Mathematische Grundlagen der Kryptografie (01321) SS 08

Klausur am 16.08.2008:

Musterlösungen

Aufgabe 1

(a) Der Geheimtext E O X P H entspricht dem numerischen Äquivalent $[4, 14, 23, 15, 7]$. Zum Entschlüsseln muss der Schlüssel 3 in $\mathbb{Z}/26\mathbb{Z}$ subtrahiert werden. Das entspricht dann $[1, 11, 20, 12, 4]$ oder B L U M E.

(b) Das Schlüsselwort T U L P E entspricht den Elementen $[19, 20, 11, 15, 4]$ aus $\mathbb{Z}/26\mathbb{Z}$. Der Geheimtext L W S A Y X M D T P U F F B I entspricht
$[11, 22, 18, 0, 24, 23, 12, 3, 19, 15, 20, 5, 5, 1, 8]$. Es müssen nun die Werte des Schlüsselwortes nacheinander von den Elementen des Geheimtextes subtrahiert werden. In $\mathbb{Z}/26\mathbb{Z}$ ergibt dies $[11 - 19 = 18, 22 - 20 = 2, 18 - 11 = 7, 0 - 15 = 11, 24 - 4 = 20, 23 - 19 = 4, 12 - 20 = 18, 3 - 11 = 18, 19 - 15 = 4, 15 - 4 = 11, 20 - 19 = 1, 5 - 20 = 11, 5 - 11 = 20, 1 - 15 = 12, 8 - 4 = 4]$ oder S C H L U E S S E L B L U M E.

(c) Um die Nachricht zu entschlüsseln, muss zunächst die Schlüsselmatrix invertiert werden. Es gilt $\det \begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix} = 1$, also folgt

$$\begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix}^{\mathrm{Ad}} = \begin{pmatrix} 5 & -2 \\ -2 & 1 \end{pmatrix}.$$

Die Geheimnachricht D K E T Q N E V als Vektor über $\mathbb{Z}/26\mathbb{Z}$ ist $\begin{pmatrix} 3 & 10 \\ 4 & 19 \\ 16 & 13 \\ 4 & 21 \end{pmatrix}$. Damit ist der Klartext

$$\begin{pmatrix} 3 & 10 \\ 4 & 19 \\ 16 & 13 \\ 4 & 21 \end{pmatrix} \begin{pmatrix} 5 & -2 \\ -2 & 1 \end{pmatrix} = \begin{pmatrix} 21 & 4 \\ 8 & 11 \\ 2 & 7 \\ 4 & 13 \end{pmatrix}$$

oder V E I L C H E N.

(d) Aus dem Schlüsselwort S C H W E R T L I L I E werden zunächst die doppelten Buchstaben gestrichen. Das ergibt S C H W E R T L I. Diese Buchstaben werden nun beginnend beim Schlüsselbuchstaben O unter das Alphabet geschrieben, und anschließend wird in alphabetischer Reihenfolge mit den restlichen Buchstaben aufgefüllt. Damit ergibt sich folgende Ver- bzw. Entschlüsselungsvorschrift:

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

T	U	V	W	X	Y	Z
R	T	L	I	A	B	D

Nun können wir von unten nach oben ablesen, dass der Klartext K R O K U S war.

Aufgabe 2

(a) Es ist
$$(\frac{3}{5147}) = -(\frac{5147}{3}) = -(\frac{2}{3}) = 1,$$
also ist 3 ein quadratischer Rest modulo 5147.

(b) Es gilt $5147 \equiv 3 \pmod 8$, also ist 2 ein quadratischer Nichtrest modulo 5147.

(c) Sei $f = T^2 + 1 \in \mathbb{F}_3[T]$, dann ist $f(0) = 1$, $f(1) = 2$ und $f(2) = 2$. Also ist f ein Polynom vom Grad 2 ohne Nullstelle und damit irreduzibel. Es folgt, dass $\mathbb{F}_3[T]/(f) \simeq \mathbb{F}_9$ gilt.

(d) Sei $g = T \in \mathbb{F}_3[T]$. Dann hat $\mathbb{F}_3[T]/(g)$ drei Elemente während $\mathbb{F}_9$ neun Elemente besitzt. Die beiden Ringe können also nicht isomorph sein.

(e) Sei $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Dann ist G eine abelsche Gruppe mit 4 Elementen. G ist nicht zyklisch, denn die Ordnung jedes Elements aus G ist höchstens 2.

Aufgabe 3

Die Faktorisierung von 91 ist $91 = 7 \cdot 13$. Es gilt also $\varphi(91) = (7-1)(13-1) = 72$. Alice und Bob benutzen den Exponenten $e = 29$ zum Verschlüsseln. Um die Nachricht entschlüsseln zu können, ist d mit $ed \equiv 1 \pmod{72}$ gesucht. Zur Berechnung von d wird der erweiterte Euklidische Algorithmus verwendet:

$$\begin{aligned} 72 &= 2 \cdot 29 + 14 \\ 29 &= 2 \cdot 14 + 1 \end{aligned}$$

Es ist also $1 = 29 - 2 \cdot 14 = 29 - 2(72 - 2 \cdot 29) = (-2)72 + 5 \cdot 29$. Damit ist $d = 5$, und wir können den Geheimtext entschlüsseln, indem wir $3^5 \bmod 91$ berechnen. Es ist $3^5 = 243 \equiv 61 \pmod{91}$, das heißt, die Nachricht war 61.

Aufgabe 4

(a) **Behauptung** Enthält eine (multiplikative) Gruppe G genau ein Element g_0 der Ordnung $n > 1$, dann ist $n = 2$.

Beweis Sei $g_0 \in G$ das einzige Element der Ordnung n. Dann gilt also $g_0^n = 1$ und $g_0^m \neq 1$ für alle $1 \leq m < n$. Sei g_0^{-1} das zu g_0 inverse Element. Dann ist $(g_0^{-1})^n = (g_0^n)^{-1} = 1^{-1} = 1$, das heißt, die Ordnung von g_0^{-1} ist höchstens n. Angenommen, die Ordnung von g_0^{-1} ist m und $m < n$. Dann folgt $g_0^m = ((g_0^{-1})^{-1})^m = ((g_0^{-1})^m)^{-1} = 1^{-1} = 1$, ein Widerspruch. Die Ordnung von g_0^{-1} ist also n. Nun ist aber g_0 das einzige Element in G der Ordnung n, also $g_0 = g_0^{-1}$ bzw. $g_0^2 = 1$. Damit gilt $n = 2$. □

(b) **Behauptung** Die Menge $\{1, g_0\}$ ist eine Untergruppe von G.

Beweis Sei $N = \{1, g_0\}$. Es ist $1^{-1} = 1$ und $g_0^{-1} = g_0$, denn die Ordnung von g_0 ist 2. Da $1 \cdot 1 = 1 \in N$, $1 \cdot g_0 = g_0 \cdot 1 = g_0 \in N$ und $g_0 \cdot g_0 = 1 \in N$ gilt, ist $ab^{-1} \in N$ für alle $a, b \in N$. Mit dem Untergruppenkriterium folgt, dass N eine Untergruppe von G ist. □

(c) **Behauptung** Die Menge $\{1, g_0\}$ ist ein Normalteiler von G.

Beweis Da in (b) bereits gezeigt wurde, dass $N = \{1, g_0\}$ eine Untergruppe von G ist, muss nur noch $h^{-1}Nh \subseteq N$ für alle $h \in G$ gezeigt werden. Sei also $h \in G$. Dann ist $h^{-1}1h = 1 \in N$. Für $h^{-1}g_0h$ gilt $(h^{-1}g_0h)^2 = h^{-1}g_0hh^{-1}g_0h = h^{-1}g_0^2h = h^{-1}h = 1$, also ist die Ordnung von $h^{-1}g_0h$ höchstens zwei. Ist $\mathrm{ord}(h^{-1}g_0h) = 1$, dann ist $h^{-1}g_0h = 1 \in N$. Ist $\mathrm{ord}(h^{-1}g_0h) = 2$, dann ist $h^{-1}g_0h = g_0 \in N$, denn g_0 ist das einzige Element der Ordnung zwei in G. Insgesamt ist damit gezeigt, dass $h^{-1}Nh \subseteq N$ für alle $h \in G$ gilt. □

Aufgabe 5

Es sei R ein kommutativer Ring, und das Ideal (T) sei ein Primideal in $R[T]$.

Behauptung R ist ein Integritätsbereich.

Beweis In jedem kommutativen Ring R gilt: Ein Ideal I ist ein Primideal genau dann, wenn R/I ein Integritätsbereich ist. Da hier (T) ein Primideal in $R[T]$ ist, ist also $R[T]/(T)$ ein Integritätsbereich. Nun gilt aber $R[T]/(T) \simeq R$, das heißt, R ist ein Integritätsbereich. □

Aufgabe 6

Gesucht sind 4 Quadratwurzeln von 4 in $\mathbb{Z}/209\mathbb{Z}$, also Elemente $a \in \mathbb{Z}/209\mathbb{Z}$ mit $a^2 \equiv 4 \pmod{209}$. Mit dem Chinesischen Restsatz gilt diese Äquivalenz genau dann, wenn $a^2 \equiv 4 \pmod{11}$ und $a^2 \equiv 4 \pmod{19}$ gilt. Da $\mathbb{Z}/11\mathbb{Z}$ und $\mathbb{Z}/19\mathbb{Z}$ Körper sind, haben diese Äquivalenzen jeweils genau zwei Lösungen, nämlich 2 und -2. Mit dem Chinesischen Restsatz erhalten wir nun insgesamt 4 Lösungen in $\mathbb{Z}/209\mathbb{Z}$, nämlich a_1, a_2, a_3, a_4 mit

$$\begin{aligned}
a_1 &\equiv 2 \pmod{11} \text{ und } a_1 \equiv 2 \pmod{19} \\
a_2 &\equiv 2 \pmod{11} \text{ und } a_2 \equiv -2 \pmod{19} \\
a_3 &\equiv -2 \pmod{11} \text{ und } a_3 \equiv 2 \pmod{19} \\
a_4 &\equiv -2 \pmod{11} \text{ und } a_4 \equiv -2 \pmod{19}
\end{aligned}$$

Nun ist klar, dass $a_1 = 2$ und $a_4 = 207$ gilt. Die anderen beiden Werte lassen sich durch Ausprobieren relativ schnell als $a_2 = 112$ und $a_3 = 97$ berechnen.

Aufgabe 7

(a) Es gilt $\mathrm{ggT}(5, 6) = 1$ und $5^5 \equiv (-1)^5 \equiv -1 \equiv 5 \pmod{6}$, also ist 6 keine Pseudoprimzahl zur Basis 5, denn dann müsste $5^5 \equiv 1 \pmod{6}$ gelten.

(b) 15 ist keine Carmichael-Zahl, denn es gilt $\mathrm{ggT}(2, 15) = 1$ und $2^{14} \equiv 2^2(2^4)^3 \equiv 4 \cdot 1^3 \equiv 4 \pmod{15}$. Wäre aber 15 eine Carmichael-Zahl, dann müsste $b^{14} \equiv 1 \pmod{15}$ für alle b mit $\mathrm{ggT}(b, 15) = 1$ gelten.

Aufgabe 8

Behauptung $G = \{2\begin{pmatrix}a\\b\\c\end{pmatrix} \mid a,b,c \in \mathbb{Z}\} \cup \{\begin{pmatrix}1\\1\\1\end{pmatrix} + 2\begin{pmatrix}a\\b\\c\end{pmatrix} \mid a,b,c \in \mathbb{Z}\}$ ist ein Gitter mit Basis $\begin{pmatrix}2\\0\\0\end{pmatrix}, \begin{pmatrix}0\\2\\0\end{pmatrix}, \begin{pmatrix}1\\1\\1\end{pmatrix}$.

Beweis Sei $L = L(\begin{pmatrix}2\\0\\0\end{pmatrix}, \begin{pmatrix}0\\2\\0\end{pmatrix}, \begin{pmatrix}1\\1\\1\end{pmatrix})$. Dann ist $G = L$ zu zeigen. Sei also $x \in G$. Dann ist entweder $x = 2\begin{pmatrix}a\\b\\c\end{pmatrix} = (a-c)\begin{pmatrix}2\\0\\0\end{pmatrix} + (b-c)\begin{pmatrix}0\\2\\0\end{pmatrix} + 2c\begin{pmatrix}1\\1\\1\end{pmatrix} \in L$ oder $x = \begin{pmatrix}1\\1\\1\end{pmatrix} + 2\begin{pmatrix}a\\b\\c\end{pmatrix} = (a-c)\begin{pmatrix}2\\0\\0\end{pmatrix} + (b-c)\begin{pmatrix}0\\2\\0\end{pmatrix} + (2c+1)\begin{pmatrix}1\\1\\1\end{pmatrix} \in L$. Es gilt also $G \subseteq L$.

Sei umgekehrt $x = a\begin{pmatrix}2\\0\\0\end{pmatrix} + b\begin{pmatrix}0\\2\\0\end{pmatrix} + c\begin{pmatrix}1\\1\\1\end{pmatrix} \in L$, wobei $a,b,c \in \mathbb{Z}$ gilt. Ist c gerade, dann ist $x = 2\begin{pmatrix}a+\frac{c}{2}\\b+\frac{c}{2}\\\frac{c}{2}\end{pmatrix}$, wobei $a+\frac{c}{2}, b+\frac{c}{2}, \frac{c}{2} \in \mathbb{Z}$ gilt. Es folgt $x \in G$. Ist c ungerade, also $c = 2k+1$ für ein $k \in \mathbb{Z}$, dann ist $x = \begin{pmatrix}1\\1\\1\end{pmatrix} + 2\begin{pmatrix}a+k\\b+k\\k\end{pmatrix} \in G$. Damit ist auch $L \subseteq G$, und es folgt die Gleichheit. □

Aufgabe 9

Jede elliptische Kurve über einem endlichen Körper ist eine endliche abelsche Gruppe, in der die Gruppenoperation effizient berechnet werden kann. Das diskreter-Logarithmus-Problem ist in elliptischen Kurven jedoch (vermutlich) schwer zu lösen. Da man außerdem effizient elliptische Kurven finden kann, die zyklisch sind und in denen man effizient erzeugende Elemente findet, kann man elliptische Kurven für alle Kryptoverfahren verwenden, die auf der Schwierigkeit des diskreter-Logarithmus-Problems beruhen. Weil die bisher bekannten Verfahren zum Lösen des diskreten-Logarithmus-Problems für elliptische Kurven längst nicht so schnell sind wie für endliche Körper, kann die Schlüssellänge erheblich kleiner gewählt werden, wenn elliptische Kurven statt endlicher Körper benutzt werden.