# Lösungsvorschläge zu ausgewählten Übungsaufgaben aus Storch/Wiebe: Lehrbuch der Mathematik Band 1, 3. Aufl. (Version 2010), Kapitel 1

## 1 Mengen und Abbildungen

**Abschnitt 1.A, Aufg. 2**, p. 5 (1.7.2010) :

Für Mengen $A$ und $B$ sind folgende Aussagen äquivalent: (1) $A \subseteq B$. (2) $A \cap B = A$. (3) $A \cup B = B$. (4) $A - B = \emptyset$. (5) $B - (B - A) = A$. (6) Für jede Menge $C$ ist $A \cup (B \cap C) = (A \cup C) \cap B$. (7) Es gibt eine Menge $C$ mit $A \cup (B \cap C) = (A \cup C) \cap B$.

**Beweis:** „(1) $\Rightarrow$ (2)" Sei $A \subseteq B$. Stets gilt natürlich $A \cap B \subseteq A$, da alle Elemente von $A \cap B$ in $A$ (und in $B$) liegen. Umgekehrt zeigen wir $A \subseteq A \cap B$. Sei dazu $x \in A$. Wegen $A \subseteq B$ ist dann auch $x \in B$ und somit $x \in A \cap B$. Insgesamt folgt $A \cap B = A$.

„(2) $\Rightarrow$ (1)" Sei $A \cap B = A$. Wir zeigen $A \subseteq B$. Sei dazu $x \in A$. Dann ist aber auch $x \in A = A \cap B$ und somit $x \in B$.

„(1) $\Rightarrow$ (3)" Sei $A \subseteq B$. Wir zeigen $A \cup B \subseteq B$. Sei dazu $x \in A \cup B$, d.h. $x \in A$ oder $x \in B$. Im ersten Fall ist $x \in A \subseteq B$, also auch $x \in B$, im zweiten Fall ist sowieso $x \in B$. $B \subseteq A \cup B$ gilt stets. Insgesamt folgt $A \cup B = B$.

„(3) $\Rightarrow$ (1)" Sei $A \cup B = B$. Wir zeigen $A \subseteq B$. Sei dazu $x \in A$. Dann ist aber auch $x \in A \cup B = B$.

„(1) $\Rightarrow$ (4)" Sei $A \subseteq B$. Wir zeigen $A - B = \emptyset$. Angenommen, es gäbe ein $x \in A - B$, d.h. mit $x \in A$ und $x \notin B$. Wegen $A \subseteq B$ folgt aus $x \in A$ aber $x \in B$ im Widerspruch zu $x \notin B$. Also kann es kein Element $x \in A - B$ geben.

„(4) $\Rightarrow$ (1)" Sei $A - B = \emptyset$. Wir zeigen $A \subseteq B$. Sei dazu $x \in A$. Wäre dann $x \notin B$, so wäre aber $x \in A - B$ im Widerspruch zu $A - B = \emptyset$. Also ist auch $x \in B$.

„(1) $\Rightarrow$ (5)" Sei $A \subseteq B$. Wir zeigen $B - (B - A) = A$. Sei dazu $x \in B - (B - A)$. Dann ist sicher $x \in B$. Wäre $x \notin A$, so wäre $x \in B - A$ und folglich $x \notin B - (B - A)$. Widerspruch. Also ist $x \in A$. Wir erhalten $B - (B - A) \subseteq A$. Nun zeigen wir die umgekehrte Inklusion: Sei dazu $x \in A$. Dann ist sicher $x \notin B - A$, aber $x \in B$ wegen $A \subseteq B$. Es folgt $x \in B - (B - A)$. Wir erhalten so $A \subseteq B - (B - A)$, also insgesamt die gewünschte Gleichheit.

„(5) $\Rightarrow$ (1)" Sei $B - (B - A) = A$. Wir zeigen $A \subseteq B$. Sei dazu $x \in A$. Dann ist aber auch $x \in B - (B - A) = A$ und somit $x \in B$.

„(1) $\Rightarrow$ (6)" Sei $A \subseteq B$. Wir zeigen $A \cup (B \cap C) = (A \cup C) \cap B$. Sei dazu $x \in A \cup (B \cap C)$. Dann ist $x \in A$ oder es ist $x \in B \cap C$. Im ersten Fall ist wegen $A \subseteq B$ auch $x \in B$ und wegen $A \subseteq A \cup C$ auch $x \in A \cup C$ und damit $x \in (A \cup C) \cap B$. Im zweiten Fall ist $x \in B$ und $x \in C$ und somit wegen $C \subseteq A \cup C$ auch $x \in A \cup C$, d.h. insgesamt $x \in (A \cup C) \cap B$. Nun zeigen wir die umgekehrte Inklusion: Sei dazu $x \in (A \cup C) \cap B$. Dann ist $x \in A \cup C$ und $x \in B$. Wegen $x \in A \cup C$ ist $x \in A$ oder $x \in C$. Im ersten Fall ist auch $x \in A \subseteq A \cup (B \cap C)$. Im zweiten Fall ist wegen $x \in B$ auch $x \in B \cap C$ und folglich $x \in A \cup (B \cap C)$.

„(6) $\Rightarrow$ (7)" Diese Implikation ist trivial, da es eine Menge $C$ gibt.

„(7) $\Rightarrow$ (1)" Sei $A \cup (B \cap C) = (A \cup C) \cap B$ für eine Menge $C$. Wir zeigen $A \subseteq B$. Sei dazu $x \in A$. Dann ist aber auch $x \in A \cup (B \cap C) = (A \cup C) \cap B$. Es folgt $x \in B$ (und $x \in A \cup C$). •

**Abschnitt 1.A, Aufg. 4b)**, p. 5 (1.7.2010) :

Für Mengen $A, B, C$ gilt: $(A \cup B) - C \subseteq A \cup (B - C)$.

**Beweis:** Sei $x \in (A \cup B) - C$. Dann ist $x \in A \cup B$ und $x \notin C$. Wegen $x \in A \cup B$ ist $x \in A$ oder $x \in B$. Im ersten Fall ist erst recht $x \in A \cup (B - C)$. Im zweiten Fall folgt $x \in B - C$ und somit ebenfalls $x \in A \cup (B - C)$. •

**Abschnitt 1.A, Zusatzaufgabe**, p. 5 (1.7.2010) :

Für Mengen $A, B, C$ gilt $(A \cup B) - C = A \cup (B - C)$ genau dann, wenn $A \cap C = \emptyset$ ist.

**Beweis:** Sei zunächst $A \cap C = \emptyset$. Wir haben dann $(A \cup B) - C = A \cup (B - C)$ zu zeigen. Wegen Aufg. 4.b) ist hierfür nur noch $(A \cup B) - C \supseteq A \cup (B - C)$ nachzuweisen. Sei dazu $x \in A \cup (B - C)$. Dann ist $x \in A$

oder $x \in B - C$. Im ersten Fall ist erst recht $x \in A \cup B$ und ferner $x \notin C$, da $x$ wegen der Voraussetzung $A \cap C = \emptyset$ nicht gleichzeitig in $A$ und $C$ liegen kann. Es folgt also $x \in (A \cup B) - C$. Im zweiten Fall ist sicher $x \in B$, also erst recht $x \in A \cup B$, und $x \notin C$. Auch in diesem Fall erhält man also $x \in (A \cup B) - C$.

Sei nun $(A \cup B) - C = A \cup (B - C)$. Wir haben $A \cap C = \emptyset$ zu zeigen. Gäbe es ein $x \in A \cap C$, so wäre $x \in A$ und $x \in C$. Wegen $x \in A$ wäre erst recht $x \in A \cup (B - C) = (A \cup B) - C$, und es ergäbe sich $x \notin C$ im Widerspruch zu $x \in C$. •

**Abschnitt 1.A,** Variante zu **Aufg. 4b)**, p. 5 (1.7.2010):

Für Mengen $A, B, C$ gilt $(A \cup B) - C \subseteq A \cup (B - C)$. – Genau dann gilt $(A \cup B) - C = A \cup (B - C)$, wenn $A \cap C = \emptyset$ ist.

**Beweis:** Wir zeigen zunächst den ersten Teil. Sei $x \in (A \cup B) - C$. Dann ist $x \in A \cup B$ und $x \notin C$. Wegen $x \in A \cup B$ ist $x \in A$ oder $x \in B$. Im ersten Fall ist erst recht $x \in A \cup (B - C)$. Im zweiten Fall folgt $x \in B - C$ und somit ebenfalls $x \in A \cup (B - C)$.

Wir zeigen nun den zweiten Teil: Sei zunächst $A \cap C = \emptyset$. Wir haben dann $(A \cup B) - C = A \cup (B - C)$ zu zeigen. Wegen des ersten Teils ist hierfür nur noch $(A \cup B) - C \supseteq A \cup (B - C)$ nachzuweisen. Sei dazu $x \in A \cup (B - C)$. Dann ist $x \in A$ oder $x \in B - C$. Im ersten Fall ist erst recht $x \in A \cup B$ und ferner $x \notin C$, da $x$ wegen der Voraussetzung $A \cap C = \emptyset$ nicht gleichzeitig in $A$ und $C$ liegen kann. Es folgt also $x \in (A \cup B) - C$. Im zweiten Fall ist sicher $x \in B$, also erst recht $x \in A \cup B$, und $x \notin C$. Auch in diesem Fall erhält man also $x \in (A \cup B) - C$.

Sei nun $(A \cup B) - C = A \cup (B - C)$. Wir haben $A \cap C = \emptyset$ zu zeigen. Gäbe es ein $x \in A \cap C$, so wäre $x \in A$ und $x \in C$. Wegen $x \in A$ wäre erst recht $x \in A \cup (B - C) = (A \cup B) - C$, und es ergäbe sich $x \notin C$ im Widerspruch zu $x \in C$. •

**Abschnitt 1.A,** Variante zu **Aufg. 4d)**, p. 5 (1.7.2010):

Für Mengen $A, B, C$ gilt $A - (B - C) \subseteq (A - B) \cup C$. – Genau dann gilt $A - (B - C) = (A - B) \cup C$, wenn $C \subseteq A$ ist.

**Beweis:** Wir zeigen zunächst den ersten Teil. Sei $x \in A - (B - C)$. Dann ist $x \in A$ und $x \notin B - C$. Wegen $x \notin B - C$ ist $x \notin B$ oder es ist $x \in C$. Im ersten Fall $x \notin B$ ist $x \in A - B$, da ja $x \in A$ war, und somit auch $x \in (A - B) \cup C$. Im zweiten Fall $x \in C$ folgt direkt $x \in (A - B) \cup C$.

Wir zeigen nun den zweiten Teil: Sei zunächst $C \subseteq A$. Wir haben dann $A - (B - C) = (A - B) \cup C$ zu zeigen. Wegen des ersten Teils ist hierfür nur noch $A - (B - C) \supseteq (A - B) \cup C$ nachzuweisen. Sei dazu $x \in (A - B) \cup C$. Dann ist $x \in A - B$ oder $x \in C$. Im ersten Fall $x \in A - B$ ist $x \in A$ und $x \notin B$. Wegen $x \notin B$ ist aber erst recht $x \notin B - C$. Da $x \in A$ ist, folgt also insgesamt $x \in A - (B - C)$. Im zweiten Fall ist $x \in C$, also erst recht $x \in A$ wegen der Voraussetzung $C \subseteq A$. Außerdem ist dann $x \notin B - C$ wegen $x \in C$. Auch im zweiten Fall erhält man also aus diesen beiden Aussagen $x \in A - (B - C)$.

Sei nun $A - (B - C) = (A - B) \cup C$. Wir haben $C \subseteq A$ zu zeigen. Sei dazu $x \in C$. Dann ist erst recht $x \in (A - B) \cup C = A - (B - C)$, also $x \in A$. Es folgt $C \subseteq A$. •

**Abschnitt 1.A, Aufg. 6e)**, p. 5 (1.7.2010):

Für Mengen $A$, $B$ und $C$ zeige man: Aus $A \triangle B = A \triangle C$ folgt stets $B = C$.

**Beweis:** Sei $A \triangle B = A \triangle C$, d.h. $(A \cup B) - (A \cap B) = (A \cup C) - (A \cap C)$. Wir zeigen $B \subseteq C$. Analog folgt dann $C \subseteq B$, da Voraussetzung und Behauptung symmetrisch in $B$ und $C$ sind, und somit $B = C$.

Sei also $x \in B$. Wir unterscheiden zwei Fälle: Im ersten Fall sei auch $x \in A$. Dann ist $x \in A \cup B$ und $x \in A \cap B$, also $x \notin (A \cup B) - (A \cap B) = (A \cup C) - (A \cap C)$. Wegen $x \in A \cup C$ ist dann auch $x \in A \cap C$ und somit $x \in C$. Im zweiten Fall sei $x \notin A$. Dann ist $x \in A \cup B$, aber $x \notin A \cap B$, also $x \in (A \cup B) - (A \cap B) = (A \cup C) - (A \cap C)$ und somit $x \in A \cup C$. Wegen $x \notin A$ folgt wieder $x \in C$. •

**Abschnitt 1.B**, Teil von **Aufg. 4**, p. 11 (1.7.2010):

Man untersuche, ob die Abbildung $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$ mit $f(x, y) := (xy, x + y)$ injektiv, surjektiv bzw. bijektiv ist. – Die entsprechende Aufgabe löse man für $g : \mathbb{R} \times \mathbb{R} - \{(0,0)\} \longrightarrow \mathbb{R} \times \mathbb{R} - \{(0,0)\}$ mit

$$g(x, y) := \left( \frac{x}{x^2 + y^2}, \frac{y}{x^2 + y^2} \right) \quad \text{für alle } (x, y) \in \mathbb{R} \times \mathbb{R} - \{(0,0)\}$$

und gebe im bijektiven Fall die Umkehrabbildung an.

**Lösung:** Wir untersuchen, für welche $(u, v) \in \mathbb{R}^2$ die Gleichung $f(x, y) = (u, v)$, d.h. $xy = u$ und $x + y = v$, lösbar ist bzw. mehrere Lösungen hat. Dies ist äquivalent zu $y = v - x$ und $u = xy = x(v-x) = vx - x^2$. Die Lösungsformel für quadratische Gleichungen liefert als einzig mögliche Lösungen der resultierenden Gleichung $x^2 - vx + u = 0$ die Werte $x = \frac{1}{2}v \pm \frac{1}{2}\sqrt{v^2 - 4u}$. Dies zeigt, dass es bei $v^2 > 4u$ zwei verschiedene Lösungen für $x$ (und dann auch für $y = x - v$) gibt und bei $v^2 < 4u$ überhaupt keine. Daher ist $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$ weder injektiv noch surjektiv. – Direkt zeigt übrigens $f(x, y) = f(y, x)$ für $x \neq y$, dass $f$ nicht injektiv ist. Da sich nach Obigem beispielsweise $(1, 1)$ nicht in der Form $f(x, y)$ schreiben lässt, ist $f$ nicht surjektiv.

Die Abbildung $g$ ist bijektiv, also erst recht injektiv und surjektiv, da sie umkehrbar ist mit $g$ selbst als Umkehrabbildung. Dazu ist nur $g \circ g = \mathrm{id}_{\mathbb{R}\times\mathbb{R}}$ zu zeigen. Dies folgt aber aus

$$(g \circ g)(x, y) = g\Big(\frac{x}{x^2+y^2}\,,\,\frac{y}{x^2+y^2}\Big) =$$

$$= \left(\frac{\frac{x}{x^2+y^2}}{\big(\frac{x}{x^2+y^2}\big)^2 + \big(\frac{y}{x^2+y^2}\big)^2}\,,\,\frac{\frac{y}{x^2+y^2}}{\big(\frac{x}{x^2+y^2}\big)^2 + \big(\frac{y}{x^2+y^2}\big)^2}\right) = \left(\frac{\frac{x}{x^2+y^2}}{\frac{1}{x^2+y^2}}\,,\,\frac{\frac{y}{x^2+y^2}}{\frac{1}{x^2+y^2}}\right) = (x\,,\,y)\,. \qquad \bullet$$

**Abschnitt 1.B**, Variante zu **Aufg. 4**, p. 11 (1.7.2010):

Man zeige, dass die Abbildung $f$ von $\mathbb{R}^2$ auf den Kreis $\mathrm{B}(0\,;1) := \big\{(u, v) \in \mathbb{R}^2 \;\big|\; u^2 + v^2 < 1\big\}$, die durch

$$f(x, y) := \Big(\frac{x}{\sqrt{x^2+y^2+1}}\,,\,\frac{y}{\sqrt{x^2+y^2+1}}\Big)$$

für alle $(x, y) \in \mathbb{R}^2$ definiert wird, bijektiv ist mit der durch

$$g(u, v) := \Big(\frac{u}{\sqrt{1-u^2-v^2}}\,,\,\frac{v}{\sqrt{1-u^2-v^2}}\Big)\,.$$

gegebenen Abbildung $g : \mathrm{B}(0\,;1) \to \mathbb{R}^2$ als Umkehrabbildung.

**Beweis:** Offenbar ist $g(u, v)$ für alle $(u, v) \in \mathrm{B}(0\,;1)$ definiert, und es gilt $f(x, y) \in \mathrm{B}(0\,;1)$ für alle $(x, y) \in R^2$. Wir haben daher nur noch $g \circ f = \mathrm{id}_{\mathbb{R}^2}$ und $f \circ g = \mathrm{id}_{\mathrm{B}(0\,;1)}$ zu zeigen. Für $(x, y) \in \mathbb{R}^2$ bzw. für alle $(u, v) \in \mathrm{B}(0\,;1)$ gilt aber:

$$(g \circ f)(x, y) = g\big(f(x, y)\big) = g\Big(\frac{x}{\sqrt{x^2+y^2+1}}\,,\,\frac{y}{\sqrt{x^2+y^2+1}}\Big)$$

$$= \left(\frac{\frac{x}{\sqrt{x^2+y^2+1}}}{\sqrt{1-\big(\frac{x}{\sqrt{x^2+y^2+1}}\big)^2-\big(\frac{y}{\sqrt{x^2+y^2+1}}\big)^2}}\,,\,\frac{\frac{y}{\sqrt{x^2+y^2+1}}}{\sqrt{1-\big(\frac{x}{\sqrt{x^2+y^2+1}}\big)^2-\big(\frac{y}{\sqrt{x^2+y^2+1}}\big)^2}}\right)$$

$$= \Big(\frac{x}{\sqrt{x^2+y^2+1-x^2-y^2}}\,,\,\frac{y}{\sqrt{x^2+y^2+1-x^2-y^2}}\Big) = (x, y) \qquad \text{und}$$

$$(f \circ g)(u, v) = f\big(g(u, v)\big) = f\Big(\frac{u}{\sqrt{1-u^2-v^2}}\,,\,\frac{v}{\sqrt{1-u^2-v^2}}\Big)$$

$$= \left(\frac{\frac{u}{\sqrt{1-u^2-v^2}}}{\sqrt{\big(\frac{u}{\sqrt{1-u^2-v^2}}\big)^2+\big(\frac{v}{\sqrt{1-u^2-v^2}}\big)^2+1}}\,,\,\frac{\frac{v}{\sqrt{1-u^2-v^2}}}{\sqrt{\big(\frac{u}{\sqrt{1-u^2-v^2}}\big)^2+\big(\frac{v}{\sqrt{1-u^2-v^2}}\big)^2+1}}\right)$$

$$= \Big(\frac{u}{\sqrt{u^2+v^2+1-u^2-v^2}}\,,\,\frac{v}{\sqrt{u^2+v^2+1-u^2-v^2}}\Big) = (u, v)\,. \qquad \bullet$$

**Abschnitt 1.B**, Variante zu **Aufg. 4**, p. 11, vgl. **Abschnitt 2.C, Aufg. 1**, p. 41 (1.7.2010):

Man zeige, dass durch $f(x) := \dfrac{x}{1+|x|}$ für $x \in \mathbb{R}$ eine bijektive Abbildung $f$ von $\mathbb{R}$ auf das Intervall $]-1, 1[\; := \{x \in \mathbb{R} \mid -1 < x < 1\}$ gegeben wird.

**Beweis:** Wegen $|x| < 1+|x|$ für alle $x$ ist stets $|f(x)| < 1$, d.h. $f(x) \in ]-1,1[$. Wir haben zu zeigen, dass es zu jedem $y \in ]-1,1[$ genau ein $x$ mit $y = f(x) = \dfrac{x}{1+|x|}$ gibt. Da $1+|x|$ stets positiv ist, ist aber $y$ in dieser Gleichung genau dann positiv bzw. negativ, wenn dies für $x$ gilt, d.h. stets ist $y|x| = |y|x$. Wegen $y + y|x| = x$ ergibt sich $y + |y|x = x$, $y = x\big(1-|y|\big)$. Zu $y \in ]-1,1[$ gibt es also genau ein $x \in \mathbb{R}$ mit $f(x) = y$, nämlich $x = \dfrac{y}{1-|y|}$. •

**Abschnitt 1.B, Aufg. 5**, p. 11 (1.7.2010):

Seien $a,b,c,d \in \mathbb{R}$ und $f:\mathbb{R}\to\mathbb{R}$, $g:\mathbb{R}\to\mathbb{R}$ die durch $f(x) := ax+b$, $g(x) = cx+d$ definierten Funktionen. Unter welchen Bedingungen ist $f\circ g = g\circ f$?

**Lösung:** Wir zeigen: Genau dann ist $f\circ g = g\circ f$, wenn $ad+b = cb+d$ gilt. Stets ist $(f\circ g)(x) = f\big(g(x)\big) = f(cx+d) = a(cx+d)+b = acx+ad+b$ und analog $(g\circ f)(x) = cax+cb+d$.

Bei $ad+b = cb+d$ gilt daher $(f\circ g)(x) = (g\circ f)(x)$ für alle $x\in\mathbb{R}$ und wegen $ac = ca$ somit $f\circ g = g\circ f$. Umgekehrt sei $(f\circ g)(x) = (g\circ f)(x)$ für alle $x\in\mathbb{R}$. Speziell für $x=0$ ergibt die obige Rechnung dann $ad+b = cb+d$. •

**Abschnitt 1.B, Aufg. 7a)**, p. 12 (1.7.2010):

Seien $f:A\to B$ und $g:B\to C$ Abbildungen. Ist $g\circ f:A\to C$ injektiv, so ist $f$ injektiv.

**Beweis:** Sei $g\circ f:A\to C$ injektiv. Für Elemente $x,y\in A$ mit $f(x) = f(y)$ gilt erst recht $(g\circ f)(x) = g\big(f(x)\big) = g\big(f(y)\big) = (g\circ f)(y)$. Da $g\circ f$ injektiv ist, liefert dies bereits $x = y$. •

**Bemerkung.** $g$ muss nicht unbedingt injektiv sein, wenn $g\circ f:A\to C$ injektiv ist. Für $A$ und $C$ nehmen wir bespielsweise die Menge, die nur aus der Zahl 1 besteht, und für $B$ die Menge $\{1,2\}$. Die Abbildung $f:A\to B$ definieren wir durch $f(1) := 1 \in B$ und die Abbildung $g:B\to C$ durch $g(1) := 1$, $g(2) := 1$. Dann ist $g\circ f:A\to C$ diejenige Abbildung, die das einzige Element 1 von $A$ auf das einzige Element 1 von $C$ abbildet, d.h. die Identität von $\{1\}$, und somit injektiv. Die Abbildung $g$ ist jedoch nicht injektiv, da sie die Elemente 1 und 2 von $B$ beide auf dasselbe Element 1 von $C$ abbildet.

**Abschnitt 1.B, Aufg. 7b)**, p. 12 (1.7.2010):

Seien $f:A\to B$ und $g:B\to C$ Abbildungen. Ist $g\circ f:A\to C$ surjektiv, so ist $g$ surjektiv.

**Beweis:** Sei $g\circ f:A\to C$ surjektiv, und sei $c\in C$. Dann gibt es ein $a\in A$ mit $(g\circ f)(a) = c$, also mit $g(b) = g\big(f(a)\big) = c$ für $b := f(a)$. Dies beweist, dass $g$ surjektiv ist. •

**Bemerkung.** $f$ muss nicht unbedingt surjektiv sein, wenn $g\circ f:A\to C$ surjektiv ist. Für $A$ und $C$ nehmen wir bespielsweise die Menge, die nur aus der Zahl 1 besteht, und für $B$ die Menge $\{1,2\}$. Die Abbildung $f:A\to B$ definieren wir durch $f(1) := 1\in B$ und die Abbildung $g:B\to C$ durch $g(1) := 1$, $g(2) := 1$. Dann ist $g\circ f:A\to C$ diejenige Abbildung, die das einzige Element 1 von $A$ auf das einzige Element 1 von $C$ abbildet, d.h. die Identität von $\{1\}$, und somit surjektiv. Die Abbildung $f$ ist jedoch nicht surjektiv, da kein Element von $A$ durch $f$ auf das Element 2 von $B$ abgebildet wird.

**Abschnitt 1.C, Aufg. 3)**, p. 15 (1.9.2010):

Seien $A$, $I$ und $J$ Mengen. Die Abbildung $f \mapsto \big(j \mapsto (i \mapsto f(i,j))\big)$ ist eine bijektive Abbildung von $A^{I\times J}$ auf $(A^I)^J$.

**1. Beweis:** Es ist zu zeigen, dass die Abbildung $F: A^{I\times J} \to (A^I)^J$ bijektiv ist, die jedem $f\in A^{I\times J}$, also jeder Abbildung $f: I\times J\to A$, die Abbildung $F(f): J\to A^I$ zuordnet, die dadurch definiert ist, dass sie jeweils $j\in J$ auf die Abbildung $\big(F(f)\big)(j): I\to A$ abbildet, die durch $\Big(\big(F(f)\big)(j)\Big)(i) := f(i,j)$ für alle $i\in I$ erklärt ist. $F$ ist bijektiv, wenn $F$ injektiv und surjektiv ist.

Wir beweisen zunächst, dass $F$ injektiv ist. Dazu betrachten wir $f, f'\in A^{I\times J}$ mit $F(f) = F(f')$ und haben $f = f'$ zu zeigen. Wegen $F(f) = F(f')$ gilt aber $\big(F(f)\big)(j) = \big(F(f')\big)(j)$ für alle $j\in J$ und dann auch $\Big(\big(F(f)\big)(j)\Big)(i) = \Big(\big(F(f')\big)(j)\Big)(i)$ für alle $j\in J$ und alle $i\in I$. Es folgt $f(i,j) = f'(i,j)$ für alle $j\in J$ und alle $i\in I$, d.h. $f = f'$.

Wir beweisen nun, dass $F$ surjektiv ist. Dazu betrachten wir $g\in (A^I)^J$ und haben ein $f\in A^{I\times J}$ anzugeben mit $F(f) = g$. Definieren wir $f: I\times J\to A$ durch $f(i,j) := \big(g(j)\big)(i)$ für alle $j\in J$ und alle $i\in I$, so ist in der Tat $\Big(\big(F(f)\big)(j)\Big)(i) = f(i,j) = \big(g(j)\big)(i)$ für alle $i,j$, also $(F(f))(j) = g(j)$ und $F(f) = g$. •

**2. Beweis:** Wir verwenden Satz 1.B.10 und zeigen, dass für die im 1. Beweis eingeführte Abbildung $F$ und die Abbildung $G:(A^I)^J \to A^{I\times J}$, die für $g \in (A^I)^J$ durch $\big(G(g)\big)(i,j) := \big(g(j)\big)(i)$, $i\in I$, $j\in J$, definiert ist, gilt: $G\circ F = \mathrm{id}_{A^{I\times J}}$ und $F\circ G = \mathrm{id}_{(A^I)^J}$. Dann ist $F$ umkehrbar (mit Umkehrabbildung $G$) und somit bijektiv.

Für $f \in A^{I\times J}$ und beliebige Elemente $i\in I$, $j\in J$ gilt nun $\big((G\circ F)(f)\big)(i,j) = \big(G\big(F(f)\big)\big)(i,j) = \big(\big(F(f)\big)(j)\big)(i) = f(i,j)$, also $(G\circ F)(f) = f$, und somit $G\circ F = \mathrm{id}_{A^{I\times J}}$.

Für $g \in (A^I)^J$ und beliebige Elemente $i\in I$, $j\in J$ gilt ferner $\big(\big((F\circ G)(g)\big)(j)\big)(i) = \big(\big(F\big(G(f)\big)\big)(j)\big)(i) = \big(G(g)\big)(i,j) = \big(g(j)\big)(i)$, also $\big((F\circ G)(g)\big)(j) = g(j)$, folglich $(F\circ G)(g) = g$, und somit schließlich $F\circ G = \mathrm{id}_{(A^I)^J}$. •

## 2 Die natürlichen Zahlen

**Abschnitt 2.A**, Teil von **Aufg. 1**, p. 24 (1.7.2010) :

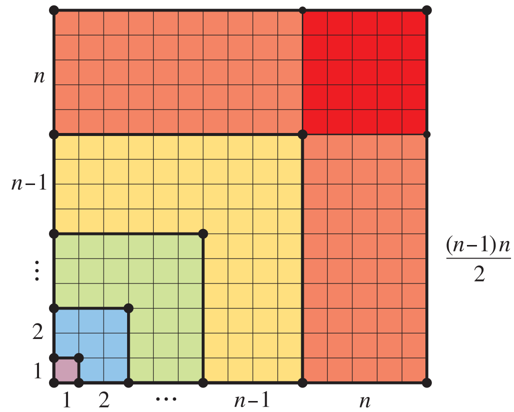
Für alle $n \in \mathbb{N}$ gilt $\displaystyle\sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2$.

**Beweis:** *Induktionsanfang*: Für $n=0$ steht auf der linken Seite die leere Summe $\displaystyle\sum_{k=1}^{0} k^3$, also 0. Dies ist auch der Wert der rechten Seite für $n=0$. (Für $n=1$ ist die Aussage ebenfalls trivialerweise richtig, da die linke Seite $\displaystyle\sum_{k=1}^{1} k^3 = 1^3$ und die rechte Seite $\left(\dfrac{1\cdot(1+1)}{2}\right)^2$ beide gleich 1 sind.)

*Induktionsschluss* (von $n$ auf $n+1$) : Nach Induktionsvoraussetzung gilt $\displaystyle\sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2$. Daraus ergibt sich die Induktionsbehauptung, d.h. die Aussage mit $n+1$ statt $n$. Man erhält nämlich

$$\sum_{k=1}^{n+1} k^3 = (n+1)^3 + \sum_{k=0}^{n} k^3 = (n+1)^3 + \left(\frac{n(n+1)}{2}\right)^2 = (n+1)^2\left(n+1+\frac{n^2}{4}\right) =$$
$$= (n+1)^2\frac{(n+2)^2}{4} = \left(\frac{(n+1)(n+2)}{2}\right)^2 . \qquad \bullet$$

**Bemerkung.** Man beachte, dass $\dfrac{n(n+1)}{2}$ die Summe $\displaystyle\sum_{k=1}^{n} k$ der ersten $n$ positiven natürlichen Zahlen ist. Es ist also $1^3+2^3+\cdots+n^3 = (1+2+\cdots+n)^2$. Dies ergibt sich wegen $2\cdot n\cdot\dfrac{(n-1)n}{2}+n^2=n^3$ auch direkt aus folgendem Bild:




Man kann die Formel auch folgendermaßen gewinnen: Man summiert beide Seiten der Identität $(k+1)^4 = k^4+4k^3+6k^2+4k+1$ von $k=1$ bis $k=n$, lässt die vierten Potenzen $2^4, 3^4, \ldots, n^4$ weg und benutzt die bereits bekannten Formeln

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2} \quad \text{und} \quad \sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6},$$

um nach $\displaystyle\sum_{k=1}^{n} k^3$ aufzulösen. Dies ergibt

$$\sum_{k=1}^{n}(k+1)^4 = \sum_{k=1}^{n}k^4 + 4\sum_{k=1}^{n}k^3 + 6\sum_{k=1}^{n}k^2 + 4\sum_{k=1}^{n}k + \sum_{k=1}^{n}1 =$$

$$= \sum_{k=1}^{n}k^4 + 4\sum_{k=1}^{n}k^3 + \frac{6n(n+1)(2n+1)}{6} + \frac{4n(n+1)}{2} + n\,,$$

$$(n+1)^4 = 1 + 4\sum_{k=1}^{n}k^3 + (n+1)\big(n(2n+1)+2n\big) + n\,,$$

$$\sum_{k=1}^{n}k^3 = \frac{1}{4}\Big((n+1)^4 - 1 - (n+1)\big(n(2n+1)+2n\big) - n\Big) =$$

$$= \frac{1}{4}\Big((n+1)^4 - (n+1)\big(n(2n+1)+2n+1\big)\Big) = \frac{1}{4}\big((n+1)^4 - (n+1)^2(2n+1)\big) =$$

$$= \frac{(n+1)^2\big((n+1)^2-(2n+1)\big)}{4} = \Big(\frac{n(n+1)}{2}\Big)^2. \qquad \bullet$$

Das letzte Verfahren systematisch durchgeführt, liefert Formeln für alle Summen $\sum_{k=1}^{n}k^m$, $m\in\mathbb{N}^*$. Dies ist kurz vor Beispiel 12.C.10 ausgeführt.

**Abschnitt 2.A**, **Aufg. 2d)**, p. 24 (1.7.2010) :

Für alle $n\in\mathbb{N}$ ist $\sum_{k=1}^{n}(2k-1)^2 = \frac{n}{3}(2n-1)(2n+1) = \frac{n}{3}(4n^2-1)$ .

**Beweis:** *Induktionsanfang*: Für $n=0$ ist die Aussage richtig, da $\sum_{k=1}^{0}(2k-1)^2$ die leere Summe, also gleich 0 ist, und die rechte Seite ebenfalls 0 ist. Natürlich prüft man auch leicht, dass die Gleichung für $n=1$ stimmt. *Induktionsschluss* (von $n$ auf $n+1$) : Nach Induktionsvoraussetzung gilt $\sum_{k=1}^{n}(2k-1)^2 = \frac{n}{3}(2n-1)(2n+1)$ . Daraus ergibt sich die Induktionsbehauptung, d.h. die Aussage mit $n+1$ statt $n$. Man erhält nämlich

$$\sum_{k=1}^{n+1}(2k-1)^2 = \Big(\sum_{k=1}^{n}(2k-1)^2\Big) + (2n+1)^2 = \frac{n}{3}(2n-1)(2n+1) + (2n+1)^2 =$$

$$= \frac{1}{3}(2n+1)\big(n(2n-1)+3(2n+1)\big) = \frac{1}{3}(2n+1)(2n^2+5n+3) = \frac{n+1}{3}\big(2(n+1)-1\big)\big(2(n+1)+1\big)\,. \qquad \bullet$$

**Abschnitt 2.A**, **Aufg. 2e)**, p. 24 (1.7.2010) :

Für alle $n\in\mathbb{N}$ gilt $\sum_{k=1}^{n}k(k+1) = \frac{1}{3}n(n+1)(n+2)$ .

**Beweis:** *Induktionsanfang*: Für $n=0$ ist $\sum_{k=1}^{0}k(k+1)$ wieder die leere Summe, also 0 wie die rechte Seite.

*Induktionsschluss* (von $n$ auf $n+1$) : Nach Induktionsvoraussetzung gilt $\sum_{k=1}^{n}k(k+1) = \frac{1}{3}n(n+1)(n+2)$ . Daraus ergibt sich die Induktionsbehauptung, d.h. die Aussage mit $n+1$ statt $n$. Es ist nämlich

$$\sum_{k=1}^{n+1}k(k+1) = (n+1)(n+2) + \sum_{k=1}^{n}k(k+1) = (n+1)(n+2) + \frac{1}{3}n(n+1)(n+2) =$$

$$= (n+1)(n+2)\big(1+\frac{n}{3}\big) = \frac{1}{3}(n+1)(n+2)(n+3)\,. \qquad \bullet$$

**Abschnitt 2.A**, **Aufg. 3a)**, p. 24 (1.7.2010) :

Für alle $n \in \mathbb{N}$ gilt $\displaystyle\sum_{k=1}^{n} \frac{1}{k(k+1)} = 1 - \frac{1}{n+1}$ .

**Beweis:** *Induktionsanfang*: Für $n=0$ gilt die Aussage trivialerweise (ebenso für $n=1$) .

*Induktionsschluss* (von $n$ auf $n+1$) : Nach Induktionsvoraussetzung gilt $\displaystyle\sum_{k=1}^{n} \frac{1}{k(k+1)} = 1 - \frac{1}{n+1}$ . Daraus ergibt sich die Induktionsbehauptung, d.h. die Aussage mit $n+1$ statt $n$. Es ist nämlich $\displaystyle\sum_{k=1}^{n+1} \frac{1}{k(k+1)} =$

$$\frac{1}{(n+1)(n+2)} + \sum_{k=1}^{n} \frac{1}{k(k+1)} = \frac{1}{(n+1)(n+2)} + 1 - \frac{1}{n+1} = 1 - \frac{(n+2)-1}{(n+1)(n+2)} = 1 - \frac{1}{n+2} . \qquad \bullet$$

**Abschnitt 2.A**, Variante zu **Aufg. 3a) , b)**, p. 24 (1.7.2010) :

Für alle $n \in \mathbb{N}$ gilt $\displaystyle\sum_{k=1}^{n} \frac{1}{(3k-2)(3k+1)} = \frac{n}{3n+1}$ .

**Beweis:** *Induktionsanfang*: Für $n=0$ gilt die Aussage trivialerweise (ebenso für $n=1$) .

*Induktionsschluss* (von $n$ auf $n+1$) : Nach Induktionsvoraussetzung gilt $\displaystyle\sum_{k=1}^{n} \frac{1}{(3k-2)(3k+1)} = \frac{n}{3n+1}$ . Daraus ergibt sich die Induktionsbehauptung , d.h. die Aussage mit $n+1$ statt $n$, wegen

$$\sum_{k=1}^{n+1} \frac{1}{(3k-2)(3k+1)} = \frac{1}{(3(n+1)-2)(3(n+1)+1)} + \sum_{k=1}^{n} \frac{1}{(3k-2)(3k+1)} = \frac{1}{(3n+1)(3n+4)} + \frac{n}{3n+1} =$$
$$= \frac{1}{(3n+1)} \cdot \frac{1+(3n+4)\,n}{3n+4} = \frac{3n^2+4n+1}{(3n+1)(3n+4)} = \frac{(3n+1)(n+1)}{(3n+1)\big(3(n+1)+1\big)} = \frac{n+1}{3(n+1)+1} . \qquad \bullet$$

Man kann die Formel auch durch eine so genannte Partialbruchzerlegung gewinnen, indem man rationale Zahlen $a, b$ mit $\displaystyle\frac{1}{(3k-2)(3k+1)} = \frac{a}{3k-2} + \frac{b}{3k+1} = \frac{(3a+3b)k + a - 2b}{(3k-2)(3k+1)}$ bestimmt. Dies gilt sicher für alle $k$, wenn die Bedingungen $3a+3b=0$ und $a-2b=1$ erfüllt sind. Die erste dieser Gleichungen liefert $b=-a$; eingesetzt in die zweite ergibt das $a+2a=1$, d. h. $a=\frac{1}{3}$ und $b=-\frac{1}{3}$ . Nun verwendet man einen so genannten Teleskoptrick, d.h. die Tatsache, dass sich die meisten Summanden wegheben in

$$\sum_{k=1}^{n} \frac{1}{(3k-2)(3k+1)} = \frac{1}{3} \sum_{k=1}^{n} \Big(\frac{1}{3k-2} - \frac{1}{3k+1}\Big) =$$
$$= \frac{1}{3}\Big(\frac{1}{1} - \frac{1}{4} + \frac{1}{4} - \frac{1}{7} + \cdots + \frac{1}{3n-5} - \frac{1}{3n-2} + \frac{1}{3n-2} - \frac{1}{3n+1}\Big) = \frac{1}{3}\Big(1 - \frac{1}{3n+1}\Big) = \frac{n}{3n+1} . \qquad \bullet$$

**Abschnitt 2.A**, **Aufg. 4a)**, p. 25 (1.7.2010) :

Für alle $n \geq 1$ gilt $\displaystyle\prod_{k=2}^{n} \Big(1 - \frac{1}{k^2}\Big) = \frac{1}{2}\Big(1 + \frac{1}{n}\Big)$ .

**Beweis:** *Induktionsanfang*: Für $n=1$ ist die Aussage richtig, da $\displaystyle\prod_{k=2}^{1} \big(1 - \frac{1}{k^2}\big)$ das leere Produkt, also 1, ist und die rechte Seite $\displaystyle\frac{1}{2}\big(1 + \frac{1}{1}\big) = 1$ ebenfalls 1 ist.

*Induktionsschluss* (von $n$ auf $n+1$) : Nach Induktionsvoraussetzung gilt $\displaystyle\prod_{k=2}^{n} \Big(1 - \frac{1}{k^2}\Big) = \frac{1}{2}\Big(1 + \frac{1}{n}\Big)$ .

Daraus ergibt sich die Induktionsbehauptung, d.h. die Aussage mit $n+1$ statt $n$, wegen $\prod_{k=2}^{n+1}\Big(1-\frac{1}{k^2}\Big) =$
$$\Big(1-\frac{1}{(n+1)^2}\Big)\prod_{k=2}^{n}\Big(1-\frac{1}{k^2}\Big)=\Big(1-\frac{1}{(n+1)^2}\Big)\frac{1}{2}\Big(1+\frac{1}{n}\Big)=\frac{n^2+2n}{(n+1)^2}\cdot\frac{n+1}{2n}=\frac{1}{2}\Big(1+\frac{1}{n+1}\Big).$$ •

**Abschnitt 2.A, Aufg. 4b)**, p. 25 (1.7.2010) :

Für alle $n\geq 1$ ist $\prod_{k=2}^{n}\Big(1-\frac{2}{k(k+1)}\Big)=\frac{1}{3}\Big(1+\frac{2}{n}\Big)$ . **Beweis:** *Induktionsanfang*: Für $n=1$ ist die Aussage trivial.

*Induktionsschluss* (von $n$ auf $n+1$) : Nach Induktionsvoraussetzung gilt $\prod_{k=2}^{n}\Big(1-\frac{2}{k(k+1)}\Big)=\frac{1}{3}\Big(1+\frac{2}{n}\Big)$. Daraus ergibt sich die Induktionsbehauptung, d.h. die Aussage mit $n+1$ statt $n$, wegen
$$\prod_{k=2}^{n+1}\Big(1-\frac{2}{k(k+1)}\Big)=\Big(1-\frac{2}{(n+1)(n+2)}\Big)\cdot\prod_{k=2}^{n}\Big(1-\frac{2}{k(k+1)}\Big)=\Big(1-\frac{2}{(n+1)(n+2)}\Big)\cdot\frac{1}{3}\Big(1+\frac{2}{n}\Big)=$$
$$=\frac{n^2+3n+2-2}{(n+1)(n+2)}\cdot\frac{n+2}{3n}=\frac{n+3}{3(n+1)}=\frac{1}{3}\Big(1+\frac{2}{n+1}\Big).$$ •

**Abschnitt 2.A**, **Aufg. 4c)**, p. 25 (1.7.2010) :

Für alle $n\geq 1$ gilt $\prod_{k=2}^{n}\frac{k^3-1}{k^3+1}=\frac{2}{3}\,\Big(1+\frac{1}{n(n+1)}\Big)$ .

**Beweis:** *Induktionsanfang*: Für $n=1$ ist die Aussage trivial

*Induktionsschluss* (von $n$ auf $n+1$) : Nach Induktionsvoraussetzung gilt $\prod_{k=2}^{n}\frac{k^3-1}{k^3+1}=\frac{2}{3}\,\Big(1+\frac{1}{n(n+1)}\Big)$ . Daraus ergibt sich die Induktionsbehauptung, d.h. die Aussage mit $n+1$ statt $n$, wegen
$$\prod_{k=2}^{n+1}\frac{k^3-1}{k^3+1}=\frac{(n+1)^3-1}{(n+1)^3+1}\cdot\prod_{k=2}^{n}\frac{k^3-1}{k^3+1}=\frac{(n+1)^3-1}{(n+1)^3+1}\cdot\frac{2}{3}\,\Big(1+\frac{1}{n(n+1)}\Big)=\frac{2}{3}\,\frac{n^3+3n^2+3n}{n^3+3n^2+3n+2}\,\frac{n^2+n+1}{n(n+1)}$$
$$=\frac{2}{3}\,\frac{n(n^2+3n+3)}{(n+2)(n^2+n+1)}\,\frac{n^2+n+1}{n(n+1)}=\frac{2}{3}\,\frac{n^2+3n+3}{(n+1)(n+2)}=\frac{2}{3}\Big(1+\frac{1}{(n+1)(n+2)}\Big)\,.$$ •

**Abschnitt 2.A**, **Aufg. 6f)**, p. 25 (1.7.2010) :

Für alle $n\in\mathbb{N}$ ist 3 ein Teiler von $2^{2n}-1=4^n-1$ (d.h. es gibt eine ganze Zahl $a$ mit $4^n-1=3a$).

**Beweis:** Wir verwenden Induktion über $n$. Bei $n=0$ ist in der Tat $4^0-1=0$ durch 3 teilbar. Beim Schluss von $n$ auf $n+1$ können wir voraussetzen, dass es ein $a\in\mathbb{Z}$ gibt mit $4^n-1=3a$. Dann ist aber $4^{n+1}-1=4^{n+1}-4^n+4^n-1=(4-1)4^n+3a=3(4^n+a)$ ebenfalls durch 3 teilbar. (Man hätte auch direkt mit der geometrischen Reihe schließen können: $4^n-1=(4-1)(4^{n-1}+4^{n-2}+\cdots+4+1)$ . ) •

**Abschnitt 2.A**, Variante zu **Aufg. 6**, p. 25 (1.7.2010) :

Für alle $n\in\mathbb{N}$ gilt: 6 teilt $n^3+5n$.

**Beweis:** Wir verwenden Induktion über $n$. *Induktionsanfang*: Für $n=0$ ist dies richtig, da $0^3+5\cdot 0=0$ durch 6 teilbar ist.

*Induktionsschluss* (von $n$ auf $n+1$): Nach Induktionsvoraussetzung ist $n^3+5n$ durch 6 teilbar, d.h. es gibt ein $k\in\mathbb{N}$ mit $n^3+5n=6k$. Daraus ergibt sich die Induktionsbehauptung: Der Ausdruck $(n+1)^3+5(n+1)=n^3+3n^2+3n+1+5n+5=n^3+5n+3n^2+3n+6=6(k+1)+3n(n+1)$ für $n+1$ statt $n$ ist nämlich auch durch 6 teilbar, da von den beiden aufeinanderfolgenden Zahlen $n$ und $n+1$ eine noch durch 2 teilbar ist. •

**Abschnitt 2.B, Aufg. 1c)**, p. 33 (1.7.2010):

Man zeige $3^n \le (n+1)!$ für alle $n \in \mathbb{N}$, $n \neq 1, 2, 3$.

**Beweis:** *Induktionsanfang* $(n=4)$: Für $n=4$ ist $3^4 = 81 \le 120 = (4+1)!$ richtig.

Beim *Induktionsschluss* von $n$ auf $n+1$ liefert die Induktionsvoraussetzung $3^n \le (n+1)!$. Daraus folgt die Induktionsbehauptung: Für $n \ge 4$ (sogar für alle $n \ge 1$) ist nämlich $3 \le n+2$ und somit $3^{n+1} = 3 \cdot 3^n \le 3 \cdot (n+1)! \le (n+2) \cdot (n+1)! = (n+2)!$. •

**Abschnitt 2.B, Aufg. 2b)**, p. 33 (1.7.2010):

Man begründe für $n \in \mathbb{N}$ die Formel $\binom{-\frac12}{n} = (-1)^n \dfrac{1 \cdot 3 \cdots (2n-1)}{2 \cdot 4 \cdots (2n)} = \left(\dfrac{-1}{4}\right)^n \binom{2n}{n}$.

**Lösung:** Nach Definition gilt

$$\begin{aligned}\binom{-\frac12}{n} &= \frac{(-\frac12)\cdot(-\frac12-1)\cdots(-\frac12-n+1)}{1\cdot 2\cdots n} = \frac{(-\frac12)\cdot(-\frac32)\cdots(-\frac{2n-1}{2})}{1\cdot 2\cdots n} = \frac{(-1)^n}{2^n}\,\frac{1\cdot 3\cdots(2n-1)}{1\cdot 2\cdots n}\\ &= (-1)^n\,\frac{1\cdot 3\cdots(2n-1)}{2\cdot 4\cdots(2n)} = (-1)^n\,\frac{(2n)!}{(2\cdot 4\cdots(2n))^2} = \left(\frac{-1}{4}\right)^n\frac{(2n)!}{(n!)^2} = \left(\frac{-1}{4}\right)^n\binom{2n}{n}.\end{aligned}$$ •

**Abschnitt 2.B, Aufg. 2c)**, p. 33 (1.7.2010):

Man begründe für $n \in \mathbb{N}$ die Formel $\binom{\frac12}{n} = \dfrac{1}{2n}\binom{-\frac12}{n-1} = \dfrac{(-1)^{n-1}}{2n}\,\dfrac{1\cdot 3\cdots(2n-3)}{2\cdot 4\cdots(2n-2)} = \dfrac{-1}{2n-1}\binom{2n}{n}$.

**Lösung:** Nach Definition gilt unter Verwendung von Aufg. 2.b)

$$\begin{aligned}\binom{\frac12}{n} &= \frac{(\frac12)\cdot(\frac12-1)\cdots(\frac12-n+1)}{1\cdot 2\cdots n} = \frac{1}{2n}\,\frac{(-\frac12)\cdot(-\frac32)\cdots(-\frac{2n-3}{2})}{1\cdot 2\cdots(n-1)} = \frac{1}{2n}\binom{-\frac12}{n-1}\\ &= \frac{1}{2n}\,(-1)^{n-1}\,\frac{1\cdot 3\cdots(2n-3)}{1\cdot 2\cdots(2n-2)} = \frac{-1}{2n-1}\,(-1)^n\,\frac{1\cdot 3\cdots(2n-1)}{2\cdot 4\cdots(2n)} = \frac{-1}{2n-1}\left(\frac{-1}{4}\right)^n\binom{2n}{n}.\end{aligned}$$ •

**Abschnitt 2.B, Aufg. 3b)**, p. 33 (1.7.2010):

Für alle $\alpha \in \mathbb{R}$ (oder $\mathbb{C}$) und $n \in \mathbb{N}$ gilt: $n\binom{\alpha}{n} + (n+1)\binom{\alpha}{n+1} = \alpha\binom{\alpha}{n}$.

**Beweis:** In der Tat ist

$$\begin{aligned} n\binom{\alpha}{n} + (n+1)\binom{\alpha}{n+1} &= n\,\frac{\alpha(\alpha-1)\cdots(\alpha-n+1)}{n!} + (n+1)\,\frac{\alpha(\alpha-1)\cdots(\alpha-n+1)(\alpha-n)}{(n+1)!} =\\ &= \left(n + (n+1)\,\frac{\alpha-n}{n+1}\right)\frac{\alpha(\alpha-1)\cdots(\alpha-n+1)}{n!} =\\ &= (n+\alpha-n)\binom{\alpha}{n} = \alpha\binom{\alpha}{n}.\end{aligned}$$ •

**Abschnitt 2.B, Aufg. 4c)**, p. 33 (1.7.2010):

Man beweise durch vollständige Induktion über $n$ die Formel $\displaystyle\sum_{k=m}^{n}\binom{k}{m} = \binom{n+1}{m+1}$, $m \in \mathbb{N}$, $m \le n$.

**Beweis:** *Induktionsanfang* $(n=m)$: $\displaystyle\sum_{k=m}^{m}\binom{k}{m} = \binom{m}{m} = 1$ und $\displaystyle\binom{m+1}{m+1} = 1$ sind offenbar gleich.

Beim *Induktionsschluss* von $n$ auf $n+1$ können wir die Aussage für $n$ voraussetzen und erhalten damit unter Verwendung der Formel vom Pascalschen Dreieck die Aussage für $n+1$ statt $n$:

$$\sum_{k=m}^{n+1}\binom{k}{m} = \left(\sum_{k=m}^{n}\binom{k}{m}\right) + \binom{n+1}{m} = \binom{n+1}{m+1} + \binom{n+1}{m} = \binom{n+2}{m+1}.$$ •

**Abschnitt 2.B**, **Aufg. 4d)**, p. 33 (1.7.2010) :

Man beweise durch vollständige Induktion für alle $n \in \mathbb{N}$: $\sum_{k=0}^{n}(-1)^k\binom{\alpha}{k} = (-1)^n\binom{\alpha-1}{n}$, $\alpha \in \mathbb{R}$.

**Beweis:** *Induktionsanfang* $(n=0)$: $\sum_{k=0}^{0}(-1)^j\binom{\alpha}{k} = (-1)^0\binom{\alpha}{0} = 1$ und $(-1)^0\binom{\alpha-1}{0} = 1\cdot 1 = 1$ sind gleich. Beim *Induktionsschluss* von $n$ auf $n+1$ können wir die Aussage für $n$ voraussetzen und erhalten so mit der Formel $\binom{\alpha-1}{n}+\binom{\alpha-1}{n+1}=\binom{\alpha}{n+1}$ die Aussage für $n+1$ statt $n$:

$$\sum_{k=0}^{n+1}(-1)^k\binom{\alpha}{k} = \left(\sum_{k=0}^{n}(-1)^k\binom{\alpha}{k}\right) + (-1)^{n+1}\binom{\alpha}{n+1} = (-1)^n\binom{\alpha-1}{n} + (-1)^{n+1}\binom{\alpha}{n+1} =$$
$$= (-1)^{n+1}\left(-\binom{\alpha-1}{n}+\binom{\alpha}{n+1}\right) = (-1)^{n+1}\binom{\alpha-1}{n+1}\,.$$

•

**Abschnitt 2.B**, **Aufg. 5b)** und Varianten davon, p. 33 (1.7.2010) :

Man berechne für $n \in \mathbb{N}$ die Summen $\sum_{m=0}^{n}(-1)^m\binom{n}{m}$, $\sum_{m=0}^{n}2^m\binom{n}{m}$, $\sum_{m=0}^{n}(-2)^{n-m}\binom{n}{m}$.

**Lösung:** Der binomische Lehrsatz liefert $\sum_{m=0}^{n}(-1)^m\binom{n}{m} = \sum_{m=0}^{n}\binom{n}{m}1^{n-m}(-1)^m = \big(1+(-1)\big)^n = 0$, $\sum_{m=0}^{n}2^m\binom{n}{m} = \sum_{m=0}^{n}\binom{n}{k}1^{n-m}2^m = (1+2)^n = 3^n$, $\sum_{m=0}^{n}(-2)^{n-m}\binom{n}{m} = \sum_{m=0}^{n}\binom{n}{m}(-2)^{n-m}1^m = \big(-2+1\big)^n = (-1)^n$. •

**Abschnitt 2.B**, **Aufg. 7**, p. 34 (1.7.2010) :

Sei $A$ eine endliche Menge mit $n$ Elementen und $B$ eine Teilmenge von $A$ mit $k$ Elementen. Man zeige, dass die Anzahl der $m$-elementigen Teilmengen von $A$, die $B$ umfassen, gleich $\binom{n-k}{m-k}$ ist.

**Beweis** Wir suchen die Anzahl derjenigen Teilmengen von $A$, die $B$ zu einer $m$-elementigen Teilmenge ergänzen. Es handelt sich also um die Anzahl der $(m-k)$-elementigen Teilmengen der $(n-k)$-elementigen Menge $A-B$. Diese ist aber gleich $\binom{n-k}{m-k}$. •

**Abschnitt 2.B**, **Aufg. 8**, p. 34 (1.7.2010) :

Für natürliche Zahlen $m, n$ mit $m \le n$ zeige man $\sum_{k=0}^{m}\binom{n}{k}\binom{n-k}{m-k} = 2^m\binom{n}{m}$.

**1. Beweis:** Wir bestimmen die Anzahl der Paare $(B, C)$ von Teilmengen $B, C$ einer $n$-elementigen Menge $A$ mit $B \subseteq C$ auf zweierlei Weise:
Zählen wir einerseits zunächst zu jeder $k$-elementigen Teilmenge $B$ von $A$ die Anzahl der $B$ umfassenden Teilmengen $C$ von $A$ mit $m$ Elementen, so erhalten wir nach Aufgabe 7 $\binom{n-k}{m-k}$. Da es $\binom{n}{k}$ solcher Teilmengen $B$ von $A$ gibt und ihre Elementezahl $k$ beliebig zwischen 0 und $m$ variieren kann, erhalten wir so insgesamt $\sum_{k=0}^{m}\binom{n}{k}\binom{n-k}{m-k}$ Möglichkeiten für die Anzahl der Paare $(B, C)$.
Andererseits bestimmen wir zunächst zu jeder $m$-elementigen Teilmenge $C$ von $A$ die Anzahl $2^m$ ihrer Teilmengen $B$ und berücksichtigen dann, dass es genau $\binom{n}{m}$ solcher Teilmengen $C$ von $A$ gibt. So erhalten wir insgesamt $2^m\binom{n}{m}$ Möglichkeiten für die Anzahl der Paare $(B, C)$. Da wir beide Male dieselbe Menge abgezählt haben, ergibt sich die obige Formel. •

**2. Beweis:** Zunächst gilt

$$\binom{n}{k}\binom{n-k}{m-k}=\frac{n!}{k!\,(n-k)!}\,\frac{(n-k)!}{(m-k)!\,(n-m)!}=\frac{n!}{k!\,(m-k)!\,(n-m)!}=\frac{n!}{m!\,(n-m)!}\,\frac{m!}{k!\,(m-k)!}=\binom{n}{m}\binom{m}{k}.$$

Wegen $\sum_{k=0}^{m}\binom{m}{k}=(1+1)^m=2^m$ folgt $\sum_{k=0}^{m}\binom{n}{k}\binom{n-k}{m-k}=\sum_{k=0}^{m}\binom{n}{m}\binom{m}{k}=\binom{n}{m}\sum_{k=0}^{m}\binom{m}{k}=2^m\binom{n}{m}$. •

**Abschnitt 2.B**, **Aufg. 9**, p. 34 (1.7.2010) :

Für $m, n, k \in \mathbb{N}$ beweise man $\sum_{j=0}^{k}\binom{m}{j}\binom{n}{k-j}=\binom{m+n}{k}$.

**1. Beweis:** Man zählt diejenigen Teilmengen einer $(m+n)$-elementigen Menge $\{x_1, \ldots, x_m, y_1, \ldots, y_n\}$, die $k$ Elemente enthalten, auf zweierlei Weise ab. Es gibt $\binom{n+m}{k}$ Möglichkeiten, aus den vorhandenen $n+m$ Elementen genau $k$ auszuwählen. Achtet man aber darauf, ob es sich um Elemente von $\{x_1, \ldots, x_n\}$ oder von $\{y_1, \ldots, y_n\}$ handelt, so gibt es für jedes $j \le k$ zunächst genau $\binom{m}{j}$ Möglichkeiten, $j$ der Elemente $x_1, \ldots, x_m$ auszuwählen, und dann genau $\binom{n}{k-j}$ aus $\{y_1, \ldots, y_n\}$ die restlichen $k-j$ Elemente auszuwählen. Dies sind insgesamt $\sum_{j=0}^{k}\binom{m}{j}\binom{n}{k-j}$ Möglichkeiten. Beide Verfahren führen zum selben Ergebnis, was die zu beweisende Formel liefert. •

**2. Beweis:** Wir verwenden vollständige Induktion. Die zu beweisende Behauptung über $n$ ist, dass die Formel für dieses $n$ und jede Wahl von $m$ und $k$ richtig ist. Induktionsanfang $n=0$: Die Summe auf der rechten Seite hat dann als einzigen Summanden $\neq 0$ den Summanden $\binom{m}{k}\binom{0}{0}=\binom{m}{k}$ für $j=k$. Auf der rechten Seite der Gleichung steht bei $n=0$ aber ebenfalls $\binom{m+0}{k}=\binom{m}{k}$.

Beim Schluss von $n$ auf $n+1$ können wir die zu beweisende Formel für $n$ und alle $k$, also insbesondere auch für $k$ und $k-1$ voraussetzen, d.h. wir dürfen $\sum_{j=0}^{k}\binom{m}{j}\binom{n}{k-j}=\binom{m+n}{k}$ und $\sum_{j=0}^{k-1}\binom{m}{j}\binom{n}{k-1-j}=\binom{m+n}{k-1}$ benutzen. Verwenden wir noch die Formel $\binom{n+1}{k'}=\binom{n}{k'}+\binom{n}{k'-1}$ vom Pascalschen Dreieck zunächst für $k' := k-j$ und später für $k'=k$, so erhalten wir für $n+1$ statt $n$:

$$\sum_{j=0}^{k}\binom{m}{j}\binom{n+1}{k-j}=\binom{m}{k}+\sum_{j=0}^{k-1}\binom{m}{j}\binom{n+1}{k-j}=\binom{m}{k}+\sum_{j=0}^{k-1}\binom{m}{j}\binom{n}{k-j}+\sum_{j=0}^{k-1}\binom{m}{j}\binom{n}{k-j-1}=$$

$$=\sum_{j=0}^{k}\binom{m}{j}\binom{n}{k-j}+\sum_{j=0}^{k-1}\binom{m}{j}\binom{n}{k-1-j}=\binom{m+n}{k}+\binom{m+n}{k-1}=\binom{m+n+1}{k}. \bullet$$

**Abschnitt 2.B**, **Aufg. 10a)**, p. 34 (1.7.2010) :

Sei $V$ ein Verein mit $n$ Mitgliedern. Die Anzahl der Möglichkeiten, einen Vorstand aus $m$ Vereinsmitgliedern und daraus einen 1., 2., ..., $k$-ten Vorsitzenden zu wählen, ist $\binom{n}{m}\cdot[m]_k=\dfrac{n!}{k!(n-m)!}$.

**Beweis:** Es gibt zunächst $\binom{n}{m}$ Möglichkeiten für die Auswahl des $m$-elementigen Vorstands, sodann $m$ Möglichkeiten für die Auswahl des 1. Vorsitzenden aus der Mitte dieses Vorstands, dann noch $m-1$ Möglichkeiten für die Auswahl des 2. Vorsitzenden aus den restlichen Vorstandsmitgliedern usw., schließlich noch $m-k+1$ Möglichkeiten den $k$-ten Vorsitzenden auszuwählen. Dies ergibt $m(m-1)\cdots(m-k+1)=[m]_k$ Möglichkeiten, eine Folge von $k$ Personen auszuwählen als 1., 2., ..., $k$-te Vorsitzende. Insgesamt bekommt man so $\sum_{m=k}^{n}[m]_k\binom{n}{m}$ Möglichkeiten. •

**Abschnitt 2.B**, **Aufg. 10b)**, p. 34 (1.7.2010) :

Sei $V$ ein Verein mit $n$ Mitgliedern. Die Anzahl der Möglichkeiten, einen 1., 2., ..., $k$-ten Vorsitzenden zu wählen und die Menge dieser Vorsitzenden zu einem Vorstand zu ergänzen, ist $[n]_k \cdot 2^{n-k}$.

**Beweis.** Wie oben sieht man, dass es $n\,(n-1)\cdots(n-k+1) = [n]_k$ Möglichkeiten gibt für die Auswahl der 1., 2., ..., $k$-ten Vorsitzenden. Ergänzt man die so ausgewählten $k$ Personen durch weitere der restlichen $n-k$ Elemente von $M$ irgendwie zu einem Vorstand aus $m$ Personen, so gibt es dafür jeweils noch $2^{n-k}$ Möglichkeiten, insgesamt also bei dieser Reihenfolge $[n]_k\,2^{n-k}$ Möglichkeiten. •

**Abschnitt 2.B**, **Aufg. 11**, p. 34 (1.7.2010) :

Man zeige (mit Hilfe von Aufg. 10): $\displaystyle\sum_{m=k}^{n}[m]_k\binom{n}{m} = [n]_k\,2^{n-k}$ für $k, n \in \mathbb{N},\ k \le n$.

**Beweis:** Die beiden Auswahlverfahren aus den Aufgaben 10.a) und 10.b) führen zum jeweils selben Ergebnis. Daher gibt es dafür auch gleich viele Möglichkeiten. Dies liefert die Behauptung. •

**Abschnitt 2.B**, **Aufg. 5a)**, p. 33 (1.7.2010) :

Sei $A$ eine nichtleere Menge mit $n$ Elementen. Die Anzahl der Teilmengen von $A$ mit gerader Elementezahl ist gleich der Anzahl der Teilmengen von $A$ mit ungerader Elementezahl.

**Beweis:** Sei $\mathcal{P}_0$ die Menge der Teilmengen von $A$ mit gerade vielen Elementen und $\mathcal{P}_1$ die Menge der Teilmengen von $A$ mit ungerade vielen Elementen. Wir fixieren ein Element $a \in A$ und betrachten die Abbildung $f$ der Potenzmenge $\mathcal{P}(A)$ von $A$ in sich, die jeder Teilmenge $B$ von $A$ die Menge $B \cup \{a\}$ zuordnet, falls $a \notin A$, und die Menge $B - \{a\}$, falls $a \in A$. Nach Konstruktion ist dann $f \circ f$ die Identität von $\mathcal{P}(A)$ und $f$ insbesondere bijektiv. Dabei ordnet $f$ jedem Element von $\mathcal{P}_0$ eines aus $\mathcal{P}_1$ zu und umgekehrt. Daher definiert $f$ (durch Beschränken des Argumentbereichs) auch eine bijektive Abbildung der Menge $\mathcal{P}_0$ auf die Menge $\mathcal{P}_1$. •

**Abschnitt 2.B**, **Aufg. 5d)**, p. 34 (1.7.2010) :

Es ist $\displaystyle\sum_{k=0}^{n}\binom{2n}{2k} = \frac{4^n}{2} = \sum_{k=0}^{n-1}\binom{2n}{2k+1}$ für $n \in \mathbb{N}^*$.

**Beweis.** Nach Aufg. 5.a) ist die Anzahl $\displaystyle\sum_{k=0}^{n}\binom{2n}{2k}$ der Teilmengen einer $2n$-elementigen Menge mit gerade vielen Elementen gleich der Anzahl $\displaystyle\sum_{k=0}^{n-1}\binom{2n}{2k+1}$ der Teilmengen dieser Menge mit ungerade vielen Elementen. Insgesamt hat die Potenzmenge einer $2n$-elementigen Menge genau $2^{2n} = 4^n$ Elemente. Jede der beiden Summen ist also gleich der Hälfte davon. •

**Abschnitt 2.D**, Teil von **Aufg. 5**, p. 51 (1.7.2010) :

Man beweise, dass es unendlich viele Primzahlen der Form $3k+2,\ k \in \mathbb{N}$, gibt.

**Beweis:** Angenommen, es gäbe nur endlich viele solcher Primzahlen, nämlich 2 und außerdem $p_1, \ldots, p_n \ge 5$. Dann betrachten wir die Primfaktorzerlegung $a = q_1 \cdots q_m$ von $a := 3p_1 \cdots p_n + 2$. Offenbar ist $a$ nicht durch 2 und 3 teilbar, d.h. es ist $q_j \ne 2$ und $q_j \ne 3$. Wären alle $q_j$ von der Form $3k+1$, so auch ihr Produkt $a$. Eines der $q_j$ muss somit von der Form $3k+2$ und daher gleich einem der $p_i$ sein. Dann wäre aber auch 2 durch dieses $p_i$ teilbar. Widerspruch! •

**Abschnitt 2.D**, Teil von **Aufg. 5** p. 48 (1.7.2010) :

Man beweise, dass es unendlich viele Primzahlen der Form $4k+3,\ k \in \mathbb{N}$, gibt.

**Beweis:** Angenommen, es gäbe nur endlich viele solcher Primzahlen, nämlich 3 und außerdem $p_1, \ldots, p_n \ge 7$. Dann betrachten wir die Primfaktorzerlegung $a = q_1 \cdots q_m$ von $a := 4p_1 \cdots p_n + 3$. $a$ ist ungerade und ferner nicht durch 3 teilbar, da $4p_1 \cdots p_n$ nicht durch 3 teilbar ist. Für alle $j$ gilt also $q_j \ne 2, \ne 3$. Wären sämtliche $q_j$ von der Form $4k+1$, so auch ihr Produkt $a$. Da Zahlen der Form $4k$ bzw. $4k+2$, $k \ge 1$, als gerade Zahlen $>2$ sicher nicht prim sind, muss eines der $q_j$ von der Form $4k+3$ und somit gleich einem der $p_i$ sein. Dann wäre aber auch 3 durch dieses $p_i$ teilbar. Widerspruch! •

**Abschnitt 2.D, Zusatzaufgabe**, p. 48 (1.7.2010):

Man beweise, dass es unendlich viele positive ganze Zahlen $n$ gibt, für die $n^2+1$ einen Primfaktor größer als $2n+\sqrt{2n}$ besitzt. (Dies ist eine Aufgabe der Internationalen Mathematikolympiade 2008.)

**Beweis:** Angenommen, es gäbe nur endlich viele positive ganze Zahlen $n$, etwa $n_1,\ldots,n_k$, für die $n^2+1$ einen Primfaktor größer als $2n+\sqrt{2n}$ besitzt. Ist $p_i$ der (eindeutig bestimmte) Primfaktor von $n_i^2+1$ mit $p_i > 2n_i+\sqrt{2n_i}$, $i=1,\ldots,k$, so bilden wir das Produkt $m=2p_1\cdots p_k\geq 2$ und betrachten einen Primfaktor $p$ von $m^2+1$, also $m^2+1=sp$ mit $s\in\mathbb{N}^*$. Es ist $p>3$ und von allen $p_1,\ldots,p_k$ verschieden. Durch Division mit Rest von $m$ durch $p$ bekommen wir $q,r\in\mathbb{N}$ mit $m=qp+r$ und $0<r<p$. Dann sind auch $r^2+1=(m-qp)^2+1=(m^2+1)-2mqp+q^2p^2=(s-2mq+q^2p)\,p$ und ebenso $(p-r)^2+1$ durch $p$ teilbar. Bezeichnen wir die kleinere der beiden Zahlen $r$ und $p-r$ mit $n$, so gilt $2n<r+(p-r)=p$ und $n^2+1=tp$ mit $t\in\mathbb{N}^*$. Außerdem ist $n\neq n_i$ für alle $i=1,\ldots,k$, da ein $n_i$ neben $p_i$ nicht noch den Primteiler $p>2n=2n_i$ haben kann. Es genügt also, $p>2n+\sqrt{2n}$ zu zeigen, um einen Widerspruch zu unserer Annahme zu erhalten.

Nun ist $0<(p-2n)^2=p^2-4pn+4(n^2+1)-4=(p-4n+4t)\,p-4$, also $p-4n+4t>0$. Da $p,n,t$ ganze Zahlen sind, folgt sogar $p-4n+4t\geq 1$ und somit $(p-2n)^2\geq p-4$, also $\big(p-(2n+(1/2))\big)^2\geq 2n-(15/4)$, $|p-\big(2n+(1/2)\big)|\geq\sqrt{2n-(15/4)}$. Daraus folgt $p-\big(2n+(1/2)\big)\geq\sqrt{2n-(15/4)}$ und $p\geq 2n+(1/2)+\sqrt{2n-(15/4)}$ wegen $p>2n$. Überdies gilt $2n+(1/2)+\sqrt{2n-(15/4)}>2n+\sqrt{2n}$ für $n>8$, wie man durch zweimaliges Quadrieren leicht bestätigt. Es ist also $p>2n+\sqrt{2n}$, falls $n>8$ ist. Diese Ungleichung ist aber auch bei $n\leq 8$ erfüllt, da man sofort feststellt, dass es zu den Primzahlen $p=5,7,11,13,19,23$ kein $n$ mit $p>2n+\sqrt{2n}$ gibt, für das $n^2+1$ durch $p$ teilbar ist, wohl aber zur Primzahl $p_1=17=n_1^2+1$ für $n_1=4$ und zu $p_2=29$ die Zahl $n_2=12$ mit $n_2^2+1=145=5\cdot 29$. Daher ist sicher unser $p>29$ und somit $p>2\cdot 8+\sqrt{2\cdot 8}=20$. •

**Bemerkung.** Es ist unbekannt, ob für unendlich viele $n\in\mathbb{N}^*$ die Zahl $n^2+1$ selbst prim ist. Übrigens ist jeder Primteiler $p\neq 2$ von $n^2+1$ notwendigerweise $\equiv 1 \bmod 4$. Denn bei $p=4k+3$ und $n^2\equiv -1 \bmod p$ ist $n^p=(n^2)^{2k+1}n\equiv(-1)^{2k+1}n\equiv -n \bmod p$. Da $p$ kein Teiler von $2n$ ist, d.h. $n\not\equiv -n \bmod p$ ist, widerspricht dies dem Kleinen Fermatschen Satz $n^p\equiv n$ aus 2.D, Aufg. 18. Insbesondere haben wir damit gezeigt, dass es auch unendlich viele Primzahlen der Form $4k+1$ gibt, vgl. die vorangehende Aufgabe.

**Abschnitt 2.D**, **Aufg. 9**, p. 48 (1.7.2010):

Seien $a,n\in\mathbb{N}$ mit $a,n\geq 2$. Ist $a^n-1$ eine prim, so ist $a=2$ und $n$ prim.

**Beweis:** Sei $a^n-1$ eine Primzahl. Wegen $a^n-1=(a-1)(a^{n-1}+\cdots+1)$ muss $a-1=1$, also $a=2$ sein. Ist $n=pm$ mit $p>1$, so muss $2^m-1=1$, d.h. $m=1$, sein wegen

$$a^n-1=2^n-1=(2^m)^p-1=(2^m-1)\big((2^m)^{p-1}+(2^m)^{p-2}+\cdots+1\big)\,.$$ •

**Abschnitt 2.D**, **Aufg. 10**, p. 48 (1.7.2010):

Seien $a,n\in\mathbb{N}^*$ mit $a\geq 2$. Ist $a^n+1$ prim, so ist $a$ gerade und $n$ eine Potenz von 2.

**Beweis:** Es ist $a^n+1\geq a^1+1\geq 2+1=3$. Da $a^n+1$ eine Primzahl ist, ist $a^n+1$ somit ungerade. Daher sind $a^n$ und folglich auch $a$ gerade. Ist $n=pm$ mit einer Primzahl $p\geq 3$, so ist $p$ ungerade, also $(-1)^p=-1$. Dann ist $a^n+1=1-(-a^m)^p=\big(1-(-a^m)\big)\big(1+(-a^m)^1+(-a^m)^2+\cdots+(-a^m)^{p-1}\big)=(1+a^m)(1-a^m+a^{2m}\pm\cdots+a^{m(p-1)})$ eine echte Zerlegung von $a^n+1$. Widerspruch! Also ist $n$ eine Potenz von 2. •

**Abschnitt 2.D**, **Aufg. 11**, p. 49 (1.12.2012):

Für $a,m,n\in\mathbb{N}^*$ mit $a\geq 2$ und $d:=\operatorname{ggT}(m,n)$ ist $\operatorname{ggT}(a^m-1\,,a^n-1)=a^d-1$.

**Beweis:** Wegen $d=\operatorname{ggT}(m,n)$ gibt es teilerfremde Zahlen $\mu,\nu\in\mathbb{N}^*$ mit $m=\mu d$ und $n=\nu d$. Für $a_0:=a^d$ ist $\operatorname{ggT}(a_0^\mu-1\,,a_0^\nu-1)=a_0-1$ zu zeigen. Nach Beispiel 2.A.3 gilt $(a_0^{\mu-1}+\cdots+a_0+1)(a_0-1)=(a_0^\mu-1)$ und $(a_0^{\nu-1}+\cdots+a_0+1)(a_0-1)=(a_0^\nu-1)$. Wir zeigen durch vollständige Induktion über $\operatorname{Max}(\mu,\nu)$, dass die beiden Faktoren $a_0^{\mu-1}+\cdots+a_0+1$ und $a_0^{\nu-1}+\cdots+a_0+1$ teilerfremd sind. Bei $\operatorname{Max}(\mu,\nu)=1$, also $\mu=\nu=1$ ist das klar. Beim Induktionsschluss können wir ohne Einschränkung der Allgemeinheit $\mu>\nu$ voraussetzen. Dann ist $\operatorname{Max}(\mu-\nu,\nu)<\operatorname{Max}(\mu,\nu)$ und daher sind nach Induktionsvoraussetzung $a_0^{\nu-1}+\cdots+a_0+1$ und $a_0^{\mu-\nu-1}+\cdots+1$ teilerfremd. Ein gemeinsamer Primteiler $p$ von $a_0^{\mu-1}+\cdots+a_0+1$ und $a_0^{\nu-1}+\cdots+a_0+1$ würde aber auch deren Differenz $a_0^{\mu-1}+\cdots+a_0^{\nu}=(a_0^{\mu-\nu-1}+\cdots+1)\,a_0^{\nu}$ teilen, also $a_0$ oder $a_0^{\mu-\nu-1}+\cdots+1$. Da $a_0^{\nu-1}+\cdots+a_0+1$ und $a_0^{\mu-\nu-1}+\cdots+1$ teilerfremd sind, muss er somit $a_0$ teilen, was nicht möglich ist, da er $a_0^{\nu-1}+\cdots+a_0+1$ teilt. •

**Bemerkung:** Gilt für natürliche Zahlen $f,q,g,r$ die Gleichung $f=qg+r$, so ist

$$a^f-1=a^{qg+r}-1=Q(a^g-1)+(a^r-1)\,,\qquad Q:=\frac{a^r(a^{qg}-1)}{a^g-1}\in\mathbb{N}^*\,.$$

Daher verläuft der Euklidische Divisionsalgorithmus für die Zahlen $m,n$ parallel zum Euklidischen Algorithmus für die Zahlen $a^m-1,\ a^n-1$, womit insbesondere $\operatorname{ggT}(a^m-1,a^n-1)=a^{\operatorname{ggT}(m,n)}-1$ bewiesen ist. Diese Kette von Divisionen mit Rest ist auch für die Polynome $x^m-1$ und $x^n-1$ gültig (wobei alle Rechnungen im Bereich der ganzen Zahlen bleiben), vgl. Abschnitt 11.B, insbesondere 11.B.1.

**Abschnitt 2.D**, **Aufg. 12**, p. 49 (1.12.2012):

**a)** Man bestimme die kanonische Primfaktorzerlegung von 81 057 226 635 000.

**b)** Ist $n=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ die Primfaktorzerlegung der positiven natürlichen Zahl $n$ mit paarweise verschiedenen Primzahlen $p_1,\ldots,p_r$, so ist $T(n):=(\alpha_1+1)\cdots(\alpha_r+1)$ die Anzahl der Teiler von $n$ in $\mathbb{N}^*$. Wie viele Teiler hat die in a) angegebene Zahl?

**Lösung:** a) Offenbar ist $81\,057\,226\,635\,000=2^3\cdot3^3\cdot5^4\cdot7^3\cdot11^2\cdot17\cdot23\cdot37$.

b) Wegen der eindeutigen Primfaktorzerlegung haben die Teiler von $n$ die Gestalt $p_1^{\beta_1}\cdots p_r^{\beta_r}$ mit Exponenten $\beta_i\in\mathbb{N}$, für die $0\le\beta_i\le\alpha_i$ gilt. Es gibt dafür also genau $(\alpha_1+1)\cdots(\alpha_r+1)$ Möglichkeiten. – Die in a) angegebene Zahl hat somit $(3+1)(3+1)(4+1)(3+1)(2+1)(1+1)(1+1)(1+1)=7680$ Teiler. •

**Abschnitt 2.D**, **Aufg. 13**, p. 49 (1.12.2012):

**a)** Sei $a\in\mathbb{N}^*$. Für wie viele $x\in\mathbb{N}^*$ ist $x(x+a)$ eine Quadratzahl? Man bestimme diese $x$ für $a\in\{15,30,60,120\}$.

**b)** Sei $n\in\mathbb{N}^*$. Die Anzahl der Paare $(u,v)\in\mathbb{N}^2$ mit $u^2-v^2=n$ ist $\lceil T(n)/2\rceil$, falls $n$ ungerade, $\lceil T(n/4)/2\rceil$, falls $4\,|\,n$, und gleich 0 sonst. Man gebe alle Darstellungen von $u^2-v^2=1000$ mit $u,v\in\mathbb{N}$ an. Die Anzahl der (paarweise inkongruenten) pythagoreischen Dreiecke (d.h. der rechtwinkligen Dreiecke mit positiven ganzzahligen Seitenlängen), deren eine Kathete gleich der vorgegebenen Zahl $a\in\mathbb{N}^*$ ist, ist $\lfloor T(a^2)/2\rfloor$, falls $a$ ungerade, und $\lfloor T(a^2/4)/2\rfloor$, falls $a$ gerade. ($T(-)$ bezeichnet die Anzahl der Teiler, vgl. Aufg. 12b).– Schwieriger ist die Aufgabe, zu vorgegebener ganzzahliger *Hypotenusen*länge $c>0$ die Anzahl der zugehörigen pythagoreischen Dreiecke zu finden, d.h. die Anzahl der Paare $(a,b)\in(\mathbb{N}^*)^2$ mit $a\le b$ und $a^2+b^2=c^2$. Man benötigt dazu die Ergebnisse von Bd. 2, 10.A, Aufg. 33, 34 zum Zwei-Quadrate-Satz. Die gesuchte Anzahl ist $\lfloor T'(c^2)/2\rfloor$, wobei $T'(c^2)$ die Anzahl derjenigen natürlichen Teiler von $c^2$ sei, deren Primteiler alle $\equiv1\bmod4$ sind. Für $c=39=3\cdot13$ gibt es also (bis auf Kongruenz) genau ein solches Dreieck (das so genannte indische Dreieck $15^2+36^2=39^2$), bei $c=65=5\cdot13$ jedoch 4 und bei $c=57=3\cdot19$ keins. – Leicht wiederum ist die Ägyptische Seilspanneraufgabe zu lösen: Die pythagoreischen Dreiecke mit *teilerfremden* Seitenlängen $a,b,c\in\mathbb{N}^*$ und gegebenem *Umfang* $a+b+c=s\in\mathbb{N}^*$ (das sind so genannte primitive pythagoreische Dreiecke) entsprechen bijektiv den Darstellungen $s=de$ mit teilerfremden $d,e\in\mathbb{N}^*$, $d\equiv1\bmod2$, $e\equiv0\bmod2$ und $d<e<2d$. Die Längen der Katheten des zugehörigen Dreiecks sind $d(e-d)$ bzw. $(d-e/2)e$, und die Länge der Hypotenuse ist $d^2-de+e^2/2$.)

**c)** Man bestimme alle Paare $(a,b)\in(\mathbb{N}^*)^2$ mit $(a^2+b^2)/ab\in\mathbb{N}^*$.

**Lösung:** a) Sei $x(x+a)$ das Quadrat $y^2$ einer positiven natürlichen Zahl $y$. Dann ist $y>x$, und es gibt ein $b\in\mathbb{N}^*$ mit $y=x+b$. Es folgt $x^2+xa=y^2=(x+b)^2=x^2+2xb+b^2$ und somit $x(a-2b)=b^2$. Umgekehrt liefert jeder Wert $b$, für den $a-2b$ ein Teiler von $b^2$ ist, ein $x=b^2/(a-2b)$ derart, dass $x(x+a)$ das Quadrat $(x+b)^2$ ist. Vergrößert man dabei $b$, so wird $a-2b$ verkleinert und folglich $x=b^2/(a-2b)$ vergrößert. Verschiedene Werte von $b$ liefern also verschiedene Werte von $x$.

Es genügt, die $b\in\mathbb{N}^*$ mit $b<a/2$ zu zählen, für die $a-2b$ Teiler von $b^2$ ist, oder auch die $c\in\mathbb{N}^*$ mit $c<a$, für die $c\equiv a \bmod 2$ ist und $c$ ein Teiler von $b^2$, $b:=(a-c)/2$. Sei dazu $a=2^{\alpha_0}p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ mit $\alpha_0\in\mathbb{N}$, $\alpha_i\in\mathbb{N}^*$ für $i=1,\ldots,r$ und paarweise verschiedenen Primzahlen $p_i\geq 3$ die kanonische Primfaktorzerlegung von $a$. Wird $b^2$ von $a-2b$ geteilt, so ist jeder Primteiler $p$ von $a-2b$ auch ein Teiler von $b^2$, also von $b$, und somit schließlich von $a$. Die Primfaktorzerlegung von $a-2b$ hat dann die Form $2^{\beta_0}p_1^{\beta_1}\cdots p_r^{\beta_r}$ mit $\beta_i\geq 0$. Folglich ist $p_i^{\beta_i}$ für $i=1,\ldots,r$ Teiler von $b^2$ und somit $p_i^{\lceil\beta_i/2\rceil}$ ein Teiler von $b$. Bei $\beta_i>2\alpha_i$ wäre dann $\lceil\beta_i/2\rceil>\alpha_i$ und daher $p_i^{\alpha_i}$ die höchste Potenz von $p_i$, die $a-2b$ teilt, d.h. $\beta_i=\alpha_i$ im Widerspruch zu $\beta_i>2\alpha_i$. Daher ist $0\leq\beta_i\leq 2\alpha_i$ für $i=1,\ldots,r$.

Bei $\alpha_0=0$ ist offensichtlich $\beta_0=0$. Bei $\alpha_0=1$ ist zunächst $\beta_0\geq 1$ und daher $b^2$ und damit $b$ gerade. Dann ist aber $a-2b$ durch 2 und nicht durch 4 teilbar, d.h. es ist $\beta_0=1$. Bei $\alpha_0\geq 2$ ist zunächst $b$ gerade und daher $\beta_0\geq 2$. Wäre $\beta_0>2\alpha_0-2$, so wäre $\lceil\beta_0/2\rceil>\alpha_0-1$, $1+\lceil\beta_0/2\rceil>\alpha_0$, und somit $2^{\alpha_0}$ die höchste Potenz von 2, die $a-2b$ teilt, d.h. $\beta_0=\alpha_0$ im Widerspruch zu $\beta_0>2\alpha_0-2\geq\alpha_0$ (wegen $\alpha_0\geq 2$). Genau dann ist also $a-2b$ ein Teiler von $b^2$, wenn für $i=1,\ldots,r$ gilt $0\leq\beta_i\leq 2\alpha_i$, und wenn $\beta_0=\alpha_0$ ist für $\alpha_0\in\{0,1\}$ bzw. $2\leq\beta_0\leq 2\alpha_0-2$ für $\alpha_0\geq 2$.

Die gesuchte Anzahl ist nunmehr bei $\alpha_0=0$ gleich der Anzahl der Teiler von $a^2$, die kleiner als $a$ sind. Da für jeden Teiler $c$ von $a^2$, der größer als $a$ ist, der Teiler $a^2/c$ von $a^2$ kleiner als $c$ ist und außerdem der Teiler $a$ selbst nicht in Frage kommt, ist die Zahl der $x$, für die $x(x+a)$ ein Quadrat ist, nach Aufg. 12b) gleich $\big(T(a^2)-1\big)/2=\big((2\alpha_1+1)\cdots(2\alpha_r+1)-1\big)/2=\lfloor T(a^2)/2\rfloor$.

Bei $\alpha_0=1$ ist $\beta_0=1$ und es kommt nur auf die Teiler $<\frac{1}{2}a$ von $(\frac{1}{2}a)^2$ an. Die Zahl der $x$, für die $x(x+a)$ ein Quadrat ist, ist also ebenfalls gleich $\big((2\alpha_1+1)\cdots(2\alpha_r+1)-1\big)/2=\lfloor T(a^2/4)/2\rfloor$.

Bei $\alpha_0\geq 2$ ist $2\leq\beta_0\leq 2\alpha_0-2$. Dann ist die Anzahl der $2^{\beta_0}p_1^{\beta_1}\cdots p_r^{\beta_r}$ zu zählen, die kleiner als $a=2^{\alpha_0}p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ sind und $\frac{1}{4}a^2=2^{2\alpha_0-2}p_1^{2\alpha_1}\cdots p_r^{2\alpha_r}$ teilen, d.h. die Anzahl der $2^{\beta_0-2}p_1^{\beta_1}\cdots p_r^{\beta_r}$, die kleiner als $\frac{1}{4}a=2^{\alpha_0-2}p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ sind und $2^{2\alpha_0-4}p_1^{2\alpha_1}\cdots p_r^{2\alpha_r}$ teilen. Dies sind analog zu der obigen Überlegung $\big((2\alpha_0-3)(2\alpha_1+1)\cdots(2\alpha_r+1)-1\big)/2=\lfloor T(a^2/16)/2\rfloor$ Stück.

**Alternative Lösung:** Nach dem ersten Absatz der vorigen Lösung kann man auch so weiterschließen: Wegen

$$\frac{4b^2}{a-2b}=\frac{a^2}{a-2b}-(a+2b)=c+d-2a\,,\qquad c=a-2b\,,\quad d:=\frac{a^2}{c}\,,$$

sind $b$ sowie $b^2/(a-2b)=b^2/c$ genau dann positive natürliche Zahlen, wenn gilt:

$$(1)\ \ c\mid a^2\ \text{ und }\ 1\leq c<a\,;\qquad (2)\ \ a\equiv c \bmod 2\,;\qquad (3)\ \ c+d-2a\equiv 0 \bmod 4\,.$$

Die Bedingungen (2) und (3) sind zusammen offenbar äquivalent zu

$$(2)\ \ a\equiv c \bmod 2\,;\qquad (3')\ \ c\equiv d \bmod 4\,.$$

Wie bei der ersten Lösung unterscheiden wir nun nach dem 2-Exponenten $v_2(a)$ von $a$. Man beachte $2v_2(a)=v_2(a^2)=v_2(c)+v_2(d)$. Ferner ist die Anzahl der Teiler $c$ von $a^2$ mit $1\leq c<a$ gleich $\lfloor T(a^2)/2\rfloor$.

(a) Sei $v_2(a)=0$, d.h. $a\equiv 1 \bmod 2$ und $a^2\equiv 1 \bmod 4$. Dann impliziert Bedingung (1) bereits (2) und (3′), denn $cd=a^2\equiv 1 \bmod 4$, also $c\equiv d\equiv 1 \bmod 4$ oder $c\equiv d\equiv -1 \bmod 4$. Die Anzahl der Lösungen ist also $\lfloor T(a^2)/2\rfloor$.

(b) Sei $v_2(a)=1$, d.h. $a\equiv 2 \bmod 4$. Dann sind (2) und (3′) äquivalent mit $c\equiv d\equiv 0 \bmod 2$ oder mit $c\equiv d\equiv 2 \bmod 4$. Die Anzahl der Lösungen ist $\lfloor T(a^2/4)/2\rfloor$.

(c) Sei $v_2(a)\geq 2$, d.h. $a\equiv 0 \bmod 4$. Dann sind (2) und (3′) äquivalent mit $c\equiv d\equiv 0 \bmod 4$. Die Anzahl der Lösungen ist $\lfloor T(a^2/16)/2\rfloor$.

Für die explizit angegebenen $a$ ergeben sich für $c=a-2b$, $b=(a-c)/2$, $b^2$, $x=b^2/c=(c+d-2a)/4$, $y=x+b$ und die Gleichung $x(x+a)=y^2$ folgende Werte:

$a=15=3\cdot 5$ mit $\big((2+1)(2+1)-1\big)/2=4$ Darstellungen:

| $c$ | $b$ | $b^2$ | $x$ | $y$ | $x(x+a)=y^2$ |
|---|---|---|---|---|---|
| 1 | 7 | 49 | 49 | 56 | $49\cdot(49+15)=56^2$ |
| 3 | 6 | 36 | 12 | 18 | $12\cdot(12+15)=18^2$ |
| 5 | 5 | 25 | 5 | 10 | $5\cdot(5+15)=10^2$ |
| 9 | 3 | 9 | 1 | 4 | $1\cdot(1+15)=4^2$ , |

$a=30 = 2\cdot 3\cdot 5$ mit $\big((2+1)(2+1)-1\big)/2 = 4$ Darstellungen:

| $c$ | $b$ | $b^2$ | $x$ | $y$ | $x(x+a)=y^2$ |
|---|---|---|---|---|---|
| 2 | 14 | 196 | 98 | 112 | $98\cdot(98+30) = 112^2$ |
| 6 | 12 | 144 | 24 | 36 | $24\cdot(24+30) = 36^2$ |
| 10 | 10 | 100 | 10 | 20 | $10\cdot(10+30) = 20^2$ |
| 18 | 6 | 36 | 2 | 8 | $2\cdot(2+30) = 8^2$ , |

$a=60 = 2^2\cdot 3\cdot 5$ mit $\big((4-3)(2+1)(2+1)-1\big)/2 = 4$ Darstellungen:

| $c$ | $b$ | $b^2$ | $x$ | $y$ | $x(x+a)=y^2$ |
|---|---|---|---|---|---|
| 4 | 28 | 784 | 196 | 224 | $196\cdot(196+60) = 224^2$ |
| 12 | 24 | 576 | 48 | 72 | $48\cdot(48+60) = 72^2$ |
| 20 | 20 | 400 | 20 | 40 | $20\cdot(20+60) = 40^2$ |
| 36 | 12 | 144 | 4 | 16 | $4\cdot(4+60) = 16^2$ . |

$a=120 = 2^3\cdot 3\cdot 5$ mit $\big((6-3)(2+1)(2+1)-1\big)/2 = 13$ Darstellungen:

| $c$ | $b$ | $b^2$ | $x$ | $y$ | $x(x+a)=y^2$ |
|---|---|---|---|---|---|
| 4 | 58 | 3364 | 841 | 899 | $841\cdot(841+120) = 899^2$ |
| 8 | 56 | 3136 | 392 | 448 | $392\cdot(392+120) = 448^2$ |
| 12 | 54 | 2916 | 243 | 363 | $243\cdot(243+120) = 363^2$ |
| 16 | 52 | 2704 | 169 | 221 | $169\cdot(169+120) = 221^2$ |
| 20 | 50 | 2500 | 125 | 175 | $125\cdot(125+120) = 175^2$ |
| 24 | 48 | 2304 | 96 | 144 | $96\cdot(96+120) = 144^2$ |
| 36 | 42 | 1764 | 49 | 91 | $49\cdot(49+120) = 91^2$ |
| 40 | 40 | 1600 | 40 | 80 | $40\cdot(40+120) = 80^2$ |
| 48 | 36 | 1296 | 27 | 63 | $27\cdot(27+120) = 63^2$ |
| 60 | 30 | 900 | 15 | 45 | $15\cdot(15+120) = 45^2$ |
| 72 | 24 | 576 | 8 | 32 | $8\cdot(8+120) = 32^2$ |
| 80 | 20 | 400 | 5 | 25 | $5\cdot(5+120) = 25^2$ |
| 100 | 10 | 100 | 1 | 11 | $1\cdot(1+120) = 11^2$ . |

b) Sei zunächst $n=2m$ mit einem ungeraden $m\in\mathbb{N}$. Gäbe es eine Darstellung $n=u^2-v^2=(u+v)(u-v)$, so wäre genau einer der beiden Faktoren $u+v$ und $u-v$ gerade und daher ihre Summe $2u$ ungerade. Widerspruch!

Sei nun $n$ ungerade und sei $n=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ mit paarweise verschiedenen Primzahlen $p_i\geq 3$, $\alpha_i\in\mathbb{N}^*$, für $i=1,\ldots,r$ die kanonische Primfaktorzerlegung von $n$. Hat man eine Darstellung $n=u^2-v^2=(u+v)(u-v)$, so sind dann $u+v\geq\sqrt{n}$ und $u-v\leq\sqrt{n}$ ungerade und ihre Summe $2u$ bzw. Differenz $2v$ gerade, woraus sich $u$ und $v$ bestimmen lassen. Ist umgekehrt $n$ keine Quadratzahl, so führt jeder der $T(n)/2$ Teiler $>\sqrt{n}$ von $n$ auf diese Weise zu einer neuen Darstellung der gewünschten Art. Genau dann wenn $n$ eine Quadratzahl ist, sind alle $\alpha_i$ gerade und $T(n)$ nach Aufg. 12 ungerade. In diesem Fall hat man noch die Zerlegung $n=\sqrt{n}\cdot\sqrt{n}$ zu berücksichtigen, die eine weitere Darstellung der angegebenen Art liefert. Insgesamt führt dies zu $\lceil T(n)/2\rceil$ Darstellungen.

Sei schließlich $n$ durch 4 teilbar. In einer Darstellung $n=u^2-v^2=(u+v)(u-v)$ müssen dann beide Faktoren $u+v$ und $u-v$ gerade sein, da andernfalls ihre Summe $2u$ nicht gerade wäre. Dies führt zu einer Zerlegung $\frac14 n=\frac12(u+v)\cdot\frac12(u-v)$, bei der $\frac12(u+v)\geq\frac12\sqrt{n}\geq\frac12(u-v)$ natürliche Zahlen sind. Umgekehrt führt jeder der Teiler $\geq\frac12\sqrt{n}$ von $\frac12 n$ zu einer neuen Darstellung der gesuchten Art, wobei der Fall, dass $\frac14 n$ und damit $n$ eine Quadratzahl ist, wie oben gesondert zu berücksichtigen ist.

Im Fall $n = 1000$ ist $\frac{1}{4}n = 250 = 2 \cdot 5^3$. $\frac{1}{4}n$ hat $(1+1)\cdot(3+1) = 8$ Teiler. Die zugehörigen Zerlegungen sind $250 = 250 \cdot 1 = 125 \cdot 2 = 50 \cdot 5 = 25 \cdot 10$. Sie liefern $u$ und $v$ als Summe bzw. Differenz der beiden Faktoren und ergeben die Darstellungen $1000 = 251^2 - 249^2 = 127^2 - 123^2 = 55^2 - 45^2 = 35^2 - 15^2$.

Die angegebene Formel für die Anzahl der pythagoreischen Dreiecke, deren eine Kathete gleich $a \in \mathbb{N}^*$ ist, d.h. die Anzahl der Paare $(u, v) \in (\mathbb{N}^*)^2$ mit $u^2 = a^2 + v^2$ oder $u^2 - v^2 = a^2$, ergibt sich daraus sofort, da $a^2$ stets ungerade oder durch 4 teilbar ist und die Lösung $a^2 - 0^2 = a^2$ nicht gezählt wird.

c) Sei $(a, b) \in \left(\mathbb{N}^*\right)^2$ ein Paar mit $a^2 + b^2 = rab$ mit einem $r \in \mathbb{N}^*$. Jeder Primteiler $p$ von $a$ teilt dann auch $b^2 = rab - a^2 = a(rb - a)$ und damit $b$. Ebenso teilt jeder Primteiler von $b$ auch $a$. Dafür folgt dann $(a/p)^2 + (b/p)^2 = r(a/p)(b/p)$. In dieser Weise fortfahrend teilt man $a$ bzw. $b$ sukzessive durch alle Primfaktoren und kommt schließlich zu einer Gleichung der Form $2 = 1^2 + 1^2 = r \cdot 1 \cdot 1 = r$. Es muss also $r = 2$ sein. Die Gleichung $a^2 + b^2 = 2ab$, also $(a - b)^2 = 0$, gilt aber genau für die Paare $(a, b)$ mit $a = b$. •

**Abschnitt 2.D**, **Aufg. 16**, p. 50 (1.7.2010) :

Seien $n, k \in \mathbb{N}^*$ teilerfremd. Man zeige, dass $\binom{n}{k}$ durch $n$ und $\binom{n-1}{k-1}$ durch $k$ teilbar ist.

**Beweis:** Es ist $\binom{n}{k} = \dfrac{n \cdot (n-1) \cdots (n-k+1)}{1 \cdots (k-1) \cdot k} = \dfrac{n}{k} \cdot \binom{n-1}{k-1}$, also $k\binom{n}{k} = n\binom{n-1}{k-1}$. Daher teilt $n$ das Produkt $k\binom{n}{k}$. Da nach Voraussetzung keiner der Primteiler von $n$ ein Teiler von $k$ ist, müssen alle diese Primteiler bereits in der Primfaktorzerlegung von $\binom{n}{k}$ vorkommen, d.h. $n$ teilt $\binom{n}{k}$. Ebenso sieht man, dass $k$ das Produkt $n\binom{n-1}{k-1}$ teilt. Wegen der Teilerfremdheit von $k$ und $n$ müssen alle Primteiler von $k$ bereits in der Primfaktorzerlegung von $\binom{n-1}{k-1}$ vorkommen, d.h. $k$ teilt $\binom{n-1}{k-1}$. •

**Abschnitt 2.D**, zu **Aufg. 24**, p. 50 (1.7.2010) :

Man bestimme den größten gemeinsamen Teiler von $a := 527$ und $b = 403$ und berechne ganze Zahlen $s$ und $t$ mit $\mathrm{ggT}(527, 403) = s \cdot 527 + t \cdot 403$.

Der Euklidische Divisionsalgorithmus liefert der Reihe nach

$$\begin{aligned} 527 &= 1 \cdot 403 + 124 \\ 403 &= 3 \cdot 124 + 31 \\ 124 &= 4 \cdot 31 \end{aligned}$$

Es folgt $\mathrm{ggT}(527, 403) = 31 = 403 - 3 \cdot 124 = 403 - 3 \cdot (527 - 1 \cdot 403) = 4 \cdot 403 - 3 \cdot 527$. •

**Abschnitt 2.D**, zu **Aufg. 24**, p. 50 (1.7.2010) :

Man bestimme den größten gemeinsamen Teiler von $a := 1173$ und $b := 867$ und berechne ganze Zahlen $s$ und $t$ mit $\mathrm{ggT}(1173, 867) = s \cdot 1173 + t \cdot 867$.

**Lösung:** Der Euklidische Divisionsalgorithmus liefert der Reihe nach

$$\begin{aligned} 1173 &= 1 \cdot 867 + 306 \\ 867 &= 2 \cdot 306 + 255 \\ 306 &= 1 \cdot 255 + 51 \\ 255 &= 5 \cdot 51 \end{aligned}$$

Es folgt $\mathrm{ggT}(1173, 867) = 51 = 306 - 1 \cdot 255 = 306 - 1 \cdot (867 - 2 \cdot 306) = 3 \cdot 306 - 1 \cdot 867 = 3 \cdot (1173 - 1 \cdot 867) - 1 \cdot 867 = 3 \cdot 1173 - 4 \cdot 867$. •

**Abschnitt 2.D**, zu **Aufg. 24**, p. 50 (1.7.2010) :

Man bestimme den größten gemeinsamen Teiler von $a := 5893$ und $b = 4331$ und berechne ganze Zahlen $s$ und $t$ mit $\mathrm{ggT}(5893, 4331) = s \cdot 5893 + t \cdot 4331$.

**Lösung:** Der Euklidische Divisionsalgorithmus liefert

$$\begin{aligned}5893 &= 1 \cdot 4331 + 1562\\ 4331 &= 2 \cdot 1562 + 1207\\ 1562 &= 1 \cdot 1207 + 355\\ 1207 &= 3 \cdot 355 + 142\\ 355 &= 2 \cdot 142 + 71\\ 142 &= 2 \cdot 71.\end{aligned}$$

Der gesuchte ggT ist also $r_6 = 71$. Bezeichnen wir die auftretenden Quotienten mit $q_i$ und setzen $s_0 := 1$, $s_1 := 0$, $t_0 := 0$, $t_1 := 1$ sowie $s_{i+1} = s_{i-1} - q_i s_i$, $t_{i+1} = t_{i-1} - q_i t_i$, so gilt $r_i = s_i a + t_i b$ und insbesondere $r_6 = s \cdot 5893 + t \cdot 4331$ mit $s = s_6 = 25$ und $t = t_6 = -34$, wie sich aus der folgenden Tabelle ergibt:

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| $q_i$ | | 1 | 2 | 1 | 3 | 2 | |
| $s_i$ | 1 | 0 | 1 | $-2$ | 3 | $-11$ | 25 |
| $t_i$ | 0 | 1 | $-1$ | 3 | $-4$ | 15 | $-34$ |

Es ist somit $\mathrm{ggT}(5893, 4331) = 71 = 25 \cdot 5893 - 34 \cdot 4331$. •

**Abschnitt 2.D, Aufg. 28**, p. 51 (1.7.2010) :

Seien $a, b \in \mathbb{Q}_+^\times$ und $b$ zwei positive rationale Zahlen. Genau dann ist $\sqrt{a} + \sqrt{b}$ rational, wenn sowohl $a$ als auch $b$ Quadrat einer rationalen Zahl ist.

**Beweis:** Natürlich sind $\sqrt{a}$ und $\sqrt{b}$ und damit auch ihre Summe rationale Zahlen, wenn $a$ und $b$ Quadrate rationaler Zahlen sind.

Nach der dritten binomischen Formel gilt $\big(\sqrt{a} + \sqrt{b}\big)\big(\sqrt{a} - \sqrt{b}\big) = \big(\sqrt{a}\big)^2 - \big(\sqrt{b}\big)^2 = a - b$. Ist also $x := \sqrt{a} + \sqrt{b}$ eine rationale Zahl, so auch $y := \sqrt{a} - \sqrt{b} = \frac{a-b}{x}$. Dann sind aber $\sqrt{a} = \frac{1}{2}(x+y)$ und $\sqrt{b} = \frac{1}{2}(x-y)$ ebenfalls rationale Zahlen, deren Quadrate gleich $a$ bzw. $b$ sind. •

**Abschnitt 2.D, Aufg. 29a)**, p. 51 (1.5.2011) :

Sei $x := a/b \in \mathbb{Q}$ ein *gekürzter* Bruch, $a, b \in \mathbb{Z}$, $b > 0$. Es gelte $a_n x^n + \cdots + a_1 x + a_0 = 0$ mit ganzen Zahlen $a_0, \ldots, a_n$ und $a_n \neq 0$, $n \geq 1$, d.h. $x$ sei Nullstelle der Polynomfunktion $a_n t^n + \cdots + a_0$. Dann ist $a$ ein Teiler von $a_0$ und $b$ ein Teiler von $a_n$. Insbesondere ist $x \in \mathbb{Z}$, wenn der höchste Koeffizient $a_n = 1$ ist (Lemma von Gauß).

**Beweis:** Nach Voraussetzung gilt

$$a_n\Big(\frac{a}{b}\Big)^n + a_{n-1}\Big(\frac{a}{b}\Big)^{n-1} + \cdots + a_1\frac{a}{b} + a_0 = 0\,,$$

also $a_n a^n + a_{n-1}a^{n-1}b + \cdots + a_1 a b^{n-1} + a_0 b^n = 0$. Es folgt einerseits $a\,(a_n a^{n-1} + \cdots + a_1 b^{n-1}) = -a_0 b^n$ und andererseits $(a_{n-1}a^{n-1} + \cdots + a_0 b^{n-1})\,b = -a_n a^n$, d.h. $a$ teilt $-a_0 b^n$ und $b$ teilt $-a_n a^n$. Da $a$ und $b$ teilerfremd sind, muss dann $a$ ein Teiler von $a_0$ und $b$ ein Teiler von $a_n$ sein. •

**Bemerkung:** Für eine Verallgemeinerung des obigen Gaußschen Lemmas siehe Bd. 2, Korollar 10.A.20.

**Abschnitt 2.D, Aufg. 29b)**, p. 51 (1.5.2011) :

Man bestimme sämtliche rationalen Nullstellen der Polynomfunktionen $t^3 + \frac{3}{4}t^2 + \frac{3}{2}t + 3$ bzw. $3t^7 + 4t^6 - t^5 + t^4 + 4t^3 + 5t^2 - 4$.

**Lösung:** Für eine rationale Nullstelle $a/b$ mit teilerfremden $a, b \in \mathbb{Z}$, $b \neq 0$, von $t^3 + \frac{3}{4}t^2 + \frac{3}{2}t + 3$, d.h. von $4t^3 + 3t^2 + 6t + 12 = t^2(4t+3) + 6\,(t+2)$, gilt $a|12$ und $b|4$ nach Aufg. 29a). Da beide Summanden für $t < -2$ negativ und für $t > -\frac{3}{4}$ nichtnegativ sind, kommen nur die Zahlen $-\frac{3}{4}, -1, -\frac{3}{2}, -2$ als Nullstellen in Frage. Dafür hat die Polynomfunktion der Reihe nach die Werte $\frac{15}{2}, 5, 0, -20$. Einzige rationale Nullstelle ist also $-\frac{3}{2}$.

Für eine Nullstelle $a/b$ mit mit teilerfremden $a, b \in \mathbb{Z}$, $b \neq 0$, von

$$3t^7+4t^6-t^5+t^4+4t^3+5t^2-4 = 3t^7+(4t-1)t^5+t^4+4t^3+(5t^2-4)$$

gilt $a|4$ und $b|3$ nach Aufg. 29a). Da alle Summanden in der zweiten Darstellung dieses Ausdrucks für $t \geq 1$ positiv sind, kommen also nur $\frac{2}{3}, \frac{1}{3}, -\frac{1}{3}, -\frac{2}{3}, -1, -\frac{4}{3}, -2, -4$ als Nullstellen in Frage. Dafür hat die Polynomfunktion der Reihe nach die Werte $0, -\frac{2392}{729}, -\frac{2604}{729}, -\frac{1792}{729}, 0, \frac{2028}{729}, 96, -31768$. Einzige rationale Nullstellen sind also $\frac{2}{3}$ und $-1$. •

**Abschnitt 2.D, Aufg. 30a)**, p. 51 (1.7.2010) :

Seien $x, y \in \mathbb{Q}_+^\times$ und $y = c/d$ eine gekürzte Darstellung von $y$ mit $c, d \in \mathbb{N}^*$. Genau dann ist $x^y$ rational, wenn $x$ die $d$-te Potenz einer rationalen Zahl ist.

**Beweis:** Ist $x = q^d$ mit $q \in \mathbb{Q}$, so ist $x^y = (q^d)^{(c/d)} = q^c$ offenbar rational.
Ist umgekehrt $x^y = q \in \mathbb{Q}$ rational, so folgt $x^c = x^{dy} = (x^y)^d = q^d$. Sind $\alpha_p \in \mathbb{Z}$ und $\beta_p \in \mathbb{Z}$ die Vielfachheiten, mit denen eine Primzahl $p$ in der Primfaktorzerlegung von $x$ bzw. $q$ vorkommt, so gilt also wegen der Eindeutigkeit der Primfaktorzerlegung $c\alpha_p = d\beta_p$. Da $c$ und $d$ nach Voraussetzung teilerfremd sind, muss dann $d$ ein Teiler von $\alpha_p$ sein, also $\alpha_p = d\alpha'_p$ mit $\alpha'_p \in \mathbb{Z}$. Folglich ist $x = \prod_{p\in P} p^{\alpha_p} = \left(\prod_{p\in P} p^{\alpha'_p}\right)^d$ die $d$-te Potenz der rationalen Zahl $\prod_{p\in P} p^{\alpha'_p}$. •

**Abschnitt 2.D, Aufg. 31**, p. 52 (1.7.2010) :

Seien $x \in \mathbb{Q}_+^\times$ und $a$ eine natürliche Zahl $\geq 2$, die nicht von der Form $b^d$ mit $b, d \in \mathbb{N}^*$, $d \geq 2$, ist. Dann ist $\log_a x$ ganzzahlig oder irrational.

**Beweis:** Mit $\alpha_p \in \mathbb{N}$ und $\beta_p \in \mathbb{Z}$ bezeichnen wir die Vielfachheiten, mit denen eine Primzahl $p$ in der Primfaktorzerlegung von $x$ bzw. $q$ vorkommt. Nach Voraussetzung gibt es dann kein $d \geq 2$ in $\mathbb{N}^*$ derart, dass alle $\alpha_p$ durch dieses $d$ teilbar sind. Ist nun $\log_a x$ rational, also etwa $\log_a x = c/d$ mit teilerfremden $c, d \in \mathbb{N}$, $d \geq 1$, so folgt $x = a^{\log_a x} = a^{c/d}$ und somit $x^d = a^c$. Wegen der Eindeutigkeit der Primfaktorzerlegung folgt $c\alpha_p = d\beta_p$ für alle Primzahlen $p$. Da $c$ und $d$ teilerfremd sind, muss $d$ also alle $\alpha_p$ teilen. Die Voraussetzung zeigt, dass dies nur bei $d = 1$ möglich ist. Dann ist aber $\log_a x = c$ eine ganze Zahl. •