EVENT: Start with the library "arith".

; The first definition is one
; whose only purpose is to specify an induction scheme later.

DEFINITION:
my-ind (x, y) =
  if (x ∈ N) ∧ (y ∈ N) ∧ (x ≠ 0) ∧ (y ≠ 0) ∧ ((x mod 2) = 0) ∧ ((y mod 2) = 0) then my-ind (x ÷ 2, y ÷ 2)
else t endif

; Here's a lemma that I found useful in a proof below. The
; theorem-prover proves this automatically. I immediately
; disable it because I'm afraid that automatic use of this lemma
; may cause infinite looping by the rewriter.

THEOREM: move-consts-to-front
((b * c) * (d * e)) = ((b * d) * (c * e))

EVENT: Disable move-consts-to-front.

; Here's a lemma that I found useful in the proof of the main
; result. Though I don't remember for sure, I think that I
; discovered this lemma and the one above it in the course of
; trying to give an interactive proof of the main result.
; However, the one following it was (I'll guess) discovered in
; the course of trying to carry out the proof of the main lemma,
; REMAINDER-TIMES-ODDS, below. That lemma, in turn, has an
; immediate corollary the one just below it, namely
; DIVIDES-2-SQUARE, and I'm sure you'll see why I could use that
; one.

THEOREM: times-cancel
(((x * y) = (x * z)))
\[ \begin{align*}
&\land (x \in \mathbb{N}) \\
&\land (x \neq 0) \\
&\land (y \in \mathbb{N}) \\
&\land (z \in \mathbb{N}) \\
\rightarrow & \quad ((y = z) = t)
\end{align*} \]

**Theorem**: remainder-0-or-1
\[
((x \mod 2) \neq 0) \rightarrow ((x \mod 2) = 1)
\]

**Theorem**: remainder-of-add1
\[
((1 + x) \mod 2) \\
= \quad \text{if } (x \mod 2) = 0 \text{ then } 1 \\
\quad \text{else } 0 \text{ endif}
\]

**Theorem**: remainder-times-odds
\[
((x * y) \mod 2) = ((x \mod 2) * (y \mod 2))
\]

**Theorem**: divides-2-square
\[
(((x * x) \mod 2) = 0) \rightarrow ((x \mod 2) = 0)
\]

**Theorem**: sqrt-2-not-rational
\[
((y \in \mathbb{N}) \land (y \neq 0)) \rightarrow ((x * x) \neq (2 * y * y))
\]
Index

divides-2-square, 2
move-consts-to-front, 1
my-ind, 1
remainder-0-or-1, 2
remainder-of-add1, 2
remainder-times-odds, 2
sqrt-2-not-rational, 2
times-cancel, 1