform von A über $\mathbb{F}_2$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

ist. Damit ist die Lösungsmenge des homogenen linearen Gleichungssystems $Ax \equiv 0(\mathrm{mod}2)$ über $\mathbb{F}_2$ die Menge $\langle \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \rangle$. Ist also $x \in L$, dann folgt $x \equiv a \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} (\mathrm{mod}2)$ mit $a \in \mathbb{F}_2$ und damit $x = a \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} + 2 \begin{pmatrix} b \\ c \\ d \end{pmatrix}$ mit $a \in \{0, 1\}$ und $b, c, d \in \mathbb{Z}$. Damit folgt

$$x = \begin{pmatrix} 2b \\ 2c \\ a + 2d \end{pmatrix} = b \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix} + c \begin{pmatrix} 0 \\ 2 \\ 0 \end{pmatrix} + (a + 2d) \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

mit $b, c, a + 2d \in \mathbb{Z}$. Also folgt $x \in L(\begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix})$, also $L \subseteq L(\begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix})$.

Sei nun $x \in L(\begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix})$, das heißt, es gibt $a, b, c \in \mathbb{Z}$ mit

$$x = a \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix} + b \begin{pmatrix} 0 \\ 2 \\ 0 \end{pmatrix} + c \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 2a \\ 2b \\ c \end{pmatrix}.$$

Nun folgt

$$\begin{pmatrix} 1 & 2 & 2 \\ 0 & 1 & 2 \\ 1 & 1 & 2 \end{pmatrix} x = \begin{pmatrix} 2a+4b+2c \\ 2b+2c \\ 2a+2b+2c \end{pmatrix} \equiv 0(\mathrm{mod}2),$$

also $x \in L$. Damit ist gezeigt, dass $L = L(\begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix})$ gilt, also ein Gitter ist. Weiter gilt $\det L = |\det \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}| = 4$. □

zu Aufgabe II.4

1. Der Primzahltest von Solovay-Strassen beruht auf dem Satz von Euler, der besagt, dass $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}}(\mathrm{mod}p)$ gilt für alle ungeraden Primzahlen p und alle $a \in \mathbb{Z}$.

2. Eingabe beim Primzahltest ist eine ungerade natürliche Zahl n. Ausgabe ist entweder „n ist zusammengesetzt“ oder „n ist wahrscheinlich prim“ .

3. Es wird ein b mit $1 < b < n$ zufällig gewählt. Gilt $\mathrm{ggT}(b, n) \neq 1$, dann wird „$n$ ist zusammengesetzt“ ausgegeben. Gilt $\mathrm{ggT}(b, n) = 1$, dann wird geprüft, ob $(\frac{b}{n}) \equiv b^{\frac{n-1}{2}}(\mathrm{mod}n)$ gilt. Wenn ja, dann wird „n ist wahrscheinlich prim“ ausgegeben. Falls nein, dann wird „n ist zusammengesetzt“ ausgegeben.

4. Der Test ist probabilistisch, weil sowohl die Laufzeit als auch möglicherweise das Ergebnis von der zufälligen Wahl von b abhängen.

zu 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.

Behauptung Es gilt $I = 30\mathbb{Z}$.

Beweis Es gilt $30 = 2^5 - 2$, also $30 \in M$ und damit auch $30 \in I$, also $30\mathbb{Z} \subseteq I$.

Sei andererseits $z \in \mathbb{Z}$. Dann gilt (weil $\mathbb{F}_2$, $\mathbb{F}_3$ und $\mathbb{F}_5$ endliche Körper sind) $z^2 \equiv z(\mathrm{mod}2)$, $z^3 \equiv z(\mathrm{mod}3)$ und $z^5 \equiv z(\mathrm{mod}5)$. Es folgt $z^5 \equiv (z^2)^2 z \equiv z^2 z \equiv z^2 \equiv z(\mathrm{mod}2)$ und $z^5 \equiv z^3 z^2 \equiv z z^2 \equiv z^3 \equiv z(\mathrm{mod}3)$. Insgesamt gilt also $z^5 \equiv z(\mathrm{mod}2)$,

$z^5 \equiv z(\mathrm{mod}3)$ und $z^5 \equiv z(\mathrm{mod}5)$. Mit dem Chinesischen Restsatz folgt nun auch $z^5 \equiv z(\mathrm{mod}30)$, also $30 \mid z^5 - z$. Damit gilt $M \subseteq 30\mathbb{Z}$, also auch $I \subseteq 30\mathbb{Z}$. $\square$