107 (Cantor's diagonal) Prove $\neg\exists f: nat \rightarrow nat \rightarrow nat \cdot \forall g: nat \rightarrow nat \cdot \exists n: nat \cdot f\ n = g$.

After trying the question, scroll down to the solution.

§ Here is a lemma. It starts with the local axiom f: $nat \to nat \to nat$.

	f: $nat \to nat \to nat$	function inclusion (or arrow) and specialization
$\Rightarrow$	$\forall m$: $nat \cdot f\ m$: $nat \to nat$	function inclusion (or arrow) and specialization
$\Rightarrow$	$\forall m, p$: $nat \cdot f\ m\ p$: nat	specialize p to m
$\Rightarrow$	$\forall m$: $nat \cdot f\ m\ m$: nat	nat construction
$\Rightarrow$	$\forall m$: $nat \cdot f\ m\ m + 1$: nat	domain law
$=$	nat: $\Box\langle m$: $nat \cdot f\ m\ m + 1\rangle \ \wedge\ \forall m$: $nat \cdot f\ m\ m + 1$: nat	function inclusion (or arrow)
$=$	$\langle m$: $nat \cdot f\ m\ m + 1\rangle$: $nat \to nat$	

Let missing domains be as in the question.

	$\neg \exists f \cdot \forall g \cdot \exists n \cdot f\ n = g$	using the lemma, specialize g to $\langle m$: $nat \cdot f\ m\ m + 1\rangle$
$\Leftarrow$	$\neg \exists f \cdot \exists n \cdot f\ n = \langle m$: $nat \cdot f\ m\ m + 1\rangle$	function equality
$=$	$\neg \exists f \cdot \exists n \cdot \Box(f\ n) = \Box\langle m$: $nat \cdot f\ m\ m + 1\rangle \wedge \forall p$: $nat \cdot f\ n\ p = \langle m$: $nat \cdot f\ m\ m + 1\rangle\ p$	domain
$=$	$\neg \exists f \cdot \exists n \cdot \Box(f\ n) = nat \wedge \forall p$: $nat \cdot f\ n\ p = \langle m$: $nat \cdot f\ m\ m + 1\rangle\ p$	apply
$=$	$\neg \exists f \cdot \exists n \cdot \Box(f\ n) = nat \wedge \forall p$: $nat \cdot f\ n\ p = f\ p\ p + 1$	specialize
$\Leftarrow$	$\neg \exists f \cdot \exists n \cdot \Box(f\ n) = nat \wedge f\ n\ n = f\ n\ n + 1$	cancellation
$=$	$\neg \exists f \cdot \exists n \cdot \Box(f\ n) = nat \wedge 0=1$	generic
$=$	$\neg \exists f \cdot \exists n \cdot \Box(f\ n) = nat \wedge \bot$	drop unused quantifiers (idempotence, domains not $null$)
$=$	$\neg \bot$	binary law
$=$	$\top$	

Cantor's diagonal argument is popularly thought to prove that there are more real numbers than integers. But it does not prove that. To prove that requires an extra axiom

$$¢A < ¢B \ = \ \neg \exists f: A \to B \cdot \forall g: B \cdot \exists n: A \cdot f\ n = g$$

Then we can prove $¢int = ¢nat$ and $¢nat < ¢(nat \to nat)$ and $¢(nat \to nat) = ¢real$, and then conclude $¢int < ¢real$. In my opinion, this extra axiom is unmotivated by any application, so I have not included it. To most mathematicians, it is somehow a fact.