D-MATH Grundstrukturen FS 2023
Prof. Richard Pink

# Musterlösung Serie 11

## Modul-Arithmetik

1. (a) Finde das multiplikative Inverse von $\overline{a}$ in $\mathbb{Z}/n\mathbb{Z}$ für $(a,n) = (2,5)$, $(4,25)$, $(17,49)$.

   (b) Bestimme alle Quadrate in $\mathbb{Z}/n\mathbb{Z}$ für $n = 4, 7, 17$.

   (c) Zeige, dass eine Summe zweier Quadrate in $\mathbb{Z}$ nicht kongruent zu 3 modulo (4) ist.

   *Lösung:*

   (a) Für gegebenes $a \in \mathbb{Z}$ suchen wir $b \in \mathbb{Z}$ mit $ab \equiv 1 \bmod (n)$. Oft findet man ein solches durch Probieren, indem man ein $b$ sucht, so dass $ab$ nahe bei $n$ oder einem anderen kleinen Vielfachen von $n$ liegt, und das Ganze eventuell mit dem Rest wiederholt. Konkret finden wir:

   $$2 \cdot 2 \equiv -1 \bmod (5) \quad \Rightarrow \quad -2 \cdot 2 \equiv 1 \bmod (5) \quad \Rightarrow \quad \overline{2}^{-1} = -\overline{2} = \overline{3} \text{ in } \mathbb{Z}/5\mathbb{Z}$$

   $$6 \cdot 4 \equiv -1 \bmod (25) \quad \Rightarrow \quad -6 \cdot 4 \equiv 1 \bmod (25) \quad \Rightarrow \quad \overline{4}^{-1} = -\overline{6} = \overline{19} \text{ in } \mathbb{Z}/25\mathbb{Z}$$

   $$3 \cdot 17 \equiv 2 \bmod (49), \quad 25 \cdot 2 \equiv 1 \bmod (49), \quad \Rightarrow \quad \overline{17}^{-1} = \overline{25 \cdot 3} = \overline{26} \text{ in } \mathbb{Z}/49\mathbb{Z}$$

   Für ein allgemeines Schema zur Berechnung des Inversen siehe Aufgabe 3 (f).

   (b) Jede ganze Zahl ist kongruent modulo $(n)$ zu einer Zahl $a$ mit $|a| \leqslant \frac{n}{2}$. Wegen $(-a)^2 = a^2$ genügt es daher, die Quadrate $a^2$ mod $(n)$ zu bestimmen für alle $0 \leqslant a \leqslant \frac{n}{2}$. Konkret bekommen wir:

| $a$ | 0 | 1 | 2 |
|---|---|---|---|
| $a^2$ | 0 | 1 | 4 |
| $a^2 \bmod (4)$ | 0 | 1 | 0 |

| $a$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| $a^2$ | 0 | 1 | 4 | 9 |
| $a^2 \bmod (7)$ | 0 | 1 | 4 | 2 |

| $a$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| $a^2$ | 0 | 1 | 4 | 9 | 16 | 25 | 36 | 49 | 64 |
| $a^2 \bmod (17)$ | 0 | 1 | 4 | 9 | 16 | 8 | 2 | 15 | 13 |

   (c) In (b) wurde gezeigt, dass die Quadrate in $\mathbb{Z}/4\mathbb{Z}$ die Kongruenzklassen von 0 und 1 sind. Also sind die Summen zweier Quadrate die Kongruenzklassen von 0, 1, oder 2, und jedenfalls nicht von 3 modulo (4).

2. Gegeben sei ein endlicher Körper $k$ der Ordnung 25 mit der Basis $1, a$ als Vektorraum über $\mathbb{F}_5$ und $a^2 = \overline{3}$. Setze $b := a + \overline{1}$.

   (a) Bestimme $a^4, a^6, b^2, b^3, b^4, b^5$ als $\mathbb{F}_5$-Linearkombinationen von $\overline{1}, a$.

   (b) Bestimme $b^{-1}$ als $\mathbb{F}_5$-Linearkombination von $\overline{1}, a$.

   (c) Folgere, dass jedes Element von $k^\times$ eine Potenz von $b$ ist.

   *Lösung:*

   (a) Wir rechnen

$$\begin{aligned}
a^4 &= \overline{3}^2 = \overline{9} = \overline{4} \\
a^6 &= a^4 a^2 = \overline{4} \cdot \overline{3} = \overline{2} \\
b^2 &= (a + \overline{1})^2 = a^2 + 2a + \overline{1} = 2a + \overline{4} = 2(a + \overline{2}) \\
b^3 &= (a + \overline{1})(2a + \overline{4}) = 2a^2 + 6a + \overline{4} = a \\
b^4 &= a(a + \overline{1}) = a^2 + a = a + \overline{3} \\
b^5 &= b^3 b^2 = a(\overline{4} + 2a) = 4a + 2a^2 = 4a + \overline{1} = 4(a + \overline{4}).
\end{aligned}$$

   (b) Wir wissen, dass $i, j \in \mathbb{F}_5$ existieren mit $b^{-1} = ia + j$. Dies bedeutet

$$\overline{1} = (ia+j)b = (ia+j)(a+1) = ia^2+ja+ia+j = 3i+ja+ia+j = (j+i)a+(3i+j).$$

   Durch Koeffizientenvergleich folgt daraus $j + i = \overline{0}$ und $3i + j = \overline{1}$. Lösen dieses linearen Gleichungssystems liefert die eindeutige Lösung $(i, j) = (\overline{3}, \overline{2})$. Somit ist $b^{-1} = \overline{3}a + \overline{2}$.

   (c) Wegen $b^3 = a$ ist $b^6 = a^2 = \overline{3}$ und folglich $b^{12} = \overline{3}^2 = \overline{4}$ und $b^{18} = \overline{3}^3 = \overline{2}$. Wegen $b^0 = \overline{1}$ ist daher jedes Element von $\mathbb{F}_5^\times$ eine Potenz von $b$. Sodann hat jedes Element von $k \smallsetminus \mathbb{F}_5$ die Form $i(a + j)$ für ein $i \in \mathbb{F}_5^\times$ und ein $j \in \mathbb{F}_5$. Die Rechnung in (a) zeigt, dass jedes $j \in \mathbb{F}_5$ schon unter den Potenzen $b, b^2, b^3, b^4, b^5$ auftritt mit einem geeigneten $i$. Da wir $i$ noch beliebig in $\mathbb{F}_5^\times$ abändern können durch Multiplikation mit $b^6 = a^2 = \overline{3}$ oder $b^{12} = a^4 = \overline{4}$ oder $b^{18} = a^6 = \overline{2}$, tritt daher jedes Paar $(i, j)$ für eine Potenz von $b$ auf.

3. Mit dem *Euklidischen Algorithmus* kann man den grössten gemeinsamen Teiler zweier natürlicher Zahlen $a_0$ und $a_1$ bestimmen und diesen als $\mathbb{Z}$-Linearkombination von $a_0$ und $a_1$ ausdrücken. Dafür nehmen wir $a_0 > 0$ an und konstruieren iterativ $a_0, a_1, \ldots$ wie folgt. Zeige:

   (a) Sind $a_{k-1}$ und $a_k$ bereits konstruiert mit $a_k > 0$, so existieren eindeutige $q_k, a_{k+1} \in \mathbb{Z}$ mit $a_{k-1} = q_k a_k + a_{k+1}$ und $0 \leqslant a_{k+1} < a_k$. *(Division mit Rest)*

   (b) Setze $(u_0, v_0, u_1, v_1) := (1, 0, 0, 1)$ und in (a) ausserdem $u_{k+1} := u_{k-1} - q_k u_k$ und $v_{k+1} := v_{k-1} - q_k v_k$ für alle $k \geqslant 1$. Dann gilt $a_k = u_k a_0 + v_k a_1$ für alle $k$.

(c) Sind $a_{k-1}$ und $a_k$ konstruiert, so gilt $\mathrm{ggT}(a_0, a_1) = \mathrm{ggT}(a_{k-1}, a_k)$.

(d) Es existiert ein $k$ mit $a_k = 0$, und für dieses gilt

$$\mathrm{ggT}(a_0, a_1) \;=\; a_{k-1} \;=\; u_{k-1}a_0 + v_{k-1}a_1.$$

(e) Bestimme $\mathrm{ggT}(25, 12)$ und $\mathrm{ggT}(497, 284)$ und $\mathrm{ggT}(864, 124)$ als Linearkombination der Ausgangszahlen.

(f) Sei $p$ eine Primzahl und $a \in \mathbb{Z}$ kein Vielfaches von $p$. Bestimme mit dem Euklidischen Algorithmus für $a_0 := p$ und $a_1 := a$ das multiplikative Inverse von $\overline{a}$ in $\mathbb{F}_p$.

(g) Berechne das multiplikative Inverse von $\overline{33}$ in $\mathbb{F}_{71}$ und von $\overline{845}$ in $\mathbb{F}_{997}$.

*Lösung:*

(a) Wir setzen $q_k := \left\lfloor \frac{a_{k-1}}{a_k} \right\rfloor$ und $a_{k+1} := a_{k-1} - q_k a_k$. Dann gilt $a_{k-1} = q_k a_k + a_{k+1}$ und $0 \leqslant \frac{a_{k-1}}{a_k} - q_k < 1$, also folgt $0 \leqslant a_{k+1} < a_k$.
Für die Eindeutigkeit nehmen wir an, wir hätten auch $a_{k-1} = q'_k a_k + a'_{k+1}$ mit $0 \leqslant a'_{k+1} < a_k$. Dann gilt $a'_{k+1} - a_{k+1} = a_k(q_k - q'_k)$ mit $|a'_{k+1} - a_{k+1}| < |a_k|$. Dies impliziert $a'_{k+1} = a_{k+1}$ und somit $q'_k = q_k$, wie gewünscht.

(b) Für $k \leqslant 1$ folgt die Aussage aus den Anfangswerten der Folgen. Sei also $k \geqslant 1$ und die Aussage gelte für $k-1$ und $k$. Damit $a_{k+1}$ überhaupt definiert ist, muss $a_k > 0$ sein. Dann folgt

$$\begin{aligned} a_{k+1} &= a_{k-1} - q_k a_k \\ &= (u_{k-1}a_0 + v_{k-1}a_1) - q_k(u_k a_0 + v_k a_1) \\ &= (u_{k-1} - q_k u_k)a_0 + (v_{k-1} - q_k v_k)a_1. \end{aligned}$$

Also gilt die Formel für $k+1$, und durch Induktion folgt sie für alle möglichen $k$.

(c) Durch Induktion genügt es zu zeigen, dass $\mathrm{ggT}(a_{k-1}, a_k) = \mathrm{ggT}(a_k, a_{k+1})$ ist für alle $k$ mit $a_k > 0$. Sei dafür $d$ irgendein gemeinsamer Teiler von $a_{k-1}$ und $a_k$. Dann ist $d$ auch ein Teiler von $a_{k+1} = q_k a_k - a_{k-1}$ und somit ein gemeinsamer Teiler von $a_k$ und $a_{k+1}$. Sei umgekehrt $d$ ein gemeinsamer Teiler von $a_k$ und $a_{k+1}$. Dann ist $d$ auch ein Teiler von $a_{k-1} = q_k a_k + a_{k+1}$ und somit ein gemeinsamer Teiler von $a_{k-1}$ und $a_k$. Insbesondere sind die jeweiligen grössten gemeinsamen Teiler gleich.

(d) Für alle $k \geqslant 1$ mit $a_k > 0$ gilt $0 \leqslant a_{k+1} < a_k$ nach Teilaufgabe (a). Da es keine unendlich strikt absteigende Folge natürlicher Zahlen gibt, muss der Prozess also terminieren bei einem $k \geqslant 1$ mit $a_k = 0$. Für diesen Index gilt dann nach Teilaufgabe (c) und (b)

$$\mathrm{ggT}(a_0, a_1) = \mathrm{ggT}(a_{k-1}, a_k) = \mathrm{ggT}(a_{k-1}, 0) = a_{k-1} = u_{k-1}a_0 + v_{k-1}a_1.$$

(e) Für $a_0 := 25$ und $a_1 := 12$ liefert der Euklidische Algorithmus

| $k$ | 0 | 1 | 2 |
|---|---|---|---|
| $a_k$ | 25 | 12 | 1 |
| $q_k$ | | 2 | 12 |
| $u_k$ | 1 | 0 | 1 |
| $v_k$ | 0 | 1 | $-2$ |

Also gilt $\mathrm{ggT}(25, 12) = 1$ und $1 = 1 \cdot 25 + (-2) \cdot 12$. Sodann berechnen wir

| $k$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| $a_k$ | 497 | 284 | 213 | 71 |
| $q_k$ | | 1 | 1 | 3 |
| $u_k$ | 1 | 0 | 1 | $-1$ |
| $v_k$ | 0 | 1 | $-1$ | 2 |

Also gilt $\mathrm{ggT}(497, 284) = 71$ und $71 = (-1) \cdot 497 + 2 \cdot 284$. Schliesslich rechnen wir

| $k$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| $a_k$ | 894 | 158 | 104 | 54 | 50 | 4 | 2 |
| $q_k$ | | 5 | 1 | 1 | 1 | 12 | 2 |
| $u_k$ | 1 | 0 | 1 | $-1$ | 2 | $-3$ | 38 |
| $v_k$ | 0 | 1 | $-5$ | 6 | $-11$ | 17 | $-215$ |

Also gilt $\mathrm{ggT}(158, 894) = 2$ und $2 = 38 \cdot 894 + (-215) \cdot 158$.

(f) Für $a_0 := p$ und $a_1 := a$ ist nach Voraussetzung $\mathrm{ggT}(p, a) = 1$. Nach (d) liefert der Euklidische Algorithmus also $u_{k-1}, v_{k-1} \in \mathbb{Z}$ mit

$$1 \;=\; \mathrm{ggT}(p, a) \;=\; u_{k-1}p + v_{k-1}a.$$

Also gilt $v_{k-1}a \equiv 1 \bmod (p)$ und somit $\overline{a}^{-1} = \overline{v_{k-1}}$ in $\mathbb{F}_p$.

(g) Für $a_0 = 71$ und $a_1 = 33$ liefert der Euklidische Algorithmus

| $k$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| $a_k$ | 71 | 33 | 5 | 3 | 2 | 1 |
| $q_k$ | | 2 | 6 | 1 | 1 | 2 |
| $v_k$ | 0 | 1 | $-2$ | 13 | $-15$ | 28 |

Somit gilt $\overline{33}^{-1} = \overline{v_5} = \overline{28}$ in $\mathbb{F}_{71}$. Schliesslich rechnen wir

| $k$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $a_k$ | 997 | 845 | 152 | 85 | 67 | 18 | 13 | 5 | 3 | 2 | 1 |
| $q_k$ | | 1 | 5 | 1 | 1 | 3 | 1 | 2 | 1 | 1 | 2 |
| $v_k$ | 0 | 1 | $-1$ | 6 | $-7$ | 13 | $-46$ | 59 | $-164$ | 223 | $-387$ |

Somit gilt $\overline{845}^{-1} = \overline{v_{10}} = \overline{-387} = \overline{610}$.

*4. Zeige, dass der Euklidische Algorithmus in $O(\log(a_1 + 1))$ Schritten terminiert.

*Lösung:* Zuerst zeigen wir:

*Behauptung 1:* Ist $k \geqslant 2$ und ist $a_{k+1}$ definiert, so gilt $0 \leqslant a_{k+1} < a_{k-1}/2$.

*Beweis:* Nach Teilaufgabe 3 (a) gilt $a_{k-1} = q_k a_k + a_{k+1}$ mit $0 \leqslant a_{k+1} < a_k$, und wegen $k \geqslant 2$ gilt aus dem gleichen Grund für $k-1$ anstatt $k$ auch $0 \leqslant a_k < a_{k-1}$. Aus der letzten Ungleichung folgt $q_k = \left\lfloor \frac{a_{k-1}}{a_k} \right\rfloor \geqslant 1$ und daraus folgt dann weiter $a_{k-1} \geqslant a_k + a_{k+1} > 2a_{k+1}$. □

*Behauptung 2:* Ist $\ell \geqslant 1$ und ist $a_{2\ell-1}$ definiert, so gilt $0 \leqslant a_{2\ell-1} \leqslant a_1/2^{\ell-1}$.

*Beweis:* Für $\ell = 1$ gilt dies tautologisch. Gilt es für $\ell$, so folgt es auch für $\ell + 1$ mit Behauptung 1 für $k = 2\ell$. □

Sei nun $k$ der grösste Index mit $a_k > 0$ und setze $\ell := \lfloor \frac{k+1}{2} \rfloor$. Im Fall $k > 1$ ist dann $\ell \geqslant 1$ und $2\ell - 1 \leqslant k$ und somit $1 \leqslant a_k \leqslant a_{2\ell-1} \leqslant a_1/2^{\ell-1}$ nach Behauptung 2. Dann ist also $2^{\ell-1} \leqslant a_1$ und daher $k \leqslant 2\ell \leqslant 2\log_2(2a_1)$. In jedem Fall folgt die gewünschte obere Schranke.