

## Definitions and Laws of Arithmetic on $\mathbb{N}$ .

Addition

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

$$m + S(n) := S(m + n) \quad (\text{RR})$$

Multiplication

$$m \cdot 0 := 0 \quad (\text{IC})$$

$$m \cdot S(n) := m \cdot n + m \quad (\text{RR})$$

Exponentiation

$$m^0 := 1 \quad (\text{IC})$$

$$m^{S(n)} := m^n \cdot m \quad (\text{RR})$$

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

(a) 0 is not a successor.

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

Laws of addition. (Provable by induction or from the definitions.)

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

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

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

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

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

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

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) (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)  $(m^n)^k = m^{n \cdot k}$