Zahlentheorie und Kryptologie, SS2014
M. Hortmann

Blatt 7

Aufgabe 1

Noch ein bischen Schieberegister:

a) Gehen Sie aus von einem Steuerregister $(a_0,\ldots,a_{n-1})$ mit Koeffizienten in einem Körper K. Betrachten Sie die nxn Schieberegistermatrix $A=(a_{ij})_{\substack{0\le i\le n-1\\0\le j\le n-1}}$ mit den Koeffizienten

$$a_{ij}=\begin{cases}1 & \text{falls} \quad j=i+1 \text{ und } i<n-1\\ a_{n-1\,j}=a_j & \text{falls} \quad i=n-1\\ 0 & \text{sonst}\end{cases}$$

Beweisen Sie, z.B. durch Induktion über *n*, daß für das charakteristische Polynom χ_A von A gilt:

$$\chi_A(X)=X^n-\sum_{i=0}^{n-1} a_i X^i \ .$$

b) Wir hatten auf dem vorigen Aufgabenzettel den Körper $K=\mathbb{Z}_2$ und das Steuerregister $(a_0,\ldots,a_{1022})$ mit $a_i=1$ für *i*=0,7 und $a_i=0$ sonst benutzt. Im Tutorium wurde gezeigt, daß das Polynom $\chi_A(X)=X^n+X^7+1$ [1]primitiv ist, so daß die zugehörige Schieberegisterfolge die (maximale) Periode $2^{1023}-1$ besitzt.
Gehen Sie aus vom Startvektor $z_0=(x_0,\ldots,x_{1022})=(1,0,\ldots,0)$.
Wie lauten die 1023 Bits der zugehörigen Schieberegisterfolge ab (einschließlich) dem Index[2]

i=237771513993965676997520992732123768372628904786921412339561600663409212308965
7854084276942077691698696258875502783946823872043531019463430437214716331

c) Sei *K* ein endlicher Körper mit *q* Elementen und $f\in K[X]$ ein normiertes[3] Polynom vom Grad *n*. Der konstante Term von f sei von Null verschieden. Es sei *E*:=*K*[*X*]/<*f*> , a priori ist *E* nur ein Ring; *E* ist ein Körper genau dann wenn *f* irreduzibel ist. Wir schreiben *x* für die Restklasse von *X* in *E*.

i) Man zeige: *x* ist Element von *E** . (*E**, die multiplikative Gruppe von *E,* besteht definitionsgemäß aus den Elementen, welche ein multiplikativ Inverses besitzen).

ii) *x* habe die Ordnung q^d-1 in E*. Man zeige, daß dann *E* ein Körper ist, daß *f* also irreduzibel ist.

Bemerkung: Den Nachweis, daß *x* die Ordnung q^d-1 besitzt, kann man, wie in der Vorlesung gezeigt, relativ einfach mit Hilfe der Primfaktorzerlegung von q^d-1 führen, so man sie kennt.

Aus ii) folgt auch, daß man in der Definition von „primitiv“ die Voraussetzung „irreduzibel“ durch die Voraussetzung $f(0)\neq 0$ ersetzen kann.

---

1 In $\mathbb{Z}_2$ ist Minus=Plus.
2 Dieser Index wurde in Pari mit dem Befehl random(2^500) erzeugt.
3 D.h. der Leitkoeffizient ist 1.