```
; From Matt Kaufmann, ICSCA, Univ. of Texas, 2/23/87
```

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** $(x \in \mathbf{N})$
$\wedge$ $(y \in \mathbf{N})$
$\wedge$ $(x \neq 0)$
$\wedge$ $(y \neq 0)$
$\wedge$ $((x \bmod 2) = 0)$
$\wedge$ $((y \bmod 2) = 0)$ **then** my-ind $(x \div 2, y \div 2)$
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
$(((x * y) = (x * z))$

$\wedge \quad (x \in \mathbf{N})$
$\wedge \quad (x \neq 0)$
$\wedge \quad (y \in \mathbf{N})$
$\wedge \quad (z \in \mathbf{N}))$
$\rightarrow \quad ((y = z) = \mathbf{t})$

THEOREM: remainder-0-or-1
$((x \textbf{ mod } 2) \neq 0) \rightarrow ((x \textbf{ mod } 2) = 1)$

THEOREM: remainder-of-add1
$((1 + x) \textbf{ mod } 2)$
$= \quad \textbf{if } (x \textbf{ mod } 2) = 0 \textbf{ then } 1$
$\quad\quad \textbf{else } 0 \textbf{ endif}$

THEOREM: remainder-times-odds
$((x * y) \textbf{ mod } 2) = ((x \textbf{ mod } 2) * (y \textbf{ mod } 2))$

THEOREM: divides-2-square
$(((x * x) \textbf{ mod } 2) = 0) \rightarrow ((x \textbf{ mod } 2) = 0)$

THEOREM: sqrt-2-not-rational
$((y \in \mathbf{N}) \wedge (y \neq 0)) \rightarrow ((x * x) \neq (2 * y * y))$

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