Musterlösung zur Serie 8
Algebra und Zahlentheorie und ihre Didaktik

Dr. Daniel Skodlerack

28. Juni 2017

Aufgabe 1. (5+5+5 Punkte)(RSA-Verfahren, Spionage) In dieser Aufgabe betätigen Sie sich als Spion. Sie wissen, dass Person A an Person B eine Nachricht schreiben möchte. Sie fangen den öffentlichen Schlüssel $T := (n, e) = (85, 5)$ von Person B ab.

1. n wurde leider nicht besonders gut gewählt, und daher kann man aus ihm leicht den geheimen Schlüssel $S = (d)$ ausrechnen. Berechnen Sie d.
2. Person A verschickt gerade Nachrichten an B. Sie fangen $1, 27$ und 55 ab. Dies sind Reste modulo 85. Entschlüsseln Sie diese, d.h. finden Sie $N_1, N_2, N_3 \in \mathbb{N}_0^{\leq 84}$, so dass $N_1 \equiv 1^d$, $N_2 \equiv 27^d$ und $N_3 \equiv 55^d$ modulo 85 gelten.
3. Wir haben die Zahl $(N_1, N_2, N_3)_{85}$ in 85-adischer Darstellung. Schreiben Sie diese in 26-adischer Darstellung und finden Sie das Wort. Null entspricht dem ersten Buchstaben im Alphabet.

Lösung:

1. Es gilt $\phi(85) = \phi(17)\phi(5) = 16 \cdot 4 = 64$, und es ist die natürliche Zahl d kleiner als 85 gesucht, so dass $5d$ kongruent zu 1 modulo 64 ist. Hinschauen ergibt $d = 13$.
2. Es ist $N_1 = 1$, und es gilt nach dem chinesischen Restsatz $N_2 \equiv_{85} 27^{13}$ genau dann, wenn
$$N_2 \equiv_5 27^4 \cdot 27 \equiv_5 27 \equiv_5 2 \wedge N_2 \equiv_{17} 3^{39} \equiv_{17} (3^{16})^2 3^7 \equiv_{17} 1 \cdot 27^2 \cdot 3 \equiv_{17} 10^2 \cdot 3 \equiv_{17} 11,$$
wobei zweimal der kleine Satz von Fermat angewandt wurde. Ansatz: $N_2 = 17s + 11$. N_2 löst das Kongruenzsystem genau dann, wenn $2s+1 \equiv_5 2$ genau dann, wenn $2s \equiv_5 1$ genau dann, wenn $s \equiv_5 3$ genau dann, wenn $N_2 \in [62]_{85}$ genau dann, wenn $N_2 = 62$, da N_2 ein Element von $\mathbb{N}_0^{\leq 84}$ ist. Ganz analog gilt $N_3 \equiv_{85} 55^{13}$ genau dann, wenn
$$N_3 \equiv_5 0 \equiv_5 55 \wedge N_3 \equiv_{17} 4^{13} \equiv_{17} (-1)^6 \cdot 4 \equiv_{17} 4 \equiv_{17} 55,$$
und wir erhalten somit $N_3 = 55$.
3. Es gilt $(1, 62, 55)_{85} = 12550 = (18, 14, 18)_{26}$, und Letzteres entspricht SOS.

Aufgabe 2. (5+5 Punkte)(Ringe von Abbildungen)

1. Es seien S ein unitärer Ring und X eine nichtleere Menge. Zeigen Sie, dass $(\mathrm{Abb}(X, S), +, \cdot)$ mit den durch $(f + g)(x) := f(x) + g(x)$ und $(f \cdot g)(x) := f(x)g(x)$ definierten Strukturen ein unitärer Ring ist.
2. Ist für alle unitären Ringe S das Tripel $(\mathrm{Abb}(S, S), +, \circ)$ ein unitärer Ring? Beweisen Sie Ihre Antwort.

Lösung:

1. $(\mathrm{Abb}(X, S), +)$ ist das direkte Produkt $\prod_{x \in X}(S, +)$ und somit laut Vorlesung eine abelsche Gruppe. Das selbe Argument zeigt, dass $(\mathrm{Abb}(X, S), \cdot)$ ein Monoid ist. Die Distributivgesetze folgen aus den Distributivgesetzen von S, da die Strukturen auf $\mathrm{Abb}(X, S)$ (gesehen als kartesisches Produkt) koordinatenweise definiert wurden.

2. Die Antwort ist Nein, da zum Beispiel $(\mathrm{Abb}(\mathbb{Z},\mathbb{Z}),+,\circ)$ nicht das erste Distributivgesetz erfüllt: Wählen Sie die Abbildung $f:\mathbb{Z}\to\mathbb{Z},\ f(z):=z^2$. Dann gilt:

$$(f\circ(f+f))(2)=f(f(2)+f(2))=f(8)=64\wedge(f\circ f+f\circ f)(2)=(2^2)^2+(2^2)^2=32.$$

Aufgabe 3. (5+5+5* Punkte)(Monoidringe und Gruppenringe) Wir betrachten einen Monoiden $(M,*)$ und einen kommutativen unitären Ring R. Wir bezeichnen für eine Abbildung $f:M\to R$ die Menge

$$\mathrm{supp}(f):=\{x\in M|\ f(x)\neq 0\}$$

als den *Träger* von f.

1. Zeigen Sie, dass
$$(RM:=\{f\in\mathrm{Abb}(M,R)|\ \mathrm{supp}(f)\text{ ist endlich. }\},+,\odot)$$
mit den durch
$$(f+g)(x):=f(x)+g(x)\text{ und }\ (f\odot g)(x):=\sum_{y,z\in M\text{ mit }y*z=x}f(y)g(z)$$
definierten Strukturen ein unitärer Ring ist. Man bezeichnet ihn als den *Monoidring* von M über R.

2. Zeigen Sie, dass ein Monoidmonomorphismus von M nach $(RM,\odot)$ existiert.

3. Zeigen Sie, dass M eine abelsche Gruppe sein muss, wenn RM ein Körper ist. Im Fall, dass M eine Gruppe ist, nennt man RM den *Gruppenring* von M über R.

Lösung:

1. $(RM,+)$ ist nach dem Untergruppenkriterium eine Untergruppe von $(\mathrm{Abb}(M,R),+)$, da die Nullabbildung ein Element von RM ist und für je zwei Elemente $f,g\in RM$ außerhalb der endlichen Menge $\mathrm{supp}(f)\cup\mathrm{supp}(g)$ die Gleichung $f(x)-g(x)=0$ gilt. Die Summe in der Definition von $\odot$ ist wohldefiniert, da $(R,+)$ abelsch ist und nur endlich viele Summanden ungleich Null sind. Die Struktur $\odot$ ist assoziativ, wie die folgende Rechnung zeigt.

$$\begin{aligned}
(h\odot(f\odot g))(u) &= \sum_{v,x\in M\text{ mit }v*x=u}h(v)(f\odot g)(x)\\
&= \sum_{v,x\in M\text{ mit }v*x=u}h(v)\sum_{y,z\in M\text{ mit }y*z=x}f(y)g(z)\\
&= \sum_{v,y,z\in M\text{ mit }v*y*z=u}h(v)(f(y)g(z))\\
&= \sum_{v,y,z\in M\text{ mit }v*y*z=u}(h(v)f(y))g(z))\\
&\overset{analog}{=} ((h\odot f)\odot g)(u).
\end{aligned}$$

$(RM,+,\odot)$ erfüllt die Distributivgesetze, da $(R,+,\cdot)$ die Distributivgesetze erfüllt. Man muss nur in der Summe aus der Definition von $\odot$ auf die Summanden das entsprechende Distributivgesetz von R anwenden. Es sei e das neutrale Element von $(M,*)$. Das Einselement von RM ist die Abbildung f_e, die e auf 1_R und jedes andere Element auf 0_R abbildet, wie die folgende Rechnung zeigt.

$$\begin{aligned}
(f_e\odot g)(x) &= \sum_{z\in M\text{ mit }e*z=x}g(z)\\
&= g(x)\\
&= \sum_{y\in M\text{ mit }y*e=x}g(y)\\
&= (g\odot f_e)(x).
\end{aligned}$$

2. Wir betrachten die Abbildung $\Phi : \ M \to RM,\ \Phi(x) := f_x$, wobei f_x die Abbildung von M nach R ist, die x auf 1_R und jedes andere Element von M auf 0_R abbildet. Insbesondere hat f_x genau ein Element im Träger. Folglich ist Φ wohldefiniert, injektiv und $\Phi(e) = 1_{RM}$. Es bleibt die Homomorphismuseigenschaft von Φ zu zeigen.

$$\begin{aligned}(\Phi(u*v))(x) &= f_{u*v}(x)\\ &= \begin{cases} 1_R, & \text{falls } u*v = x\\ 0_R, & \text{sonst}\end{cases}\\ &= \sum_{y,z\in M \text{ mit } y*z=x} f_u(y)f_v(z)\\ &= (f_u \odot f_v)(x)\\ &= (\Phi(u)\odot\Phi(v))(x),\end{aligned}$$

wobei die dritte Gleichheit daraus folgt, dass der Summand $f_u(y)f_v(z)$ nur für den Fall $(y,z) = (u,v)$ ungleich Null und in diesem Fall auch gleich 1_R ist.

3. Die Elemente $\Phi(x),\ x \in M$, bilden eine R-Basis von RM mit der skalaren Multiplikation: $\cdot_{R,RM} : R \times RM \to RM$, $(r \cdot_{R,RM} f)(x) := rf(x)$ (Wir schreiben ab jetzt $\cdot$ statt $\cdot_{R,RM}$), denn

   - $f \in RM$ erfüllt $f = \sum_{x\in\mathrm{supp}(f)} f(x)\cdot\Phi(x)$, d.h. $\mathrm{im}(\Phi)$ ist ein R-Erzeugendensystem von RM, und
   - $\mathrm{im}(\Phi)$ ist linear unabhängig über R, da für paarweise verschiedene $x_1, \dots x_l \in M$ aus

   $$\sum_{i=1}^{l} r_i \cdot \Phi(x_i) = 0_{RM} \in RM$$

   sofort für alle $j \in \mathbb{N}^{\leq l}$ die Gleichung

   $$r_j = r_j\Phi(x_j)(x_j) = \sum_{i=1}^{l} r_i\Phi(x_i)(x_j) = \left(\sum_{i=1}^{l} r_i \cdot \Phi(x_i)\right)(x_j) = 0_{RM}(x_j) = 0_R$$

   folgt.

   Wir identifizieren $x \in M$ mit $\Phi(x)$ und können dann die Elemente von RM in der Form

   $$\sum_{x\in M} r_x \cdot x,\ r_x = 0 \text{ für fast alle } x \in M,$$

   schreiben. Es bedeutet "fast alle" alle bis auf endlich viele. Es sei nun RM ein Körper. Damit ist $(RM, \odot)$ abelsch und somit ist die Struktur auf $M \subseteq RM$ abelsch. Wir müssen zeigen, dass jedes Element von M bezüglich $*$ ein Inverses besitzt. Für $x \in M$ gibt es ein Inverses $\sum_{y\in M} r_y y$ bezüglich $\odot$ in RM, da x ungleich 0_{RM} und RM ein Körper ist. Wir erhalten somit die Gleichung:

   $$e = x \odot \left(\sum_{y\in M} r_y \cdot y\right) = \sum_{y\in M} r_y \cdot (x * y). \tag{1}$$

   Die Basiseigenschaft von M ergibt, dass in der Gleichung (1) unter den $x*y,\ y \in M$, das Element e vorkommen muss. Also besitzt x in M ein Inverses bezüglich $*$.

Aufgabe 4. (10 Punkte)(Polynome und endliche Körper) Es sei P ein nichtkonstantes ganzzahliges Polynom, d.h. ein Element aus $\mathbb{Z}[X] \setminus \mathbb{Z}$. Zeigen Sie, dass ein endlicher Körper existiert, in dem P eine Nullstelle hat.

Lösung: Wir zeigen zuerst, dass für jedes Polynom Q ungleich Null mit ganzzahligen Koeffizienten eine ganze Zahl existiert, die keine Nullstelle von Q ist. Wenn Q konstant ist, dann hat Q gar keine Nullstelle in $\mathbb{Z}$, da Q als ungleich Null vorausgesetzt wurde. Im Falle höheren Grades hat Q entweder keine ganzzahlige Nullstelle, oder es hat eine Nullstelle a und es lässt sich durch Division mit Rest in der Form $Q = (X-a)S + R$ mit $R \in \mathbb{Z},\ S \in \mathbb{Z}[X]$, schreiben, wobei $R = R(a) = Q(a) = 0$ sein

muss. Also $Q = (X - a)S$, und S hat einen kleineren Grad als Q und ist ungleich dem Nullpolynom. Also hat S nach Induktionsvoraussetzung höchstens $\deg(S)$-viele Nullstellen. Eine Nullstelle von Q ist aufgrund der Nullteilerfreiheit von $\mathbb{Z}$ eine Nullstelle von $(X - a)$ oder eine Nullstelle von S. Also hat Q höchstens $\deg(S) + 1$ $(= \deg(Q))$ viele Nullstellen.

Wir kommen nun zur Aufgabe: Das Polynom P^2 hat den Grad $2\deg(P)$, also einen Grad größer gleich 2, da P als nicht konstant vorausgesetzt wurde, und somit ist $P^2 - 1$ nicht das Nullpolynom. Nach Teil 1 gibt es eine ganze Zahl z, so dass $|P(z)|$ ungleich 1 ist, und es gibt eine Primzahl p, die $|P(z)|$ teilt. Wir schließen mit der Gleichung:

$$P([z]_p) = [P(z)]_p = [0]_p$$

im Körper $\mathbb{Z}/p\mathbb{Z}$.