Übungen zur Kryptologie 1 Wintersemester 07/08

Johannes Köbler/Sebastian Kuhnert

Übungsblatt 10

Aufgabe 42 (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 $g(x)=x^4+x^2+2x$ 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 43 (mündlich)

Seien a, b Elemente einer abelschen Gruppe G mit Ordnungen $ord(a)$ und $ord(b)$.

a) Zeigen Sie, dass ab die Ordnung $ord(ab)=ord(a)ord(b)$ hat, falls $ord(a)$ und $ord(b)$ teilerfremd sind.

b) Lässt sich die Aussage in Teilaufgabe a) zu $ord(ab)=\mathrm{kgV}(ord(a),ord(b))$ verallgemeinern?

Aufgabe 44 (mündlich)

a) Zeigen Sie, dass ein Polynom $p(x)\in\mathbb{F}[x]$ vom Grad $n\geq 1$ über einem Körper $\mathbb{F}$ höchstens n Nullstellen besitzt.

b) Finden Sie ein Polynom $q(x)\in\mathbb{Z}_6[x]$ vom Grad 2 mit möglichst vielen Nullstellen.

Aufgabe 45 (mündlich)

Zeigen Sie, dass die multiplikative Gruppe $\mathbb{F}^*$ eines endlichen Körpers $\mathbb{F}$ zyklisch ist.

Hinweis: Sei $h=\Pi p_i^{e_i}$ die Primfaktorzerlegung der Gruppenordnung $h=\|\mathbb{F}^*\|$. Finden Sie Elemente $b_i\in\mathbb{F}^*$ der Form $b_i=a_i^{h/p_i^{e_i}}$ mit $ord(b_i)=p_i^{e_i}$, indem Sie die Anzahl der Nullstellen des Polynoms $x^{h/p_i}-1$ abschätzen, und verwenden Sie Aufgabe 43.

Aufgabe 46 (mündlich)

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.

Aufgabe 47 (schriftlich, 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.