ETH Zürich, D-INFK
HS 2016, 28. Oktober 2016

Prof. Ueli Maurer
Daniel Tschudi

Diskrete Mathematik

Lösung 7

7.1 Der grösste gemeinsame Teiler

a) Seien $a, b, u, v \in \mathbb{Z} - \{0\}$ mit $ua + vb = 1$. Aus der Definition des ggT folgt $\mathrm{ggT}(a, b) \mid a$ und $\mathrm{ggT}(a, b) \mid b$, d.h. es existieren $c, d \in \mathbb{Z}$ mit $a = c \cdot \mathrm{ggT}(a, b)$ und $b = d \cdot \mathrm{ggT}(a, b)$. *(1 Punkt)*

Daraus folgt $1 = ua + vb = (uc + vd) \cdot \mathrm{ggT}(a, b)$, also $\mathrm{ggT}(a, b) \mid 1$. *(1 Punkt)*

Da 1 der einzige positive Teiler von 1 ist, gilt somit $\mathrm{ggT}(a, b) = 1$. *(1 Punkt)*

b) Sei $d \in \mathbb{N} - \{0, 1\}$. Setze $a := 3$, $b := 2$, $u := d$ und $v := -d$. *(1 Punkt)*

Dann gilt $ua + vb = 3d - 2d = d$ und $\mathrm{ggT}(a, b) = \mathrm{ggT}(3, 2) = 1 \neq d$. *(1 Punkt)*

7.2 Erweiterter Euklidischer Algorithmus

a) Folgende Tabelle zeigt die Werte von s_1, s_2, u_1, u_2, v_1 und v_2 jeweils nach der Initialisierung und nach jedem Schleifendurchlauf des Algorithmus aus Figur 6.1.

	s_1	s_2	u_1	u_2	v_1	v_2
nach Initialisierung	553	26	1	0	0	1
nach Schleifendurchlauf 1	26	7	0	1	1	−21
nach Schleifendurchlauf 2	7	5	1	−3	−21	64
nach Schleifendurchlauf 3	5	2	−3	4	64	−85
nach Schleifendurchlauf 4	2	1	4	−11	−85	234
nach Schleifendurchlauf 5	1	0	−11	26	234	−553

Daraus folgt mit Theorem 4.6 $\mathrm{ggT}(553, 26) = 1$ sowie dass für $u := -11, v := 234$ die Gleichung $553u + 26v = \mathrm{ggT}(553, 26)$ gilt.

b) Nach Aufgabenteil a) gilt $234 \cdot 26 - 11 \cdot 553 = 1$. Da $234 \cdot 26 \equiv_{26} 0$ gilt, folgt mit Lemma 4.17 (i), dass $-11 \cdot 553 \equiv_{26} 1$. Wir können also $a := -11$ wählen. Analog sieht man, dass $b := 234$ die Kongruenz $b \cdot 26 \equiv_{553} 1$ erfüllt.

7.3 Irrationalität von Logarithmen

a) Wir führen einen Widerspruchsbeweis und nehmen dazu an, es existieren $n \in \mathbb{N}$, $m \in \mathbb{N} - \{0\}$ mit $\log_7(11) = \frac{n}{m}$. Es folgt (nach Definition von log), $7^{\frac{n}{m}} = 11$ und damit $7^n = 11^m$. Die positive ganze Zahl 7^n lässt sich nach Theorem 4.8 eindeutig als Produkt von Primzahlen schreiben. Dies ist ein Widerspruch dazu, dass 7 und

11 verschiedene Primzahlen sind. Also existieren keine solchen n, m und $\log_7(11)$ ist irrational.

b) Sei $A := \{(a, b) \mid a < b \text{ und } a, b \text{ sind Primzahlen}\}$. Da es nach Theorem 4.10 unendlich viele Primzahlen gibt, enthält A unendlich viele Elemente. Sei $(a, b) \in A$. Angenommen, $\log_a(b)$ ist rational. Dann existieren $n \in \mathbb{N}$, $m \in \mathbb{N} - \{0\}$ mit $\log_a(b) = \frac{n}{m}$, d.h. $a^{\frac{n}{m}} = b$. Daraus folgt $a^n = b^m$. Die positive ganze Zahl a^n lässt sich nach Theorem 4.8 eindeutig als Produkt von Primzahlen schreiben. Da a und b Primzahlen sind, folgt daraus $a = b$ und $n = m$. Dann ist aber im Widerspruch zur Annahme $(a, b) \notin A$. Also folgt, dass $\log_a(b)$ irrational ist.

7.4 Kongruenz

a) Aus $a \equiv_m b$ bzw $c \equiv_m d$ folgt, dass es $s, t \in \mathbb{Z}$ gibt mit $a - b = ms$ und $c - d = mt$ und somit $a = ms + b$ und $c = mt + d$. Also gilt

$$ac = (ms + b)(mt + d) = m^2st + msd + mtb + bd \equiv_m bd.$$

Im letzten Schritt wurde verwendet, dass m die Zahl $(m^2st + msd + mtb + bd) - bd$ teilt.

b) Nach dem Binomialsatz gilt

$$(a + b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k}b^k = a^p + b^p + \sum_{k=1}^{p-1} \binom{p}{k} a^{p-k}b^k.$$

Es genügt also zu zeigen, dass $\binom{p}{k}$ für $k \in \{1, \ldots, p-1\}$ durch p teilbar ist. Dazu betrachten wir Zähler und Nenner von $\binom{p}{k} = \frac{p!}{k!\ (p-k)!}$. Der Zähler enthält den Primfaktor p. Im Nenner ist keiner der Faktoren durch p teilbar, da diese alle kleiner als p sind. Nach Lemma 4.7 ist also der Nenner nicht durch p teilbar. Da $\binom{p}{k} \in \mathbb{N}$, muss somit auch $\frac{(p-1)!}{k!\ (p-k)!} \in \mathbb{N}$ sein. Damit ist p ein Teiler von $\binom{p}{k} = p \cdot \frac{(p-1)!}{k!\ (p-k)!}$.

7.5 Modulare Arithmetik

a) Nach Theorem 4.1 existiert ein $q \in \mathbb{Z}$ mit $n = qe + R_e(n)$. Damit ist

$$\begin{aligned} R_m(a^n) &= R_m\left(a^{qe+R_e(n)}\right) \\ &= R_m\left((a^e)^q \cdot a^{R_e(n)}\right) \\ &= R_m\left(\left(R_m\left(a^e\right)\right)^q \cdot R_m\left(a^{R_e(n)}\right)\right), \end{aligned}$$

wobei im letzten Schritt Lemma 4.18 (ii) wiederholt angewendet wurde. *(1 Punkt)*
Da wir $R_m(a^e) = 1$ angenommen haben, ist $R_m(a^n) = R_m(a^{R_e(n)})$. *(1 Punkt)*

b) Nach Aufgabenteil a) gilt $R_{11}(4^{2015}) = R_{11}(4^{R_{10}(2015)}) = R_{11}(4^5) = R_{11}(2^{10}) = 1$. *(1 Punkt)*

c) Aus iterativer Anwendung von Lemma 4.18 (ii) folgt $R_9(10^k) = R_9(R_9(10)^k) = 1$ für $k \in \mathbb{N}$. Es folgt für $0 \leq b \leq 9$ und $k \in \mathbb{N}$, dass $R_9(b \cdot 10^k) = R_9(R_9(b) \cdot R_9(10^k)) = R_9(b)$. *(1 Punkt)*

Damit gilt für a mit Dezimaldarstellung $a_n a_{n-1} \dots a_0$:

$$R_9(a) = R_9\big(\sum_{i=0}^{n} a_i \cdot 10^i\big) = R_9\big(\sum_{i=0}^{n} R_9(a_i \cdot 10^i)\big) = R_9\big(\sum_{i=0}^{n} R_9(a_i)\big) = R_9\big(\sum_{i=0}^{n} a_i\big)$$

(1 Punkt)

d) Mit Aufgabenteil c) folgt:

$$\begin{aligned} & R_9(98877766665555544444433333332222222211111111) \\ =& R_9\big(1 \cdot 9 + 2 \cdot 8 + \dots + 8 \cdot 2 + 9 \cdot 1\big) = R_9(165) \\ =& R_9\big(1 + 6 + 5\big) = R_9(12) = 3 \end{aligned}$$

(1 Punkt)

7.6 Die Insel

Sei x die Anzahl der Kokosnüsse, die insgesamt gesammelt wurden. Aus dem Aufgabentext erhält man folgendes System linearer Kongruenzen:

$$\begin{aligned} x &\equiv_8 1 \\ x &\equiv_7 2 \\ x &\equiv_5 3 \end{aligned}$$

Da 8, 7 und 5 paarweise teilerfremd sind, können wir Theorem 4.20 anwenden. Sei $m_1 = 8$, $m_2 = 7$, $m_3 = 5$, $M = 8 \cdot 7 \cdot 5 = 280$, $M_1 = 280/8 = 35$, $M_2 = 280/7 = 40$ und $M_3 = 280/5 = 56$. Wir suchen nun N_1, N_2, N_3 mit $M_i N_i \equiv_{m_i} 1$ für $i \in \{1, 2, 3\}$. Durch Probieren finden wir $N_1 = 3$, $N_2 = 3$ und $N_3 = 1$. Nach der Formel im Beweis von Theorem 4.20 werden obige Kongruenzen erfüllt von

$$R_{280}(1 \cdot 35 \cdot 3 + 2 \cdot 40 \cdot 3 + 3 \cdot 56 \cdot 1) = R_{280}(513) = 233.$$

Weiter folgt aus diesem Theorem, dass dies die einzige Lösung x mit $0 \leq x < 280$ ist. Da es auf der ganzen Insel nicht mehr als 250 Kokosnüsse gibt, muss $x = 233$ gelten.

Die 5 überlebenden Piraten teilen also 233 Kokosnüsse untereinander auf. Daher bekommt jeder von ihnen 46 Stück und der Affe bekommt nur die verbleibenden 3.