8. Übungsblatt zu Mathematik für Informatiker II, SS 2004

JOACHIM VON ZUR GATHEN & MICHAEL NÜSKEN

Abgabe bis Montag, 28. Juni 2004, 12^{23} Uhr
in den jeweils richtigen Kasten auf dem D1-Flur.

Aufgabe 8.1 (Polynomdivision). (8 Punkte)

Dividiere a mit Rest durch b für

(i) $a = x^7 - 5x^6 + 3x^2 + 1$, $b = x^2 + 1$ in $\mathbb{R}[x]$.

(ii) $a = x^6 + 2$, $b = x^2 + x + 1$ in $\mathbb{F}_3[x]$.

(iii) $a = x^{10} - 1$, $b = x^4 - 1$ in $\mathbb{F}_3[x]$.

(iv) $a = x^5 + x - 2$, $b = x^3 + 3x - 1$ in $\mathbb{R}[x]$.

Berechne den größten gemeinsamen Teiler der Polynome

(v) $a = x^7 - 5x^6 + 3x^2 + 1$, $b = x^2 + 1$ in $\mathbb{R}[x]$.

(vi) $a = x^{10} - 1$, $b = x^4 - 1$ in $\mathbb{F}_3[x]$.

Lexikon. Sei F ein Körper. Ein Polynom $a = a_d x^d + \cdots + a_1 x + a_0 \in F[x]$ heißt *normiert*, wenn $a_d = 1$ gilt. Der *größte gemeinsame Teiler* $\mathrm{ggT}(a, b)$ von $a, b \in F[x]$ ist das eindeutige normierte Polynom $g \in F[x]$ mit den folgenden Eigenschaften: (i) g ist ein *gemeinsamer Teiler*, dh. g teilt a und b, (ii) wenn $f \in F[x]$ ein gemeinsamer Teiler von a und b ist (also die Polynome a und b teilt), so teilt f auch g. Der ggT ist das normierte Polynom größten Grades, welches a und b teilt. Wie bei den ganzen Zahlen kann der ggT mit Hilfe des Euklidischen Algorithmus berechnet werden.

Aufgabe 8.2 (Erweiterter Euklidischer Algorithmus). (7 Punkte)

Wir untersuchen den Erweiterten Euklidischen Algorithmus für Polynome über einem Körper F.

Algorithmus. Erweiterter Euklidischer Algorithmus.
Eingabe: $a, b \in F[x]$ mit $\deg a \geq \deg b$.
Ausgabe: $\ell \in \mathbb{N}$, $g, s, t \in F[x]$ wie unten berechnet.

1. $r_0 \leftarrow a, \quad r_1 \leftarrow b$.
2. $s_0 \leftarrow 1, \quad t_0 \leftarrow 0$.

3. $s_1 \leftarrow 0, \quad t_1 \leftarrow 1$.
4. $i \leftarrow 1$.
5. Solange $r_i \neq 0$ erledige 6–10
6. $\quad q_i \leftarrow r_{i-1} \operatorname{quo} r_i$.
7. $\quad r_{i+1} \leftarrow r_{i-1} - q_i r_i$.
8. $\quad s_{i+1} \leftarrow s_{i-1} - q_i s_i$.
9. $\quad t_{i+1} \leftarrow t_{i-1} - q_i t_i$.
10. $\quad i \leftarrow i + 1$.
11. $\ell \leftarrow i - 1$.
12. Antworte ℓ, $g = r_\ell / \operatorname{lc}(r_\ell)$, $s = s_\ell / \operatorname{lc}(r_\ell)$, $t = t_\ell / \operatorname{lc}(r_\ell)$.

Hierbei bezeichnet $\operatorname{lc}(f)$ den *Leitkoeffizient* von f. Dies ist der Koeffizient des Terms höchsten Grades von f. Zeige:

(i) Für $1 \leq i < \ell$ gilt $\deg r_{i+1} < \deg r_i$.

(ii) Der Algorithmus terminiert nach höchstens $\deg b + 1$ Schleifendurchläufen.

(iii) Für alle $0 \leq i < \ell$ gilt: $g = \operatorname{ggT}(r_i, r_{i+1}) = \operatorname{ggT}(a, b)$ [*Hinweis.* Zeige $\operatorname{ggT}(r_{i-1}, r_i) = \operatorname{ggT}(r_i, r_{i+1})$ und benutze dann Induktion].

(iv) Für $0 \leq i \leq \ell$ gilt $r_i = s_i a + t_i b$. Insbesondere ist $g = sa + tb$.

(v) Ist $\operatorname{ggT}(a, b) = 1$, so folgt $sa \equiv 1 \bmod b$.

Aufgabe 8.3 (Irreduzible Polynome). (5+1 Punkte)

Sei F ein Körper. Ein Polynom $f \in F[x] \setminus F$ heißt *irreduzibel*, wenn aus $f = gh$ entweder $g \in F \setminus \{0\}$ oder $h \in F \setminus \{0\}$ folgt. Andernfalls heißt f *zerlegbar*.

In dieser Aufgabe wollen wir irreduzible Polynome untersuchen.

(i) Zeige, dass Polynome der Form $\alpha x + \beta$, $\alpha \neq 0, \beta \in F$, irreduzibel sind.

(ii) Zeige, dass wenn a eine Nullstelle eines Polynomas $f \in F[x]$ ist, d.h. wenn $f(a) = 0$ gilt, das Polynom f von $x - a$ geteilt wird. Ist der Grad von f echt größer als eins, so folgt insbesondere, dass f nicht irreduzibel ist.

(iii) Zeige anhand eines Beispiels in $\mathbb{R}[x]$, dass die Umkehrung nicht gilt, d.h., gib ein *zerlegbares* Polynom in $\mathbb{R}[x]$ an, welches keine reelle Nullstelle besitzt.

(iv) Beweise: Hat $f \in F[x]$ Grad zwei oder drei, so ist f *genau dann* zerlegbar, wenn es eine Nullstelle in F besitzt.

(v) Bestimme alle irreduziblen Polynome vom Grad 3 in $\mathbb{F}_2[x]$. [*Hinweis.* Jedes Polynom von Grad 3 in $\mathbb{F}_2[x]$ ist von der Form $x^3 + \alpha x^2 + \beta x + \gamma$ mit $\alpha, \beta, \gamma \in \mathbb{F}_2$. Benutze nun das Nullstellenkriterium aus (iv).]

(vi*) Eine Form des Fundamentalsatzes der Algebra besagt, dass jedes irreduzible Polynom in $\mathbb{C}[x]$ linear, d.h. von der Form $\alpha x + \beta$, mit $\alpha \neq 0, \beta \in \mathbb{C}$, ist. Benutze dies um zu folgern, dass jedes Polynom vom Grad $d \geq 1$ in $\mathbb{C}[x]$ sich als Produkt von d Linearfaktoren schreiben läßt.

Aufgabe 8.4 ($\mathbb{F}_8$). (8 Punkte)

Wir wollen hier den Körper mit acht Elementen kennenlernen.

(i) Zeige, dass $x^3 + x + 1$ über $\mathbb{F}_2$ irreduzibel ist, sich also nicht als ein nichttriviales Produkt schreiben lässt.

Für $g \in \mathbb{F}_2[x]$ besteht der Ring $\mathbb{F}_2[x]/\langle g \rangle$ aus den Resten $f \operatorname{rem} g$ ($f \in \mathbb{F}_2[x]$); Addition und Multiplikation erfolgen modulo g.

(ii) Bestimme eine Liste aller Elemente in $\mathbb{F}_8 = \mathbb{F}_2[x]/\left\langle x^3 + x + 1 \right\rangle$. [Bezeichne mit a das zu $x \in \mathbb{F}_2[x]$ gehörige Element in $\mathbb{F}_8$.]

(iii) Berechne $a(a^2 + a + 1)$, $a^2(a^2 + a + 1)$ und a^{-1} in $\mathbb{F}_8$.

(iv) Ist $\mathbb{F}_8$ ein Körper?

(v) Zeige, dass für alle $z \in \mathbb{F}_8 \setminus \{0\}$ die Gleichung $z^7 = 1$ gilt. Das verallgemeinert den kleinen Satz von Fermat.

(vi) Zeige, dass $z^{-1} = z^6$ für $z \neq 0$.

(vii) Ist $\mathbb{Z}_8$ ein Körper?

***Aufgabe 8.5** (Nicht alltäglich, knifflig). (0+5 Punkte)

Ein Ring R heisst *euklidisch,* wenn er eine Division mit Rest erlaubt, dh. es gibt eine *euklidische Normfunktion* $\nu\colon R \setminus \{0\} \to \mathbb{N}$ so, dass es für alle $a, b \in R$ mit $b \neq 0$ passende $q, r \in R$ gibt mit $a = q \cdot b + r$ und $r = 0$ oder $\nu(r) < \nu(b)$.

Satz. *Der Ring $\mathbb{Z}[x]$ der Polynome mit ganzzahligen Koeffizienten ist nicht euklidisch, erlaubt also keine Division mit Rest.*

Dafür müssen wir zeigen, dass egal welche Funktion ν wir versuchen, es nie für alle $a, b \in \mathbb{Z}[x]$ mit $b \neq 0$ passende $q, r \in \mathbb{Z}[x]$ geben wird mit $a = q \cdot b + r$ und $r = 0$ oder $\nu(r) < \nu(b)$.

(i*) Division mit Rest bezüglich des Grades $\nu = \deg$ ist nicht möglich. [Finde $a, b \in \mathbb{Z}[x]$ mit $b \neq 0$, sodass ...]

(ii*) Bestimme *alle* Teiler von $2 \in \mathbb{Z}[x]$ und *alle* Teiler von $x \in \mathbb{Z}[x]$.

(iii*) Angenommen $\nu\colon \mathbb{Z}[x] \setminus \{0\} \to \mathbb{N}$ ist gegeben. Zeige: Dann gibt es ein Element $g = a \cdot 2 + b \cdot x$ mit $g \neq 0$, $a, b \in \mathbb{Z}[x]$ und $\nu(g)$ minimal unter allen solchen Elementen, also $\nu(g) \leq \nu(h)$ für alle $h = a' \cdot 2 + b' \cdot x \neq 0$, $a', b' \in \mathbb{Z}[x]$.

(iv*) Nimm nun an, dass ν eine euklidische Normfunktion ist. Zeige: Dann gilt $g \mid 2$ und $g \mid x$ in $\mathbb{Z}[x]$.

(v*) Führe dies zum Widerspruch.

8. Übungsblatt zu Mathematik für Informatiker II, SS 2004, Mündlicher Teil

JOACHIM VON ZUR GATHEN & MICHAEL NÜSKEN

Mündliche Aufgabe 8.6 (Polynomdivision).

Dividiere a mit Rest durch b für

(i) $a = x^7 + x^6 + x + 2$, $b = x^2 - 1$ in $\mathbb{R}[x]$.

(ii) $a = x^9 - 1$, $b = x^2 + x + 1$ in $\mathbb{F}_5[x]$.

(iii) $a = x^6 - 1$, $b = x^4 - 1$ in $\mathbb{F}_5[x]$.

(iv) $a = x^5 + x - 2$, $b = x^2 - 3$ in $\mathbb{R}[x]$.

Berechne den größten gemeinsamen Teiler der Polynome

(v) $a = x^7 + x^6 + x + 2$, $b = x^2 - 1$ in $\mathbb{R}[x]$.

(vi) $a = x^6 - 1$, $b = x^4 - 1$ in $\mathbb{F}_5[x]$.

Mündliche Aufgabe 8.7 (Exponentialgrad).

Sei F ein beliebiger Körper, etwa $F = \mathbb{R}$. Für ein Polynom $f \in F[x]$ definieren wir den *Exponentialgrad*

$$\operatorname{edeg} f := \begin{cases} 2^{\deg f}, & \text{falls } f \neq 0 \text{ gilt,} \\ 0, & \text{falls } f = 0. \end{cases}$$

(i) Zeige, dass edeg: $(F[x], \cdot) \to (\mathbb{N}, \cdot)$ ein Homorphismus von Halbgruppen ist.

Definition: Eine Halbgruppe ist eine Menge H mit einer binären Operation $\circ\colon H \times H \to H$, die assoziativ ist, und so, dass ein neutrales Element existiert.

(ii) Welche bemerkenswerte Eigenschaft erfüllt edeg bezüglich der Addition von Polynomen? [Beweis!]

(iii) Wir wissen, dass in $F[x]$ eine Division mit Rest möglich ist, wobei der Grad des Restes kleiner als der Grad des Dividenden ist. Eine Funktion $\nu\colon F[x] \setminus \{0\} \to \mathbb{N}$ nennen wir allgemeiner *euklidische Normfunktion*, falls es für alle $a, b \in F[x]$ mit $b \neq 0$ jeweils $q, r \in F[x]$ gibt mit

$$a = q \cdot b + r, \qquad r = 0 \text{ oder } \nu(r) < \nu(b).$$

(Statt Werte in $\mathbb{N}$ können wir auch eine andere wohlgeordnete Menge zulassen, etwa $\mathbb{N} \cup \{-\infty\}$.) Ist edeg eine solche euklidische Normfunktion?

Mündliche Aufgabe 8.8 (Faktorisieren).

Bestimme jeweils die vollständige Zerlegung in Faktoren von

(i) $x^4 - 1$ in $\mathbb{R}[x]$.

(ii) $x^4 - 1$ in $\mathbb{C}[x]$.

(iii) $x^5 - 1$ in $\mathbb{R}[x]$.

(iv) $x^5 - 1$ in $\mathbb{C}[x]$.

(v) $x^5 + x^4 + 1$ in $\mathbb{F}_2[x]$.

(vi) $x^5 + x^4 + 1$ in $\mathbb{F}_4[x]$, wobei $\mathbb{F}_4 = \{0, 1, a, 1 + a\}$ „der“ Körper mit vier Elementen ist und $a^2 + a + 1 = 0$ gilt. (Vergleiche Brill, Tabelle 7.8 und 7.9 mit $b = 1 + a$.)

Mündliche Aufgabe 8.9 ($\mathbb{F}_4$).

Wir wollen hier den Körper mit vier Elementen genauer kennenlernen.

(i) Zeige, dass $x^2 + x + 1$ über $\mathbb{F}_2$ irreduzibel ist, sich also nicht als ein nichttriviales Produkt schreiben lässt.

(ii) Bestimme eine Liste aller Elemente in $\mathbb{F}_4 = \mathbb{F}_2[x]/\langle x^2 + x + 1\rangle$. [Bezeichne mit a das zu $x \in \mathbb{F}_2[x]$ gehörige Element in $\mathbb{F}_4$.]

(iii) Ist $\mathbb{F}_4$ ein Körper?

(iv) Berechne $(a + 1)(a + 1)$ und a^{-1} in $\mathbb{F}_4$.

(v) Zeige, dass für alle $z \in \mathbb{F}_4 \setminus \{0\}$ die Gleichung $z^3 = 1$ gilt. Das verallgemeinert den kleinen Satz von Fermat.

(vi) Zeige, dass $z^{-1} = z^2$ für $z \neq 0$.