UE Einführung in die Algebra und Diskrete Mathematik
KV Algebra und Diskrete Mathematik

8. Übungszettel, 13. Mai 2013

Lösungen

1. Sei G eine Gruppe, $g \in G$. Zeigen Sie mindestens 2 der folgenden 4 Sätze.
   (a) Durch $k \mapsto gkg^{-1}$ wird ein Automorphismus von G definiert.
   (b) Für jede Untergruppe K und jedes $g \in G$, ist gKg^{-1} wieder eine Untergruppe, und K ist genau dann normal, wenn für alle g gilt: $gKg^{-1} = K$.
   (c) Ist K die einzige Untergruppe der Ordnung $|K|$, dann ist K normal.
   (d) Ist K eine Untergruppe des Zentrums, dann ist K normal; insbesondere ist $Z(G)$ stets normal.
2. Wählen Sie 17 und 11 als „große" Primzahlen, und verschlüsseln und signieren Sie damit eine Nachricht Ihrer Wahl.
3. Finden Sie alle Lösungen von

$$\begin{aligned} x &\equiv 0 \pmod 3, \\ x &\equiv 1 \pmod 7. \end{aligned}$$

Lösung:
Wegen $3 \perp 7$ gibt es λ, μ, sodass $\lambda \cdot 3 + \mu \cdot 7 = 1$, z.B.

$$-2 \cdot 3 + 1 \cdot 7.$$

Es ist dann

$$\begin{aligned} -6 = (-2) \cdot 3 &\equiv 0 \pmod 3, \\ -6 = 1 + 1 \cdot 7 &\equiv 1 \pmod 7). \end{aligned}$$

Die Lösung ist modulo $3 \cdot 7 = 21$ eindeutig bestimmt. Die Lösungsmenge ist daher $-6 + 21\mathbb{Z} = \{\ldots, -27, -6, 15, 36, \ldots\}$.

Weitere Anmerkungen: Nennen wir eine dieser Lösungen e_7. Genauso erhalten wir eine Lösung $e_3 = 7$ von

$$\begin{aligned} x &\equiv 1 \pmod 3, \\ x &\equiv 0 \pmod 7. \end{aligned}$$

Aus diesen beiden Lösungen erhalten wir dann durch lineares Kombinieren eine Lösung von einem System mit beliebiger rechter Seite, z.B.

$$\begin{aligned} x &\equiv 2 \pmod 3, \\ x &\equiv 4 \pmod 7. \end{aligned}$$

hat die Lösung $2 \cdot e_3 + 5 \cdot e_7 = 2 \cdot 7 + 4 \cdot (-6) = -10 = 11 \pmod{21}$.

Noch allgemeiner betrachten wir das System

$$\begin{aligned} x &\equiv 2 \pmod{3}, \\ x &\equiv 3 \pmod{5}, \\ x &\equiv 4 \pmod{7}. \end{aligned}$$

Alle Moduln sind paarweise teilerfremd, daher ist jeder Modul auch teilerfrem zum Produkt aller anderen Moduln, und wir können daher alle zugehörigen diophantischen Gleichungen lösen:

$$\begin{aligned} 3 \perp 35: &\quad 12 \cdot 3 - 1 \cdot 35 = 1; \\ 5 \perp 21: &\quad -4 \cdot 5 + 1 \cdot 21 = 1; \\ 7 \perp 15: &\quad -2 \cdot 7 + 1 \cdot 15 = 1. \end{aligned}$$

Damit definieren wir

$$\begin{aligned} e_3 &= -35, \\ e_5 &= 21, \\ e_7 &= 15. \end{aligned}$$

Für diese gilt:

$$\begin{aligned} e_3 &\equiv 1 \pmod{3}, & e_3 &\equiv 0 \pmod{5}, & e_3 &\equiv 0 \pmod{7}, \\ e_5 &\equiv 0 \pmod{3}, & e_5 &\equiv 1 \pmod{5}, & e_5 &\equiv 0 \pmod{7}, \\ e_7 &\equiv 0 \pmod{3}, & e_7 &\equiv 0 \pmod{5}, & e_7 &\equiv 1 \pmod{7}. \end{aligned}$$

Die Lösung des obigen Systems ergibt sich durch lineares Kombinieren dieses Basislösungen:

$$x = 2 \cdot e_3 + 3 \cdot e_5 + 4 \cdot e_7 = 2 \cdot (-35) + 3 \cdot 21 + 4 \cdot 15 = -70 + 63 + 60 = 53.$$

Die Lösung ist eindeutig modulo $3 \cdot 5 \cdot 7 = 105$.

Dies ist genau die Vorgangsweise beim Chinesischen Restsatz.

4. Sei $f = x^6 + 3x^5 + 4x^4 + 6x^3 + 6x^2 + 3x + 3$, $g = x^2 + x + 2$. Berechnen Sie $f + g$, $\mathrm{Gd}(f - g)$, $\mathrm{Gd}(f \cdot g)$ und bestimmen Sie Polynome q, r, mit $\mathrm{Gd}\, r < \mathrm{Gd}\, g$ sodass $f = q \cdot g + r$. Ist g ein Teiler von f? Lösen Sie die Aufgabe sowohl unter der Annahme $f, g, q, r \in \mathbb{Z}[x]$ als auch $f, g, q, r \in \mathbb{Z}_5[x]$. Vergleichen Sie die Rechnungen auch mit der Division von 1346633 durch 112.

   Lösung:

```
1  3  4  6  6  3  3   :   1  1  2   =   1  2  0  2  4
   2  2  6
         2  6  3
            4 -1  3
              -5 -5
```

Also: $q = x^4 + 2x^3 + 2x + 4$, $r = -5x - 5$. *Über* $\mathbb{Z}_5$ *ist* $r = 0$, *somit* g *ein Teiler von* f. *Die Rechnungen sind genauso wie bei ganzen Zahlen, aber ohne Übertrag, und damit eigentlich einfacher.*

5. Finden Sie Polynome r und s, sodass

$$r \cdot (x^2 + 1) + s \cdot (x^3 - 1) = 1.$$

Lösen Sie das Problem sowohl für Polynome in $\mathbb{Z}[x]$ als auch $\mathbb{Z}_2[x]$.

Lösung:
Über $\mathbb{Z}$ *ergibt sich* 2 *als ggT, und der erweiterte euklidische Algorithmus liefert:*

$$(-x^2 + x + 1) \cdot (x^2 + 1) + (x - 1) \cdot (x^3 - 1) = 2.$$

Division durch 2 *ergibt die Lösung* $r = \frac{1}{2}(-x^2 + x + 1)$ *und* $s = \frac{1}{2}(x - 1)$. *Diese liegt allerdings in* $\mathbb{Q}[x]$. *Über* $\mathbb{Z}_2$ *ist* $x + 1$ *ein gemeinsamer Teiler, das Problem daher definitiv unlösbar.*