ETH Zürich, D-INFK
HS 2016, 28. November 2016

Prof. Ueli Maurer
Daniel Tschudi

Diskrete Mathematik

Übung 11

11.1 Der Ring $F[x]_{m(x)}$

a) ($\star$) Bestimmen Sie alle Nullteiler im Ring $\mathrm{GF}(3)[x]_{x^2+2x}$.

b) ($\star$) Zählen Sie die Elemente des Rings $\mathrm{GF}(3)[x]_{x^2+2}$ und der multiplikativen Gruppe $\mathrm{GF}(3)[x]^*_{x^2+2}$ auf.

c) ($\star\,\star$) Berechnen Sie das Inverse des Polynoms x in $\mathrm{GF}(3)[x]_{x^2+2}$.

d) ($\star\,\star\,\star$) Sei F ein endlicher Körper und $n > 1$ eine natürliche Zahl. Finden Sie eine notwendige und hinreichende Bedingung für die Koeffizienten von $a(x)$ damit $a(x)$ in $F[x]_{x^n}$ invertierbar ist. Beweisen Sie Ihre Behauptung.

11.2 Körper

a) ($\star$) Sei $\langle F; +, \cdot\rangle$ ein Körper. Betrachten Sie die Algebra $\langle F \times F; \oplus, \otimes\rangle$ mit

$$(a, b) \oplus (c, d) = (a + c, b + d)$$
$$(a, b) \otimes (c, d) = (a \cdot c, b \cdot d)$$

für alle $(a, b), (c, d)$ in $F \times F$. Ist die Algebra $F \times F$ ein Körper?

b) ($\star\,\star$) Zeigen Sie, dass es in einem endlichen Körper mit q Elementen genau $q - 1$ Lösungen der Gleichung $x^{q-1} - 1 = 0$ gibt.

11.3 Endliche Körper *(14 Punkte)*

a) ($\star$) Geben Sie einen Körper K mit 9 Elementen an und listen Sie alle seine Elemente auf. Begründen Sie Ihre Antwort! *(6 Punkte)*

b) ($\star\,\star$) Finden Sie einen Generator der multiplikativen Gruppe des Körpers K aus Aufgabe a). Beweisen Sie, dass es sich dabei um einen Generator handelt. *(5 Punkte)*

c) ($\star\,\star$) Bestimmen Sie alle Nullstellen von $p(y) := xy^2 + y + (x+1) \in \mathrm{GF}(2)[x]_{x^2+x+1}[y]$. *Hinweis:* $p(y)$ ist ein Polynom über $\mathrm{GF}(2)[x]_{x^2+x+1}$ mit Grad 2 und hat Koeffizienten x, 1 und $x + 1$. *(3 Punkte)*

11.4 Lineare Codes ($\star\star\star$)

Sei $C \subseteq \mathbb{F}^n$ ein linearer Code bestehend aus n-Tupeln über dem endlichen Körper $\mathbb{F}$. Linear heisst, dass C eine Gruppe bezüglich der komponentenweisen Addition bildet. Weiter sei das Hamminggewicht eines Codeworts $(c_0, \ldots, c_{n-1}) \in C$ die Anzahl c_i, die verschieden von 0 sind. Zeigen Sie, dass die minimale Distanz von C gerade dem kleinsten Hamminggewicht aller Codewörter in $C - \{(0, \ldots, 0)\}$ entspricht.

11.5 Beweissysteme ($\star\star$)

Alice und Bob führen ein Diffie-Hellman Protokoll über der zyklischen Gruppe G mit Ordnung n und Generator g aus. Vic und Peggy haben den Kanal zwischen Alice und Bob angezapft. So erfahren Sie, die ausgetauschten Werte $a, b \in G$. Peggy behauptet nun, dass $c \in G$ dem vereinbarten Schlüssel zwischen Alice und Bob entspricht. Wie kann Peggy Vic von ihrer Behauptung überzeugen, wenn Vic nur effiziente Berechnungen machen kann? Betrachten Sie dazu ein Beweissystem $\Pi = (\mathcal{S}, \mathcal{P}, \tau, \phi)$, wobei $\mathcal{S} = \{(a, b, c) \mid a, b, c \in G\}$ die Menge aller Tripel über G ist. Sei weiter $\tau\big((a, b, c)\big) = 1$, genau dann wenn c der vereinbarte Schlüssel ist für das Diffie-Hellman Protokoll mit ausgetauschten Nachrichten a, b. Geben Sie für $\mathcal{P} = \mathbb{N}$ ein ϕ an, so dass Π vollständig und korrekt ist. Begründen Sie ihre Antwort.

Abgabe am 28./29. November 2016
Korrigiert wird Aufgabe 11.3