

EVENT: Start with the initial **nqthm** theory.

THEOREM: plus-right-id2
 $(y \notin \mathbf{N}) \rightarrow ((x + y) = \text{fix}(x))$

THEOREM: plus-add1
 $(x + (1 + y))$
 $= \text{if } y \in \mathbf{N} \text{ then } 1 + (x + y)$
 $\text{else } 1 + x \text{ endif}$

THEOREM: commutativity2-of-plus
 $(x + y + z) = (y + x + z)$

THEOREM: commutativity-of-plus
 $(x + y) = (y + x)$

THEOREM: associativity-of-plus
 $((x + y) + z) = (x + y + z)$

THEOREM: plus-equal-0
 $((a + b) = 0) = ((a \simeq 0) \wedge (b \simeq 0))$

THEOREM: difference-x-x
 $(x - x) = 0$

THEOREM: difference-plus
 $((x + y) - x) = \text{fix}(y) \wedge ((y + x) - x) = \text{fix}(y)$

THEOREM: plus-cancellation
 $((a + b) = (a + c)) = (\text{fix}(b) = \text{fix}(c))$

THEOREM: difference-0
 $(y \not\leq x) \rightarrow ((x - y) = 0)$

THEOREM: equal-difference-0
 $(0 = (x - y)) = (y \not\leq x)$

THEOREM: difference-cancellation-0
 $(x = (x - y)) = ((x \in \mathbf{N}) \wedge ((x = 0) \vee (y \simeq 0)))$

THEOREM: difference-cancellation-1
 $((x - y) = (z - y))$
 $= \text{if } x < y \text{ then } y \not\leq z$
 $\text{elseif } z < y \text{ then } y \not\leq x$
 $\text{else } \text{fix}(x) = \text{fix}(z) \text{ endif}$

THEOREM: times-zero2
 $(y \notin \mathbf{N}) \rightarrow ((x * y) = 0)$

THEOREM: distributivity-of-times-over-plus
 $(x * (y + z)) = ((x * y) + (x * z))$

THEOREM: times-add1
 $(x * (1 + y))$
 $= \text{if } y \in \mathbf{N} \text{ then } x + (x * y)$
 $\text{else fix}(x) \text{ endif}$

THEOREM: commutativity-of-times
 $(x * y) = (y * x)$

THEOREM: commutativity2-of-times
 $(x * y * z) = (y * x * z)$

THEOREM: associativity-of-times
 $((x * y) * z) = (x * y * z)$

THEOREM: equal-times-0
 $((x * y) = 0) = ((x \simeq 0) \vee (y \simeq 0))$

DEFINITION:
 $\text{exp}(i, j)$
 $= \text{if } j \simeq 0 \text{ then } 1$
 $\text{else } i * \text{exp}(i, j - 1) \text{ endif}$

THEOREM: exp-plus
 $\text{exp}(i, j + k) = (\text{exp}(i, j) * \text{exp}(i, k))$

THEOREM: equal-lessp
 $((x < y) = z)$
 $= \text{if } x < y \text{ then } t = z$
 $\text{else } f = z \text{ endif}$

THEOREM: difference-elim
 $((y \in \mathbf{N}) \wedge (y \not< x)) \rightarrow ((x + (y - x)) = y)$

THEOREM: remainder-quotient
 $((x \bmod y) + (y * (x \div y))) = \text{fix}(x)$

THEOREM: remainder-wrt-1
 $(y \bmod 1) = 0$

THEOREM: remainder-wrt-12
 $(x \notin \mathbf{N}) \rightarrow ((y \bmod x) = \text{fix}(y))$

THEOREM: lessp-remainder2

$$((x \bmod y) < y) = (y \neq 0)$$

THEOREM: remainder-x-x

$$(x \bmod x) = 0$$

THEOREM: remainder-quotient-elim

$$((y \neq 0) \wedge (x \in \mathbf{N})) \rightarrow (((x \bmod y) + (y * (x \div y))) = x)$$

THEOREM: lessp-times-1

$$(i \neq 0) \rightarrow ((i * j) \not< j)$$

THEOREM: lessp-times-2

$$(i \neq 0) \rightarrow ((j * i) \not< j)$$

THEOREM: lessp-quotient1

$$((i \div j) < i) = ((i \neq 0) \wedge ((j \simeq 0) \vee (j \neq 1)))$$

THEOREM: lessp-remainder1

$$((x \bmod y) < x) = ((y \neq 0) \wedge (x \neq 0) \wedge (x \not< y))$$

THEOREM: difference-plus1

$$((x + y) - x) = \text{fix}(y)$$

THEOREM: difference-plus2

$$((y + x) - x) = \text{fix}(y)$$

THEOREM: difference-plus-cancellation

$$((x + y) - (x + z)) = (y - z)$$

THEOREM: times-difference

$$(x * (c - w)) = ((c * x) - (w * x))$$

DEFINITION: divides $(x, y) = ((y \bmod x) \simeq 0)$

THEOREM: divides-times

$$((x * z) \bmod z) = 0$$

THEOREM: difference-plus3

$$((b + a + c) - a) = (b + c)$$

THEOREM: difference-add1-cancellation

$$((1 + (y + z)) - z) = (1 + y)$$

THEOREM: remainder-add1

$$((y \neq 0) \wedge (y \neq 1)) \rightarrow (((1 + (x * y)) \bmod y) \neq 0)$$

THEOREM: divides-plus-rewrite1

$$(((x \bmod z) = 0) \wedge ((y \bmod z) = 0)) \rightarrow (((x + y) \bmod z) = 0)$$

THEOREM: divides-plus-rewrite2

$$(((x \bmod z) = 0) \wedge ((y \bmod z) \neq 0)) \rightarrow (((x + y) \bmod z) \neq 0)$$

THEOREM: divides-plus-rewrite

$$((x \bmod z) = 0) \rightarrow (((x + y) \bmod z) = 0) = ((y \bmod z) = 0)$$

THEOREM: lessp-plus-cancellation

$$((x + y) < (x + z)) = (y < z)$$

THEOREM: divides-plus-rewrite-commuted

$$((x \bmod z) = 0) \rightarrow (((y + x) \bmod z) = 0) = ((y \bmod z) = 0)$$

THEOREM: euclid

$$\begin{aligned} & ((x \bmod z) = 0) \\ \rightarrow & (((y - x) \bmod z) = 0) \\ = & \text{if } x < y \text{ then } (y \bmod z) = 0 \\ & \text{else t endif} \end{aligned}$$

THEOREM: lessp-times-cancellation

$$((x * z) < (y * z)) = ((z \neq 0) \wedge (x < y))$$

THEOREM: lessp-plus-cancellation3

$$(y < (x + y)) = (x \neq 0)$$

THEOREM: quotient-times1

$$\begin{aligned} & ((y \in \mathbf{N}) \wedge (x \in \mathbf{N}) \wedge (x \neq 0) \wedge \text{divides}(x, y)) \\ \rightarrow & ((x * (y \div x)) = y) \end{aligned}$$

THEOREM: quotient-lessp

$$((x \neq 0) \wedge (x < y)) \rightarrow ((y \div x) \neq 0)$$

DEFINITION:

$$\begin{aligned} & \text{greatereqpr}(w, z) \\ = & \text{if } w \simeq 0 \text{ then } z \simeq 0 \\ & \text{elseif } w = z \text{ then t} \\ & \text{else greatereqpr}(w - 1, z) \text{ endif} \end{aligned}$$

THEOREM: times-id-iff-1

$$(z = (w * z)) = ((z \in \mathbf{N}) \wedge ((z = 0) \vee (w = 1)))$$

THEOREM: greatereqpr-lessp

$$\text{greatereqpr}(x, y) = (x \not< y)$$

THEOREM: greaterreqpr-remainder

$$((z \neq (1 + v)) \wedge \text{divides}(z, 1 + v)) \rightarrow \text{greaterreqpr}(v, z)$$

THEOREM: divides-times1

$$(a = (z * y)) \rightarrow ((a \mathbf{mod} z) = 0)$$

THEOREM: times-identity1

$$((y \in \mathbf{N}) \wedge (y \neq 1) \wedge (y \neq 0) \wedge (x \neq 0)) \rightarrow (x \neq (x * y))$$

THEOREM: times-identity

$$(x = (x * y)) = ((x = 0) \vee ((x \in \mathbf{N}) \wedge (y = 1)))$$

THEOREM: quotient-divides

$$((y \in \mathbf{N}) \wedge ((x * (y \div x)) \neq y)) \rightarrow ((y \mathbf{mod} x) \neq 0)$$

THEOREM: remainder-times

$$((y * x) \mathbf{mod} y) = 0$$

THEOREM: quotient-times

$$\begin{aligned} & ((y * x) \div y) \\ = & \text{ if } y \simeq 0 \text{ then } 0 \\ & \text{ else fix}(x) \text{ endif} \end{aligned}$$

THEOREM: distributivity-of-divides

$$((a \not\approx 0) \wedge \text{divides}(a, w)) \rightarrow ((c * (w \div a)) = ((c * w) \div a))$$

THEOREM: if-times-then-divides

$$((c \not\approx 0) \wedge (\neg \text{divides}(c, x))) \rightarrow ((c * y) \neq x)$$

THEOREM: times-equal-1

$$\begin{aligned} & ((a * b) = 1) \\ = & ((a \neq 0) \\ & \wedge (b \neq 0) \\ & \wedge (a \in \mathbf{N}) \\ & \wedge (b \in \mathbf{N}) \\ & \wedge ((a - 1) = 0) \\ & \wedge ((b - 1) = 0)) \end{aligned}$$

THEOREM: divides-implies-times

$$((a \not\approx 0) \wedge (c \in \mathbf{N}) \wedge ((a * c) = b)) \rightarrow ((c = (b \div a)) = \mathbf{t})$$

THEOREM: difference-1

$$(x - 1) = (x - 1)$$

THEOREM: difference-2

$$((1 + (1 + x)) - 2) = \text{fix}(x)$$

THEOREM: half-plus

$$((x + x + y) \div 2) = (x + (y \div 2))$$

THEOREM: times-1

$$(1 * x) = \text{fix}(x)$$

THEOREM: exp-of-0

$$\begin{aligned} &\text{exp}(0, k) \\ &= \text{if } k \simeq 0 \text{ then } 1 \\ &\quad \text{else } 0 \text{ endif} \end{aligned}$$

THEOREM: exp-of-1

$$\text{exp}(1, k) = 1$$

THEOREM: exp-by-0

$$\text{exp}(x, 0) = 1$$

THEOREM: exp-times

$$\text{exp}(i * j, k) = (\text{exp}(i, k) * \text{exp}(j, k))$$

THEOREM: exp-exp

$$\text{exp}(\text{exp}(i, j), k) = \text{exp}(i, j * k)$$

THEOREM: remainder-plus-times-1

$$((x + (i * j)) \bmod j) = (x \bmod j)$$

THEOREM: remainder-plus-times-2

$$((x + (j * i)) \bmod j) = (x \bmod j)$$

THEOREM: remainder-times-1

$$((b * a * c) \bmod a) = 0$$

THEOREM: remainder-of-1

$$\begin{aligned} &(1 \bmod x) \\ &= \text{if } x = 1 \text{ then } 0 \\ &\quad \text{else } 1 \text{ endif} \end{aligned}$$

DEFINITION:

length(*lst*)

$$\begin{aligned} &= \text{if listp}(\text{lst}) \text{ then } 1 + \text{length}(\text{cdr}(\text{lst})) \\ &\quad \text{else } 0 \text{ endif} \end{aligned}$$

THEOREM: equal-length-0

$$(\text{length}(x) = 0) = (x \simeq \text{nil})$$

THEOREM: remainder-difference-times

$$(((p * x) - (p * y)) \bmod p) = 0$$

THEOREM: lessp-remainder-divisor
 $(y \neq 0) \rightarrow ((x \mathbf{mod} y) < y)$

EVENT: Make the library "**arith**".

Index

- associativity-of-plus, 1
- associativity-of-times, 2

- commutativity-of-plus, 1
- commutativity-of-times, 2
- commutativity2-of-plus, 1
- commutativity2-of-times, 2

- difference-0, 1
- difference-1, 5
- difference-2, 5
- difference-add1-cancellation, 3
- difference-cancellation-0, 1
- difference-cancellation-1, 1
- difference-elim, 2
- difference-plus, 1
- difference-plus-cancellation, 3
- difference-plus1, 3
- difference-plus2, 3
- difference-plus3, 3
- difference-x-x, 1
- distributivity-of-divides, 5
- distributivity-of-times-over-plus, 2
- divides, 3–5
- divides-implies-times, 5
- divides-plus-rewrite, 4
- divides-plus-rewrite-commuted, 4
- divides-plus-rewrite1, 4
- divides-plus-rewrite2, 4
- divides-times, 3
- divides-times1, 5

- equal-difference-0, 1
- equal-length-0, 6
- equal-lessp, 2
- equal-times-0, 2
- euclid, 4
- exp, 2, 6
- exp-by-0, 6
- exp-exp, 6

- exp-of-0, 6
- exp-of-1, 6
- exp-plus, 2
- exp-times, 6

- greaterreqpr, 4, 5
- greaterreqpr-lessp, 4
- greaterreqpr-remainder, 5

- half-plus, 6

- if-times-then-divides, 5

- length, 6
- lessp-plus-cancellation, 4
- lessp-plus-cancellation3, 4
- lessp-quotient1, 3
- lessp-remainder-divisor, 7
- lessp-remainder1, 3
- lessp-remainder2, 3
- lessp-times-1, 3
- lessp-times-2, 3
- lessp-times-cancellation, 4

- plus-add1, 1
- plus-cancellation, 1
- plus-equal-0, 1
- plus-right-id2, 1

- quotient-divides, 5
- quotient-lessp, 4
- quotient-times, 5
- quotient-times1, 4

- remainder-add1, 3
- remainder-difference-times, 6
- remainder-of-1, 6
- remainder-plus-times-1, 6
- remainder-plus-times-2, 6
- remainder-quotient, 2
- remainder-quotient-elim, 3
- remainder-times, 5

remainder-times-1, 6
remainder-wrt-1, 2
remainder-wrt-12, 2
remainder-x-x, 3

times-1, 6
times-add1, 2
times-difference, 3
times-equal-1, 5
times-id-iff-1, 4
times-identity, 5
times-identity1, 5
times-zero2, 2