6. Musterlösung zu Mathematik für Informatiker I, WS 2003/04

OLAF MÜLLER, MICHAEL NÜSKEN, KATHRIN TOFALL

Aufgabe 6.1 (Teilbarkeit). (2 Punkte)

Seien $s, t, x, y, d \in \mathbb{Z}$. Zeige:

(i) $d \mid x \wedge d \mid y \Longrightarrow d \mid (s \cdot x + t \cdot y)$.

Lösung. Aus $d \mid x \wedge d \mid y$ folgt, dass $u, v \in \mathbb{Z}$ existieren mit $u \cdot d = x$ und $v \cdot d = y$. Also können wir in $sx + ty$ wie folgt x und y ersetzen:

$$sx + ty = sud + tvd = d \cdot (su + tv).$$

Also gilt $d \mid (sx + ty)$. ◯

(ii) $s \cdot x + t \cdot y = d \Longrightarrow \text{ggT}(x, y) \mid d$.

Lösung. Sei $g := \text{ggT}(x, y)$. Dann gilt offensichtlich $g \mid x$ und $g \mid y$. Mit (i) folgt $g \mid sx + ty$, das ist $g \mid d$. ◯

Aufgabe 6.2 (Primfaktorzerlegung, ggT, kgV). (7 Punkte)

(i) Seien $a, b \in \mathbb{R}$. Zeige: $a + b = \min\{a, b\} + \max\{a, b\}$.

Lösung.

1. Fall $a < b$: $\min\{a, b\} + \max\{a, b\} = a + b$.
2. Fall $b < a$: $\min\{a, b\} + \max\{a, b\} = b + a = a + b$.
3. Fall $a = b$: $\min\{a, b\} + \max\{a, b\} = a + a = b + b = a + b$. ◯

Seien $r \in \mathbb{N}_{\geq 1}$, $p_1, \ldots, p_r$ prim und paarweise verschieden, $e_1, \ldots, e_r, f_1, \ldots, f_r \in \mathbb{N}$.

(ii) Zeige: Für $x \in \mathbb{N}$ gilt:

$$\begin{aligned} & x \mid (p_1^{f_1} \cdot \ldots \cdot p_r^{f_r}) \\ \iff & \exists\, e_1, \ldots, e_r \in \mathbb{N} \quad x = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r} \wedge e_1 \leq f_1 \wedge \ldots \wedge e_r \leq f_r. \end{aligned}$$

Lösung.

„⇒“ Es gibt also ein $t \in \mathbb{N}_{\geq 1}$ mit $x \cdot t = p_1^{f_1} \cdot \ldots \cdot p_r^{f_r}$. Zuerst nehmen wir an, x hätte einen Primfaktor q, der nicht in $p_1, \ldots, p_r$ enthalten ist. Dann enthält auch $x \cdot t$ diesen Primfaktor, also auch $p_1^{f_1} \cdot \ldots \cdot p_r^{f_r}$, im Widerspruch zur Eindeutigkeit der Primfaktorzerlegung. Also besitzt x höchstens die Primfaktoren $p_1, \ldots, p_r$ und es existieren $e_1, \ldots, e_r \in \mathbb{N}$ mit $x = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$. Das ist der erste Teil der Behauptung. Nehmen wir nun an, für ein $i \in \mathbb{N}$ mit $1 \leq i \leq n$ würde $e_i > f_i$ gelten. Wir können der Einfachheit halber annehmen, dass $i = 1$ gilt, indem wir gegebenenfalls die Primzahlen $p_1, \ldots, p_r$ umnummerieren. Indem wir

$$p_1^{e_1} \cdot \ldots \cdot p_r^{e_r} \cdot t = p_1^{f_1} \cdot \ldots \cdot p_r^{f_r}$$

durch $p_1^{f_1}$ teilen, erhalten wir

$$p_1^{e_1 - f_1} \cdot p_e^{f_2} \cdot \ldots \cdot p_r^{e_r} \cdot t = p_2^{f_2} \cdot \ldots \cdot p_r^{f_r}.$$

Da $e_1 - f_1 > 0$ ist, ist p_1 ein Primfaktor der linken Seite. Da aber $p_2, \ldots, p_r$ nach Voraussetzung alle von p_1 verschieden sind, ist p_1 kein Primfaktor der rechten Seite, was erneut ein Widerspruch zur Eindeutigkeit der Primfaktorzerlegung ist.

„⇐“ Seien also $e_1, \ldots, e_r \in \mathbb{N}$ mit $x = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r} \wedge e_1 \leq f_1 \wedge \ldots \wedge e_r \leq f_r$. Wegen

$$x \cdot p_1^{f_1 - e_1} \cdot \ldots \cdot p_r^{f_r - e_r} = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r} \cdot p_1^{f_1 - e_1} \cdot \ldots \cdot p_r^{f_r - e_r} = p_1^{f_1} \cdot \ldots \cdot p_r^{f_r}$$

gilt $x \mid (p_1^{f_1} \cdot \ldots \cdot p_r^{f_r})$. ◯

Wir erinnern an die Definition des ggT:

Definition (ggT). *Seien $a, b \in \mathbb{N}$. Eine Zahl $g \in \mathbb{N}$ heißt* größter gemeinsamer Teiler von a und b *genau dann, wenn*

- $g \mid a$ *und* $g \mid b$ *gilt (g ist ein gemeinsamer Teiler), und*
- $\forall t \in \mathbb{N} \quad t \mid a \ \wedge \ t \mid b \Rightarrow t \mid g$ *gilt (jeder gemeinsame Teiler t teilt g).*

Wir schreiben dann auch $g = \mathrm{ggT}(a, b)$.

(iii) Zeige: $\mathrm{ggT}(p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}, p_1^{f_1} \cdot \ldots \cdot p_r^{f_r}) = p_1^{\min\{e_1, f_1\}} \cdot \ldots \cdot p_r^{\min\{e_r, f_r\}}$.

Lösung. Wir rechnen die Eigenschaften aus der Definition des ggT nach mit $a = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$, $b = p_1^{f_1} \cdot \ldots \cdot p_r^{f_r}$ und $g = p_1^{\min\{e_1,f_1\}} \cdot \ldots \cdot p_r^{\min\{e_r,f_r\}}$.

Wegen $\min\{e_1, f_1\} \leq e_1 \wedge \ldots \wedge \min\{e_r, f_r\} \leq e_r$ folgt mit (ii), dass $g \mid a$ gilt. Analog erhält man $g \mid b$.

Sei nun $t \in \mathbb{Z}$ mit $t \mid (p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}) \wedge t \mid (p_1^{f_1} \cdot \ldots \cdot p_r^{f_r})$. Dann existieren nach (ii) $d_1, \ldots, d_r \in \mathbb{N}$ mit $t = p_1^{d_1} \cdot \ldots \cdot p_r^{d_r}$ und $d_1 \leq e_1 \wedge \ldots \wedge d_r \leq e_r$ sowie $d_1 \leq f_1 \wedge \ldots \wedge d_r \leq f_r$. Also gilt für alle i, $1 \leq i \leq r$: $d_i \leq \min\{e_i, f_i\}$. Wiederum mit (ii) folgt daraus $t \mid g$. ◯

Die Definition des kgV ist ganz analog zu der des ggT:

Definition (kgV). *Seien $a, b \in \mathbb{N}$. Eine Zahl $k \in \mathbb{N}$ heißt* kleinstes gemeinsames Vielfaches von a und b *genau dann, wenn*

- $a \mid k$ *und* $b \mid k$ *gilt (k ist ein gemeinsames Vielfaches), und*
- $\forall v \in \mathbb{N} \quad a \mid v \ \wedge \ b \mid v \Rightarrow k \mid v$ *gilt (jedes gemeinsame Vielfache v ist ein Vielfaches von k).*

Wir schreiben dann auch $k = \mathrm{kgV}(a, b)$.

(iv) Zeige: $\mathrm{kgV}(p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}, p_1^{f_1} \cdot \ldots \cdot p_r^{f_r}) = p_1^{\max\{e_1,f_1\}} \cdot \ldots \cdot p_r^{\max\{e_r,f_r\}}$.

Lösung. Wir rechnen die Eigenschaften aus der Definition des kgV nach mit $a = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$, $b = p_1^{f_1} \cdot \ldots \cdot p_r^{f_r}$ und $k = p_1^{\max\{e_1,f_1\}} \cdot \ldots \cdot p_r^{\max\{e_r,f_r\}}$.

Wegen $e_1 \leq \max\{e_1, f_1\} \wedge \ldots \wedge e_r \leq \max\{e_r, f_r\}$ folgt mit (ii), dass $a \mid k$ gilt. Analog erhält man $b \mid k$.

Sei nun $v \in \mathbb{Z}$, $v = p_1^{w_1} \cdot \ldots \cdot p_r^{w_r} \cdot p_{r+1}^{w_{r+1}} \cdot \ldots \cdot p_\ell^{w_\ell}$, mit $a \mid v \wedge b \mid v$. Dann sind nach (ii) $e_1 \leq w_1 \wedge \ldots \wedge e_r \leq w_r$ sowie $f_1 \leq w_1 \wedge \ldots \wedge f_r \leq w_r$. Also gilt für alle i, $1 \leq i \leq r$: $w_i \geq \max\{e_i, f_i\}$. Wiederum mit (ii) folgt daraus $k \mid v$. ◯

(v) Seien $x, y \in \mathbb{N}$. Zeige: $\mathrm{ggT}(x, y) \cdot \mathrm{kgV}(x, y) = x \cdot y$.

Lösung. Sei $x = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$ die Primfaktorzerlegung von x und $y = p_1^{f_1} \cdot \ldots \cdot p_r^{f_r}$ die von y. Dann gilt mit (iii) und (iv):

$$\begin{aligned}
\mathrm{ggT}(x, y) \cdot \mathrm{kgV}(x, y) &= p_1^{\min\{e_1,f_1\}} \cdot \ldots \cdot p_r^{\min\{e_r,f_r\}} \\
&\quad \cdot p_1^{\max\{e_1,f_1\}} \cdot \ldots \cdot p_r^{\max\{e_r,f_r\}} \\
&= p_1^{\min\{e_1,f_1\}+\max\{e_1,f_1\}} \cdot \ldots \cdot p_r^{\min\{e_r,f_r\}+\max\{e_r,f_r\}} \\
&\overset{\text{(ii)}}{=} p_1^{e_1+f_1} \cdot \ldots \cdot p_r^{e_r+f_r} \\
&= p_1^{e_1} \cdot \ldots \cdot p_r^{e_r} \cdot p_1^{f_1} \cdot \ldots \cdot p_r^{f_r} \\
&= x \cdot y.
\end{aligned}$$

◯

(vi) Betrachte $x = 1\,639\,032\,613$ und $y = 3\,278\,156\,593$. Berechne (von Hand) ggT(x, y) und kgV(x, y). [*Tipp*: Primfaktorzerlegung ist hier nicht notwendig.]

Lösung. Der Euklidische Algorithmus arbeitet mit Divisionen mit Rest. Zuerst wird hier y durch x geteilt:

$$\begin{array}{rcl} 3\,278\,156\,593 & = & 1\,639\,032\,613 \cdot 2 + 91\,367 \\ \underline{3\,278\,065\,226} & & \\ 91\,367 & & \end{array}$$

Dann wird x durch den Rest dieser Division geteilt:

$$\begin{array}{rcl} 1\,639\,032\,613 & = & 91\,367 \cdot 17\,939 + 0 \\ \underline{913\,67} & & \\ 725\,362 & & \\ \underline{639\,569} & & \\ 85\,793\,6 & & \\ \underline{82\,230\,3} & & \\ 3\,563\,31 & & \\ \underline{2\,741\,01} & & \\ 822\,303 & & \\ \underline{822\,303} & & \\ 0 & & \end{array}$$

Also ist hier der ggT von x und y genau $91\,367$. Um jetzt das kgV zu berechnen, benutzen wir die Formel aus (v):

$$\begin{aligned} \text{kgV}(x, y) &= \frac{x \cdot y}{\text{ggT}(x, y)} = \frac{1\,639\,032\,613 \cdot 3\,278\,156\,593}{91\,367} \\ &= 17\,939 \cdot 3\,278\,156\,593 \\ &= 58\,806\,851\,121\,827. \end{aligned}$$

◯

Aufgabe 6.3 (Erweiterter Euklidischer Algorithmus). (5 Punkte)

Betrachte den folgenden Algorithmus:

Algorithmus. Erweiterter Euklidischer Algorithmus.
Eingabe: $a, b \in \mathbb{Z}$.
Ausgabe: $\ell \in \mathbb{N}$, $r_i, s_i, t_i \in \mathbb{Z}$ für $0 \leq i \leq \ell + 1$, und $q_i \in \mathbb{Z}$ für $1 \leq i \leq \ell$, 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. While $r_i \neq 0$ do 6–10
6. $\quad q_i \leftarrow r_{i-1}$ 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. Return ℓ, r_i, s_i, t_i für $0 \leq i \leq \ell + 1$, und q_i für $1 \leq i \leq \ell$.

(i) Führe den Algorithmus für $a = 219\,215$ und $b = 807\,959$ durch. Notiere ℓ sowie in einer Tabelle i, r_i, q_i, s_i, t_i.

Lösung.

i	Kommentar	r_i	q_i	s_i	t_i
0		$219\,215$	–	1	0
1		$807\,959$	0	0	1
2	$219\,215 = 0 \cdot 807\,959 + 219\,215$	$219\,215$	3	1	0
3	$807\,959 = 3 \cdot 219\,215 + 150\,314$	$150\,314$	1	-3	1
4	$219\,215 = 1 \cdot 150\,314 + 68\,901$	$68\,901$	2	4	-1
5	$150\,314 = 2 \cdot 68\,901 + 12\,512$	$12\,512$	5	-11	3
6	$68\,901 = 5 \cdot 12\,512 + 6\,341$	$6\,341$	1	59	-16
7	$12\,512 = 1 \cdot 6\,341 + 6\,171$	$6\,171$	1	-70	19
8	$6\,341 = 1 \cdot 6\,171 + 170$	170	36	129	-35
9	$6\,171 = 36 \cdot 170 + 51$	51	3	$-4\,714$	$1\,279$
10	$170 = 3 \cdot 51 + 17$	$\mathbf{17}$	3	$\mathbf{14\,271}$	$\mathbf{-3\,872}$
11	$51 = 3 \cdot 17 + 0$	0	–	$-47\,527$	$12\,895$

und $\ell = 10$.

Zur Probe prüfen wir — wie immer! — die letzte Zeile nach: $-47\,527 \cdot 219\,215 + 12\,895 \cdot 807\,959 = 0$. Tatsächlich ist $14\,271 = 807\,959/17$ und $-3\,872 = -219\,215/17$. So etwas gilt immer, wie man zeigen kann: $s_{\ell+1} = \pm b/g$, $t_{\ell+1} = \mp a/g$, wobei g der ggT von a und b ist. Sind a und b teilerfremd ist das besonders einfach zu sehen! Diese bedeutet dann nämlich $(b) \cdot a + (-a) \cdot b = 0$ oder $(-b) \cdot a + (a) \cdot b = 0$.

Also ist der ggT hier 17 und

$$17 = s_{10} \cdot a + t_{10} \cdot b = 14\,271 \cdot 219\,215 - 3\,872 \cdot 807\,959. \qquad \bigcirc$$

(ii) Zeige, dass für $0 \leq i \leq \ell + 1$ gilt: $r_i = s_i \cdot a + t_i \cdot b$.

Lösung. Wir zeigen das Geforderte durch Induktion:

Induktionsanfang:

Für $i = 0$ gilt $r_0 = a = 1 \cdot a + 0 \cdot b = s_0 \cdot a + t_0 \cdot b$.

Für $i = 1$ gilt $r_1 = b = 0 \cdot a + 1 \cdot b = s_1 \cdot a + t_1 \cdot b$.

Induktionsschritt $i - 1, i \to i + 1$, solange $i \leq \ell$:

$$\begin{aligned} r_{i+1} &= r_{i-1} - q_i r_i \\ &= s_{i-1}a + t_{i-1}b - q_i \left(s_i a + t_i b\right) \\ &= s_{i-1}a + t_{i-1}b - q_i s_i a - q_i t_i b \\ &= \left(s_{i-1} - q_i s_i\right) a + \left(t_{i-1} - q_i t_i\right) b \\ &= s_{i+1}a + t_{i+1}b. \end{aligned}$$

◯

(iii) Schließe, dass es ganze Zahlen $s, t \in \mathbb{Z}$ gibt mit $\text{ggT}(a, b) = s \cdot a + t \cdot b$.

Lösung. Da der Euklidische Algorithmus im Erweiterten Euklidischen Algorithmus enthalten ist, ist r_ℓ der ggT der eingegebenen Zahlen und das kann nach (ii) dargestellt werden als $r_\ell = s_\ell \cdot a + t_\ell \cdot b$. ◯

Aufgabe 6.4 (Mersenne-Zahlen). (4 Punkte)

Ziel dieser Aufgabe ist es folgenden Satz zu zeigen.

Satz. *Wenn die Mersenne-Zahl $2^k - 1$ prim ist, dann ist k prim.*

Dazu ist zu zeigen, dass für $a, b \in \mathbb{N}_{>1}$ die Zahl $2^{ab} - 1$ zusammengesetzt ist.

(i) Bestimme die Binärdarstellung von $2^k - 1$. (Mit Beweis!)

Lösung. Wir zeigen per Induktion $\forall k \in \mathbb{N}\ 2^k - 1 = (\underbrace{1 \ldots 1}_{k})_2$.

Induktionsanfang $k = 1$: $2^1 - 1 = 1 = (1)_2$.

Es ist auch möglich den Induktionsanfang für $k = 0$ zu machen: $2^0 - 1 = 0 = ()_2$. Dass die leere 2-adische Darstellung gleich 0 ist, scheint auf den ersten Blick zwar etwas komisch, passt aber in den Rahmen; denkt an ein entsprechendes Programm.

Induktionsschritt $k \to k+1$:

$$\begin{aligned} 2^{k+1} - 1 &= 2^{k+1} - 2 + 1 \\ &= 2 \cdot \left(2^k - 1\right) + 1 \\ &\overset{\text{IV}}{=} (10)_2 \cdot (\underbrace{1 \ldots 1}_{k}) + (1)_2 \\ &= (\underbrace{1 \ldots 1}_{k} 0) + (1)_2 \\ &= (\underbrace{1 \ldots 1}_{k+1}). \end{aligned}$$ ◯

(ii) Bestimme die Binärdarstellung von $(2^7 - 1)(2^{42} + 2^{14} + 1)$.

Lösung. Aus (i) kennen wir die Binärdarstellung von $2^7 - 1$ und die des andern Faktors besteht offensichtlich fast nur aus Nullen, außer an den Stellen 0, 14 und 42:

$$\begin{aligned} &(111\,1111)_2 \cdot (1 \underbrace{0 \ldots 0}_{27} 1 \underbrace{0 \ldots 0}_{13} 1)_2 \\ &= (\underbrace{1 \ldots 1}_{7} \underbrace{0 \ldots 0}_{21} \underbrace{1 \ldots 1}_{7} \underbrace{0 \ldots 0}_{7} \underbrace{1 \ldots 1}_{7})_2 \end{aligned}$$ ◯

(iii) Zerlege die Zahl

$$a := (111\,1100\,0001\,1111\,1111\,1000\,0011\,1111\,1111\,0000\,0000\,0000\,0001\,1111)_2$$

in Faktoren.

Lösung. Offensichtlich kommt der Faktor $(1\,1111)_2 = (31)_{10}$ häufig in dieser Zahl vor:

$$\begin{aligned} a =& (1\,1111)_2 \cdot \\ & (100\,0000\,0001\,0000\,1000\,0000\,0010\,0001\,0000\,0000\,0000\,0000\,0001)_2. \end{aligned}$$ ◯

Im Dezimalsystem durch Zweierpotenzen ausgedrückt, bedeutet das hier:

$$a = (2^5 - 2^0) \cdot (2^{50} + 2^{40} + 2^{35} + 2^{25} + 2^{20} + 2^0).$$

(iv) Bestimme die 2^5-adische Darstellung von $2^{35} - 1$. [Man könnte die Ziffern wiederum 2-adisch darstellen.]

Lösung. Die 2^5-adische Darstellung von $2^{35} - 1$ ist

$$(31, 31, 31, 31, 31, 31, 31)_{2^5}$$

oder

$$((1\,1111)_2, (1\,1111)_2, (1\,1111)_2, (1\,1111)_2, (1\,1111)_2, (1\,1111)_2, (1\,1111)_2)_{2^5}.$$

Die Länge dieser Darstellung ist 7. $31 = 2^5 - 1$ kann man nach (i) binär darstellen als $(1\,1111)_2$. Die Länge hier ist 5. ◯

(v) Schreibe $2^{35} - 1$ als echtes Produkt.

Lösung. Nach (iv) wissen wir, daß 31 ein Faktor dieser Zahl ist:

$$2^{35} - 1 = (1\,1111)_2 \cdot (100\,0010\,0001\,0000\,1000\,0100\,0010\,0001)_2.$$

Die dezimale Faktorisierung ist dann $2^{35} - 1 = 31 \cdot 1\,127\,033\,812\,811\,777$. Der zweite Faktor läßt sich natürlich noch weiter zerlegen, aber die Zerlegung ist aus der Binärdarstellung nicht ersichtlich. ◯

(vi) Bestimme die 2^a-adische Darstellung von $2^{ab} - 1$.

Lösung. Die Darstellung ist von der Form $(\underbrace{2^a - 1, \ldots, 2^a - 1}_{b})_{2^a}$ wie folgende Rechnung zeigt:

$$\begin{aligned}
(\underbrace{2^a - 1, \ldots, 2^a - 1}_{b})_{2^a} &= \sum_{i=0}^{b-1} (2^a - 1) \cdot (2^a)^i \\
&= (2^a - 1) \cdot \sum_{i=0}^{b-1} (2^a)^i \\
\text{(Mit geometrischer Summe)} &= (2^a - 1) \cdot \frac{(2^a)^{(b-1)+1} - 1}{2^a - 1} \\
&= (2^a - 1) \cdot \frac{2^{ab} - 1}{2^a - 1} \\
&= 2^{ab} - 1.
\end{aligned}$$

◯

(vii) Schreibe $2^{ab} - 1$ als echtes Produkt. Beweise den Satz.

Lösung. Nach (vi) gilt $2^{ab} - 1 = (2^a - 1) \cdot \sum_{i=0}^{b-1} (2^a)^i$. Wir bemerken, dass hier keiner der beiden Faktoren gleich 1 ist.

Beweis (Satz). Nach Voraussetzung ist $2^k - 1$ prim. Wenn wir annehmen, dass k nicht prim ist, dann gibt es Zahlen $a, b \in \mathbb{N}_{>1}$ mit $k = ab$. Aber dann ist ja $2^k - 1 = 2^{ab} - 1$ zusammengesetzt, wie wir gerade gesehen haben, im Widerspruch zur Voraussetzung. Also ist unsere Annahme, dass k nicht prim sei, falsch und der Satz bewiesen. □

◯

Aufgabe 6.5 (Induktion). (3 Punkte)

Sei φ eine Formel mit einem Parameter. Beweise:

$$\forall n \in \mathbb{N} \Big(\big(\forall i \in \mathbb{N}_{<n}\ \varphi(i)\big) \ \Rightarrow\ \varphi(n) \Big) \implies \forall n \in \mathbb{N}\ \varphi(n).$$

In Worten: Wenn für jedes $n \in \mathbb{N}$ aus der Gültigkeit der Formel φ für alle $i \in \mathbb{N}$ mit $i < n$ auf die Gültigkeit von φ für n geschlossen werden kann, dann gilt φ für alle natürlichen Zahlen.

Tipps: Was bedeutet die Voraussetzung für $n = 0$? Betrachte versuchsweise einige weitere kleine n. Bezeichne mit $\psi(n)$ die Aussage $\forall i \in \mathbb{N}_{<n}\ \varphi(i)$ und betrachte diese.

Bemerkung: Das ist eine abgewandelte Form der vollständigen Induktion. Hier kann man alle vorher erreichten Zwischenergebnisse im Induktionsschritt nutzen und braucht verblüffenderweise keinen separaten Induktionsanfang.

Lösung. Wir nehmen an, dass $\forall n \in \mathbb{N}\ \big(\forall i < n\ \varphi(i)\big) \Rightarrow \varphi(n)$ gilt, und zeigen per Induktion: $\forall n \in \mathbb{N}\ \psi(n)$.

Induktionsanfang $n = 0$: Zu zeigen ist $\psi(0) \equiv w$. Das stimmt, weil der Allquantor in ψ über eine leere Menge quantifiziert. Fertig.

Fall $n = 1$ als vertrauenschaffende Maßnahme: Zu zeigen ist $\psi(1) \equiv \varphi(0)$. Wenn wir die Annahme für $n = 0$ lesen, haben wir:

$$(\forall i < 0 : \varphi(i)) \Rightarrow \varphi(0).$$

Da links über nichts quantifiziert wird, ist dies wahr und also gilt $\varphi(0)$. Damit ist auch der Fall $n = 1$ bewiesen.

Induktionsschritt $n \to n + 1$: Wir wissen nach Induktionsvoraussetzung, dass $\psi(n) \equiv \varphi(0) \wedge \ldots \wedge \varphi(n-1)$ gilt. Zu zeigen ist $\psi(n+1) \equiv \varphi(0) \wedge \ldots \wedge \varphi(n-1) \wedge \varphi(n)$. Die Annahme für n gelesen bedeutet $\psi(n) \Rightarrow \varphi(n)$. Also haben wir $\varphi(n)$ und zusammen mit $\psi(n)$ ist das ja schon $\psi(n+1) \equiv \varphi(0) \wedge \ldots \wedge \varphi(n-1) \wedge \varphi(n)$. Damit ist der Induktionsschritt auch erledigt.

Wir haben also

$$\forall n \in \mathbb{N}\ \psi(n),$$

woraus sich wegen $\psi(n+1) \Rightarrow \varphi(n)$ sofort die Behauptung $\forall n \in \mathbb{N}\ \varphi(n)$ ergibt. ◯

Aufgabe 6.6 (Erweiterter Euklidischer Algorithmus). (3 Punkte)

Berechne den ggT g von a und b und eine Darstellung der Form $g = sa + tb$.

- $a = 3\,795$ und $b = 2\,574$.

  Lösung.

i	r_i	q_i	s_i	t_i	Kommentar	
0	3 795	–	1	0		
1	2 574	1	0	1		
2	1 221	2	1	−1	3 795	$= 1 \cdot 2\,574 + 1\,221$
3	132	9	−2	3	2 574	$= 2 \cdot 1\,221 + 132$
4	**33**	4	**19**	**−28**	1 221	$= 9 \cdot 132 + 33$
5	0	–	−78	115	132	$= 4 \cdot 33 + 0$

  Probe: $-78 \cdot 3795 + 115 \cdot 2574 = 0$.

  Also $g = 33$, $s = 19$ und $t = -28$, somit $33 = 19 \cdot 3795 - 28 \cdot 2574$. ◯

- $a = 5\,978$ und $b = 6\,699$.

  Lösung.

i	r_i	q_i	s_i	t_i	Kommentar	
0	5 978	–	1	0		
1	6 699	0	0	1		
2	5 978	1	1	0	5 978	$= 0 \cdot 6\,699 + 5\,978$
3	721	8	−1	1	6 699	$= 1 \cdot 5\,978 + 721$
4	210	3	9	−8	5 978	$= 8 \cdot 721 + 210$
5	91	2	−28	25	721	$= 3 \cdot 210 + 91$
6	28	3	65	−58	210	$= 2 \cdot 91 + 28$
7	**7**	4	**−223**	**199**	91	$= 3 \cdot 28 + 7$
8	0	–	957	−854	28	$= 4 \cdot 7 + 0$

  Probe: $957 \cdot 5978 - 854 \cdot 6699 = 0$.

  Also $g = 7$, $s = -223$ und $t = 199$, somit $7 = -223 \cdot 5978 + 199 \cdot 6699$. ◯

- $a = 610$ und $b = 377$.

Lösung.

i	r_i	q_i	s_i	t_i	Kommentar
0	610	–	1	0	
1	377	1	0	1	
2	233	1	1	−1	$610 = 1 \cdot 377 + 233$
3	144	1	−1	2	$377 = 1 \cdot 233 + 144$
4	89	1	2	−3	$233 = 1 \cdot 144 + 89$
5	55	1	−3	5	$144 = 1 \cdot 89 + 55$
6	34	1	5	−8	$89 = 1 \cdot 55 + 34$
7	21	1	−8	13	$55 = 1 \cdot 34 + 21$
8	13	1	13	−21	$34 = 1 \cdot 21 + 13$
9	8	1	−21	34	$21 = 1 \cdot 13 + 8$
10	5	1	34	−55	$13 = 1 \cdot 8 + 5$
11	3	1	−55	89	$8 = 1 \cdot 5 + 3$
12	2	1	89	−144	$5 = 1 \cdot 3 + 2$
13	**1**	2	**−144**	**233**	$3 = 1 \cdot 2 + 1$
14	0	–	377	−610	$2 = 2 \cdot 1 + 0$

Probe: $377 \cdot 610 - 610 \cdot 377 = 0$.

Also $g = 1$, $s = -144$ und $t = 233$, somit $1 = -144 \cdot 610 + 233 \cdot 377$. ◯