ETH Zürich, D-INFK
HS 2016, 7. November 2016

Prof. Ueli Maurer
Daniel Tschudi

Diskrete Mathematik
Übung 8

8.1 Chinesischer Restsatz

a) ($\star\star\star$) Zeigen Sie für alle $a, b \in \mathbb{Z}$ und $n, m \geq 1$ mit $\mathrm{ggT}(n, m) = 1$ gilt

$$a \equiv_{nm} b \;\Leftrightarrow\; a \equiv_n b \;\wedge\; a \equiv_m b$$

b) ($\star\star\star$) Seien a, b, c drei teilerfremde ganze Zahlen. Für $n = ab$ und $m = ac$ seien folgende Kongruenzen mit $0 \leq y_1 < n,\ 0 \leq y_2 < m$ gegeben:

$$x \equiv_n y_1$$
$$x \equiv_m y_2$$

Wie viele Lösungen $0 \leq x < nm$ gibt es abhängig von a, b, c und y_1, y_2?

8.2 Diffie-Hellman

a) ($\star\star$) Führen Sie das Diffie-Hellman Protokoll für $p = 19$, $g = 2$, $x_A = 6$ und $x_B = 11$ aus und bestimmen Sie den gemeinsamen Schlüssel $k_{AB} = k_{BA}$.

b) ($\star\star$) Alice und Bob führen ein Diffie-Hellman Protokoll aus mit $p = 11$ und $g = 2$. Sie wollen die Kommunikation abhören und haben den Kanal zwischen Alice und Bob angezapft. So erfahren Sie die Werte $y_A = 4$ und $y_B = 6$. Berechnen Sie den vereinbarten Schlüssel.

c) ($\star\star\star$) Alice wählt x_A zufällig aus $\{0, \ldots, p-2\}$. Falls Alice $x_A = 0$ wählt, schickt sie $y_A = R_p(g^0) = 1$ und es gilt $k_{AB} = R_p(y_B^0) = 1$. Ein Angreifer kann in diesem Fall also den vereinbarten Schlüssel direkt ermitteln. Sollte Alice daher besser x_A zufällig aus $\{1, \ldots, p-2\}$ wählen?

8.3 Operationen auf den ganzen Zahlen ($\star\star$)

Betrachten Sie die beiden folgenden Operationen auf der Menge der ganzen Zahlen:

$$a \star b := a^2 + b^2 \qquad\qquad a \diamond b := a + b + 2ab$$

Beweisen oder widerlegen Sie jeweils:

a) Die Verknüpfung ist assoziativ.

b) Die Verknüpfung ist kommutativ.

c) Es existiert ein Neutralelement.

d) Für jede ganze Zahl existiert ein Inverses.

8.4 Rechtsneutrales Element ($\star$ $\star$)

Zeigen Sie, dass es genügt in den Gruppenaxiomen die Existenz eines rechtsneutralen Elements zu fordern. Das heisst, es ist zu zeigen, dass das Gruppenaxiom **G2** aus den Axiomen **G1** , **G2'** und **G3** folgt, wobei

G2': Es existiert ein (rechtsneutrales) Element e, so dass $a * e = a$ für jedes $a \in G$.

8.5 Gruppenoperationen ($\star$ $\star$) *(5 Punkte)*

Ziel dieser Aufgabe ist es, Teile von Lemma 5.3 zu beweisen. Sei dazu $\langle G; *, \widehat{\ }, e\rangle$ eine Gruppe und seien $a, b, c \in G$. Zeigen Sie:

a) $\widehat{(\widehat{a})} = a$ *(2 Punkte)*

b) $\widehat{a * b} = \widehat{b} * \widehat{a}$ *(2 Punkte)*

c) $a * b = a * c \;\Rightarrow\; b = c$ *(1 Punkt)*

8.6 Symmetrien des Würfels

In der Ecke eines Schlafzimmers steht ein Sofa in der Form eines Würfels, dessen Ecken mit $0, 1, \ldots, 7$ nummeriert sind.

a) ($\star$) Auf wie viele Arten kann man diesen Würfel in die Ecke stellen?

Man kann nun den Würfel aus der Ecke nehmen, ihn irgendwie drehen, und dann wieder in die Ecke stellen. Wir wollen nur Drehungen b_1 und b_2 unterscheiden, falls die Lage des Würfels nach Drehung b_1 eine andere ist als nach b_2. Bezeichne R die Menge dieser Drehungen.

b) ($\star$ $\star$) Bestimmen Sie $|R|$. Können Sie jedes Element von R als eine Rotation um eine Achse beschreiben? (Für unterschiedliche Elemente können die Achsen verschieden sein.)

c) ($\star$ $\star$) Sei $b_2 \circ b_1$ das Ausführen von Drehung b_1 gefolgt von Drehung b_2. Ist $\langle R; \circ\rangle$ eine Gruppe?

d) ($\star$) Ist $\circ$ kommutativ?

Abgabe am 14./15. November 2016
Korrigiert wird Aufgabe 8.5