Mathematische Grundlagen der Kryptografie (1321) SoSe 06

Klausur am 19.08.2006:

Lösungsvorschläge zu den Aufgaben

zu Aufgabe I.1

(a) Das numerische Äquivalent zu KLAUSUR ist die Folge $[10, 11, 0, 20, 18, 20, 17]$. Zu jedem Element der Folge wird nun in $\mathbb{Z}/26\mathbb{Z}$ der Schlüssel 15 addiert. Dies ergibt die Folge $[25, 0, 15, 9, 7, 9, 6]$ oder ZAPJHJG.

(b) Aus dem Schlüsselwort KRYPTOGRAFIE werden alle mehrfachen Buchstaben gestrichen. Das ergibt KRYPTOGAFIE. Diese Buchstabenfolge wird nun, beginnend beim Schlüsselbuchstaben S, unter die Klartextbuchstaben geschrieben, und anschließend wird mit den restlichen Buchstaben in alphabetischer Reihenfolge aufgefüllt.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
F	I	E	B	C	D	H	J	L	M	N	Q	S	U	V	W

Q	R	S	T	U	V	W	X	Y	Z
X	Z	K	R	Y	P	T	O	G	A

Das Wort KLAUSUR wird also zu NQFYKYZ.

(c) In I.1(a) haben wir bereits gesehen, dass Klausur als Folge von Zahlen aus $\mathbb{Z}/26\mathbb{Z}$ zu $[10, 11, 0, 20, 18, 20, 17]$ wird. Das Schlüsselwort EUKLID wird zu $[4, 20, 10, 11, 8, 3]$. Es wird also zu der Folge $[10, 11, 0, 20, 18, 20, 17]$ die Folge $[4, 20, 10, 11, 8, 3, 4]$ addiert. Dies ergibt $[14, 5, 10, 5, 0, 23, 21]$ oder OFKFAXV.

(d) Beim Selbstschlüsselkryptosystem mit Schlüssel 10 und Klartext $[10, 11, 0, 20, 18, 20, 17]$ ist die Schlüsselfolge $[10, 10, 11, 0, 20, 18, 20]$. Damit wird $[10, 11, 0, 20, 18, 20, 17]$ zu $[20, 21, 11, 20, 12, 12, 11]$ oder UVLUMML.

zu Aufgabe I.2

(a) Es gilt $(\frac{117}{37}) = (\frac{6}{37}) = (\frac{2}{37})(\frac{3}{37}) = -(\frac{3}{37}) = -(\frac{37}{3}) = -(\frac{1}{3}) = -1$.

(b) Es gilt $(\frac{58}{113}) = (\frac{2}{113})(\frac{29}{113}) = (\frac{29}{113}) = (\frac{113}{29}) = (\frac{26}{29}) = (\frac{2}{29})(\frac{13}{29}) = -(\frac{13}{29}) = -(\frac{29}{13}) = -(\frac{3}{13}) = -(\frac{13}{3}) = -(\frac{1}{3}) = -1$.

zu Aufgabe I.3

(a) Sei $\phi : \mathbb{Z}/4\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z}$ mit $a \mapsto a \bmod 2$, also $\phi(0) = 0, \phi(1) = 1, \phi(2) = 0$ und $\phi(3) = 1$. Dann ist ϕ ein Ringhomomorphismus, denn $\phi(a+b) = (a+b) \bmod 2 = (a \mod 2) + (b \bmod 2)$ und $\phi(ab) = ab \bmod 2 = (a \bmod 2)(b \bmod 2)$, wie wir jetzt zeigen werden: Es ist

$$\begin{aligned}
\phi(0+0) &= \phi(0) = 0 = \phi(0) + \phi(0) \\
\phi(0+1) &= \phi(1) = 1 = \phi(0) + \phi(1) \\
\phi(0+2) &= \phi(2) = 0 = \phi(0) + \phi(2) \\
\phi(0+3) &= \phi(3) = 1 = \phi(0) + \phi(3) \\
\phi(1+1) &= \phi(2) = 0 = \phi(1) + \phi(1) \\
\phi(1+2) &= \phi(3) = 1 = \phi(1) + \phi(2) \\
\phi(1+3) &= \phi(0) = 0 = \phi(1) + \phi(3) \\
\phi(2+2) &= \phi(0) = 0 = \phi(2) + \phi(2) \\
\phi(2+3) &= \phi(1) = 1 = \phi(2) + \phi(3) \\
\phi(3+3) &= \phi(2) = 0 = \phi(3) + \phi(3).
\end{aligned}$$

Da $\mathbb{Z}/4\mathbb{Z}$ und $\mathbb{Z}/2\mathbb{Z}$ kommutativ sind, gilt schon $\phi(a+b) = \phi(a) + \phi(b)$ für alle $a, b \in \mathbb{Z}/4\mathbb{Z}$.

Genauso gilt

$$\begin{aligned}
\phi(0 \cdot 0) &= \phi(0) = 0 = \phi(0) \cdot \phi(0) \\
\phi(0 \cdot 1) &= \phi(0) = 0 = \phi(0) \cdot \phi(1) \\
\phi(0 \cdot 2) &= \phi(0) = 0 = \phi(0) \cdot \phi(2) \\
\phi(0 \cdot 3) &= \phi(0) = 0 = \phi(0) \cdot \phi(3) \\
\phi(1 \cdot 1) &= \phi(1) = 1 = \phi(1) \cdot \phi(1) \\
\phi(1 \cdot 2) &= \phi(2) = 0 = \phi(1) \cdot \phi(2) \\
\phi(1 \cdot 3) &= \phi(3) = 1 = \phi(1) \cdot \phi(3) \\
\phi(2 \cdot 2) &= \phi(0) = 0 = \phi(2) \cdot \phi(2) \\
\phi(2 \cdot 3) &= \phi(2) = 0 = \phi(2) \cdot \phi(3) \\
\phi(3 \cdot 3) &= \phi(1) = 1 = \phi(3) \cdot \phi(3).
\end{aligned}$$

Wieder gilt wegen der Kommutativität von $\mathbb{Z}/2\mathbb{Z}$ und $\mathbb{Z}/4\mathbb{Z}$, dass für alle $a, b \in \mathbb{Z}/4\mathbb{Z}$ gilt $\phi(a \cdot b) = \phi(a)\phi(b)$. Es gilt auch $\phi(1) = 1$, also ist ϕ ein Ringhomomorphismus. Dass ϕ surjektiv ist, sieht man sofort. Weiter ist $\mathbb{Z}/4\mathbb{Z}$ kein Integritätsbereich, aber $\mathbb{Z}/2\mathbb{Z}$ ist einer.

(b) Sei $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z}$ mit $a \mapsto a \bmod 4$. Dies ist ein surjektiver Ringhomomorphismus und $\mathbb{Z}$ ist ein Integritätsbereich und $\mathbb{Z}/4\mathbb{Z}$ ist keiner.

zu Aufgabe I.4

Das Gitter $L = L\left(\begin{pmatrix}3\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\5\end{pmatrix}\right)$ ist ein Gitter von der gewünschten Form: Die Vektoren $\begin{pmatrix}3\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\5\end{pmatrix}$ sind eine Basis von $\mathbb{R}^3$, also spannen sie ein Gitter im $\mathbb{R}^3$ auf. Weiter gilt

$$\det L = \det \begin{pmatrix}3 & 0 & 0\\0 & 1 & 0\\0 & 0 & 5\end{pmatrix} = 15$$

und $\begin{pmatrix}0\\2\\0\end{pmatrix} = 2\begin{pmatrix}0\\1\\0\end{pmatrix}$, also $\begin{pmatrix}0\\2\\0\end{pmatrix} \in L$.

zu Aufgabe II.1

Um die Nachricht zu entschlüsseln, müssen wir zunächst die Schlüsselmatrix K über $\mathbb{Z}/26\mathbb{Z}$ invertieren. Es gilt $\det(K) = -17 = 9$, also ist K invertierbar und $\det(K)^{-1} = 3$. Weiter gilt

$$K^{\mathrm{Ad}} = \begin{pmatrix}-8 & 9\\9 & -8\end{pmatrix},$$

also

$$K^{-1} = 3\begin{pmatrix}-8 & 9\\9 & -8\end{pmatrix} = \begin{pmatrix}2 & 1\\1 & 2\end{pmatrix}.$$

Die Nachricht übersetzt in Elemente aus $\mathbb{Z}/26\mathbb{Z}$ ist $[20, 7, 20, 18, 16, 7, 10, 23]$. Zu berechnen ist also

$$\begin{pmatrix}20 & 7\\20 & 18\\16 & 7\\10 & 23\end{pmatrix}\begin{pmatrix}2 & 1\\1 & 2\end{pmatrix} = \begin{pmatrix}21 & 8\\6 & 4\\13 & 4\\17 & 4\end{pmatrix}$$

oder VIGENERE.

zu Aufgabe II.2

1. **Behauptung** $(\mathbb{Z}, +)$ ist ein Normalteiler von $(\mathbb{Q}, +)$.

   Beweis Wir wissen, dass $(\mathbb{Z}, +)$ eine Teilmenge von $\mathbb{Q}$ und mit der Verknüpfung $+$ von $\mathbb{Q}$ eine Gruppe ist. Also ist $(\mathbb{Z}, +)$ eine Untergruppe von $(\mathbb{Q}, +)$. Weiter ist $(\mathbb{Q}, +)$ eine abelsche Gruppe, und in einer abelschen Gruppe ist jede Untergruppe ein Normalteiler. □

2. **Behauptung** Jedes Element von $\mathbb{Q}/\mathbb{Z}$ besitzt endliche Ordnung.

   Beweis Sei $\frac{a}{b} \in \mathbb{Q}$ mit $a, b \in \mathbb{Z}$ und $b > 0$. Dann gilt $b(\frac{a}{b}+\mathbb{Z}) = b\frac{a}{b}+\mathbb{Z} = a+\mathbb{Z} = \mathbb{Z}$. Also ist die Ordnung von $\frac{a}{b} + \mathbb{Z}$ höchstens b und damit endlich. □

3. **Behauptung** $\mathbb{Q}/\mathbb{Z}$ besitzt unendlich viele Elemente.

   Beweis Seien $p \neq q$ Primzahlen. Angenommen, $\frac{1}{p}+\mathbb{Z} = \frac{1}{q}+\mathbb{Z}$. Mit dem Kriterium zur Gleichheit von Nebenklassen folgt $\frac{1}{p} - \frac{1}{q} \in \mathbb{Z}$, also $\frac{q-p}{pq} \in \mathbb{Z}$. Damit folgt $pq \mid q-p$, also gibt es ein $a \in \mathbb{Z}$ mit $apq = q-p$. Es folgt $p(aq+1) = q$, das heißt, $p \mid q$, ein Widerspruch. Also gilt: Sind $p \neq q$ verschiedene Primzahlen, dann sind auch die Nebenklassen $\frac{1}{p} + \mathbb{Z}$ und $\frac{1}{q} + \mathbb{Z}$ verschieden. Damit ist in $\mathbb{Q}/\mathbb{Z}$ die Menge aller Nebenklassen $\frac{1}{p} + \mathbb{Z}$, wobei p eine Primzahl ist, eine unendliche Menge. □

zu Aufgabe II.3

(a) **Behauptung** $11^{84} - 5^{84}$ ist durch 7 teilbar.

Beweis Es gilt $\mathrm{ggT}(7, 11) = 1$, also mit dem kleinen Satz von Fermat $11^6 \equiv 1(\mathrm{mod}7)$. Damit folgt $11^{84} \equiv (11^6)^{14} \equiv 1^{14} \equiv 1(\mathrm{mod}7)$. Analog gilt $\mathrm{ggT}(5, 7) = 1$, also $5^6 \equiv 1(\mathrm{mod}7)$ und $5^{84} \equiv 1(\mathrm{mod}7)$. Zusammen ist dann $11^{84} - 5^{84} \equiv 0(\mathrm{mod}7)$, das heißt, 7 teilt $11^{84} - 5^{84}$. □

(b) **Behauptung** Für alle $n \in \mathbb{N}$ mit $\mathrm{ggT}(n, 72) = 1$ gilt $n^{12} \equiv 1(\mathrm{mod}72)$.

Beweis Sei $n \in \mathbb{N}$ mit $\mathrm{ggT}(n, 72) = 1$. Dann folgt auch $\mathrm{ggT}(n, 8) = \mathrm{ggT}(n, 9) = 1$. Mit dem Satz von Euler gilt dann $n^{\varphi(8)} = n^4 \equiv 1(\mathrm{mod}8)$ und $n^{\varphi(9)} = n^6 \equiv 1(\mathrm{mod}9)$ und damit auch $n^{12} = (n^4)^3 \equiv 1(\mathrm{mod}8)$ und $n^{12} = (n^6)^2 \equiv 1(\mathrm{mod}9)$. Mit dem chinesischen Restsatz folgt nun auch $n^{12} \equiv 1(\mathrm{mod}72)$. □

zu Aufgabe II.4

Behauptung Vielfache von 21 können keine Carmichael-Zahlen sein.

Beweis Angenommen, $n \in \mathbb{N}$ ist eine Carmichael-Zahl und Vielfaches von 21. Da in der Primfaktorzerlegung einer Carmichael-Zahl jeder Primfaktor nur einfach vorkommt, können wie annehmen, dass die Primfaktorzerlegung von n von der Form $\prod_{i=1}^{r} p_i$ ist, wobei $p_1 = 3$ und $p_2 = 7$ gilt. Mit dem Satz von Korselt gilt nun weiter $p - 1 \mid n - 1$ für jede Primzahl p, die n teilt. Es folgt also $2 \mid n - 1$ und $6 \mid n - 1$. Aus der letzten Aussage folgt nun $3 \mid n - 1$, also $3 \mid (3 \prod_{i=2}^{r} p_i - 1)$, ein Widerspruch. □

zu Aufgabe II.5

Alice und Bob möchten mit dem Diffie-Hellman-Verfahren einen Schlüssel austauschen. Sie vereinbaren als endlichen Körper $\mathbb{F}_8 = \mathbb{F}_2[T]/(T^3+T+1)$ und als primitives Element $[T] = T \bmod (T^3 + T + 1)$. Alice wählt $e_A = 6$ und Bob wählt $e_B = 3$.

Der Schlüssel ist $[T]^{e_A e_B} = [T]^{18}$. Da $[T]$ ein primitives Element von $\mathbb{F}_8$ ist und $\mathbb{F}_8^\times$ gerade 7 Elemente besitzt, ist die Ordnung von $[T]$ ebenfalls 7. Es gilt also $[T]^{18} = ([T]^7)^2[T]^4 = [1]^2[T]^4 = [T]^4$ und $[T]^4 = [T][T]^3 = [T][T + 1] = [T^2 + T]$. Der Schlüssel ist also $[T^2 + T]$.

zu Aufgabe II.6

(a) Der öffentliche Schlüssel beim RSA-Kryptosystem ist ein Paar (m, e), wobei m das Produkt von zwei verschiedenen Primzahlen ist, und e eine ganze Zahl mit der Eigenschaft $\mathrm{ggT}(e, \varphi(m)) = 1$ ist.

(b) Der geheime Schlüssel besteht aus der Faktorisierung $m = pq$ in das Produkt von zwei Primzahlen und einer ganzen Zahl d mit $ed \equiv 1 (\mathrm{mod} \varphi(m))$.

(c) Möchte Bob eine Nachricht $N \in \mathbb{Z}/m\mathbb{Z}$ an Alice schicken, dann berechnet er $N^e \bmod m$ und schickt diese Zahl.

(d) Wenn Alice eine Nachricht M empfängt, dann berechet sie $M^d \bmod m$.

(e) Das RSA-Kryptosystem ist sicher, weil vermutet wird, dass man ganze Zahlen faktorisieren können muss, um das Kryptosystem brechen zu können. Weiter wird vermutet, dass es keinen effizienten Algorithmus gibt, um ganze Zahlen zu faktorisieren.

(f) Das RSA-Kryptosystem ist ein effizientes Verfahren, weil die beiden Primzahlen p und q, die zur Schlüsselerzeugung benötigt werden, mit einem effizienten Primzahltest gefunden werden können. Diese beiden Zahlen müssen dann multipliziert werden, was ebenfalls effizient möglich ist. Anschließend wird $\varphi(m) = (p-1)(q-1)$ berechnet, und auch das ist effizient möglich. Die Zahl e wird zufällig gewählt, und dann wird mit dem Euklidischen Algorithmus überprüft, ob $\mathrm{ggT}(e, \varphi(m)) = 1$ gilt. Die Zahl d wird mit dem erweiterten Euklidischen Algorithmus berechnet. Sowohl der Euklidische Algorithmus als auch der erweiterte Euklidische Algorithmus sind effiziente Algorithmen. Das Chiffrieren und Dechiffrieren sind dann nur noch Potenzieren in $\mathbb{Z}/m\mathbb{Z}$, und das ist mit Wiederholtem Quadrieren effizient möglich.