ETH Zürich, D-INFK
HS 2016, 17. November 2016

Prof. Ueli Maurer
Daniel Tschudi

# Diskrete Mathematik

# Lösung 8

### 8.1 Chinesischer Restsatz

**a)** $\Longrightarrow$: Aus $a \equiv_{nm} b$ folgt, dass es $k \in \mathbb{Z}$ gibt mit $a - b = k(nm)$ und somit auch $a - b = (kn)m$ und $a - b = (km)n$. Also gilt $a \equiv_n b \wedge a \equiv_m b$.

$\Longleftarrow$: Aus $a \equiv_n b$ und $a \equiv_m b$ folgt dass $x, y \in \mathbb{Z}$ mit $xn = a - b = ym$ existieren. Daraus folgt $n \mid ym$ und da $n$ und $m$ teilerfremd sind, auch $n \mid y$. Also existiert ein $z \in \mathbb{Z}$ mit $zn = y$. Wir erhalten damit $a - b = ym = znm$, also $a \equiv_{nm} b$.

**b)** Da $nm$ und $nm$ nicht teilerfremd sind, können wir den chinesischen Restsatz (CRS) nicht direkt anwenden, um die Lösungsmenge zu bestimmen. Wir formen daher das Gleichungssystem um.

Nach Teilaufgabe a) erhalten wir das äquivalente Gleichungssystem

$$x \equiv_a y_1 \tag{1}$$
$$x \equiv_b y_1 \tag{2}$$
$$x \equiv_a y_2 \tag{3}$$
$$x \equiv_c y_2 \tag{4}$$

Falls $y_1 \not\equiv_a y_2$ gibt es keine Lösungen. Andernfalls sind Gleichungen (1) und (3) äquivalent und wir können (3) streichen. Nach Lemma Lemma 4.17 erhalten wir das äquivalente Gleichungssystem

$$x \equiv_a R_a(y_1) \tag{5}$$
$$x \equiv_b R_b(y_1) \tag{6}$$
$$x \equiv_c R_c(y_2) \tag{7}$$

Da $a, b, c$ teilerfremd sind, garantiert nun der CRS eine eindeutige Lösung $x_0$ im Intervall $[0, abc)$. Allgemeine Lösungen haben die Form $x_0 + k(abc)$ für $k \in \mathbb{N}$. Da $nm = a^2bc$, gibt es genau $a$ Lösungen im Intervall $[0, nm)$.

### 8.2 Diffie-Hellman

**a)**

| Alice | unsicherer Kanal | Bob |
|---|---|---|
| $x_A = 6$<br>$y_A = R_p(g^{x_A}) = R_{19}(2^6) = 7$ | | $x_B = 11$<br>$y_B = R_p(g^{x_B}) = R_{19}(2^{11}) = 15$ |
| | $y_A = 7 \longrightarrow$ | |
| | $\longleftarrow y_B = 15$ | |
| $k_{AB} = R_p(y_B^{x_A}) = R_{19}(15^6) = 11$ | | $k_{BA} = R_p(y_A^{x_B}) = R_{19}(7^{11}) = 11$ |

**b)** Es gilt $4 = y_A = R_p(g^{x_A}) = R_{11}(2^{x_A})$. Durch Ausprobieren sieht man, dass $x_A = 2$ eine Lösung dieser Gleichung ist. Damit ist $k_{AB} = R_p(y_B^{x_A}) = R_{11}(6^2) = 3$.

Alternativ kann natürlich auch $x_B$ durch Ausprobieren ermittelt und daraus $k_{BA} = k_{AB}$ berechnet werden.

In der Praxis werden natürlich viel grössere Zahlen verwendet, was es viel schwieriger macht, $x_A$ (oder $x_B$) zu ermitteln. Möchte man alle Zahlen in $\{0, \ldots, p-2\}$ durchprobieren, müsste man bei einer Primzahl mit 2048 Bits etwa $2^{2048} \approx 10^{616}$ Zahlen betrachten. Zum Vergleich: Die Anzahl der Atome im sichtbaren Universum wird auf weniger als $10^{80}$ geschätzt.

**c)** Nein, denn jedes fixe $x_A$ gibt es das gleiche „Problem“: Ein Angreifer kann leicht nachprüfen, ob $y_A = R_p(g^{x_A})$ gilt. Ist dies der Fall, kann $k_{AB} = R_p(y_B^{x_A})$ berechnet werden, da dann $p, y_B$ und $x_A$ bekannt sind. Insofern unterscheidet sich $x_A = 0$ nicht wesentlich von irgendeiner anderen Wahl für $x_A$. Dies stellt kein Problem für die Sicherheit des Protokolls dar, weil jeder fixe Wert für $x_A$ (für grosse $p$) nur mit extrem kleiner Wahrscheinlichkeit gewählt wird. Bereitet sich also ein Angreifer darauf vor, das Protokoll zu brechen, wenn Alice ein bestimmtes $x_A$ wählt, wird er mit sehr grosser Wahrscheinlichkeit keinen Erfolg haben.

### 8.3 Operationen auf den ganzen Zahlen

**a)** Die Operation $\star$ ist nicht assoziativ, wie man an folgendem Gegenbeispiel sieht:

$$2 \star (0 \star 0) = 2 \star 0 = 4 \neq 16 = 4 \star 0 = (2 \star 0) \star 0$$

Die Operation $\diamond$ ist hingegen assoziativ, denn für alle ganzen Zahlen $a, b, c$ gilt:

$$\begin{aligned} a \diamond (b \diamond c) &= a \diamond (b + c + 2bc) = a + (b + c + 2bc) + 2a(b + c + 2bc) \\ &= a + b + c + 2bc + 2ab + 2ac + 4abc \\ &= (a + b + 2ab) + c + 2(a + b + 2ab)c = (a \diamond b) + c + 2(a \diamond b)c \\ &= (a \diamond b) \diamond c \end{aligned}$$

**b)** Die Operationen $\star$ und $\diamond$ sind beide kommutativ, denn für alle ganzen Zahlen $a, b$ gilt wegen der Kommutativität von $+$ und $\cdot$

$$a \star b = a^2 + b^2 = b^2 + a^2 = b \star a$$

und

$$a \diamond b = a + b + 2ab = b + a + 2ba = b \diamond a.$$

**c)** Die Operation $\star$ besitzt kein Neutralelement. Wir zeigen dies durch Widerspruch und nehmen wir an, $e$ ist ein Neutralelement. Dann muss für jede ganze Zahl $a$ gelten $e \star a = e^2 + a^2 = a$. Das gilt insbesondere für $a = 2$, also $e^2 = -2$. Es gibt aber keine ganze Zahl $e$, die diese Gleichung erfüllt.

Die Operation $\diamond$ besitzt ein Neutralelement $e$ und zwar $e = 0$, denn für jede ganze Zahl $a$ gilt $0 \diamond a = 0 + a + 2 \cdot 0 \cdot a = 0 + a + 0 = a$.

Da $\diamond$ nach Aufgabenteil ii) kommutativ ist, gilt auch $a \diamond 0 = 0 \diamond a = a$.

**d)** Da $\star$ kein Neutralelement besitzt, gibt es auch keine Inversen (diese sind gar nicht definiert).

Auch bezüglich $\diamond$ existiert nicht für jede ganze Zahl ein Inverses. Wir zeigen dies mit einem Beweis durch Widerspruch und nehmen dazu an, jede ganze Zahl besitzt ein Inverses. Nach Aufgabenteil iii) ist das Neutralelement $0$. Da $2 \in \mathbb{Z}$, existiert demnach ein $a \in \mathbb{Z}$ mit $0 = 2 \diamond a = 2 + a + 4a = 2 + 5a$. Daraus folgt $5a = -2$, d.h. $5$ ist ein Teiler von $-2$. Dies ist ein Widerspruch, also existiert kein solches $a$.

### 8.4 Rechtsneutrales Element

Sei $\langle G; *, \widehat{\ }, e\rangle$ eine Gruppe. Wir müssen zeigen, dass jedes $e \in G$ mit $a * e = a \; \forall a \in G$ auch ein linksneutrales Element der Gruppe ist (ohne **G2** zu verwenden). Es gilt:

$$e * a \overset{\text{G3}}{=} (a * \widehat{a}) * a \overset{\text{G1}}{=} a * (\widehat{a} * a) \overset{\text{G3}}{=} a * e \overset{\text{G2'}}{=} a$$

### 8.5 Gruppenoperationen

**a)** Dies kann direkt gezeigt werden:

$$a \overset{\text{G2}}{=} a * e \overset{\text{G3}}{=} a * \left(\widehat{a} * \widehat{(\widehat{a})}\right) \overset{\text{G1}}{=} (a * \widehat{a}) * \widehat{(\widehat{a})} \overset{\text{G3}}{=} e * \widehat{(\widehat{a})} \overset{\text{G2}}{=} \widehat{(\widehat{a})}$$

*(2 Punkte)*

Man könnte aber auch mit der Eindeutigkeit des Inversen argumentieren (Lemma 5.2), da sowohl $a$ als auch $\widehat{(\widehat{a})}$ ein Inverses von $\widehat{a}$ sind.

**b)** Es gilt $(a * b) * (\widehat{b} * \widehat{a}) = e$, da:

$$(a * b) * (\widehat{b} * \widehat{a}) \overset{\text{G1}}{=} a * \left(b * (\widehat{b} * \widehat{a})\right) \overset{\text{G1}}{=} a * \left((b * \widehat{b}) * \widehat{a}\right) \overset{\text{G3}}{=} a * (e * \widehat{a}) \overset{\text{G2}}{=} a * \widehat{a} \overset{\text{G3}}{=} e \qquad (8)$$

*(1 Punkt)*

Dadurch erhalten wir:

$$\widehat{a*b} \overset{\text{G2}}{=} \widehat{a*b}*e \overset{(8)}{=} \widehat{a*b}*\Big((a*b)*(\widehat{b}*\widehat{a})\Big)$$
$$\overset{\text{G1}}{=} \Big(\widehat{a*b}*(a*b)\Big)*(\widehat{b}*\widehat{a}) \overset{\text{G3}}{=} e*(\widehat{b}*\widehat{a}) \overset{\text{G2}}{=} \widehat{b}*\widehat{a}$$

*(1 Punkt)*

Man könnte aber auch mit der Eindeutigkeit des Inversen argumentieren (Lemma 5.2), da sowohl $\widehat{a*b}$ als auch $\widehat{b}*\widehat{a}$ ein Inverses von $a*b$ sind.

**c)** Wir nehmen an, es gilt $a*b = a*c$. Daraus folgt

$$b \overset{\text{G2}}{=} e*b \overset{\text{G3}}{=} (\widehat{a}*a)*b \overset{\text{G1}}{=} \widehat{a}*(a*b) \overset{\text{Ann.}}{=} \widehat{a}*(a*c) \overset{\text{G1}}{=} (\widehat{a}*a)*c \overset{\text{G3}}{=} e*c \overset{\text{G2}}{=} c.$$

*(1 Punkt)*

### 8.6 Symmetrien des Würfels

**a)** Man muss sich zuerst für eine Ecke des Würfels entscheiden, die in der Ecke des Raumes zuliegen kommt. Dafür gibt es $8$ Möglichkeiten. Wenn eine Würfelecke ausgesucht wurde, gibt es $3$ Nachbarecken, von denen eine nach oben kommt. Danach ist die Lage vollständig bestimmt. Insgesamt gibt es also $24$ Möglichkeiten.

**b)** Nehmen wir an, die Ecken des Würfels seien mit $0, 1, \ldots, 7$ nummeriert und vor der Drehung sei $0$ in der Ecke des Zimmers und $1$ darüber. Die Drehung ist eindeutig bestimmt, wenn man weiss, wo und in welcher Orientierung die Kante $(0, 1)$ zu liegen kommt. Es gibt also höchstens so viele Drehungen, wie Möglichkeiten in Teilaufgabe a). Andererseits kann der Würfel mit nur einer Drehung in jede Position gebracht werden. Es gibt also genau $24$ Drehungen.

Die Elemente von $R$ lassen sich wie folgt als Rotationen um eine Achse beschreiben:

- Die Identität.
- Rotation um die Zentren gegenüberliegender Seiten um $90$, $180$ und $270$ Grad. Es gibt drei Paare gegenüberliegender Seiten, was total $9$ Rotationen ergibt.
- Rotation um gegenüberliegende Ecken um $120$ und $240$ Grad. Es gibt vier Paare gegenüberliegender Ecken, was total $8$ Rotationen ergibt.
- Rotation um die Zentren gegenüberliegender Kanten um $180$ Grad. Es gibt $6$ Paare gegenüberliegender Kanten, somit $6$ Rotationen.

Man kann sich leicht überlegen, dass keine zwei der oben beschriebenen Rotationen das gleiche erreichen, und damit können wir tatsächlich jedes Element von $R$ durch *eine einzige* Rotation beschreiben.

**c)** Die Operation $\circ$ ist assoziativ, da die Verknüpfung von Funktionen assoziativ ist. Es gibt ein Neutralelement, die Identität. Weiterhin hat jedes Element ein Inverses, nämlich die Rotation um dieselbe Achse um $360°$ minus des Winkels. Somit ist $\langle R; \circ \rangle$ eine Gruppe.

**d)** Die Operation $\circ$ ist nicht kommutativ, da wie Abbildung 1 illustriert Rotationen existieren, die nicht kommutieren.

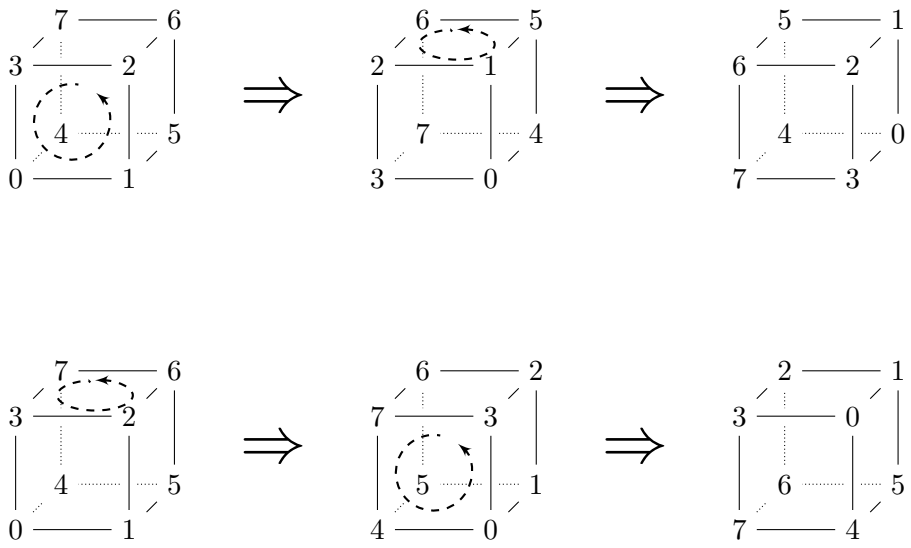


Abbildung 1: $\langle R; \circ \rangle$ ist nicht kommutativ.