Musterlösungen

June 29, 2013

Aufgabe 1:

- 4 von 1000 Angestellten sollen zum Tresor: Wähle große Primzahl p ($> 10^{100}$), ein $S \epsilon \mathbb{Z}_p$, ein Polynom f dritten Grades und gebe an die Angestellten die Werte von f an den Stellen 1,2,...,1000 aus.
- $f \epsilon P_n$ist in DNF $:\Longleftrightarrow \forall (i_1, \ldots, i_n) \epsilon \{0,1\}^n \exists d_{i_1 \ldots i_n} \epsilon \{0,1\} : f = \Sigma d_{i_1 \ldots i_n} {x_1}^{i_1} \ldots x_n^{i_n}$
- Alle Untergruppen der $(\mathbb{Z}_{27}, +)$: Müssen wieder zyklisch sein und eine Ordnung haben, die 27 teilt., also 1,3,9 oder 27. Bei 1 und 27 ist alles klar. Ordnung 3: muss ein <a> sein mit 3a=27, also kommt nur {0,9,18} in Frage. Analog bei Ordnung 9: es muss {0,3,6,9,12,15,18,21,24} sein.
- Kann jede Teilmenge einer freien Halbgruppe zu einer Basis erweitert werden? Nein, denn alle Basen sind gleichmächtig.
- Alle Lösungen von 20x-16y=28 in $\mathbb{N}^2$: x=7+5t, y=7+4t mit t$\geq$-1.
- Alle Körper mit 9, 10, 11 und 12 Elementen: 10 und 12 sind keine Primzahlpotenzen, also gibt´s keine Körper. 9 Elemente: GF(9) = $\mathbb{Z}_3[x]/(x^2+1)$. 11 Elemente: $\mathbb{Z}_{11}$.
- Alle abelschen Gruppen mit 9, 10, 11 und 12 Elementen: Bei 9: $\mathbb{Z}_3 \times \mathbb{Z}_3$ und $\mathbb{Z}_9$; bei 10 und 11 nur $\mathbb{Z}_{10}$ bzw. $\mathbb{Z}_{11}$. Bei 12: $\mathbb{Z}_{12}$ und $\mathbb{Z}_2 \times \mathbb{Z}_6$.
- Gd(f)=4: f kann in 2 quadratische irreduzible Faktoren zerfallen. [Wenn jemand geschrieben hat, dass f in seinem Zerfällungskörper in Linearfaktoren zerfallen muss, habe ich es auch gelten lassen.]

Aufgabe 2: Ein (n,k)-Code mit Korrektur- und Informationsrate >0.5: Sei H die Kontrollmatrix. Wegen 2k>n, also 2k$\geq$n+1 ist d = rg(H)+1$\leq$n-k+1$\leq$k und wegen 2d>n analog auch k$\leq$d, somit k=d. Mit n-k<k=d Kontrollstellen kann man aber nicht <d Fehler erkennen, ausser n-k=d-1=k-1, daher will man mit n-k = k-1 Kontrollstellen d-1 Fehler erkennen, was nur bei n-k=1 geht (zB Parity-Check). Aber dann ist k=d=1, was n=1 impliziert. Und das geht auch nicht. Der "Freund" wollte Sie also verarschen - ich hoffe, es ist nicht IHR Freund. [Wer auch nur einiges davon hingeschrieben hat, wurde mit Punkten gut belohnt.]

Aufgabe 3: Hat jeder richtig oder fast richtig gemacht.

Aufgabe 4: Für einen Körper K mit 16 Elementen ist K* zyklisch.

1. Möglichkeit: wie in der Vorlesung ausführlich zeigen, dass eine Nullstelle a von x^5-1 die Ordnung 5 und eine Nullstelle b von x^3-1 die Ordnung 3 haben müssen und dass dann ab die Ordnung 15 hat. 2. Möglichkeit (für Blitzgneißer): (K*,·) ist abelsch mit 15 Elementen und ist nach dem Hauptsatz über abelsche Gruppen zyklisch. 3. Möglichkeit: K ≅GF(16) (was man aber zu diesem Zeitpunkt noch nicht weiß) und GF(16)=$\mathbb{Z}_2[x]/(x^4+x+1)$ hat [x] als erzeugendes Element.

FEHLER (die mehr als 1x passiert sind):

- 27 ist eine Primzahl
- 11 ist keine Primzahl
- Bei 1c): $\mathbb{Z}_3$ ist keine Untergruppe von $\mathbb{Z}_{27}$ (nicht einmal eine Teilmenge!).
- "Ein endlicher Körper muß Primzahlordnung haben"
- "Keine Gruppe hat eine Primzahlordnung"
- Bei 1a): Manche haben es mit einer Schaltung mit 1000 Eingängen versucht. Geht aber nicht, weil dann ev. mit weniger als 4 offenen Schaltern doch "Strom fließen" kann. Manche haben das RSA-Verfahren versucht; da haben aber alle 1000 Beschäftigten den (öffentlichen) Code!