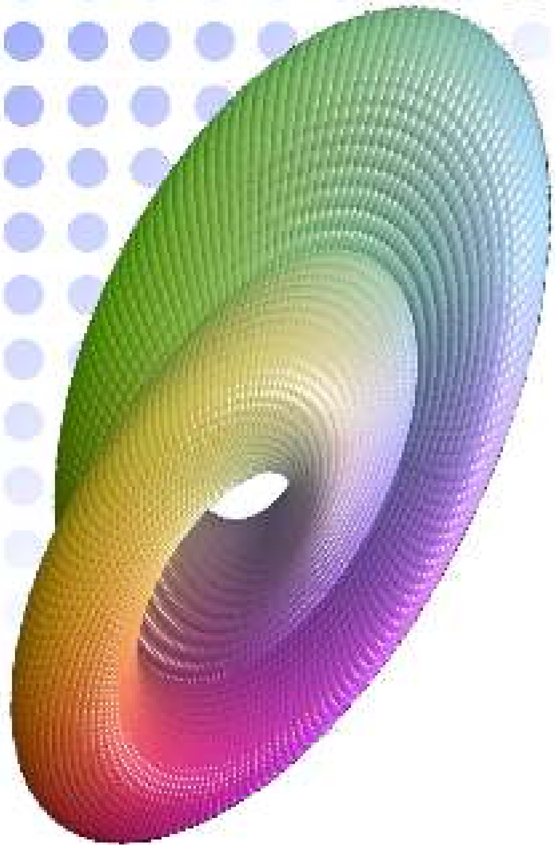
Michigan Math Club

Thursday at 4pm in the Commons

Free Pizza and Pop



Redefining "Proof"

Zachary Scherr

Abstract for 3 December 2009

One can think of a mathematical proof as a sequence of logical statements which can be written down by the prover and then checked line by line for correctness and soundness by the verifier. I will discuss interesting ways in which one can modify this proof model.

(1) Is there any way for the prover to convince the verifier of the veracity of a statement without actually giving away the proof?

(2) Is there any way to add redundancy to proofs in such a way that the verifier can be convinced by only reading a tiny portion of the proof?

The answers to these questions are "Yes"! Examples will be given.