

## Definitions and Laws of Arithmetic on $\mathbb{N}$ . [With Hints!](#)

Addition

$$\begin{aligned} m + 0 &:= m && \text{(IC)} \\ m + S(n) &:= S(m + n) && \text{(RR)} \end{aligned}$$

Multiplication

$$\begin{aligned} m \cdot 0 &:= 0 && \text{(IC)} \\ m \cdot S(n) &:= m \cdot n + m && \text{(RR)} \end{aligned}$$

Exponentiation

$$\begin{aligned} m^0 &:= 1 && \text{(IC)} \\ m^{S(n)} &:= m^n \cdot m && \text{(RR)} \end{aligned}$$

(Each of these operations is defined by recursion on its *second* variable.)

Laws of successor. (These should be proved first.)

- (a) 0 is not a successor. Every nonzero natural number is the successor of some natural number.

For the first part,  $0 = \emptyset$  has no elements, while any successor has at least one element ( $x \in x \cup \{x\} = S(x)$ ).

For the second part, the set of natural numbers that are successors of natural numbers, together with 0, namely the set

$$\{n \in \mathbb{N} \mid \exists k((k \in \mathbb{N}) \wedge (n = S(k)))\} \cup \{0\},$$

is an inductive subset of  $\mathbb{N}$ , hence equals  $\mathbb{N}$ . This implies that every nonzero element  $n \in \mathbb{N}$  is the successor of some element  $k \in \mathbb{N}$ .

- (b) Successor is injective. ( $S(m) = S(n)$  implies  $m = n$ .)

If  $S(x) = S(y)$ , then  $x \cup \{x\} = y \cup \{y\}$ . Our goal is to prove  $x = y$ , so let's assume that this is not the case and derive a contradiction.

We have  $x \in x \cup \{x\}$ , and  $x \cup \{x\} = y \cup \{y\}$ , so  $x \in y \cup \{y\}$ . We have assumed that  $x \neq y$ , so we must have  $x \in y$ . A similar argument shows that  $y \in x$ . This contradicts the Axiom of Foundation. (Specifically, the unordered pair  $\{x, y\}$  has no  $\in$ -minimal element.)

Laws of addition.

(a)  $S(n) = n + 1$

$$\begin{aligned} n + 1 &= n + S(0) && \text{(Defn of 1)} \\ &= S(n + 0) && \text{((RR), +)} \\ &= S(n) && \text{((IC), +)} \end{aligned}$$

(b) (Associative Law)  $m + (n + k) = (m + n) + k$

We prove this by induction on  $k$ .

(Base Case:  $k = 0$ )

$$\begin{aligned} m + (n + 0) &= m + n && \text{((IC), +)} \\ &= (m + n) + 0 && \text{((IC), +)} \end{aligned}$$

(Inductive Step: Assume true for  $k$ , prove true for  $S(k)$ )

$$\begin{aligned} m + (n + S(k)) &= m + S(n + k) && \text{((RR), +)} \\ &= S(m + (n + k)) && \text{((RR), +)} \\ &= S((m + n) + k) && \text{(IH)} \\ &= (m + n) + S(k) && \text{((RR), +)} \end{aligned}$$

(c) (Unit Law for 0)  $m + 0 = 0 + m = m$

The fact that  $m + 0 = m$  is part of the definition of addition, so we only need to prove that  $0 + m = m$ . We argue this by induction on  $m$ .

(Base Case:  $m = 0$ )

$$0 + 0 = 0 \quad \text{((IC), +)}$$

(Inductive Step: Assume true for  $m$ , prove true for  $S(m)$ )

$$\begin{aligned} 0 + S(m) &= S(0 + m) && \text{((RR), +)} \\ &= S(m) && \text{(IH)} \end{aligned}$$

(d) (Commutative Law)  $m + n = n + m$

We argue this by induction on  $n$ .

(Base Case:  $n = 0$ )

$$m + 0 = 0 + m \quad (\text{Part (c), } +)$$

Before proceeding to the inductive step, we prove a lemma. It is the “ $n = 1$  case” of the Commutative Law.

**Lemma.**  $m + 1 = 1 + m$ .

*Proof of Lemma.*

(Base Case:  $m = 0$ )

$$\begin{aligned} m + 1 = 0 + 1 &= 0 + S(0) && (\text{Defn of } 1) \\ &= S(0 + 0) && ((\text{RR}), +) \\ &= S(0) && ((\text{IC}), +) \\ &= 1 && (\text{Defn of } 1) \\ &= 1 + 0 = 1 + m && ((\text{IC}), +) \end{aligned}$$

(Inductive Step: Assume  $m + 1 = 1 + m$  for some  $m$ , prove  $S(m) + 1 = 1 + S(m)$ )

$$\begin{aligned} 1 + S(m) &= S(1 + m) && ((\text{RR}), +) \\ &= S(m + 1) && (\text{IH}) \\ &= S(S(m)) && (\text{Part (a), } S) \\ &= S(m) + 1 && (\text{Part (a), } S) \end{aligned}$$

Now we give the Inductive Step for the proof of (d). We assume that  $m + n = n + m$  holds and derive that  $m + S(n) = S(n) + m$ .

$$\begin{aligned} m + S(n) &= S(m + n) && ((\text{RR}), +) \\ &= S(n + m) && (\text{IH}) \\ &= n + S(m) && ((\text{RR}), +) \\ &= n + (m + 1) && (\text{Part (a), } S) \\ &= n + (1 + m) && (\text{Lemma}) \\ &= (n + 1) + m && (\text{Part (b), } +) \\ &= S(n) + m && ((\text{RR}), +) \end{aligned}$$

(e) (+-Irreducibility of 0)  $m + n = 0$  implies  $m = n = 0$ .

If  $n \neq 0$ , then  $n = S(k)$  by Part (a) of the Laws of Successor. Then  $0 = m + n = m + S(k) = S(m + k)$ , contradicting that 0 is not a successor. Hence  $0 = m + n$  forces  $n = 0$ . But now  $0 = m + n = m + 0 = m$ , so  $m = 0$  too.

(f) (Cancellation)  $m + k = n + k$  implies  $m = n$ .

(Base Case:  $k = 0$ )

$$\begin{array}{ll} m &= m + 0 && ((IC), +) \\ &= n + 0 && (\text{assumption}) \\ &= n && ((IC), +) \end{array}$$

(Inductive Step: Assume that  $m + k = n + k$  implies  $m = n$ . Prove that  $m + S(k) = n + S(k)$  implies  $m = n$ .)

Assume that  $m + S(k) = n + S(k)$ . Then by  $((RR), +)$  we have  $S(m + k) = S(n + k)$ . But the successor function is injective, by Part (b) of the Laws of Successor. Thus,  $m + k = n + k$ . Now, by the inductive hypothesis, we derive that  $m = n$ .

Laws of multiplication (and addition).

- (a) (Associative Law)  $m \cdot (n \cdot k) = (m \cdot n) \cdot k$
- (b) (Unit Law for 1)  $m \cdot 1 = 1 \cdot m = m$
- (c) (Commutative Law)  $m \cdot n = n \cdot m$
- (d) (0 is absorbing)  $m \cdot 0 = 0 \cdot m = 0$
- (e) ( $\cdot$ -Irreducibility of 1)  $m \cdot n = 1$  implies  $m = n = 1$
- (f) (Distributive Law)  $m \cdot (n + k) = (m \cdot n) + (m \cdot k)$

Laws of exponentiation (and multiplication and addition).

- (a)  $m^0 = 1$ ,  $m^1 = m$ ,  $0^m = 0$  (if  $m > 0$ ), and  $1^m = 1$ .
- (b)  $m^{n+k} = m^n \cdot m^k$
- (c)  $(m \cdot n)^k = m^k \cdot n^k$
- (d)  $(m^n)^k = m^{n \cdot k}$