Unique existence

The notation

$$\exists! x. P(x)$$

stands for

the unique existence of an \( x \) for which the property \( P(x) \) holds.

That is,

$$\exists x. P(x) \land (\forall y. \forall z. (P(y) \land P(z)) \implies y = z)$$

existence \underline{uniqueness}
The congruence property modulo \( m \) uniquely characterises the natural numbers from 0 to \( m-1 \).

**Proposition.** Let \( m \) be a positive integer and let \( n \) be an integer.

Define

\[
P(z) = \text{def} \left[ 0 \leq z < m \land z \equiv n \pmod{m} \right]
\]

Then

\[
\forall x, y . P(x) \land P(y) \Rightarrow x = y
\]
PROOF: Let \( m \) be a positive integer and let \( n \) be an integer.
Let \( x \) and \( y \) be arbitrary.
Assume: (1) \( 0 \leq x < m \) \( \land \) (2) \( x \equiv n \) \((\text{mod } m)\)
(3) \( 0 \leq y < m \) \( \land \) (4) \( y \equiv n \) \((\text{mod } m)\)

\[ \text{RTP: } x = y \]

From (2) and (4), \( x - y = km \) for some integer \( k \).
Therefore \( km = x - y < m \) by (1) and (3); and so
\( k \leq 0 \). Also \( -km = y - x < m \) by (1) and (3); and so
\( -k \leq 0 \). Thus, \( k = 0 \) and so \( x = y \). \( \square \)
A proof strategy

To prove

\[ \forall x. \exists! y. P(x,y) \]

given an arbitrary \( x \) construct the unique witness and name it, say \( f(x) \), showing that

\[ P(x, f(x)) \]

and

\[ \forall y. P(x,y) \Rightarrow y = f(x) \]

hold.