Algebra I

Universität Bielefeld, WS 2017/18

LÖSUNGEN ZUM WEIHNACHTSZETTEL

Aufgabe 1.

(a) Für $r = X^6 + X^5 + X^2 + X + 1$ berechnet man modulo $f = X^8 + X^4 + X^3 + X^2 + 1$:

$$\begin{aligned}
X^{2^4} &\equiv (X^8)^2 \\
&\equiv X^8 + X^6 + X^4 + 1 \\
&\equiv (X^4 + X^3 + X^2 + 1) + X^6 + X^4 + 1 \\
&\equiv X^6 + X^3 + X^2 \\
r(X^{2^4} - 1) &\equiv (X^6 + X^5 + X^2 + X + 1)(X^6 + X^3 + X^2 + 1) \\
&\equiv X^{12} + X^{11} + X^9 + X^8 + X + 1 \\
&\equiv (X^4 + X^3 + X + 1)(X^4 + X^3 + X^2 + 1) + X + 1 \\
&\equiv X^8 + X^4 + X^3 + X^2 \\
&\equiv 1
\end{aligned}$$

Also sind f und $X^{2^4} - 1$ teilerfremd. Weiterhin ist:

$$\begin{aligned}
X^{2^5} &\equiv (X^{2^4})^2 \\
&\equiv X^{12} + X^6 + X^4 \\
&\equiv X^4(X^4 + X^3 + X^2 + 1) + X^6 + X^4 \\
&\equiv X^8 + X^7 \\
&\equiv X^7 + X^4 + X^3 + X^2 + 1 \\
X^{2^6} &\equiv (X^{2^5})^2 \\
&\equiv X^{14} + X^8 + X^6 + X^4 + 1 \\
&\equiv X^6(X^4 + X^3 + X^2 + 1) + X^8 + X^6 + X^4 + 1 \\
&\equiv X^{10} + X^9 + X^4 + 1 \\
&\equiv (X^2 + X)(X^4 + X^3 + X^2 + 1) + X^4 + 1 \\
&\equiv X^6 + X^4 + X^3 + X^2 + X + 1 \\
X^{2^7} &\equiv (X^{2^6})^2 \\
&\equiv X^{12} + X^8 + X^6 + X^4 + X^2 + 1 \\
&\equiv (X^{12} + X^6 + X^4) + X^8 + X^2 + 1 \\
&\equiv (X^7 + X^4 + X^3 + X^2 + 1) + X^8 + X^2 + 1 \\
&\equiv X^7 + X^2 + 1 \\
X^{2^8} &\equiv (X^{2^7})^2 \\
&\equiv X^{14} + X^4 + 1 \\
&\equiv (X^{14} + X^8 + X^6 + X^4 + 1) + X^8 + X^6 \\
&\equiv (X^6 + X^4 + X^3 + X^2 + X + 1) + X^8 + X^6 \\
&\equiv X
\end{aligned}$$

Nach dem Rabinschen Kriterium ist f damit irreduzibel. Aufgaben 8.2 (c) und 9.4 (a) implizieren nun, dass $\mathbb{B} = \mathbb{F}_2[X]/(f)$ ein Körper ist.

(b) Wegen $|\mathbb{B}^\times| = 255 = 3 \cdot 5 \cdot 17$ reicht es aus $\alpha^{\frac{3 \cdot 5 \cdot 17}{s}} \neq 1$ für alle $s \in \{3, 5, 17\}$ zu überprüfen. Eine Rechnung zeigt $\alpha^{3 \cdot 5} = \texttt{00100110}$, $\alpha^{3 \cdot 17} = \texttt{00001010}$, und $\alpha^{5 \cdot 17} = \texttt{11010110}$:

$$\begin{aligned}
X^{3 \cdot 5} &\equiv (X^{2^4}) \cdot w \\
&\equiv (X^6 + X^3 + X^2) \cdot (X^7 + X^3 + X^2 + X) \\
&\equiv X^{13} + X^{10} + X^8 + X^7 + X^6 + X^3 \\
&\equiv (X^5 + X^2 + 1)(X^4 + X^3 + X^2 + 1) + X^7 + X^6 + X^3 \\
&\equiv (X + 1)(X^4 + X^3 + X^2 + 1) + 1 \\
&\equiv X^5 + X^2 + X \\
X^{3 \cdot 17} &\equiv X^3 \cdot X^{2^4} \cdot X^{2^5} \\
&\equiv X^3(X^6 + X^3 + X^2)(X^7 + X^4 + X^3 + X^2 + 1) \\
&\equiv (X^9 + X^6 + X^5)(X^7 + X^4 + X^3 + X^2 + 1) \\
&\equiv X^{2^4} + X^{11} + X^{10} + X^9 + X^7 + X^6 + X^5 \\
&\equiv (X^6 + X^3 + X^2) + (X^3 + X^2 + X)(X^4 + X^3 + X^2 + 1) + X^7 + X^6 + X^5 \\
&\equiv X^3 + X \\
X^{5 \cdot 17} &\equiv X^5 \cdot X^{2^4} \cdot X^{2^6} \\
&\equiv X^5(X^6 + X^3 + X^2)(X^6 + X^4 + X^3 + X^2 + X + 1) \\
&\equiv X \cdot X^{2^4} + X^{15} + X^{11} + X^7 \\
&\equiv X(X^6 + X^3 + X^2) + (X^7 + X^3)(X^4 + X^3 + X^2 + 1) + X^7 \\
&\equiv X^{11} + X^{10} + X^9 + X^6 + X^5 + X^4 \\
&\equiv (X^3 + X^2 + X)(X^4 + X^3 + X^2 + 1) + X^6 + X^5 + X^4 \\
&\equiv X^7 + X^6 + X^4 + X^2 + X
\end{aligned}$$

(d) Es ist $\log(x) = 24$ und $\log(y) = 12$ sowie $(q-1) - 24 = 231$ und $(q-1) - 12 = 243$. Damit berechnet man leicht:

$$\begin{array}{rcccl} x+y & = & & & \texttt{01000010} \\ xy & = & \alpha^{36} & = & \texttt{00100101} \\ x^{-1} & = & \alpha^{231} & = & \texttt{11110101} \\ y^{-1} & = & \alpha^{243} & = & \texttt{01111101} \end{array}$$

Aufgabe 2.

(a) Die Elemente $\alpha^0, \alpha^1, \ldots, \alpha^{k-1}$ sind paarweise verschiedene Nullstellen von $h = Y^{q-1} - 1$ wegen $k < |\mathbb{B}^\times| = q - 1$. Also ist $g = (Y - \alpha^0)(Y - \alpha^1) \cdots (Y - \alpha^{k-1})$ ein Teiler von h.

(b) Laut Logarithmentafel haben wir $[m] = \big[\texttt{00111010 00101001}\big]_2 = [\alpha^9 Y^2 + \alpha^{147} Y]$. Außerdem ist $g = Y + 1$ wegen $k = 1$. Polynomdivision liefert mit $\beta = \alpha^{147} + \alpha^9$

$$m \;=\; (\alpha^9 Y + \beta) \cdot g + \beta\,.$$

Wegen $\alpha^9 = \texttt{00111010}$ ist $\beta = \texttt{00010011}$ und die kodierte Nachricht ist

$$[\mathfrak{c}(m)] \;=\; \big[\texttt{00111010 00101001 00010011}\big]_3\,.$$

(c) (i) Da $Y - \alpha^i$ für $i = 0, 1, \ldots, k-1$ die irreduziblen Faktoren von g sind und diese in g jeweils mit einfacher Vielfachheit auftauchen, ist $\tilde{c}$ genau dann ein Vielfaches von g, wenn alle α^i mit $i = 0, 1, \ldots, k-1$ Nullstellen von $\tilde{c}$ sind.

(ii) Angenommen ε hat Gewicht $< k$ und $[\tilde{c}]$ ist eine kodierte Nachricht. Dann ist

$$\varepsilon \;=\; \big[\varepsilon_{s_0} Y^{n-s_0} + \varepsilon_{s_1} Y^{n-s_1} + \cdots + \varepsilon_{s_{k-1}} Y^{n-s_{k-1}}\big]$$

mit $1 \le s_0 < s_1 < \cdots < s_{k-1} \le n$ und $\varepsilon = [\tilde{c}] + c$ ist auch eine kodierte Nachricht. Nach (i) gilt also $\varepsilon(\alpha^i) = 0$ für alle $i = 0, 1, \ldots, k-1$. Mit anderen Worten

$$Ax = 0$$

für $A = \big(\alpha^{i(n-s_j)}\big)_{i,j}$ und $x = (\varepsilon_{s_0} \cdots \varepsilon_{s_{k-1}})^T$. Es folgt $x = 0$, d.h. $\varepsilon = 0$, wegen

$$\det(A) \;=\; \prod_{i<j} (\alpha^{n-s_j} - \alpha^{n-s_i}) \;\neq\; 0$$

wobei die linke Gleichheit aus der Formel für Determinanten von Vandermonde-Matrizen folgt und die rechte Ungleichheit aus $\alpha^i \neq \alpha^j$ für alle $0 \le i < j < q-1$.

(iii) Wenn die beiden Nachrichten ε und ε' Gewicht $< \frac{k}{2}$ haben, hat $\varepsilon + \varepsilon'$ Gewicht $< k$. Gilt nun $c + \varepsilon = c' + \varepsilon'$ für kodierte Nachrichten c und c', so ist auch $c + c'$ eine kodierte Nachricht. Nach (ii) muss dann aber $c + c' = 0 + (\varepsilon + \varepsilon') = 0$ gelten. Also ist $c = c'$.

(d)