CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

Prof. Bernd Finkbeiner, Ph.D.
Jana Hofmann, M.Sc.
Reactive Systems Group

Programmierung 1 (WS 2020/21)
Zusatztutorium 3 (Lösungsvorschläge)
Mathematische Prozeduren

Hinweis: Diese Aufgaben wurden von den Tutoren für das Zusatztutorium erstellt. Sie sind für die Klausur weder relevant noch irrelevant. 🤔 markiert potentiell schwerere Aufgaben.

Mengen und Graphen

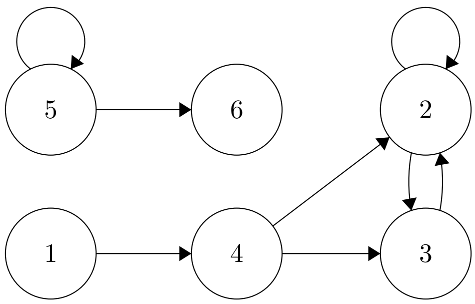
Aufgabe Z3.1 *(Dom, Ran und Ver)*
Betrachten Sie folgende Relation:

$$R = \{(1,4),(2,2),(2,3),(3,2),(4,2),(4,3),(5,5),(5,6)\}$$

Bestimmen Sie den Definitions- und Wertebereich sowie die Knotenmenge von R und zeichnen Sie die graphische Darstellung.

Lösungsvorschlag Z3.1

$$Dom\, R = \{1,2,3,4,5\}$$
$$Ran\, R = \{2,3,4,5,6\}$$
$$Ver\, R = \{1,2,3,4,5,6\}$$



Aufgabe Z3.2 *(Rekursion)*
Sei folgende Prozedur gegeben:

$$p : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$$
$$\begin{aligned} p\,(x,y) &= x + y && \text{für } x < 7 \\ p\,(x,y) &= p\,(x-2,y) && \text{für } 6 < x < 13 \\ p\,(x,y) &= p\,(x-3,y) + p\,(x-3,y) && \text{sonst} \end{aligned}$$

(a) Zeichen Sie den Rekursionsbaum für das Argument $(13, 37)$.

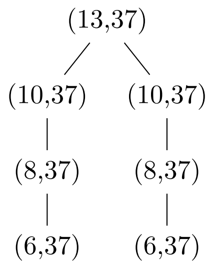
(b) Bestimmen Sie die Rekursionsfunktion von p.

(c) Geben Sie die Rekursionsrelation von p an.

(d) Geben Sie eine natürliche Terminierungsfunktion von p an.

Lösungsvorschlag Z3.2

(a) Rekursionsbaum für das Argument $(13, 37)$:

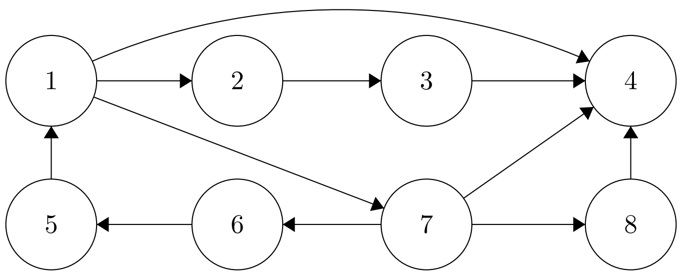


(b) Rekursionsfunktion:
$r = \lambda(x, y) \in \mathbb{N}^2.\ if\ x < 7\ then\ \langle\rangle\ else\ if\ x < 13\ then\ \langle(x-2, y)\rangle\ else\ \langle(x-3, y), (x-3, y)\rangle$

(c) Rekursionsrelation:
$R = \{((x, y), (x-2, y)\ \in (\mathbb{N} \times \mathbb{N})^2\ \mid\ 6 < x < 13\} \ \cup\ \{((x, y), (x-3, y)\ \in (\mathbb{N} \times \mathbb{N})^2\ \mid\ x > 12\}$

(d) Terminierungsfunktion:
$\lambda(x, y) \in \mathbb{N}^2.\ x$

Aufgabe Z3.3 *(Ein Graph)*
Gegeben sei der folgende Graph:



(a) Finden Sie, wenn vorhanden, eine Wurzel, eine Quelle, eine Senke, einen isolierten Knoten sowie einen Zyklus.

(b) Geben Sie die Relation an, die der Graph darstellt.

(c) Ist diese Menge funktional? Falls nein, geben Sie die größte funktionale Teilmenge dieser Relation an.

(d) Ist diese Menge injektiv? Falls nein, geben Sie die größte injektive Teilmenge dieser Relation an.

(e) Ist diese Menge total auf $\{n \in \mathbb{N}_+ \mid n \leq 8\}$? Falls nein, geben Sie die größte Menge an, auf der diese Relation total ist.

Lösungsvorschlag Z3.3

(a)
- Wurzel: 7
- Quelle: nicht vorhanden
- Senke: 4
- isolierter Konten: nicht vorhanden
- Zyklus: $\langle 1, 7, 6, 5, 1\rangle$

(b) $\{(1,2),(1,4),(1,7),(2,3),(3,4),(5,1),(6,5),(7,4),(7,6)(7,8),(8,4)\}$

(c) Nein, sie ist nicht funktional. Funktionale Teilmenge: z.B. $\{(1,2),(2,3),(3,4),(5,1),(6,5),(7,4),(8,4)\}$

(d) Nein, sie ist nicht injektiv. Injektive Teilmenge: z.B. $\{(1,2),(1,4),(1,7),(2,3),(5,1),(6,5),(7,6)(7,8)\}$

(e) Nein, die Menge ist nicht total auf $\{n \in \mathbb{N}_+ \mid n \leq 8\}$, aber total auf $\{n \in \mathbb{N}_+ \mid n \leq 8 \land n \neq 4\}$

Terminierung

Aufgabe Z3.4 *(Welche sind gültig?)*
Gegeben sei die folgende mathematische Prozedur p:

$$\begin{aligned} & p : \mathscr{L}(\mathbb{N}) \times \mathbb{N} \to \mathbb{N} \\ & p\,(nil, n) = 0 \\ & p\,(xs, 0) = 0 && \text{für } xs \neq nil \\ & p\,(x :: xr, n) = p(xr, n-1) && \text{für } n > 0 \end{aligned}$$

Welche der folgenden Funktionen sind gültige Terminierungsfunktionen für p? Begründen Sie, falls sie ungültig sind.

- ☐ $\lambda n \in \mathbb{N}.\ n$ (ungültiger Argumentbereich)
- ☐ $\lambda z \in \mathbb{Z}.\ |z|$ (ungültiger Argumentbereich)
- ■ $\lambda(xs, n) \in \mathscr{L}(\mathbb{N}) \times \mathbb{N}.\ xs$
- ■ $\lambda(xs, n) \in \mathscr{L}(\mathbb{N}) \times \mathbb{N}.\ |xs|$
- ■ $\lambda(xs, n) \in \mathscr{L}(\mathbb{N}) \times \mathbb{N}.\ |xs| + 42$
- ☐ $\lambda(x :: xr, n) \in \mathscr{L}(\mathbb{N}) \times \mathbb{N}.\ x$ (Argument ([1,2,3], 5))
- ☐ $\lambda(xs, n) \in \mathscr{L}(\mathbb{N}) \times \mathbb{N}.\ 42 :: xs$ (ungültiger Wertebereich)
- ☐ $\lambda(xs, n) \in \mathscr{L}(\mathbb{N}) \times \mathbb{N}.\ xs\ @\ xs$ (ungültiger Wertebereich)

Aufgabe Z3.5 *(Terminierungsfunktionen)*
Geben Sie (wenn vorhanden) Terminierungsfunktionen für folgende Prozeduren an:

(a) $$\begin{aligned} & a : \mathbb{N} \to \mathbb{N} \\ & a(n) = 0 && n < 10 \\ & a(n) = a(n-3) \cdot a(n-1) && n \geq 10 \end{aligned}$$

(b) $$\begin{aligned} & b : \mathbb{Z} \to \mathbb{N} \\ & b(n) = 7 - n && n < -100 \\ & b(n) = b(n-1) - b(n-1) && n \geq -100 \end{aligned}$$

(c) $$\begin{aligned} & c : \mathbb{N} \to \mathbb{N} \\ & c(n) = 123 && n > 15 \\ & c(n) = c(n+1) && n \leq 15 \end{aligned}$$

(d) $$\begin{aligned} & d : \mathbb{Z} \to \mathbb{Z} \\ & d(n) = 100 + d(n \operatorname{div} 10) && n \mod 2 = 0 \\ & d(n) = d(n+1) && n \mod 2 \neq 0 \end{aligned}$$

(e) $$\begin{aligned} & e : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \\ & e(m,n) = e(m-1,n) && m > 4 \\ & e(m,n) = e(m,n-1) && m \leq 4 \ \land\ n > 10 \\ & e(m,n) = m^n \cdot m && m \leq 4 \ \land\ n \leq 10 \end{aligned}$$

(f) $$\begin{aligned} & f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \\ & f(m,n) = 100 \cdot n - m && m > n \\ & f(m,n) = f(m+2, n+1) && m \leq n \end{aligned}$$

(g) $$\begin{aligned} & g : \mathbb{Z} \times \mathbb{Z} \to \mathbb{N} \\ & g(m,n) = g(m-1,n) && m > n \\ & g(m,n) = g(n, m+1) && m < n \\ & g(m,n) = 3 && m = n \end{aligned}$$

(h) $$\begin{aligned} & h : \mathscr{L}(X) \to \mathbb{N} \\ & h(nil) = 4 \\ & h(x :: xr) = 2 \cdot h(xr) + 1 \end{aligned}$$

Lösungsvorschlag Z3.5

(a) $\lambda n \in \mathbb{N}.n$

(b) $\lambda n \in \mathbb{Z}.\text{if } n < -100 \text{ then } 0 \text{ else } n + 101$

(c) $\lambda n \in \mathbb{N}.\text{if } n > 15 \text{ then } 0 \text{ else } 16 - n$

(d) d terminiert nicht.

(e) $\lambda(m,n) \in \mathbb{N} \times \mathbb{N}.m + n$

(f) $\lambda(m,n) \in \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}.\ \text{if } m > n \text{ then } 0 \text{ else } n - m + 1$

(g) $\lambda(m,n) \in \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}.\, |m-n|$

(h) $\lambda xs \in \mathscr{L}(X).xs$

Aufgabe Z3.6 *(Strukturelle Terminierung)*
Die Konkatenation von Listen sei wie folgt definiert:

$$
\begin{aligned}
@ : \mathscr{L}(X) \times \mathscr{L}(X) &\to \mathscr{L}(X) \\
nil@ys &= ys \\
(x :: xr)@ys &= x :: (xr@ys)
\end{aligned}
$$

Welche der folgenden Funktionen ist eine strukturelle Terminierungsfunktion für @?

- ☐ $\lambda(xs, ys) \in \mathscr{L}(X)^2 .\ |xs|$
- ☐ $\lambda(xs, ys) \in \mathscr{L}(X)^2 .\ (xs, ys)$
- ■ $\lambda(xs, ys) \in \mathscr{L}(X)^2 .\ xs$
- ☐ $\lambda(xs, ys) \in \mathscr{L}(X)^2 .\ ys$
- ■ $\lambda(xs, ys) \in \mathscr{L}(X)^2 .\ xs@ys$,wobei @ die Ergebnisfunktion der oben definierten Prozedur ist.

Korrektheitssatz

Aufgabe Z3.7 *(Korrektheit I)*
Zeigen Sie, dass die Prozedur $p : \mathbb{N} \to \mathbb{N}$, die durch

$$p\ n = \text{if } n < 1 \text{ then } 1 \text{ else } p(n-1) + 2n + 1$$

definiert ist, die Funktion $\lambda n \in \mathbb{N}.\, (n+1)^2$ berechnet.

Lösungsvorschlag Z3.7
Sei $f = \lambda n \in \mathbb{N}.\, (n+1)^2$.
Beweis mit dem Korrektheitssatz.
Die natürliche Terminierungsfunktion $\lambda n \in \mathbb{N}.\, n$ zeigt, dass $Dom\, p = \mathbb{N}$ und somit $Dom\, f \subseteq Dom\, p$.
Laut Satz 9.10 wird f dann von p berechnet, falls f die definierenden Gleichungen von p für alle $n \in \mathbb{N}$ erfüllt.
Für den Fall $n = 0$ ist dies klar, da $(0+1)^2 = 1$. Sei also $n > 0$, dann gilt

$$
\begin{aligned}
f\,n &= (n+1)^2 && \text{(Definition von } f\text{)} \\
&= n^2 + 2n + 1 && \text{(Binomische Formel)} \\
&= ((n-1)+1)^2 + 2n + 1 && \text{(Arithmetik)} \\
&= f(n-1) + 2n + 1 && \text{(Definition von } f\text{)} \\
&= \text{if } n < 1 \text{ then } 1 \text{ else } f(n-1) + 2n + 1 && (n > 0)
\end{aligned}
$$

Aufgabe Z3.8 *(Korrektheit II)*
Gegeben seien folgende Prozeduren, geben Sie jeweils die Ergebnisfunktion an und beweisen Sie ihre Korrektheit mit dem Korrektheitssatz.

(a)
$$
\begin{aligned}
&a : \mathbb{N} \to \mathbb{N} \\
&a\ n = 1 && \text{für } n = 0 \\
&a\ n = 2 \cdot a(n-1) + 2 \cdot a(n-1) && \text{für } n > 0
\end{aligned}
$$

(b)
$$
\begin{aligned}
&b : \mathbb{Z} \times \mathbb{N} \to \mathbb{Z} \\
&b(n,m) = 1 && \text{für } m = 0 \\
&b(n,m) = n \cdot b(n, m-1) && \text{für } m \neq 0
\end{aligned}
$$

(c) $$\begin{aligned} &c : \mathbb{N} \to \mathbb{Z} \\ &c\ 0 = 0 \\ &c\ n = c\ (n-1) - 2 \quad \text{für } n > 0 \end{aligned}$$

(d) $$\begin{aligned} &d : \mathbb{N} \to \mathbb{N} \\ &d\ 0 = 0 \\ &d\ 1 = 1 \\ &d\ n = 1 + d(n-2) \quad \text{für } n > 1 \end{aligned}$$

Lösungsvorschlag Z3.8

(a) Ergebnisfunktion: $f = \lambda n \in \mathbb{N}.4^n$
Beweis mit dem Korrektheitssatz. Wir zeigen zuerst, dass $Dom\ f \subseteq Dom\ a$ gilt. Dafür zeigen wir mithilfe einer natürlichen Terminierungsfunktion, dass a für alle $n \in \mathbb{N}$ terminiert: $\lambda n \in \mathbb{N}.n$
Somit gilt $Dom\ f = \mathbb{N} = Dom\ a$
Nun bleibt noch zu zeigen, dass f die definierenden Gleichungen von a erfüllt.

- 1. Fall: $n = 0$

$$\begin{aligned} 1 &= 4^0 && \text{Arithmetik} \\ &= f\ 0 && \text{Definition von f} \end{aligned}$$

- 2. Fall: $n > 0$

$$\begin{aligned} 2 \cdot f(n-1) + 2 \cdot f(n-1) &= 2 \cdot 4^{n-1} + 2 \cdot 4^{n-1} && \text{Definition von } f \\ &= 2 \cdot (2 \cdot 4^{n-1}) && \text{Arithmetik} \\ &= 4 \cdot 4^{n-1} && \text{Arithmetik} \\ &= 4^n && \text{Arithmetik} \\ &= f\ n && \text{Definition von } f \end{aligned}$$

(b) Ergebnisfunktion: $g = \lambda(n, m) \in \mathbb{Z} \times \mathbb{N}.n^m$
Beweis mit dem Korrektheitssatz. Wir zeigen zuerst, dass $Dom\ g \subseteq Dom\ b$ gilt. Dafür zeigen wir mithilfe einer natürlichen Terminierungsfunktion, dass b für alle $(n, m) \in \mathbb{Z} \times \mathbb{N}$ terminiert: $\lambda(n, m) \in \mathbb{Z} \times \mathbb{N}.m$
Somit gilt $Dom\ g = \mathbb{N} = Dom\ b$
Nun bleibt noch zu zeigen, dass g die definierenden Gleichungen von b erfüllt.

- 1. Fall: $m = 0$

$$\begin{aligned} 1 &= n^0 && \text{Arithmetik} \\ &= g\ (n, 0) && \text{Definition von } g \end{aligned}$$

- 2. Fall: $m > 0$

$$\begin{aligned} n \cdot g\ (n, m-1) &= n \cdot n^{m-1} && \text{Definition von } g \\ &= n^m && \text{Arithmetik} \\ &= g\ (n, m) && \text{Definition von } g \end{aligned}$$

(c) Ergebnisfunktion: $h = \lambda n \in \mathbb{N}.{-2} \cdot n$
Beweis mit dem Korrektheitssatz. Wir zeigen zuerst, dass $Dom\ h \subseteq Dom\ c$ gilt. Dafür zeigen wir mithilfe einer natürlichen Terminierungsfunktion, dass c für alle $n \in \mathbb{N}$ terminiert: $\lambda n \in \mathbb{N}.n$
Somit gilt $Dom\ h = \mathbb{N} = Dom\ c$
Nun bleibt noch zu zeigen, dass h die definierenden Gleichungen von c erfüllt.

- 1. Fall: $n = 0$

$$\begin{aligned} 0 &= -2 \cdot 0 && \text{Arithmetik} \\ &= h\ 0 && \text{Definition von } h \end{aligned}$$

- 2. Fall: n>0

$$\begin{aligned} h(n-1)-2 &= -2\cdot(n-1)-2 && \text{Definition von } h \\ &= -2n+2-2 && \text{Arithmetik} \\ &= -2n && \text{Arithmetik} \\ &= h\ n && \text{Definition von } h \end{aligned}$$

(d) Ergebnisfunktion: $i := \lambda n \in \mathbb{N}.\lceil \frac{n}{2} \rceil$
Beweis mit dem Korrektheitssatz. Wir zeigen zuerst, dass $Dom\ i \subseteq Dom\ d$ gilt. Dafür zeigen wir mithilfe einer natürlichen Terminierungsfunktion, dass d für alle $n \in \mathbb{N}$ terminiert: $\lambda n \in \mathbb{N}.n$
Somit gilt $Dom\ i = \mathbb{N} = Dom\ d$
Nun bleibt noch zu zeigen, dass i die definierenden Gleichungen von d erfüllt.

- 1. Fall: $n = 0$

$$\begin{aligned} i\ 0 &= \left\lceil \frac{0}{2} \right\rceil && \text{Definition } i \\ &= 0 && \text{Arithmetik, Definition von } \lceil\cdot\rceil \end{aligned}$$

- 2. Fall: $n = 1$

$$\begin{aligned} i\ 1 &= \left\lceil \frac{1}{2} \right\rceil && \text{Definition von } i \\ &= 1 && \text{Arithmetik, Definition von } \lceil\cdot\rceil \end{aligned}$$

- 3. Fall: $n > 1$

$$\begin{aligned} i\ n &= \left\lceil \frac{n}{2} \right\rceil && \text{Definition von } i \\ &= 1 + \left\lceil \frac{n}{2} \right\rceil - 1 && \text{Arithmetik} \\ &= 1 + \left\lceil \frac{n}{2} - 1 \right\rceil && \text{Arithmetik, Definition von } \lceil\cdot\rceil \\ &= 1 + \left\lceil \frac{n-2}{2} \right\rceil && \text{Arithmetik} \\ &= 1 + i\ (n-2) && \text{Definition von } i \end{aligned}$$

Aufgabe Z3.9 *(Korrektheit III)*
Beweisen Sie, dass die Prozedur

$$\begin{aligned} &\mathit{fak} : \mathbb{N} \to \mathbb{N} \\ &\mathit{fak}(n) = 1 && \text{für } n = 0 \\ &\mathit{fak}(n) = n \cdot \mathit{fak}(n-1) && \text{für } n > 0 \end{aligned}$$

die Funktion $\mathit{fac} := \lambda n \in \mathbb{N}.n!$ berechnet.

Lösungsvorschlag Z3.9
Beweis mit dem Korrektheitssatz.
Zunächst zeigen wir, dass die Prozedur *fak* terminiert. Dazu geben wir eine natürliche Terminierungsfunktion an: $\lambda n \in \mathbb{N}.n$. Also ist $Dom\,\mathit{fac} \subseteq Dom\,\mathit{fak}$.
Nun bleibt zu zeigen, dass *fac* die definierenden Gleichungen von *fak* erfüllt. Dafür machen wir eine Fallunterscheidung:

- 1. Fall: $n = 0$:

$$\begin{aligned} 1 &= 0! && \text{Arithmetik} \\ &= \mathit{fac}(0) && \text{Definition } \mathit{fac} \end{aligned}$$

- 2. Fall: $n > 0$:

$$\begin{aligned} n \cdot \mathit{fac}(n-1) &= n \cdot (n-1)! && \text{Definition von } \mathit{fac} \\ &= n! && \text{Arithmetik} \\ &= \mathit{fac}(n) && \text{Definition von } \mathit{fac} \end{aligned}$$

Aufgabe Z3.10 *(Addition)*
Wir wollen zeigen, dass sich Addition nur mit Inkrementierung (Erhöhen einer Zahl um 1) und Dekrementierung (Reduzieren einer Zahl um 1) berechnen lässt.

(a) Schreiben Sie eine mathematische Prozedur, die Addition $x + y$ für $x, y \geq 0$ berechnet. Wenn sie den Operator + verwenden, dürfen Sie dabei nur $x + 1$ für ein beliebiges x schreiben. Wenn Sie den Operator - verwenden, dürfen Sie nur $x - 1$ für ein beliebiges x schreiben.

(b) Beweisen Sie mithilfe des Korrektheitssatzes, dass ihre Prozedur die folgende Funktion berechnet:

$$f \in \mathbb{N}^2 \to \mathbb{N}$$
$$f(x, y) = x + y$$

Lösungsvorschlag Z3.10

(a)

$$\begin{aligned} &\mathit{add} : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \\ &\mathit{add}(x, 0) = x \\ &\mathit{add}(x, y) = \mathit{add}(x, y-1) + 1 && \text{für y} > 0 \end{aligned}$$

(b) *Beweis mit dem Korrektheitssatz.*

(i) Zu zeigen ist, dass $\mathit{Dom}\ f \subseteq \mathit{Dom}\ \mathit{add}$.

$\lambda(x, y) \in \mathbb{N}^2. y$ ist eine natürliche Terminierungsfunktion für *add*. Also terminiert *add* für alle Argumente und daher gilt $\mathit{Dom}\ \mathit{add} = \mathbb{N}^2 = \mathit{Dom}\ f$.

(ii) Nun ist zu zeigen, dass f für alle $(x, y) \in \mathbb{N}^2$ die definierenden Gleichungen von *add* erfüllt. Wir unterscheiden zwei Fälle:

- Fall x beliebig, $y = 0$:

$$\begin{aligned} f(x, y) &= f(x, 0) && y = 0 \\ &= x + 0 && \text{Definition } f \\ &= x && \text{Definition } f, \text{da } x \in \mathbb{N} \end{aligned}$$

- Fall x beliebig, y > 0:

$$\begin{aligned} f(x, y) &= f(x, y-1) + 1 && \text{Definition add, y} > 0 \\ x + y &= x + (y - 1) + 1 && \text{Definition } f,\ x, y-1 \in \mathbb{N} \\ &= (x + y) + (-1 + 1) && \text{Arithmetik} \\ &= x + y && \text{Arithmetik} \end{aligned}$$

wahr.

Somit berechnet die Prozedur *add* die Funktion f. ∎

Aufgabe Z3.11 *(Quadratzahlen)*
Gegeben sei folgenden mathematische Prozedur:

$$\begin{aligned}
&p : \mathbb{N} \to \mathbb{N} \\
&p\ 0 = 0 \\
&p\ n = p\ (n-1) + n \cdot n && \text{für } n > 0
\end{aligned}$$

Beweisen Sie, dass diese Prozedur die Summe der ersten n Quadratzahlen, also die Funktion $f \in \mathbb{N} \to \mathbb{N}$ mit $f = \lambda n \in \mathbb{N}. \sum_{i=1}^{n} i^2$ berechnet.

Lösungsvorschlag Z3.11

Beweis mit dem Korrektheitssatz. Man zeige zunächst, dass gilt $Dom\ f \subseteq Dom\ p$. Dazu zeige man, dass $Dom\ p = \mathbb{N}$, indem man eine natürliche Terminierungsfunktion für p angibt und damit zeigt, dass p für alle Argumente terminiert:

$\lambda n \in \mathbb{N}. n$ ist eine gültige natürliche Terminierungsfunktion, die die Terminierung von p garantiert.

Man zeige nun, dass f die definierenden Gleichungen von p erfüllt. Wir unterscheiden zwei Fälle.

- Fall: n = 0

$$\begin{aligned}
f\ 0 &= \sum_{i=1}^{0} i^2 && \text{Definition } f \\
&= 0 && \text{Arithmetik}
\end{aligned}$$

- Fall: n > 0

$$\begin{aligned}
f\ n &= \sum_{i=1}^{n} i^2 && \text{Definition } f \\
&= \sum_{i=1}^{n-1} i^2 + n^2 && \text{Arithmetik} \\
&= \sum_{i=1}^{n-1} i^2 + n \cdot n && \text{Arithmetik} \\
&= f\ (n-1) + n \cdot n && \text{Definition } f
\end{aligned}$$

∎