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

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

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

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
$((a + b) = \mathsf{0}) = ((a \simeq \mathsf{0}) \wedge (b \simeq \mathsf{0}))$

THEOREM: difference-x-x
$(x - x) = \mathsf{0}$

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

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

THEOREM: difference-0
$(y \not< x) \rightarrow ((x - y) = \mathsf{0})$

THEOREM: equal-difference-0
$(\mathsf{0} = (x - y)) = (y \not< x)$

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

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

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

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

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

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
$((x * y) = \mathtt{0}) = ((x \simeq \mathtt{0}) \vee (y \simeq \mathtt{0}))$

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

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

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

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

THEOREM: remainder-quotient
$((x \textbf{ mod } y) + (y * (x \div y))) = \mathrm{fix}\,(x)$

THEOREM: remainder-wrt-1
$(y \textbf{ mod } \mathtt{1}) = \mathtt{0}$

THEOREM: remainder-wrt-12
$(x \notin \mathbf{N}) \rightarrow ((y \textbf{ mod } x) = \mathrm{fix}\,(y))$

THEOREM: lessp-remainder2
$((x \ \mathbf{mod} \ y) < y) = (y \not\simeq 0)$

THEOREM: remainder-x-x
$(x \ \mathbf{mod} \ x) = 0$

THEOREM: remainder-quotient-elim
$((y \not\simeq 0) \wedge (x \in \mathbf{N})) \rightarrow (((x \ \mathbf{mod} \ y) + (y * (x \div y))) = x)$

THEOREM: lessp-times-1
$(i \not\simeq 0) \rightarrow ((i * j) \not< j)$

THEOREM: lessp-times-2
$(i \not\simeq 0) \rightarrow ((j * i) \not< j)$

THEOREM: lessp-quotient1
$((i \div j) < i) = ((i \not\simeq 0) \wedge ((j \simeq 0) \vee (j \neq 1)))$

THEOREM: lessp-remainder1
$((x \ \mathbf{mod} \ y) < x) = ((y \not\simeq 0) \wedge (x \not\simeq 0) \wedge (x \not< y))$

THEOREM: difference-plus1
$((x + y) - x) = \mathrm{fix}\,(y)$

THEOREM: difference-plus2
$((y + x) - x) = \mathrm{fix}\,(y)$

THEOREM: difference-plus-cancelation
$((x + y) - (x + z)) = (y - z)$

THEOREM: times-difference
$(x * (c - w)) = ((c * x) - (w * x))$

DEFINITION: divides $(x, y) = ((y \ \mathbf{mod} \ x) \simeq 0)$

THEOREM: divides-times
$((x * z) \ \mathbf{mod} \ z) = 0$

THEOREM: difference-plus3
$((b + a + c) - a) = (b + c)$

THEOREM: difference-add1-cancellation
$((1 + (y + z)) - z) = (1 + y)$

THEOREM: remainder-add1
$((y \not\simeq 0) \wedge (y \neq 1)) \rightarrow (((1 + (x * y)) \ \mathbf{mod} \ y) \neq 0)$

THEOREM: divides-plus-rewrite1
$(((x \textbf{ mod } z) = \mathsf{0}) \land ((y \textbf{ mod } z) = \mathsf{0})) \rightarrow (((x + y) \textbf{ mod } z) = \mathsf{0})$

THEOREM: divides-plus-rewrite2
$(((x \textbf{ mod } z) = \mathsf{0}) \land ((y \textbf{ mod } z) \neq \mathsf{0})) \rightarrow (((x + y) \textbf{ mod } z) \neq \mathsf{0})$

THEOREM: divides-plus-rewrite
$((x \textbf{ mod } z) = \mathsf{0}) \rightarrow ((((x + y) \textbf{ mod } z) = \mathsf{0}) = ((y \textbf{ mod } z) = \mathsf{0}))$

THEOREM: lessp-plus-cancelation
$((x + y) < (x + z)) = (y < z)$

THEOREM: divides-plus-rewrite-commuted
$((x \textbf{ mod } z) = \mathsf{0}) \rightarrow ((((y + x) \textbf{ mod } z) = \mathsf{0}) = ((y \textbf{ mod } z) = \mathsf{0}))$

THEOREM: euclid
$((x \textbf{ mod } z) = \mathsf{0})$
$\rightarrow \quad ((((y - x) \textbf{ mod } z) = \mathsf{0})$
$\quad\quad = \textbf{if } x < y \textbf{ then } (y \textbf{ mod } z) = \mathsf{0}$
$\quad\quad\quad \textbf{else t endif})$

THEOREM: lessp-times-cancellation
$((x * z) < (y * z)) = ((z \not\simeq \mathsf{0}) \land (x < y))$

THEOREM: lessp-plus-cancellation3
$(y < (x + y)) = (x \not\simeq \mathsf{0})$

THEOREM: quotient-times1
$((y \in \mathbf{N}) \land (x \in \mathbf{N}) \land (x \neq \mathsf{0}) \land \mathrm{divides}\,(x,\, y))$
$\rightarrow \quad ((x * (y \div x)) = y)$

THEOREM: quotient-lessp
$((x \not\simeq \mathsf{0}) \land (x < y)) \rightarrow ((y \div x) \neq \mathsf{0})$

DEFINITION:
$\mathrm{greatereqpr}\,(w,\, z)$
$= \quad \textbf{if } w \simeq \mathsf{0} \textbf{ then } z \simeq \mathsf{0}$
$\quad \textbf{elseif } w = z \textbf{ then t}$
$\quad \textbf{else } \mathrm{greatereqpr}\,(w - 1,\, z) \textbf{ endif}$

THEOREM: times-id-iff-1
$(z = (w * z)) = ((z \in \mathbf{N}) \land ((z = \mathsf{0}) \lor (w = \mathsf{1})))$

THEOREM: greatereqpr-lessp
$\mathrm{greatereqpr}\,(x,\, y) = (x \not< y)$

THEOREM: greatereqpr-remainder
$((z \neq (1 + v)) \land \text{divides}\,(z,\, 1 + v)) \rightarrow \text{greatereqpr}\,(v,\, z)$

THEOREM: divides-times1
$(a = (z * y)) \rightarrow ((a \mathbf{\ mod\ } z) = \mathsf{0})$

THEOREM: times-identity1
$((y \in \mathbf{N}) \land (y \neq \mathsf{1}) \land (y \neq \mathsf{0}) \land (x \neq \mathsf{0})) \rightarrow (x \neq (x * y))$

THEOREM: times-identity
$(x = (x * y)) = ((x = \mathsf{0}) \lor ((x \in \mathbf{N}) \land (y = \mathsf{1})))$

THEOREM: quotient-divides
$((y \in \mathbf{N}) \land ((x * (y \div x)) \neq y)) \rightarrow ((y \mathbf{\ mod\ } x) \neq \mathsf{0})$

THEOREM: remainder-times
$((y * x) \mathbf{\ mod\ } y) = \mathsf{0}$

THEOREM: quotient-times
$((y * x) \div y)$
$= \quad \mathbf{if}\ y \simeq \mathsf{0}\ \mathbf{then}\ \mathsf{0}$
$\quad\quad \mathbf{else}\ \text{fix}\,(x)\ \mathbf{endif}$

THEOREM: distributivity-of-divides
$((a \not\simeq \mathsf{0}) \land \text{divides}\,(a,\, w)) \rightarrow ((c * (w \div a)) = ((c * w) \div a))$

THEOREM: if-times-then-divides
$((c \not\simeq \mathsf{0}) \land (\neg\ \text{divides}\,(c,\, x))) \rightarrow ((c * y) \neq x)$

THEOREM: times-equal-1
$((a * b) = \mathsf{1})$
$= \quad ((a \neq \mathsf{0})$
$\quad\quad \land \quad (b \neq \mathsf{0})$
$\quad\quad \land \quad (a \in \mathbf{N})$
$\quad\quad \land \quad (b \in \mathbf{N})$
$\quad\quad \land \quad ((a - 1) = \mathsf{0})$
$\quad\quad \land \quad ((b - 1) = \mathsf{0}))$

THEOREM: divides-implies-times
$((a \not\simeq \mathsf{0}) \land (c \in \mathbf{N}) \land ((a * c) = b)) \rightarrow ((c = (b \div a)) = \mathbf{t})$

THEOREM: difference-1
$(x - \mathsf{1}) = (x - 1)$

THEOREM: difference-2
$((1 + (1 + x)) - \mathsf{2}) = \text{fix}\,(x)$

THEOREM: half-plus
$((x + x + y) \div 2) = (x + (y \div 2))$

THEOREM: times-1
$(1 * x) = \text{fix}(x)$

THEOREM: exp-of-0
$\exp(0, k)$
$= \ \textbf{if}\ k \simeq 0\ \textbf{then}\ 1$
$\quad \textbf{else}\ 0\ \textbf{endif}$

THEOREM: exp-of-1
$\exp(1, k) = 1$

THEOREM: exp-by-0
$\exp(x, 0) = 1$

THEOREM: exp-times
$\exp(i * j, k) = (\exp(i, k) * \exp(j, k))$

THEOREM: exp-exp
$\exp(\exp(i, j), k) = \exp(i, j * k)$

THEOREM: remainder-plus-times-1
$((x + (i * j))\ \textbf{mod}\ j) = (x\ \textbf{mod}\ j)$

THEOREM: remainder-plus-times-2
$((x + (j * i))\ \textbf{mod}\ j) = (x\ \textbf{mod}\ j)$

THEOREM: remainder-times-1
$((b * a * c)\ \textbf{mod}\ a) = 0$

THEOREM: remainder-of-1
$(1\ \textbf{mod}\ x)$
$= \ \textbf{if}\ x = 1\ \textbf{then}\ 0$
$\quad \textbf{else}\ 1\ \textbf{endif}$

DEFINITION:
$\text{length}(lst)$
$= \ \textbf{if}\ \text{listp}(lst)\ \textbf{then}\ 1 + \text{length}(\text{cdr}(lst))$
$\quad \textbf{else}\ 0\ \textbf{endif}$

THEOREM: equal-length-0
$(\text{length}(x) = 0) = (x \simeq \textbf{nil})$

THEOREM: remainder-difference-times
$(((p * x) - (p * y))\ \textbf{mod}\ p) = 0$

THEOREM: lessp-remainder-divisor
$(y \not\simeq \mathsf{0}) \rightarrow ((x \ \mathbf{mod} \ y) < y)$

EVENT: Make the library `"arith"`.

Index