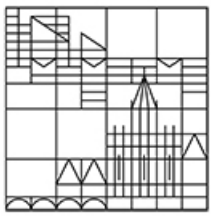
Fachbereich Informatik und
Informationswissenschaft

Universität
Konstanz



Skriptum

zum Brückenkurs

Mathematik

gehalten im Wintersemester 2008/09, 2009/10, 2010/11, 2011/12, 2012/13 und im Sommersemester 2011, 2012, 2013

von

Sven Kosub

12. April 2013

Version v4.4

Inhaltsverzeichnis

Arithmetik 1

1.1 Zahlenbereiche

Natürliche Zahlen. $\mathbb{N}$ ist die Menge der *natürlichen* Zahlen: $0, 1, 2, 3, \ldots$

Die natürliche Zahl a ist eine Abkürzung für $\underbrace{1+1+\cdots+1}_{a-\text{mal}}$; a^n ist eine Abkürzung für $\underbrace{a \cdot a \cdot \ldots \cdot a}_{a-\text{mal}}$.

0 ist eine natürliche Zahl. (In der Mathematik wird sehr häufig 0 nicht als natürliche Zahl aufgefasst; wenn 0 zu den natürlichen Zahlen gezählt werden soll, wird $\mathbb{N}_0$ verwendet.) Wird 0 als natürliche Zahl ausgeschlossen, so schreiben $\mathbb{N}_+$. (In der Mathematik wird dann $\mathbb{N}$ verwendet.)

Rechenregeln: Es seien k, n, m natürliche Zahlen.

1. $\left.\begin{aligned}(k+n)+m &= k+(n+m)\\ (k\cdot n)\cdot m &= k\cdot(n\cdot m)\end{aligned}\right\}$ Assoziativgesetze
2. $k\cdot(n+m) = k\cdot n + k\cdot m$ Distributivgesetz
3. $\left.\begin{aligned}n+m &= m+n\\ n\cdot m &= m\cdot n\end{aligned}\right\}$ Kommutativgesetze
4. $\left.\begin{aligned}n+0 &= n\\ n\cdot 1 &= n\end{aligned}\right\}$ neutrale Elemente
5. $n\cdot 0 = 0$

Ganze Zahlen. $\mathbb{Z}$ ist die Menge der *ganzen* Zahlen: $\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$

Die ganzen Zahlen ermöglichen es, alle Subtraktionen stets auch ausführen zu können, wie z.B. $3-5=-2$. Die Zahl $-a$ (mit der natürlichen Zahl a) ist dabei eine Abkürzung für $\underbrace{(-1)+(-1)+\ldots+(-1)}_{a-\text{mal}} = a\cdot(-1)$.

Rechenregeln:

1.-5. übertragen sich von $\mathbb{N}$

6. Für ganze Zahl n gilt $n + (-n) = 0$ inverses Element

Beispiel: Wieso ist die Regel $(-1) \cdot (-1) = 1$ plausibel?

Mit Hilfe der Rechenregeln erhalten wir:

$$\begin{aligned} 0 &= (-1) \cdot 0 && \text{(5. Regel)} \\ &= (-1) \cdot (1 + (-1)) && \text{(6. Regel, inverses Element zu 1 für } +) \\ &= (-1) \cdot 1 + (-1) \cdot (-1) && \text{(2. Regel, Distributivgesetz)} \\ &= -1 + (-1) \cdot (-1) && \text{(4. Regel, neutrales Element 1 für } \cdot) \end{aligned}$$

Somit folgt weiter:

$$\begin{aligned} 1 &= 1 + 0 && \text{(4. Regel, neutrales Element 0 für } +) \\ &= 1 + (-1) + (-1) \cdot (-1) && \text{(siehe oben)} \\ &= 0 + (-1) \cdot (-1) && \text{(6. Regel, inverses Element zu 1 für } +) \\ &= (-1) \cdot (-1) && \text{(4. Regel, neutrales Element 0 für } +) \end{aligned}$$

Rationale Zahlen. $\mathbb{Q}$ ist die Menge der rationalen Zahlen, d.h. die Menge der Brüche $\frac{p}{q}$ mit $q \neq 0$ sowie p, q ganze Zahlen.

Die rationalen Zahlen ermögliches es, jede lineare Gleichung $q \cdot x - p = 0$ stets zu lösen. Zur Definition der rationalen Zahlen genügt es auch zu fordern:

- p ist ganze Zahl und q ist natürliche Zahl, $q \neq 0$
- p ist natürliche Zahl und q ist ganze Zahl, $q \neq 0$

Dezimalschreibweise:

- $\frac{1}{2} = 0,5$ (Periodenlänge 0)
- $\frac{1}{3} = 0,333\ldots = 0,\overline{3}$ (Periodenlänge 1)
- $\frac{1}{7} = 0,\overline{142857}$ (Periodenlänge 6)
- $\frac{1}{30} = 0,0\overline{3}$ (schließlich periodisch)

Beachte: Die Dezimalschreibweise ist nicht eindeutig. Zum Beispiel gilt $1 = 0,\overline{9}$, denn

$$\begin{aligned} x &= 0,\overline{9} \\ 10x &= 9,\overline{9} \end{aligned}$$

Dann gilt $9x = 10x - x = 9,\overline{9} - 0,\overline{9} = 9$, d.h. $x = 1$.

Rechenregeln:

1.-6. übertragen sich von $\mathbb{Z}$

7. Für $p \neq 0, q \neq 0$ gilt $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = 1$. inverses Element

Als Schreibweise verwenden wir: $\left(\frac{p}{q}\right)^{-1} = \frac{1}{\frac{p}{q}} =_{\text{def}} \frac{q}{p}$.

Reelle Zahlen. $\mathbb{R}$ ist die Menge aller *reellen* Zahlen, d.h., die Menge der endlichen und unendlichen Dezimalzahlen.

Beispiele:

- Jede rationale Zahl ist reell; r ist rational genau dann, wenn r eine schließlich periodische Darstellung besitzt.
- $\pi = 3,141592\ldots$ ist irrational und transzendent.
- $e = 2,7182818\ldots$ ist irrational und transzendent.
- $\sqrt{2} = 1,41421356\ldots$ ist irrational aber algebraisch.
- Irrationalität von $\pi + e$ ist offen.

Rechenregeln:

1.-7. übertragen sich von $\mathbb{Q}$ (mit $r \cdot \frac{1}{r} = 1$ für $r \neq 0$ bei der 7. Regel)

Komplexe Zahlen. $\mathbb{C}$ ist die Menge der komplexen Zahlen, d.h., die Mengen der Zahlenpaare (a, b), wobei a und b reelle Zahlen sind, mit den folgenden Operationen:

1. Addition of $\mathbb{C}$: $(a, b) + (c, d) =_{\text{def}} (a + c, b + d)$
2. Multiplikation auf $\mathbb{C}$: $(a, b) \cdot (c, d) =_{\text{def}} (ac - bd, ad + bc)$

Eine alternative und die übliche Schreibweise für komplexe Zahlen ist mit $i =_{\text{def}} (0, 1)$:

$$(a, b) = a + b \cdot i$$

Hierbei steht i für die *imaginäre Einheit*: $i = \sqrt{-1}$. Damit gilt

$$i^1 = i, \quad i^2 = -1, \quad i^3 = -i \quad \text{sowie} \quad i^4 = 1$$

Ist $z = a + b \cdot i$, so sind $\text{Re}(z)$ der *Realteil* von z und $\text{Im}(z)$ der *Imaginärteil* von z. Eine komplexe Zahl z heißt reell, falls $\text{Im}(z) = 0$ gilt; z heißt *imaginär*, falls $\text{Re}(z) = 0$.

Rechenregeln:

1.-7. übertragen sich von $\mathbb{R}$

1.2 Primzahlen

Es seien n und m ganze Zahlen. Dann *teilt* m die Zahl n (symbolisch $m|n$), falls es eine ganze Zahl k gibt mit

$$n = k \cdot m.$$

Bei dieser Definition ist zu beachten, dass jede Zahl 0 teilt.

Eine Zahl n heißt *Primzahl*, falls 1 und n die einzigen natürlichen Zahlen sind, die n teilen.

Die ersten Primzahlen sind somit: $1, 2, 3, 5, 7, 11, 13, 17, \ldots$, wobei 1 üblicherweise nicht zu den Primzahlen gezählt wird.

Theorem 1.1 (Primzahlzerlegung) *Es sei n ein natürliche Zahl $n \geq 2$. Dann gibt es eindeutig bestimmte Primzahlen $2 \leq p_1 < p_2 < \ldots < p_k$ und positive natürliche Zahlen $a_1, a_2, \ldots, a_k$ mit*

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}.$$

Bevor wir das Theorem beweisen, wollen wir es an einigen Beispiel verdeutlichen.

Beispiele: Die folgenden Zahlenbeispiele illustrieren das Konzept der Primzahlzerlegung.

- $24 = 2 \cdot 12 = 2 \cdot 2 \cdot 6 = 2 \cdot 2 \cdot 2 \cdot 3 = 2^3 \cdot 3^1$
- $111 = 3^1 \cdot 37^1$
- $113 = 113^1$
- $36 = 6^2 = 2 \cdot 3 \cdot 2 \cdot 3 = 2^2 \cdot 3^2$

Beweis: Wir beweisen die Aussage in zwei Schritten:

- *Existenz*: Es sei $n \geq 2$ eine natürliche Zahl. Dann gibt es zwei Fälle:
  - Ist n eine Primzahl, dann sind wir fertig.
  - Ist n keine Primzahl, dann gibt es natürliche Zahlen $n_1, n_2 \geq 2$ mit $n = n_1 \cdot n_2$. Für n_1 und n_2 können wir nun wieder die gleichen Überlegungen anstellen, d.h., sind $n_1 = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}$ sowie $n_2 = q_1^{b_1} \cdot q_2^{b_2} \cdot \ldots \cdot q_m^{a_k}$ Primzahlzerlegungen, so gilt
    $$n = n_1 \cdot n_2 = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k} \cdot q_1^{b_1} \cdot q_2^{b_2} \cdot \ldots \cdot q_m^{a_k}.$$
    Durch Zusammenfassen gleicher Faktoren erhalten wir die gewünschte Zerlegung. Das stets $n > n_1, n_2$ gilt, bricht das Verfahren nach endlich vielen Schritten ab.

Somit existiert eine Primzahlzerlegung stets.

- *Eindeutigkeit*: Es seien für $n \geq 2$ zwei Zerlegungen gegeben:

$$n = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k} = q_1^{b_1} \cdot \ldots \cdot q_m^{b_m}$$

Wir betrachten die kleinste als Faktor vorkommende Primzahl. Ohne Beeinträchtigung der Allgemeinheit sei dies p_1. Dann teilt p_1 sowohl die linke als auch die rechte Zerlegung. Somit gibt es ein j mit $p_1 | q_j$. Da q_j eine Primzahl ist, gilt $p_1 = q_j$. Dividieren wir also beide Prinzahlzerlegungen durch p_1, so erhalten wir zwei Primzahlzerlegungen mit einem Faktor weniger. Diese Argumentation können wir wiederholen, bis auf einer Seite keine Faktoren mehr übrig sind. Dann sind aber auch auf der anderen Seite keine Faktoren übrig. Somit kommen alle Faktoren auf der linken Seite als Faktoren auf der rechten Seite vor und auch umgekehrt.

Damit ist das Theorem bewiesen. ■

1.3 Divisionsreste

Es seien n eine ganze Zahl, m eine natürliche Zahl, $m \geq 2$. Dann *teilt* m die Zahl n *mit Rest* r, $0 \leq r \leq m-1$, falls eine ganze Zahl k existiert mit

$$n = k \cdot m + r.$$

Die in der Definition vorkommende Zahl k ist eindeutig, denn aus $k \cdot m + r = k' \cdot m + r$ folgt $(k - k') \cdot m = 0$, also $k = k'$.

Damit definieren wir die *Modulo-Funktion* für n und m:

$$\mathrm{mod}(n, m) = r \quad \Longleftrightarrow_{\mathrm{def}} \quad m \text{ teilt } n \text{ mit Rest } r$$

Beispiele: Wir bestimmen die Werte der Modulo-Funktion für verschiedene Argumente:

- $\mathrm{mod}(7, 3) = 1$, denn $7 = 2 \cdot 3 + 1$
- $\mathrm{mod}(-7, 3) = 2$, denn $-7 = (-3) \cdot 3 + 2$
- $\mathrm{mod}(9, 3) = 0$, denn $9 = 3 \cdot 3$
- $\mathrm{mod}(-9, 3) = 0$, denn $-9 = (-3) \cdot 3$

Das folgende Theorem, das wir ohne Beweis angeben, fasst wichtige Rechenregeln für Divisionsreste zusammen.

Theorem 1.2 *Es seien k, n und m ganze Zahlen, $m \geq 2$.*

1. $\mathrm{mod}(k + n, m) = \mathrm{mod}(\mathrm{mod}(k, m) + \mathrm{mod}(n, m), m)$.
2. $\mathrm{mod}(k \cdot n, m) = \mathrm{mod}(\mathrm{mod}(k, m) \cdot \mathrm{mod}(n, m), m)$.
3. $\mathrm{mod}(n^k, m) = \mathrm{mod}(\mathrm{mod}(n, m)^k, m)$, *falls* $k > 0$.

Beispiele: Die ersten drei Beispiele veranschaulichen die Korrektheit der drei Rechenregeln aus Theorem 1.2:

$$\begin{aligned}
\mathrm{mod}(5 \cdot 7, 4) &= \mathrm{mod}(\mathrm{mod}(5,4) \cdot \mathrm{mod}(7,4), 4) \\
&= \mathrm{mod}(1 \cdot 3, 4) \\
&= 3 \\
&= \mathrm{mod}(35, 4)
\end{aligned}$$

$$\begin{aligned}
\mathrm{mod}(5 + 7, 4) &= \mathrm{mod}(\mathrm{mod}(5,4) + \mathrm{mod}(7,4), 4) \\
&= \mathrm{mod}(1 + 3, 4) \\
&= 0 \\
&= \mathrm{mod}(12, 4)
\end{aligned}$$

$$\begin{aligned}
\mathrm{mod}(5^7, 4) &= \mathrm{mod}(\mathrm{mod}(5,4)^7, 4) \\
&= \mathrm{mod}(1^7, 4) \\
&= 1 \\
&= \mathrm{mod}(78125, 4)
\end{aligned}$$

Die Rechenregeln können verwendet werden, um Divisionsreste komplexer Ausdrücke zu bestimmen, ohne diese explizit auszurechnen:

$$\begin{aligned}
&\mathrm{mod}\left(13^{73} \cdot 17^{25} + (-2)^{113}, 4\right) \\
&\quad = \mathrm{mod}\left(\mathrm{mod}(13,4)^{73} \cdot \mathrm{mod}(17,4)^{25} + \mathrm{mod}((-2)^2, 4)^{56} \cdot \mathrm{mod}(-2,4), 4\right) \\
&\quad = \mathrm{mod}\left(1^{73} \cdot 1^{25} + 0, 4\right) \\
&\quad = 1
\end{aligned}$$

Wie finden wir die in der Definition der Teilbarkeit von n durch m mit Rest r angegebene Zahl k, so dass $n = k \cdot m + r$ gilt? Dafür verwenden wir Rundungsregeln, die durch Gauss-Klammern ausgedrückt werden. Für eine beliebige reelle Zahl x definieren wir:

$$\begin{aligned}
\lfloor x \rfloor &=_{\mathrm{def}} \text{ größte ganze Zahl } z \text{ mit } z \leq x \\
\lceil x \rceil &=_{\mathrm{def}} \text{ kleinste ganze Zahl } z \text{ mit } z \geq x
\end{aligned}$$

Die *untere* Gauss-Klammer $\lfloor x \rfloor$ bewirkt, dass die Zahl x auf die nächst kleinere ganze Zahl abgerundet wird; mit der *oberen* Klammer $\lceil x \rceil$ wird x zur nächst größeren ganzen Zahl aufgerundet.

Beispiele: Einige Zahlbeispiele verdeutlichen die Rundungsregeln:

$$\left\lfloor \frac{3}{2} \right\rfloor = 1, \quad \left\lceil \frac{3}{2} \right\rceil = 2, \quad \left\lfloor \frac{-3}{2} \right\rfloor = -2, \quad \left\lceil \frac{-3}{2} \right\rceil = -1$$

Mit Hilfe der Gauss-Klammern kann die Modulo-Funktion wie folgt dargestellt werden (ohne dass auf eine geeignetes k abgestellt werden muss):

$$a = \left\lfloor \frac{a}{m} \right\rfloor \cdot m + \mathrm{mod}(a, m)$$

für ganze Zahlen a und m mit $m \geq 2$. Dies ist leicht einzusehen: Für $r = \mathrm{mod}(a, m)$ gibt es ein k mit $a = k \cdot m + r$. Also gilt wegen $r < m$

$$\left\lfloor \frac{a}{m} \right\rfloor = \left\lfloor k + \frac{r}{m} \right\rfloor = k.$$

Proposition 1.3 *Für jede ganze Zahl n gilt* $\left\lfloor \frac{n}{2} \right\rfloor + \left\lceil \frac{n}{2} \right\rceil = n.$

Beweis: (*Fallunterscheidung*) Es sei n eine ganze Zahl.

- *1. Fall*: n ist gerade, d.h., es gilt $n = 2k$ für eine ganze Zahl k. Dann gilt

$$\left\lfloor \frac{n}{2} \right\rfloor + \left\lceil \frac{n}{2} \right\rceil = \left\lfloor \frac{2k}{2} \right\rfloor + \left\lceil \frac{2k}{2} \right\rceil = \lfloor k \rfloor + \lceil k \rceil = 2k = n.$$

- *2. Fall*: n ist ungerade, d.h., es gilt $n = 2 \cdot k + 1$ für eine ganze Zahl k. Dann gilt

$$\left\lfloor \frac{n}{2} \right\rfloor + \left\lceil \frac{n}{2} \right\rceil = \left\lfloor \frac{2k+1}{2} \right\rfloor + \left\lceil \frac{2k+1}{2} \right\rceil = \left\lfloor k + \frac{1}{2} \right\rfloor + \left\lceil k + \frac{1}{2} \right\rceil = k + (k+1) = 2k+1 = n.$$

Damit ist die Proposition bewiesen. ■

1.4 Euklidischer Algorithmus

Definition 1.4 *Es seien n und m positive natürliche Zahlen.*

1. *Das* kleinste gemeinsame Vielfache *von n und m, symbolisch* $\mathrm{kgV}(n, m)$*, ist die kleinste natürliche Zahl k, so dass n und m jeweils k teilen.*
2. *Der* größte gemeinsame Teiler *von n und m, symbolisch* $\mathrm{ggT}(n, m)$*, ist die größte natürliche Zahl k, so dass k jeweils n und m teilt.*

Beispiele:

1. $\mathrm{kgV}(3, 5) = 15$ und $\mathrm{ggT}(3, 5) = 1$.
2. $\mathrm{kgV}(3, 6) = 6$ und $\mathrm{ggT}(3, 6) = 3$.
3. $\mathrm{kgV}(4, 6) = 12$ und $\mathrm{ggT}(4, 6) = 2$.

Lemma 1.5 *Es seien n und m positive natürliche Zahlen mit Primfaktordarstellungen $n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ \cdots \ \cdot p_k^{a_k}$ und $m = p_1^{b_1} \cdot p_2^{b_2} \cdot \ \cdots \ \cdot p_k^{b_k}$, wobei $a_i = 0$ bzw. $b_i = 0$, falls n bzw. m nicht durch p_i teilbar ist. Es gelte weiterhin $b_k > 0$ oder $a_k > 0$. Dann gelten folgende Gleichungen:*

$$\begin{aligned} \mathrm{kgV}(n,m) &= p_1^{\max(a_1,b_1)} \cdot p_2^{\max(a_2,b_2)} \cdot \ \cdots \ \cdot p_k^{\max(a_k,b_k)} \\ \mathrm{ggT}(n,m) &= p_1^{\min(a_1,b_1)} \cdot p_2^{\min(a_2,b_2)} \cdot \ \cdots \ \cdot p_k^{\min(a_k,b_k)} \end{aligned}$$

Beweis: (*nur erste Gleichung*) Es seien n und m mit den Primfaktordarstellungen wie oben beschrieben gegeben. Es sei $x = p_1^{\max(a_1,b_1)} \cdot p_2^{\max(a_2,b_2)} \cdot \ \cdots \ \cdot p_k^{\max(a_k,b_k)}$. Dann teilen die Primfaktoren $p_i^{a_i}$ von n und $p_i^{b_i}$ von m jeweils $p_i^{\max(a_i,b_i)}$. Mithin teilen n und m die Zahl x. Jede weitere Zahl y, die von n und m geteilt wird, muss durch die Primfaktoren $p_i^{a_i}$ und $p_i^{b_i}$ teilbar sein, also auch durch $p_i^{\max(a_i,b_i)}$. Damit teilt x die Zahl y. Also gilt $x \leq y$. Folglich gilt $\mathrm{kgV}(n,m) = x$. ∎

Beispiele: Mit den Primzahlzerlegungen $24 = 2^3 \cdot 3^1$ und $36 = 2^2 \cdot 3^2$ gilt

$$\mathrm{kgV}(24,36) = 2^3 \cdot 3^2 = 72 \text{ sowie } \mathrm{ggT}(24,36) = 2^2 \cdot 3^1 = 12.$$

Theorem 1.6 *Es seien n und m positive natürliche Zahlen. Dann gilt:*

$$n \cdot m = \mathrm{kgV}(n,m) \cdot \mathrm{ggT}(n,m)$$

Beweis: Es seien $n = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$ und $m = p_1^{b_1} \cdot \ldots \cdot p_k^{b_k}$ Primfaktorzerlegungen wie in Lemma 1.5 beschrieben. Nach Lemma 1.5 folgt:

$$\begin{aligned} \mathrm{kgV}(n,m) \cdot \mathrm{ggT}(n,m) &= p_1^{\max(a_1,b_1)} \cdot \ldots \cdot p_k^{\max(a_k,b_k)} \cdot p_1^{\min(a_1,b_1)} \cdot \ldots \cdot p_k^{\min(a_k,b_k)} \\ &= p_1^{\max(a_1,b_1)+\min(a_1,b_1)} \cdot \ldots \cdot p_k^{\max(a_k,b_k)+\min(a_k,b_k)} \\ &= p_1^{a_1+b_1} \cdot \ldots \cdot p_k^{a_k+b_k} \\ &= p_1^{a_1} \cdot \ldots \cdot p_k^{a_k} \cdot p_1^{b_1} \cdot \ldots \cdot p_k^{b_k} \\ &= n \cdot m \end{aligned}$$

Damit ist das Theorem bewiesen. ∎

Korollar 1.7 *Es seien n und m natürliche Zahlen. Dann gilt*

$$\mathrm{kgV}(n,m) = \frac{n \cdot m}{\mathrm{ggT}(n,m)} \quad \textit{bzw.} \quad \mathrm{ggT}(n,m) = \frac{n \cdot m}{\mathrm{kgV}(n,m)}.$$

Algorithmus: EUKLID
Eingabe: positive natürliche Zahlen n, m mit $m \leq n$
Ausgabe: $\mathrm{ggT}(m, n)$

```
1.  IF m teilt n
2.      RETURN m
3.  ELSE
4.      RETURN EUKLID(mod(n, m), m)
```

Abbildung 1.1: Algorithmus von EUKLID

Wie bestimmen wir $\mathrm{ggT}(n, m)$? Sind die Primfaktorzerlegungen von n und m bekannt, so gibt uns Lemma 1.5 eine einfache Möglichkeit dafür an die Hand. Allerdings ist die Bestimmung von Primfaktorzerlegungen algorithmisch nicht einfach. Einen eleganten Ausweg, der ohne die Primfaktorzerlegung auskommt, ist der Algorithmus von EUKLID (siehe Abbildung 1.1). Dieser ist eine direkte Umsetzung der rekursiven Anwendung der folgenden Resultate.

Lemma 1.8 *Sind m, n positive natürliche Zahlen mit $m \leq n$ und m teilt nicht n, so gilt*

$$\mathrm{ggT}(m, n) = \mathrm{ggT}(n - m, m).$$

Beweis: Wir müssen zeigen: Jeder Teiler von m und n ist auch ein Teiler von $n - m$ und m und umgekehrt. Zunächst sei d ein Teiler von n und m, d.h., $d|n$ und $d|m$. Es gilt $n = k \cdot d$ und $m = k' \cdot d$ für geeignete k, k'. Somit gilt $n - m = k \cdot d - k' \cdot d = (k - k') \cdot d$ und mithin $d|n - m$. Es sein nun d ein Teiler von $n - m$ und m, d.h., $d|n - m$ und $d|m$. Es gilt wieder $n - m = k \cdot d$ und $m = k' \cdot d$ für geeignete k, k'. Somit erhalten wir $n = n - m + m = k \cdot d + k' \cdot d = (k + k') \cdot d$ und mithin $d|n$. ■

Korollar 1.9 *Sind m und n positive natürliche Zahlen mit $m \leq n$ und m teilt nicht n, so gilt*

$$\mathrm{ggT}(m, n) = \mathrm{ggT}(\mathrm{mod}(n, m), m).$$

Beweis: Es sei $n = k \cdot m + \mathrm{mod}(n, m)$ für geeignetes $k \geq 0$. Durch wiederholte Anwendung von Lemma 1.8 erhalten wir

$$\begin{aligned} \mathrm{ggT}(m, n) &= \mathrm{ggT}(m, n - m) = \mathrm{ggT}(m, n - 2m) = \mathrm{ggT}(m, n - k \cdot m) \\ &= \mathrm{ggT}(m, n\mathrm{mod}(n, m)) \end{aligned}$$

Damit ist das Korollar bewiesen. ■

Beispiele: Wir wollen die Anwendungen des Euklidischen Algorithmus an zwei Beispielen verdeutlichen, die auch einen Eindruck davon geben, wie unterschiedlich die Anzahlen der rekursiven Aufrufe sein können.

$$\begin{aligned} \textsc{Euklid}(36, 120) &= \textsc{Euklid}(12, 36) \\ &= 12 \end{aligned}$$

Die jeweiligen Primfaktorzerlegungen sind $36 = 2^2 \cdot 3^2$ sowie $120 = 2^3 \cdot 3^1 \cdot 5^1$. Gemäß Lemma 1.5 gilt $\mathrm{ggT}(36, 120) = 2^2 \cdot 3^1 \cdot 5^0 = 12$.

$$\begin{aligned} \textsc{Euklid}(89, 144) &= \textsc{Euklid}(55, 89) \\ &= \textsc{Euklid}(34, 55) \\ &= \textsc{Euklid}(21, 34) \\ &= \textsc{Euklid}(13, 21) \\ &= \textsc{Euklid}(8, 13) \\ &= \textsc{Euklid}(5, 8) \\ &= \textsc{Euklid}(3, 5) \\ &= \textsc{Euklid}(2, 3) \\ &= \textsc{Euklid}(1, 2) \\ &= 1 \end{aligned}$$

Die beiden Zahlen 89 und 144 sind benachbarte Fibonacci-Zahlen, die für den Algorithmus von Euklid schlechteste Eingaben bezüglich der Rekursionsanzahl darstellen.

Polynome 2

2.1 Definitionen

Ein *univariates Polynom* p ist eine Funktion der Form

$$p(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \cdots + a_1 \cdot x + a_0,$$

wobei n eine natürliche Zahl und $a_0, a_1, \ldots, a_n$ die *Koeffizienten* des Polynoms sind.

Sind die Koeffzienten reelle Zahlen, so heißt p *reelles* Polynom; sind die Koeffizienten komplex, so heißt p *komplexes* Polynom.

Ein Term x^n heißt *Monom*.

Der Grad eines Polynoms $p(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \cdots + a_1 \cdot x + a_0$ ist die größte Zahl m mit $a_m \neq 0$.

Beispiele:

- $x^2 - x + 1$ ist ein Polynom vom Grad 2.
- Die (quasi-)lineare Funktion $a \cdot x + b$ mit $a \neq 0$ ist ein Polynom vom Grad 1.
- Konstante Funktionen $f(x) = c$ sind Polynome vom Grad 0.

2.2 HORNER-Schema

Um den Wert eines Polynoms p an einer Stelle x_0 auszurechnen, sollte man wie folgt vorgehen:

$$\begin{aligned}
p(x) &= a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + a_{n-2} \cdot x^{n-2} + \cdots + a_2 \cdot x^2 + a_1 \cdot x + a_0 \\
&= (a_n \cdot x^{n-1} + a_{n-1} \cdot x^{n-2} + a_{n-2} \cdot x^{n-3} + \cdots + a_2 \cdot x + a_1) \cdot x + a_0 \\
&= ((a_n \cdot x^{n-2} + a_{n-1} \cdot x^{n-3} + a_{n-2} \cdot x^{n-4} + \cdots + a_2) \cdot x + a_1) \cdot x + a_0 \\
&\vdots \\
&= ((\ldots((a_n \cdot x + a_{n-1}) \cdot x + a_{n-2}) \cdot x + \cdots) \cdot x + a_1) \cdot x + a_0
\end{aligned}$$

In dieser gewonnen Darstellung wird das Polynom nun an der Stelle x_0 von innen nach außen sukzessive ausgewertet.

Beispiel: Wir wollen den Wert von $p(x) =_{\text{def}} x^4 + 3x^3 - 2x^2 + 11x - 1 = (((x+3)x-2)x+11)x-1$ an der Stelle $x_0 = 3$ bestimmen. Die Auswertung kann durch folgendes Schema von HORNER veranschaulicht werden:

	a_5	a_4	a_3	a_2	a_1	a_0
p	–	1	3	-2	11	-1
	–	0	3	18	48	177
$p(3)$	0	1	6	16	59	**176**

Wenn die Koeffizienten in einem Feld (Array) `A[0..n]` (mit `A[i]`$=a_i$) gespeichert sind, so wird der Funktionswert $p(x_0)$ wie folgt berechnet:

```
p=A[n];
for (int i=n-1; i>=0; i--) p=p*x0+A[i]
```

Mit dem HORNER-Schema sind somit nur n Multiplikationen notwendig. Im Vergleich benötigt die Standardauswertung gemäß der Polynomdefinition insgesamt

$$\sum_{i=1}^{n} i = \frac{n(n-1)}{2} = \frac{1}{2}n^2 - \frac{1}{2}n = O(n^2)$$

Multiplikationen.

2.3 Rechnen mit Polynomen

Addition. Es seien zwei Polynome $a(x) =_{\text{def}} a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \cdots + a_1 \cdot x + a_0$ und $b(x) =_{\text{def}} b_n \cdot x^n + b_{n-1} \cdot x^{n-1} + \cdots + b_1 \cdot x + b_0$ gegeben. Bei unterschiedlichem Grad der Polynome werden die fehlenden Koeffizienten auf 0 gesetzt. Die Summe von a und b ist definiert als

$$(a+b)(x) =_{\text{def}} c_n \cdot x^n + c_{n-1} \cdot x^{n-1} + \cdots + c_1 \cdot x + c_0,$$

wobei $c_i =_{\text{def}} a_i + b_i$.

Es gilt $\text{grad}(a+b) \leq \max(\text{grad}(a), \text{grad}(b))$.

Beispiel:

- Für $a(x) =_{\text{def}} x^4+2x^2-3x+7$ und $b(x) =_{\text{def}} -x^5+7x^3+4x^2+5x-4$ gilt $(a+b)(x) = -x^5+x^4+7x^3+6x^2+2x+3$ und $\text{grad}(a+b) = 5 = \text{grad}(b)$.
- Für $a(x) =_{\text{def}} x^4 + 1$ und $b(x) =_{\text{def}} -x^4 + 1$ gilt $(a+b)(x) = 2$ und $\text{grad}(a+b) = 0 < 4 = \max(\text{grad}(a), \text{grad}(b))$

Multiplikation. Es seien zwei Polynome $a(x) =_{\text{def}} a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \cdots + a_1 \cdot x + a_0$ und $b(x) =_{\text{def}} b_m \cdot x^m + b_{m-1} \cdot x^{m-1} + \cdots + b_1 \cdot x + b_0$ gegeben. Das Produkt von a und b ist definiert als

$$(a \cdot b)(x) =_{\text{def}} c_{n+m} \cdot x^{n+m} + \cdots + c_1 \cdot x + c_0,$$

wobei $c_i =_{\text{def}} \sum_{j=0}^{i} a_j \cdot b_{i-j}$ (mit $a_{n+1} = \cdots = a_{n+m} = b_{m+1} = \cdots = b_{n+m} = 0$).

Es gilt $\text{grad}(a + b) = \text{grad}(a) + \text{grad}(b)$.

Beispiel: Für $a(x) =_{\text{def}} x^2 - 3x + 5$ und $b(x) =_{\text{def}} 4x + 2$ ergibt sich

$$\begin{aligned}(a \cdot b)(x) &= (1 \cdot 4)x^3 + (1 \cdot 2 + (-3) \cdot 4)x^2 + ((-3) \cdot 2 + 5 \cdot 4)x + (5 \cdot 2) \\ &= 4x^3 - 10x^2 + 14x + 10\end{aligned}$$

Division. Die Division von zwei Polynomen ist analog zur Division ganzer Zahlen mit Rest definiert. Wir führen sie daher an Hand eines Beispiels vor.

Beispiel: Für $a(x) =_{\text{def}} 2x^4 + x^3 + x + 3$ und $b(x) =_{\text{def}} x^2 + x - 1$ berechne

$$\begin{array}{rrrrrrrrrrrrr}
2^4 & + & x^3 & & & + & x & + & 3 & : & x^2 + x - 1 & = & 2x^2 - x + 3 \\
-2x^4 & - & 2x^3 & + & 2x^2 & & & & & & & & \\
 & & -x^3 & + & 2x^2 & + & x & + & 3 & & & & \\
 & & x^3 & + & x^2 & - & x & & & & & & \\
 & & & & 3x^2 & & & + & 3 & & & & \\
 & & & & -3x^2 & - & 3x & + & 3 & & & & \\
 & & & & & & -3x & + & 6 & & & &
\end{array}$$

Damit gilt

$$\underbrace{2x^4 + x^3 + x + 3}_{a(x)} = \underbrace{(2x^2 - x + 3)}_{t(x)} \cdot \underbrace{(x^2 + x + 1)}_{b(x)} + \underbrace{(-3x + 6)}_{r(x)}$$

mit $\text{grad}(r) < \text{grad}(b)$.

Theorem 2.1 *Für Polynome $a(x)$ und $b(x)$ mit $b \neq 0$ gibt es eindeutig bestimmte Polynome $t(x)$ und $r(x)$ mit $a(x) = t(x) \cdot b(x) + r(x)$ und $r = 0$ oder $\text{grad}(r) < \text{grad}(b)$.*

2.4 Binomische Formeln

Es gelten die folgenden binomischen Formeln:

$$\begin{aligned}(x + y)^2 &= x^2 + 2xy + y^2 \\ (x - y)^2 &= x^2 - 2xy + y^2 \\ (x + y) \cdot (x - y) &= x^2 - y^2\end{aligned}$$

Eine Verallgemeinerung auf die dritte Potenz ist wie folgt:

$$\begin{aligned}(x+y)^3 &= (x^2+2xy+y^2)\cdot(x+y)\\ &= x^3+2x^2y+xy^2+x^2y+2xy^2+y^3\\ &= x^3+3x^2y+3xy^2+y^3\end{aligned}$$

Im Allgemeinen kann man den Ansatz

$$(x+y)^n = \sum_{k=0}^{n} a_{n,k}x^k y^{n-k}$$

aufstellen, wobei $a_{n,k}$ gerade die Anzahl der Möglichkeiten angibt, die Binome $x^k y^{n-k}$ aus den Faktoren x und y zusammenzusetzen. Damit gilt:

$$a_{n,k} = \binom{n}{k} =_{\text{def}} \frac{n!}{k!(n-k)!}$$

Dabei setzen wir $\binom{n}{k} =_{\text{def}} 0$ für $n < k$ bzw. $k < 0$ sowie $\binom{n}{k} =_{\text{def}} 1$.

Theorem 2.2 (Binomialtheorem) *Für alle reellen Zahlen x und y und jede natürliche Zahl n gilt*

$$(x+y)^n = \sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k}.$$

Wie können wir den Binomialkoeffizienten $\binom{n}{k}$ bestimmen, ohne algorithmisch teure Multiplikationen auszuführen?

Lemma 2.3 (PASCALsches Dreieck) *Für natürliche Zahlen $n > 0$ und k gilt*

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

Beweis: (*rechnerisch; ohne Randfälle*) Für $0 < k < n$ rechnen wir aus:

$$\begin{aligned}\binom{n-1}{k-1}+\binom{n-1}{k} &= \frac{(n-1)!}{(k-1)!(n-k)!} + \frac{(n-1)!}{k!(n-1-k)!}\\ &= \frac{(n-1)!}{(k-1)!(n-k)!}\cdot\frac{k}{k} + \frac{(n-1)!}{k!(n-1-k)!}\cdot\frac{n-k}{n-k}\\ &= \frac{(n-1)!\cdot k}{k!(n-k)!} + \frac{(n-1)!(n-k)}{k!(n-k)!}\\ &= \frac{(n-1)!(k+n-k)}{k!(n-k)!}\end{aligned}$$

$$= \frac{(n-1)! \cdot n}{k!(n-k)!}$$
$$= \binom{n}{k}$$

Damit ist das Lemma durch Nachrechnen bewiesen. ■

Beispiel: Der Dreiecksaufbau des rekursiven Zusammenhangs in Lemma 2.3 lässt sich leicht veranschaulichen und ist schon aus der Schule bekannt:

$$\begin{array}{ccccccccc}
 & & & \binom{0}{0} & & & & & \\
 & & \binom{1}{0} & & \binom{1}{1} & & & & \\
 & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & & \\
\binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & & \\
\binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} \\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots
\end{array}
\qquad
\begin{array}{ccccccccc}
 & & & 1 & & & & & \\
 & & 1 & & 1 & & & & \\
 & 1 & & 2 & & 1 & & & \\
1 & & 3 & & 3 & & 1 & & \\
1 & & 4 & & 6 & & 4 & & 1 \\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots
\end{array}$$

2.5 Nullstellen

Es sei $p(x)$ ein Polynom. Eine Zahl x_0 heißt *Nullstelle* von $p(x)$, falls $p(x_0) = 0$ gilt.

Beispiel:

- Das Polynom $x^2 - 1$ hat die Nullstellen 1 und -1.
- Das Polynom $x^2 + 1$ hat keine Nullstellen (in den reellen Zahlen).
- Es sei $p(x) =_{\text{def}} ax^2 + bx + c$ mit den reellen Zahlen a, b, c gegeben. Zur Bestimmung der Nullstellen von p rechnen wir:

$$\begin{aligned} ax^2 + bx + c &= a\left(x^2 + \frac{b}{a} \cdot x + \frac{c}{a}\right) \\ &= a\left(x + \frac{b}{2a}\right)^2 - \frac{b^2}{4a} + c \end{aligned}$$

Für $p(x) = 0$ gilt somit

$$a\left(x + \frac{b}{2a}\right)^2 = \frac{b^2}{4a} - c \quad \text{bzw.} \quad \left(x + \frac{b}{2a}\right)^2 = \frac{b^2}{4a^2} - \frac{c}{a}.$$

Durch Ziehen der Wurzel auf beiden Seiten erhalten wir

$$\left|x + \frac{b}{2a}\right| = \sqrt{\frac{b^2}{4a^2} - \frac{c}{a}},$$

oder aufgelöst nach x:

$$x = -\frac{b}{2a} \pm \sqrt{\frac{b^2}{4a^2} - \frac{c}{a}} = -\frac{b}{2a} \pm \frac{1}{2a}\sqrt{b^2 - 4ac}$$

Damit eine Lösungen im Bereich der reellen Zahlen existiert, muss also $b^2 - 4ac \geq 0$ gelten. Gilt $b^2 - 4ac > 0$, so hat das Polynom p zwei verschiedene reelle Nullstellen.

- Das Polynom $p(x) =_{\text{def}} -x^3 + 3x^2 - x - 1$ hat die Nullstellen $1, 1 + \sqrt{2}$ und $1 - \sqrt{2}$, denn:

$$(x-1)\left(x - \left(1 + \sqrt{2}\right)\right)\left(x - \left(1 - \sqrt{2}\right)\right) = x^3 + 3x^2 - x - 1.$$

Theorem 2.4 *Ein reelles Polynom $p(x) \neq 0$ mit dem Grad n hat höchstens n Nullstellen in den reellen Zahlen.*

Beweis: Ist p vom Grad 0, so gilt die Aussage wegen $p(x) \neq 0$. Ist p vom Grad $n > 0$, so hat p entweder keine Nullstelle (womit die Aussage gilt) oder p besitzt mindestens eine Nullstelle x_0. Nach Theorem 2.1 gibt es somit Polynome $t(x)$ und $r(x)$ mit

$$p(x) = t(x) \cdot (x - x_0) + r(x)$$

und $\text{grad}(r) < \text{grad}(x - x_0)$. Wegen $\text{grad}(x - x_0) = 1$ gilt $\text{grad}(r) = 0$, d.h., $r(x) = r_0$ für eine reelle Zahl r_0. Damit gilt aber

$$0 = p(x_0) = t(x_0)(x_0 - x_0) + r_0 = r_0$$

Mithin gilt $p(x) = t(x) \cdot (x - x_0)$ mit $\text{grad}(t) = n - 1$. Wenn wir bereits wissen, dass Polynome bis zum Grad $n - 1$ höchstens $n - 1$ Nullstellen besitzen, so hat folglich p höchstens n Nullstellen. ■

Ohne Beweis geben wir die allgemeine Aussage für die Anzahl der Nullstellen von Polynomen an.

Theorem 2.5 (Fundamentalsatz der Algebra) *Jedes komplexe Polynom p mit $p \neq 0$ und Grad n hat genau n komplexe Nullstellen (mit Vielfachheiten).*

Ein Polynom $p(x) =_{\text{def}} a_n x^n + \cdots + a_0$ von Grad n heißt *normiert*, falls $a_n = 1$.

Korollar 2.6 *Es seien p und q normierte Polynome vom Grad n. Stimmen p und q bei n paarweise verschiedenen Argumenten überein, so sind p und q identisch.*

Als Anmerkung sei erwähnt, dass das Korollar auch für komplexe Argumente gilt.

Beweis: Es seien p und q normiert vom Grad n. Es seien $x_1, \ldots, x_n$ paarweise verschiedene reelle Zahlen mit $p(x_i) = q(x_i)$. Betrachten wir das Differenzpolynom $r(x) =_{\text{def}} p(x) - q(x)$, so gilt $r(x_i) = 0$ für alle x_i, d.h., r besitzt n Nullstellen. Da p und q normiert sind, gilt $\text{grad}(r) \leq n - 1$. Nach Theorem 2.4 muss folglich $r = 0$ gelten. Damit gilt $p = q$. ■

Korollar 2.7 *Es sei p ein normiertes Polynom vom Grad n mit den paarweise verschiedenen Nullstellen $\alpha_1, \ldots, \alpha_n$. Dann gilt*

$$p(x) = (x - \alpha_1) \cdot (x - \alpha_2) \cdot \ldots \cdot (x - \alpha_n).$$

Beweis: Es sei $q(x) =_{\text{def}} (x - \alpha_1) \cdot (x - \alpha_2) \cdot \ldots \cdot (x - \alpha_n)$. Dann ist q normiert und vom Grad n. Weiterhin besitzen p und q die gleichen n Nullstellen. Folglich gilt $p = q$. ■

Eine Verallgemeinerung des Korollars auf vielfache Nullstellen ist möglich.

Induktion 3

3.1 Vollständige Induktion

Die vollständige Induktion ist eine Methode zur Lösung des folgenden Problems:

> *Wie weisen wir nach, dass alle natürlichen Zahlen eine bestimmte Eigenschaft E erfüllen?*

Die Lösungsmethode „Vollständige Induktion von $n-1$ nach n“ besteht in zwei Schritten, die zusammengenommen folgenden logischen Schluss ermöglichen:

- *Induktionsanfang*: Erfüllt 0 die Eigenschaft E und
- *Induktionsschritt*: folgt für alle $n > 0$ die Gültigkeit von E für n aus der Tatsache, dass $n-1$ die Eigenschaft E erfüllt (*Induktionsvoraussetzung*),

so erfüllen alle Zahlen die Eigenschaft E.

Wir wollen diese Beweismethode an einigen Beispielaussagen nachvollziehten:

Proposition 3.A *Für alle natürlichen Zahlen n gilt* $\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$.

Beweis: (*Induktion*) Wir definieren zunächst für alle natürlichen Zahlen n:

$$a_n =_{\text{def}} \sum_{k=0}^{n} k$$

Die Eigenschaft E, die wir für alle natürlichen Zahlen zeigen wollen, ist die Gleichheit:

$$E(n) \quad : \qquad a_n = \frac{n(n+1)}{2}$$

Wir führen einen Beweis mittels vollständiger Induktion über n.

- *Induktionsanfang*: Für $n = 0$ gilt $a_0 = \sum_{k=0}^{0} k = 0 = \frac{0 \cdot (0+1)}{2}$, d.h., $E(0)$ gilt.

- *Induktionsschritt*: Für $n > 0$ führen wir die Aussage $E(n)$ auf die Aussage $E(n-1)$ zurück, um daraus mittels Induktionsvoraussetzung die Aussage $E(n)$ zu beweisen. Für $n-1$ lautet die als wahr vorausgesetzte Aussage

$$E(n-1) \quad : \qquad a_{n-1} = \frac{(n-1)((n-1)+1)}{2} = \frac{(n-1)n}{2}$$

Damit erhalten wir durch Abspalten des Summanden für $k = n$ aus a_n:

$$\begin{aligned} a_n &= n + a_{n-1} \\ &= n + \frac{(n-1)n}{2} && \text{(nach Induktionsvoraussetzung)} \\ &= \frac{2n + (n-1)n}{2} \\ &= \frac{n(2 + (n-1))}{2} \\ &= \frac{n(n+1)}{2} \end{aligned}$$

Damit ist die Proposition bewiesen. ■

Proposition 3.B *Für alle natürlichen Zahlen n gilt* $\sum_{k=0}^{n}(2k+1) = (n+1)^2$.

Beweis: (*Induktion*) Die Eigenschaft E, die wir für alle natürlichen Zahlen zeigen wollen, ist die Gleichheit:

$$E(n) \quad : \qquad \sum_{k=0}^{n}(2k+1) = (n+1)^2$$

Wir führen einen Beweis mittels vollständiger Induktion über n.

- *Induktionsanfang*: Für $n = 0$ gilt $(2 \cdot 0 + 1) = 1 = (0+1)^2$, d.h., $E(0)$ gilt.
- *Induktionsschritt*: Für $n > 0$ führen wir die Aussage $E(n)$ auf die Aussage $E(n-1)$ zurück, um daraus mittels Induktionsvoraussetzung die Aussage $E(n)$ zu beweisen. Für $n-1$ lautet die Aussage

$$E(n-1) \quad : \qquad \sum_{k=0}^{n-1}(2k+1) = ((n-1)+1)^2 = n^2$$

Damit erhalten wir durch Abspalten des Summanden für $k = n$:

$$\begin{aligned} \sum_{k=0}^{n}(2k+1) &= 2n + 1 + \sum_{k=0}^{n-1}(2k+1) \\ &= 2n + 1 + n^2 && \text{(nach Induktionsvoraussetzung)} \\ &= (n+1)^2 \end{aligned}$$

Damit ist die Proposition bewiesen. ■

Proposition 3.C *Für alle natürlichen Zahlen n gilt* $\sum_{k=0}^{n} k^3 = \frac{n^2(n+1)^2}{4}$.

Beweis: (*Induktion*) Die Eigenschaft E, die wir für alle natürlichen Zahlen zeigen wollen, ist die Gleichheit:

$$E(n) \quad : \qquad \sum_{k=0}^{n} k^3 = \frac{n^2(n+1)^2}{4}$$

Wir führen einen Beweis mittels vollständiger Induktion über n.

- *Induktionsanfang*: Für $n = 0$ gilt $0^3 = 0 = \frac{0^2 \cdot (0+1)^2}{4}$, d.h., $E(0)$ gilt.
- *Induktionsschritt*: Für $n > 0$ führen wir die Aussage $E(n)$ auf die Aussage $E(n-1)$ zurück. Für $n-1$ lautet die Eigenschaft E:

  $$E(n-1) \quad : \qquad \sum_{k=0}^{n-1} k^3 = \frac{(n-1)^2((n-1)+1)^2}{4} = \frac{(n-1)^2 n^2}{4}$$

  Damit erhalten wir durch Abspalten des Summanden für $k = n$:

$$\begin{aligned}
\sum_{k=0}^{n} k^3 &= n^3 + \sum_{k=0}^{n-1} k^3 \\
&= n^3 + \frac{(n-1)^2 n^2}{4} && \text{(nach Induktionsvoraussetzung)} \\
&= \frac{4n^3 + n^4 - 2n^3 + n^2}{4} \\
&= \frac{n^4 + 2n^3 + n^2}{4} \\
&= \frac{n^2(n^2 + 2n + 1)}{4} \\
&= \frac{n^2(n+1)^2}{4}
\end{aligned}$$

Damit ist die Proposition bewiesen. ■

Ein wichtiges Resultat ist die folgende explizite Formel für die *geometrische Reihe*.

Proposition 3.D *Es sei $q \neq 1$. Für alle natürlichen Zahlen n gilt* $\sum_{k=0}^{n} q^k = \frac{q^{n+1} - 1}{q - 1}$.

Insbesondere ergibt sich für den Spezialfall $q = 2$:

$$\sum_{k=0}^{n} 2^k = 2^{n+1} - 1$$

Beweis: (*Induktion*) Die Eigenschaft E, die für alle natürlichen Zahlen bewiesen werden soll, lautet:

$$E(n) \quad : \qquad \sum_{k=0}^{n} q^k = \frac{q^{n+1} - 1}{q - 1}$$

Wir führen einen Beweis mittels vollständiger Induktion über n.

- *Induktionsanfang*: Für $n = 0$ gilt $q^0 = 1 = \dfrac{q^{0+1} - 1}{q - 1}$ für $q \neq 1$, d.h., $E(0)$ gilt.
- *Induktionsschritt*: Für $n > 0$ führen wir die Aussage $E(n)$ wieder geeignet auf die Aussage $E(n-1)$ zurück. Dieses hat folgendes Aussehen:

  $$E(n-1) \quad : \qquad \sum_{k=0}^{n-1} q^k = \frac{q^{(n-1)+1} - 1}{q - 1} = \frac{q^n - 1}{q - 1}$$

  Durch Abspalten des Summanden für $k = n$ erhalten wir somit:

  $$\begin{aligned} \sum_{k=0}^{n} q^k &= q^n + \sum_{k=0}^{n-1} q^k \\ &= q^n + \frac{q^n - 1}{q - 1} && \text{(nach Induktionsvoraussetzung)} \\ &= \frac{q^n(q-1) + q^n - 1}{q - 1} \\ &= \frac{q^{n+1} - q^n + q^n - 1}{q - 1} \\ &= \frac{q^{n+1} - 1}{q - 1} \end{aligned}$$

Damit ist die Proposition bewiesen. ■

Proposition 3.E *Für alle natürlichen Zahlen n gilt $(n+1)! \geq 2^n$.*

Beweis: (*Induktion*) Wir führen einen Beweis mittels vollständiger Induktion über n.

- *Induktionsanfang*: Für $n = 0$ gilt $(0+1)! = 1 \geq 1 = 2^0$.

- *Induktionsschritt*: Für $n > 0$ erhalten wir mittels Abspaltung des größten Faktors:

$$\begin{aligned}(n+1)! &= (n+1)\cdot n! \\ &\geq (n+1)\cdot 2^{n-1} && \text{(nach Induktionsvoraussetzung)} \\ &\geq 2\cdot 2^{n-1} && \text{(wegen } n \geq 1\text{)} \\ &= 2^n\end{aligned}$$

Damist die Proposition bewiesen. ■

Theorem 2.2 (Binomialtheorem) *Für alle reellen Zahlen x und y und jede natürliche Zahl n gilt*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

Beweis: (*Induktion*) Für beliebige reelle Zahlen x und y führen wir einen Beweis mittels vollständiger Induktion über n.

- *Induktionsanfang*: Es sei $n = 0$. Dann gilt $(x+y)^0 = 1 = \binom{0}{0} x^0 y^0$.

- *Induktionsschritt*: Es sei $n > 0$. Dann gilt:

$$\begin{aligned}&(x+y)^n \\ &= (x+y)\cdot(x+y)^{n-1} \\ &= (x+y)\cdot \sum_{k=0}^{n-1} \binom{n-1}{k} x^k y^{n-1-k} && \text{(nach Induktionsvoraussetzung)} \\ &= \sum_{k=0}^{n-1} \binom{n-1}{k} x^{k+1} y^{n-(k+1)} \;+\; \sum_{k=0}^{n-1} \binom{n-1}{k} x^k y^{n-k} \\ &= \sum_{k=1}^{n} \binom{n-1}{k-1} x^k y^{n-k} \;+\; \sum_{k=0}^{n-1} \binom{n-1}{k} x^k y^{n-k} \\ &= \binom{n-1}{n-1} x^n y^{n-n} \;+\; \sum_{k=1}^{n-1} \left[\binom{n-1}{k-1} + \binom{n-1}{k} \right] x^k y^{n-k} \;+\; \binom{n-1}{0} x^0 y^{n-0} \\ &= \binom{n}{n} x^n y^{n-n} \;+\; \sum_{k=1}^{n-1} \binom{n}{k} x^k y^{n-k} \;+\; \binom{n}{0} x^0 y^{n-0} && \text{(nach Lemma 2.3)} \\ &= \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}\end{aligned}$$

Damit ist das Theorem bewiesen. ■

Mittels Induktion können wir sogar die folgende sensationelle Proposition beweisen.

Proposition 3.F *Alle natürlichen Zahlen sind gleich.*

Beweis: Um die Aussage der Proposition zu beweisen, zeigen wir folgende Aussage. Für alle natürlichen Zahlen m, a, b gilt:

$$\text{Ist } \max(a, b) = m, \text{ so gilt } a = b. \tag{3.1}$$

Dies ist leicht einzusehen mittels folgenden Induktionsbeweises über m:

- *Induktionsanfang*: Es sei $m = 0$. Ist $\max(a, b) = 0$, so folgt $a = b = 0$.
- *Induktionsschritt*: Es sei $m > 0$. Ist $\max(a, b) = m$, so ist $\max(a - 1, b - 1) = m - 1$. Nach Induktionsvoraussetzung gilt somit $a - 1 = b - 1$ und mithin $a = b$.

Damit ist die Aussage (3.1) bewiesen.

Es seien nun a und b natürliche Zahlen. Es sei $m =_{\text{def}} \max(a, b)$. Wegen Aussage (3.1) sind alle natürlichen Zahlen gleich m. ■

Da die Aussage der Proposition ganz offensichtlich falsch ist, haben wir im Beweis einen Fehler gemacht. Welchen?

3.2 Allgemeine Form der vollständigen Induktion

Die Lösungsmethode besteht in zwei Schritten, die zusammengenommen folgenden logischen Schluss ermöglichen:

E sei die nachzuweisende Eigenschaft E und n_0 sie eine natürliche Zahl:

- *Induktionsanfang*: Erfüllen $0, 1, \ldots, n_0$ die Eigenschaft E und
- *Induktionsschritt*: folgt für alle $n > n_0$ die Gültigkeit von E für n aus der Tatsache, dass alle $m < n$ die Eigenschaft E erfüllen (*Induktionsvoraussetzung*),

so erfüllen alle Zahlen die Eigenschaft E.

Wir wollen auch diese Beweismethode an einigen Beispielaussagen nachvollziehten:

Proposition 3.G *Für alle natürlichen Zahlen $n \geq 4$ gilt $n! \geq 2^n$.*

Beweis: (*Induktion*) Wir führen einen Bewies mittels Induktion über n für $n \geq 4$. (Wir setzen $n_0 =_{\text{def}} 4$.)

- *Induktionsanfang*: Für $n = 0, 1, 2, 3$ muss nichts gezeigt werden, d.h., die Aussage ist richtig. Für $n = 4$ gilt $4! = 24 \geq 16 = 2^4$.
- *Induktionsschritt*: Für $n > 4$ erhalten wir mittels Abspaltung des größten Faktors:

$$\begin{aligned} n! &= n \cdot (n-1)! \\ &\geq n \cdot 2^{n-1} && \text{(nach Induktionsvoraussetzung)} \\ &\geq 2 \cdot 2^{n-1} && \text{(wegen } n \geq 5\text{)} \\ &= 2^n \end{aligned}$$

Damit ist die Proposition bewiesen. ∎

Die FIBONACCI-Folge (in der hier verwendeten Form) ist wie folgt rekursiv definiert:

$$F_0 =_{\text{def}} 1, \qquad F_1 =_{\text{def}} 2, \qquad F_n =_{\text{def}} F_{n-1} + F_{n-2} \quad \text{für } n \geq 2$$

Die ersten Glieder dieser Folge sind: $1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots$ Im Folgende wollen wir zeigen, dass die FIBONACCI-Folge exponentiell wächst. Wegen der rekursiven Definition der Folgenglieder bietet sich dafür ein Induktionsbeweis geradezu an.

Proposition 3.G *Für alle natürlichen Zahlen n gilt* $F_n \geq \left(\frac{\sqrt{5}+1}{2}\right)^n$.

Beweis: (*Induktion*) Wir führen einen Beweis mittels Induktion über n.

- *Induktionsanfang*: Wir überprüfen zwei Fälle. Für $n = 0$ gilt $F_0 = 1 = \left(\frac{\sqrt{5}+1}{2}\right)^0$ und für $n = 1$ gilt $F_1 = 2 \geq \left(\frac{\sqrt{5}+1}{2}\right)^1$.
- *Induktionsschritt*: Für $n > 1$ erhalten aus der Definition von F_n:

$$\begin{aligned} F_n &= F_{n-1} + F_{n-2} \\ &\geq \left(\frac{\sqrt{5}+1}{2}\right)^{n-1} + \left(\frac{\sqrt{5}+1}{2}\right)^{n-2} && \text{(nach Induktionsvoraussetzung)} \\ &= \left(\frac{\sqrt{5}+1}{2}\right)^{n-2} \left(\frac{\sqrt{5}+1}{2} + 1\right) \end{aligned}$$

$$
\begin{aligned}
&= \left(\frac{\sqrt{5}+1}{2}\right)^{n-2}\left(\frac{\sqrt{5}+1}{2}\right)^{2}\\
&= \left(\frac{\sqrt{5}+1}{2}\right)^{n}
\end{aligned}
$$

Damit ist die Proposition bewiesen. ■

3.3 Strukturelle Induktion

Wir wollen das Induktionsprinzip zu einer Beweismethode über induktiv definierten Mengen erweitern. Dabei führen wir nur den Spezialfall mittels einer Operation aus.

Es sei $f : A^n \to A$ eine n-stellige Funktion (Operation). Dann sind die Abbildungen $\Gamma_f : \mathcal{P}(A) \to \mathcal{P}(A)$ sowie $\Gamma_f^k : \mathcal{P}(A) \to \mathcal{P}(A)$ für alle $k \in \mathbb{N}$ wie folgt definiert (für $B \subseteq A$):

$$
\begin{aligned}
\Gamma_f^0(B) &=_{\text{def}} B\\
\Gamma_f^k(B) &=_{\text{def}} \Gamma_f^{k-1}(B) \cup \left\{ f(a_1,\ldots,a_n) \mid a_1,\ldots,a_n \in \Gamma_f^{k-1}(B) \right\}\\
\Gamma_f(B) &=_{\text{def}} \bigcup_{k=0}^{\infty} \Gamma_f^k(B)
\end{aligned}
$$

Die Menge $\Gamma_f(B)$ heißt *Abschluss* von B unter f.

Anschaulich gehören zur Menge $\Gamma_f(B)$ alle diejenigen Elemente von A, die sich durch eine endliche Anzahl von Hintereinanderausführungen der Operation f aus den Elementen der Menge B konstruieren lassen.

Beispiele: Wir wollen die Begriffsbildung an Beispielen nachvollziehen.

- Wenn wir die Operation $\text{inc} : \mathbb{N} \to \mathbb{N} : n \mapsto n+1$ betrachten, so gilt:

$$
\begin{aligned}
\Gamma_{\text{inc}}^0(\{0\}) &= \{0\}\\
\Gamma_{\text{inc}}^1(\{0\}) &= \{0\} \cup \{1\} = \{0,1\}\\
\Gamma_{\text{inc}}^2(\{0\}) &= \{0,1\} \cup \{1,2\} = \{0,1,2\}\\
\Gamma_{\text{inc}}^3(\{0\}) &= \{0,1,2\} \cup \{1,2,3\} = \{0,1,2,3\}\\
&\vdots\\
\Gamma_{\text{inc}}^k(\{0\}) &= \{0,1,\ldots,k\}\\
&\vdots\\
\Gamma_{\text{inc}}(\{0\}) &= \mathbb{N}
\end{aligned}
$$

  Der Beweis der Gleichheit $\Gamma_{\text{inc}}^k(\{0\}) = \{0,1,\ldots,k\}$ für alle $k \in \mathbb{N}$ kann mittels vollständiger Induktion über k geführt werden.

- Wenn wir die Operation $+ : \mathbb{N}^2 \to \mathbb{N} : (n, m) \mapsto n+m$ betrachten, so gilt:

$$\begin{aligned}
\Gamma^0_{\text{inc}}(\{1\}) &= \{1\} \\
\Gamma^1_{\text{inc}}(\{1\}) &= \{1\} \cup \{2\} = \{1,2\} \\
\Gamma^2_{\text{inc}}(\{1\}) &= \{1,2\} \cup \{2,3,4\} = \{1,2,3,4\} \\
\Gamma^3_{\text{inc}}(\{1\}) &= \{1,2,3,4\} \cup \{2,3,4,5,6,7,8\} = \{1,2,3,4,5,6,7,8\} \\
&\vdots \\
\Gamma^k_{\text{inc}}(\{1\}) &= \{1,2,\ldots,2^k\} \\
&\vdots \\
\Gamma_{\text{inc}}(\{1\}) &= \mathbb{N}_+
\end{aligned}$$

  Auch hier kann der Beweis der Gleichheit $\Gamma^k_{\text{inc}}(\{1\}) = \{1,2,\ldots,2^k\}$ für alle $k \in \mathbb{N}$ mittels vollständiger Induktion über k geführt werden.

Eine Menge $B \subseteq A$ heißt *induktiv definiert* (oder *endlich erzeugt*) aus $B_0 \subseteq A$, falls es eine Funktion $f : A^n \to A$ gibt mit $B = \Gamma_f(B_0)$.

Für endlich erzeugte Mengen können wir das Beweisprinzip der strukturelle Induktion beschreiben:

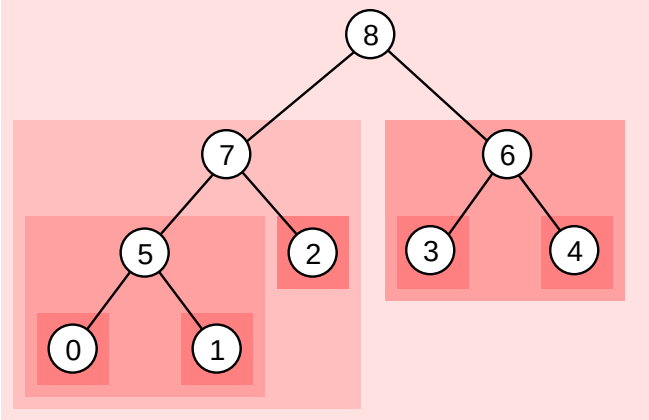
- *Induktionsanfang* (IA): Zeige $A(x)$ für alle $x \in B_0$.

- *Induktionsschritt* (IS): Zeige $A(x)$ für ein allgemeines $x \in B \setminus B_0$ unter der Annahme (*Induktionsvoraussetzung*, IV), dass $A(y_1), \ldots, A(y_n)$ für $x = f(y_1, \ldots, y_n)$ gilt. (Hier ist unter technischen Gesichtspunkten darauf zu achten, dass $y_1, \ldots, y_n$ einfacher sind, d.h. ist $x \in \Gamma^k_f(B_0)$, so muss $y_1, \ldots, y_n \in \Gamma^{k-1}_f(B_0)$ gelten.)

Wir wollen uns ein Beispiel für die in der Informatik typische konstruktive Vorgehensweise anschauen.

Eine wichtige Datenstruktur in der Informatik sind Binärbäume als Verallgemeinerung von Listen. In einer Liste hat jedes Element bis auf das letzte genau einen Nachfolger und jedes Element bis auf das erste genau einen Vorgänger. Verlangt man nur die Eigenschaft das jedes Element bis auf eines genau einen Vorgänger besitzt (und Kreise ausgeschlossen

werden), gelangt man zu Bäumen. Eine Sonderklasse von Bäumen sind volle, gewurzelte Binärbäume. Ein Beispiel ist der folgende Baum:



Die Menge aller vollen, gewurzelten Binärbäume kann man wie folgt induktiv definieren. Bäume sind Tripel (V, E, r), wobei V für die Menge der Knoten, $E \subseteq V^2$ für die Menge der Kanten sowie $r \in V$ für die Wurzel stehen. Wir geben nun eine Menge B_0 und eine Operation f an:

$$\begin{aligned} B_0 &=_{\text{def}} \{\ (\{r\}, \emptyset, r) \mid r \in \mathbb{N}\ \} \\ f((V_1, E_1, r_1), (V_2, E_2, r_2)) &=_{\text{def}} (V_1 \cup V_2 \cup \{r\}, E_1 \cup E_2 \cup \{(r, r_1), (r, r_2)\}, r), \\ &\qquad \text{wobei } V_1 \cap V_2 = \emptyset \text{ sowie } r \notin V_1 \cup V_2 \text{ gilt} \end{aligned}$$

Die Menge der vollen, gewurzelten Binärbäume ist dann gerade die Menge $\Gamma_f(B_0)$.

Bevor wir unseren zu beweisende Eigenschaften formulieren, führen wir noch zwei Begriffe ein. Es sei $T = (V, E, r)$ ein voller, gewurzelter Binärbaum. Ein Element $v \in V$ heißt *Blatt* (bzw. *Blattknoten*), falls es kein $u \in V$ mit $(v, u) \in E$ gibt; sonst heißt v *innerer Knoten*.

Proposition 3.H *Für einen vollen, gewurzelten Binärbaum T seien n_T die Anzahl innerer Knoten und m_T die Anzahl der Blätter. Dann gilt stets $n_T = m_T - 1$.*

Beweis: (*Induktion über den Aufbau der Bäume*)

- *Induktionsanfang*: Ist $T = (\{r\}, \emptyset, r)$, so gilt $n_T = 0$ und $m_T = 1$.
- *Induktionsschritt*: Es sei $T = f(T_1, T_2)$ für geeignete Bäume $T_1 = (V_1, E_1, r_1)$ und $T_2 = (V_2, E_2, r_2)$. Dann gilt insbesondere, dass die Blätter bzw. inneren Knoten von

T_1 und T_2 auch Blätter bzw. innere Knoten von T sind, da in T nur die Paare (r, r_1) und (r, r_2) hinzukommen. Mithin gilt:

$$\begin{aligned} n_T &= n_{T_1} + n_{T_2} + 1 && (r \text{ ist ein innerer Knoten von } T) \\ &= (m_{T_1} - 1) + (m_{T_2} - 1) + 1 && (\text{nach } \textit{Induktionsvoraussetzung}) \\ &= (m_{T_1} + m_{T_2}) - 1 \\ &= m_T - 1 \end{aligned}$$

Damit ist die Proposition bewiesen. ■

Literaturverzeichnis

[MM06] Christoph Meinel und Martin Mundhenk. *Mathematische Grundlagen der Informatik. Mathematisches Denken und Beweisen. Eine Einführung.* 3., überarbeitete und erweiterte Auflage. B. G. Teubner Verlag, Wiesbaden, 2006.

[Ste07] Angelika Steger. *Diskrete Strukturen. Band 1: Kombinatorik-Graphentheorie-Algebra.* 2. Auflage. Springer-Verlag, Berlin, 2007.

[SS02] Thomas Schickinger und Angelika Steger. *Diskrete Strukturen. Band 2: Wahrscheinlichkeitstheorie und Statistik.* Springer-Verlag, Berlin, 2002.

[WHK04] Manfred Wolff, Peter Hauck und Wolfgang Küchlin. *Mathematik für Informatik und Bioinformatik.* Springer-Verlag, Berlin, 2004.