Mathematische Grundlagen der Kryptografie (1321)SoSe 07

Nachklausur am 29.9.2007:

Lösungsvorschläge zu den Aufgaben

zu Aufgabe 1

(a) Der Text V K A Z G entspricht der Zahlenfolge $[21, 10, 0, 25, 6]$. Ist der Schlüssel beim Verschiebe-Kryptosystem 21, dann wird zum Entschlüsseln in $\mathbb{Z}/26\mathbb{Z}$ jeweils 21 subtrahiert. Das entspricht der Addition von 5 in $\mathbb{Z}/26\mathbb{Z}$. Es ergibt sich die Zahlenfolge $[0, 15, 5, 4, 11]$ oder A P F E L.

(b) Der Text V J E U S F J X entspricht der Zahlenfolge $[21, 9, 4, 20, 18, 5, 9, 23]$, und der Schlüssel entspricht $[14, 1, 18, 19]$. Der Schlüssel wird nun komponentenweise in $\mathbb{Z}/26\mathbb{Z}$ von der Zahlenfolge subtrahiert. Es ergibt sich $[7, 8, 12, 1, 4, 4, 17, 4]$ oder H I M B E E R E.

(c) Um den Text zu entschlüsseln, muss zunächst die Schlüsselmatrix $A = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$ invertiert werden. Wegen $\det(A) = 1$ gilt $A^{-1} = A^{\mathrm{Ad}}$, also $A^{-1} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix}$. Nun ist B B N N R V als Zahlenfolge $[1, 1, 13, 13, 17, 21]$, es muss also

$$\begin{pmatrix} 1 & 1 \\ 13 & 13 \\ 17 & 21 \end{pmatrix} \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 13 & 0 \\ 13 & 4 \end{pmatrix}$$

berechnet werden. Als Nachricht ergibt sich damit B A N A N E.

(d) Wird beim affinen Kryptosystem mit dem Schlüssel $(9, 1)$ verschlüsselt, dann wird beim Verschlüsseln x auf $9x + 1$ abgebildet. Beim Entschlüsseln wird dann y auf $9^{-1}(y - 1)$, also auf $3(y - 1)$ abgebildet. Nun ist K V Y O L als Zahlenfolge $[10, 21, 24, 14, 11]$, und mit der berechneten Entschlüsselung ergibt sich $[1, 8, 17, 13, 4]$ oder B I R N E.

zu Aufgabe 2

(a) Wir betrachten in $\mathbb{R}^2$ das Gitter $L(\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix})$ und die Matrix $A = \begin{pmatrix}1 & 1\\1 & 2\end{pmatrix} \in \mathrm{M}_{22}(\mathbb{Z})$. Wegen $\det(A) = 1$ ist A über $\mathbb{Z}$ invertierbar. Setzt man also $(b_1|b_2) = (a_1|a_2)A = A$ und damit $b_1 = \begin{pmatrix}1\\1\end{pmatrix}$ und $b_2 = \begin{pmatrix}1\\2\end{pmatrix}$, dann sind b_1, b_2 eine Basis des Gitters. Es gilt also $L(a_1, a_2) = L(b_1, b_2)$.

(b) Sei $f = T^3 + 2T + 1 \in \mathbb{F}_3[T]$. Dann gilt $f(0) = 1$, $f(1) = 1$ und $f(2) = 1$ in $\mathbb{F}_3$. Das Polynom f besitzt also keine Nullstelle in $\mathbb{F}_3$, und weil der Grad von f drei ist, heißt das schon, dass f über $\mathbb{F}_3$ irreduzibel ist. Damit ist $\mathbb{F}_3[T]/(f) = \mathbb{F}_{27}$.

zu Aufgabe 3

Die Struktur einer elliptischen Kurve als abelsche Gruppe ist immer $(\mathbb{Z}/d_1\mathbb{Z}) \times (\mathbb{Z}/d_2\mathbb{Z})$ mit $d_1 \mid d_2$. Da die elliptische Kurve 100 Elemente besitzt, muss $d_1 d_2 = 100$ gelten. Damit kann es folgende Fälle geben: $d_1 = 1, d_2 = 100$ oder $d_1 = 2, d_2 = 50$ oder $d_1 = 5, d_2 = 20$ oder $d_1 = 10, d_2 = 10$, also

$$\mathbb{Z}/100\mathbb{Z}, (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/50\mathbb{Z}), (\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/20\mathbb{Z}), (\mathbb{Z}/10\mathbb{Z}) \times (\mathbb{Z}/10\mathbb{Z}).$$

zu Aufgabe 4

Das quadratische Reziprozitätsgesetz für das Legendresymbol: Seien p, q zwei verschiedene Primzahlen mit $p, q > 2$. Dann gilt

$$(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \begin{cases} 1, & \text{falls } p \bmod 4 = 1 \text{ oder } q \bmod 4 = 1 \\ -1, & \text{falls } p \bmod 4 = q \bmod 4 = 3. \end{cases}$$

zu Aufgabe 5

Sei $G = (\mathbb{Z}/27\mathbb{Z})^\times$.

(a) Es ist $|G| = \varphi(27) = 18$.

(b) Die Anzahl der erzeugenden Elemente von G ist $\varphi(18) = \varphi(2)\varphi(9) = 6$.

(c) Die erzeugenden Elemente sind von der Form 2^k mit $\mathrm{ggT}(k, 18) = 1$, also $2^1 = 2$, $2^5 = 5$, $2^7 = 20$, $2^{11} = 23$, $2^{13} = 11$ und $2^{17} = 14$.

(d) Die Untergruppe der Ordnung 3 wird von einem Element der Ordnung drei erzeugt. Nun ist die Ordnung von 2^k in G gerade $\frac{18}{\mathrm{ggT}(18,k)}$. Für $k = 6$ ist also die Ordnung von $2^6 = 10$ gerade drei. Damit ist $\{2^6 = 10, 2^{12} = 20, 2^{18} = 1\}$ die Untergruppe der Ordnung drei.

(e) Mit dem Struktursatz endlicher zyklischer Gruppen ist

$$(\mathbb{Z}/27\mathbb{Z})^\times \simeq \mathbb{Z}/18\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}.$$

zu Aufgabe 6

(a) Um die letzten drei Ziffern von 3^{2405} zu bestimmen, reicht es $3^{2405} \bmod 1000$ zu kennen. Mit dem Satz von Euler gilt $3^{\varphi(1000)} \equiv 1 \bmod 1000$, denn $\mathrm{ggT}(3, 1000) = 1$. Weiter ist $\varphi(1000) = \varphi(8)\varphi(125) = 4 \cdot 100 = 400$. Damit folgt $3^{2405} \equiv (3^{400})^6 \cdot 3^5 \equiv 1^6 \cdot 3^5 \equiv 3^5 \equiv 243 \pmod{1000}$. Die letzten drei Ziffern von 3^{2405} sind also 243.

(b) **Behauptung:** Es gibt ein $b \in \mathbb{Z}$ mit $64959 \mid b^2 - 7$.

Beweis: Es gilt $(\frac{7}{3}) = (\frac{1}{3}) = 1$, also gibt es ein $b_1 \in \mathbb{Z}$ mit $b_1^2 \equiv 7 \pmod 3$. Weiter ist $(\frac{7}{59}) = -(\frac{59}{7}) = -(\frac{3}{7}) = (\frac{7}{3}) = 1$, also gibt es ein $b_2 \in \mathbb{Z}$ mit $b_2^2 \equiv 7 \pmod{59}$. Nun ist auch noch $(\frac{7}{367}) = -(\frac{367}{7}) = -(\frac{3}{7}) = (\frac{7}{3}) = 1$, also gibt es ein $b_3 \in \mathbb{Z}$ mit $b_3^2 \equiv 7 \pmod{367}$. Mit dem Chinesischen Restsatz gibt es nun ein $b \in \mathbb{Z}$ mit $b \equiv b_1 \pmod 7$, $b \equiv b_2 \pmod{59}$ und $b \equiv b_3 \pmod{367}$. Für dieses b gilt dann $b^2 \equiv b_1^2 \equiv 7 (\mathrm{mod} 7)$, $b^2 \equiv b_2^2 \equiv 7 \pmod{59}$ und $b^2 \equiv b_3^2 \equiv 7 \pmod{367}$. Wieder mit dem Chinesischen Restsatz folgt dann auch $b^2 \equiv 7 \pmod{64959}$, also $64959 \mid b^2 - 7$. □

zu Aufgabe 7

Sei $a \in \mathbb{Z}$ mit $a \neq 0$.

Behauptung: Es gibt nur endlich viele Ideale in $\mathbb{Z}$, die a enthalten.

Beweis: Alle Ideale in $\mathbb{Z}$ sind von der Form $m\mathbb{Z}$ mit $m \in \mathbb{Z}$. Gilt nun $a \in m\mathbb{Z}$ für ein $m \in \mathbb{Z}$, dann gibt es also ein $x \in \mathbb{Z}$ mit $a = mx$, das heißt $m \mid a$. Es kann also nur dann $a \in m\mathbb{Z}$ gelten, wenn $m \mid a$ gilt. Da $a \neq 0$ gilt, besitzt a nur endlich viele Teiler und ist damit auch nur in endlich vielen Idealen enthalten. □

zu Aufgabe 8

Sei R ein endlicher Ring und $a \in R$, so dass $ra \neq 0$ für alle $r \in R$ mit $r \neq 0$ gilt.

Behauptung: a ist invertierbar.

Beweis: Wir betrachten die Abbildung $f : R \longrightarrow R$, $r \mapsto ra$, und zeigen, dass diese Abbildung injektiv ist. Seien also $r, s \in R$ mit $f(r) = f(s)$. Dann gilt $ra = sa$, also $(r-s)a = 0$. Mit der Voraussetzung folgt nun, dass $r - s = 0$, also $r = s$ gilt. Damit ist f injektiv. Das R endlich ist, ist eine injektive Abbildung von R nach R auch schon surjektiv. Wenn f aber surjektiv ist, dann gibt es ein $b \in R$ mit $f(b) = ba = 1$.

Angenommen $r \in R$ mit $rb = 0$. Dann folgt durch Multiplikation der Gleichung mit a von rechts, dass $rba = r1 = r = 0a = 0$ gilt. Also gilt auch für b, dass $rb \neq 0$ für alle $r \in R$ mit $r \neq 0$ gilt. Mit dem gleichen Argument wie oben gibt es also ein $c \in R$ mit $cb = 1$. Multiplikation dieser Gleichung von rechts mit a ergibt: $cba = a$, und $cba = c(ba) = c$, also insgesamt $a = c$. Es gilt also nun $ab = 1 = ba$, und damit ist a invertierbar. $\square$

zu Aufgabe 9

Alice schickt die Elemente (g^k, Ng^{ak}), wobei N die Nachricht ist. Bob berechnet als erstes $(g^k)^{q-1-a}$, in diesem Fall also $[T^2+T]^4$. Nun ist $(T^2+T)^4 = T^8+T^4$ in $\mathbb{F}_2[T]$, also $[T^2+T]^4 = [T^8+T^4]$. Weiter gilt $[T^3+T+1] = 0$, also $[T]^3 = [T+1]$. Damit ist $[T^8+T^4] = [T]^8+[T]^4 = [T]^2[T+1]^2+[T][T+1] = [T]^2[T^2+1]+[T^2+T] = [T^4]+[T^2]+[T^2]+[T] = [T][T+1]+[T] = [T^2]$. Das Element $(g^k)^{q-1-a} = g^{-ak}$ wird nun mit dem zweiten Teil der Nachricht multipliziert. Wir müssen also $[T^2][T+1] = [T^3+T^2] = [T+1]+[T^2] = [T^2+T+1]$ berechnen. Damit ist die Nachricht $[T^2+T+1]$ oder als Bit-Folge $(1, 1, 1)$.