Übungsblatt 10

Abgabe der schriftlichen Lösungen am 18. 1. 2018 bis 13.10 Uhr

Aufgabe 46 ***mündlich***

(a) Bestimmen Sie in $\mathbb{Z}_5[x]/3x^2+1$ den Repräsentanten für die Restklasse, in der das Polynom $2x^5+x^4+4x+3$ enthalten ist.

(b) Bestimmen Sie alle irreduziblen Polynome $m(x)$ vom Grad 2 in $\mathbb{Z}_2[x]$. Stellen Sie jeweils die Additions- und Multiplikationstafeln für den Polynomrestklassenring $\mathbb{Z}_2[x]/m(x)$ auf.

(c) Sei $m(x)=x^2+2$. Stellen Sie die Additions- und Multiplikationstafeln für den Polynomrestklassenring $\mathbb{Z}_3[x]/m(x)$ auf. Ist $\mathbb{Z}_3[x]/m(x)$ ein Körper?

(d) Berechnen Sie das multiplikative Inverse von $a(x)=x^4+x^2+2x$ in $\mathbb{Z}_3[x]/m(x)$, wobei $m(x)=2x^6+x^3+x^2+2$ ist. Ist $m(x)$ irreduzibel über $\mathbb{Z}_3$?

Aufgabe 47 ***mündlich***

(a) Zeigen Sie, dass $\mathbb{F}_{p^n}$ zusammen mit der Addition auf $\mathbb{F}_{p^n}$ und der Einschränkung der Multiplikation auf Skalarprodukte der Form $a(x)b(x)$ mit $a(x)=a_0\in\mathbb{F}_p$ und $b(x)=b_{n-1}x^{n-1}+\cdots+b_1x+b_0\in\mathbb{F}_{p^n}$ einen n-dimensionalen Vektorraum $(\mathbb{F}_p)^n$ über $\mathbb{F}_p$ bildet (falls wir $b(x)\in\mathbb{F}_{p^n}$ als Vektor $(b_{n-1},\ldots,b_0)$ darstellen).

(b) Zeigen Sie, dass die Multiplikation mit einem festen Körperelement $a=(a_{n-1},\ldots,a_0)$ in $\mathbb{F}_{p^n}$, also die Abbildung $f_a\colon(b_{n-1},\ldots,b_0)\mapsto(a_{n-1},\ldots,a_0)\cdot(b_{n-1},\ldots,b_0)$ eine lineare Abbildung $f_a\colon(\mathbb{F}_p)^n\to(\mathbb{F}_p)^n$ ist.

(c) Folgern Sie, dass jede lineare Abbildung $f\colon(\mathbb{F}_{p^n})^l\to(\mathbb{F}_{p^n})^k$ über dem Körper $\mathbb{F}_{p^n}$ auch eine lineare Abbildung $f\colon(\mathbb{F}_p)^{nl}\to(\mathbb{F}_p)^{nk}$ über $\mathbb{F}_p$ ist. Gilt hiervon auch die Umkehrung?

Aufgabe 48 ***10 Punkte***

(a) Bestimmen Sie in $\mathbb{Z}_7[x]/3x^2+1$ den Repräsentanten für die Restklasse, in der das Polynom $p(x)=2x^5+x^4+4x+3$ enthalten ist.

(b) Bestimmen Sie alle irreduziblen Polynome $m(x)$ vom Grad 2 in $\mathbb{Z}_3[x]$.

(c) Stellen Sie die Additions- und Multiplikationstafeln für den Polynomrestklassenring $\mathbb{Z}_3[x]/m(x)$ auf, wobei $m(x)$ das lexikographisch kleinste irreduzible Polynom vom Grad 2 in $\mathbb{Z}_3[x]$ ist.

Aufgabe 49 ***5 Zusatzpunkte***

(a) Alice verschlüsselt die Klartextblöcke $x_1,x_2,\ldots,x_n$ mit einer Blockchiffre zu Kryptotextblöcken $y_1,y_2,\ldots,y_n$ und sendet sie an Bob, der sie wieder entschlüsselt. Wie viele Klartextblöcke werden durch einen bei der Übertragung von Block y_i auftretenden Fehler maximal verfälscht, wenn der ECB-, CBC-, OFB-, CFB- beziehungsweise Counter-Mode benutzt wird? Unterscheiden Sie ggf. auch unterschiedliche Segmentlängen t.

(b) Wie wirkt sich der Verlust eines Blockes y_i bei der Übertragung auf den von Bob berechneten Klartext aus?

Aufgabe 50 ***mündlich, optional***

(a) Zeigen Sie, dass der Polynomrestklassenring $\mathbb{Z}_p[x]/m(x)$ genau dann ein Körper ist, wenn $m(x)$ irreduzibel über $\mathbb{Z}_p$ ist.

(b) Zeigen Sie, dass zu jedem Polynom $f(x)$ in $\mathbb{Z}_p[x]$ ein endlicher Körper K existiert, der $\mathbb{Z}_p$ als Unterkörper enthält und in dem $f(x)$ in Linearfaktoren zerfällt (der kleinste solche Körper $K_p(f(x))$ ist bis auf Isomorphie eindeutig bestimmt und heißt der Zerfällungskörper für $f(x)$ über $\mathbb{Z}_p$).

(c) Zeigen Sie, dass der Zerfällungskörper $K=K_p(x^{p^n}-x)$ genau p^n Elemente enthält. Schließen Sie hieraus auf die Existenz eines irreduziblen Polynoms $m(x)$ vom Grad n über $\mathbb{Z}_p$, indem Sie zu einem beliebigen Erzeuger g der multiplikativen Gruppe K^* von K ein Polynom $m(x)$ kleinsten Grades mit $m(g)=0$ bestimmen.

Hinweis: Sie dürfen für diese Aufgabe bereits nutzen, dass die multiplikative Gruppe eines endlichen Körpers zyklisch ist, dies wird später in Aufgabe 55.b gezeigt. D.h. für einen endlichen Körper K existiert ein $g\in K\setminus\{0\}$, sodass alle seine Elemente außer 0 als g^i, $0\le i\le\|K\|$ darstellbar sind.