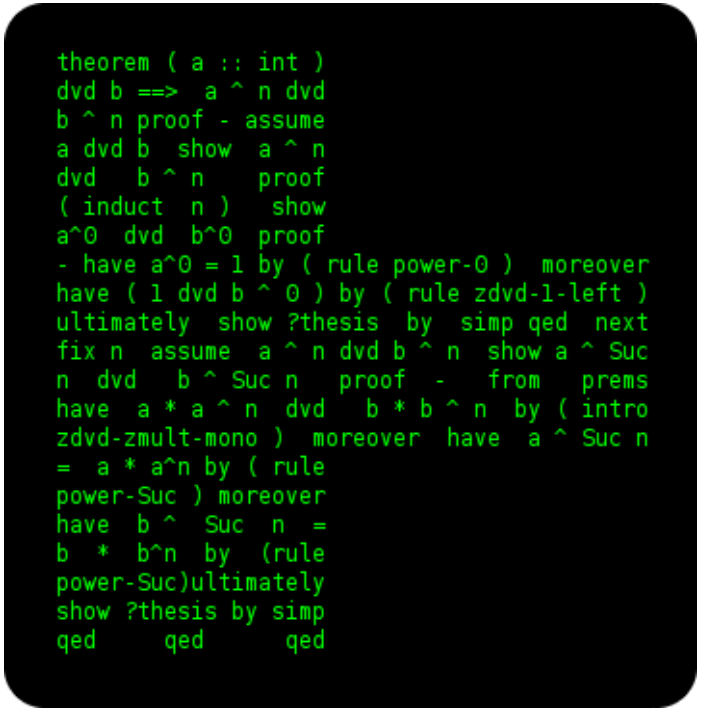


```
theorem ( a :: int )
dvd b ==>  a ^ n dvd
b ^ n proof - assume
a dvd b  show  a ^ n
dvd   b ^ n    proof
( induct  n )   show
a^0  dvd  b^0  proof
- have a^0 = 1 by ( rule power-0 )  moreover
have ( 1 dvd b ^ 0 ) by ( rule zdvd-1-left )
ultimately  show ?thesis  by  simp qed  next
fix n  assume  a ^ n dvd b ^ n  show a ^ Suc
n  dvd   b ^ Suc n   proof  -   from   prems
have  a * a ^ n  dvd   b * b ^ n  by ( intro
zdvd-zmult-mono )  moreover  have  a ^ Suc n
=  a * a^n by ( rule
power-Suc ) moreover
have  b ^  Suc  n  =
b  *  b^n  by  (rule
power-Suc)ultimately
show ?thesis by simp
qed     qed      qed
```

vdash.org: a formal math commons

Cameron Freer

freer@mit.edu

MIT Dept. of Mathematics

Ignite Boston 4

September 11, 2008

“I demand satisfaction!”

What if Wikipedia allowed only true statements?

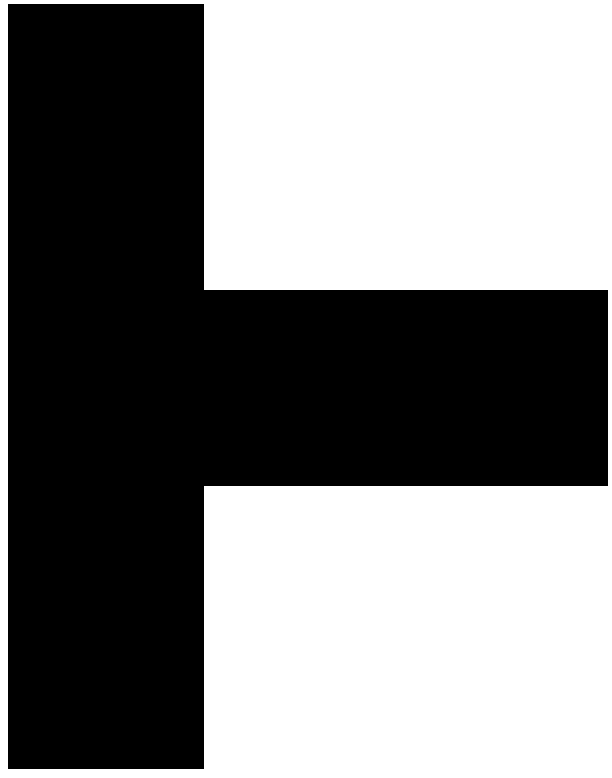
vdash

- wiki of formally verified math
- one road towards a "Math Commons"

vdash $=$ interactive theorem prover
$+$ computer-checked math library
$+$ web interface

\vdash is $\vdash$ in LaTeX.

$A \vdash B$
if B can be
proved from A.



Cantor's Theorem

```
theorem "∃S. S ∉ range (f :: 'a ⇒ 'a set)"
```

```
proof
  let "?S = {x. x ∉ f x}"
  show "?S ∉ range f"
  proof
    assume "?S ∈ range f"
    then obtain y where fy: "?S = f y" ..
    show False
    proof cases
      assume "y ∈ ?S"
      hence "y ∉ f y"    by simp
      hence "y ∉ ?S"     by (simp add: fy)
      thus False         by contradiction
    next
      assume "y ∉ ?S"
      hence "y ∈ f y"    by simp
      hence "y ∈ ?S"     by (simp add: fy)
      thus False         by contradiction
    qed
  qed
qed
```

navigation

- Main Page
- Community portal
- Current events
- Recent changes
- Random page
- Help

search

Go Search

toolbox

- What links here
- Related changes
- Upload file
- Special pages
- Printable version
- Permanent link

```
proof
  let " ?S = {x. x ∉ f x} "
  show "?S ∉ range f"
  proof
    assume "?S ∈ range f"
    then obtain y where fy: "?S = fy" ..
    show False
    proof cases
      assume " y ∈?S "
      hence " y ∉ f y "     by simp
```

Why *Formalized* Math?

- Certainty
- Complete explanation
- Modularity & reusability
- Instant verification
- Interactivity

Knowledge Base for Robot Mathematicians?

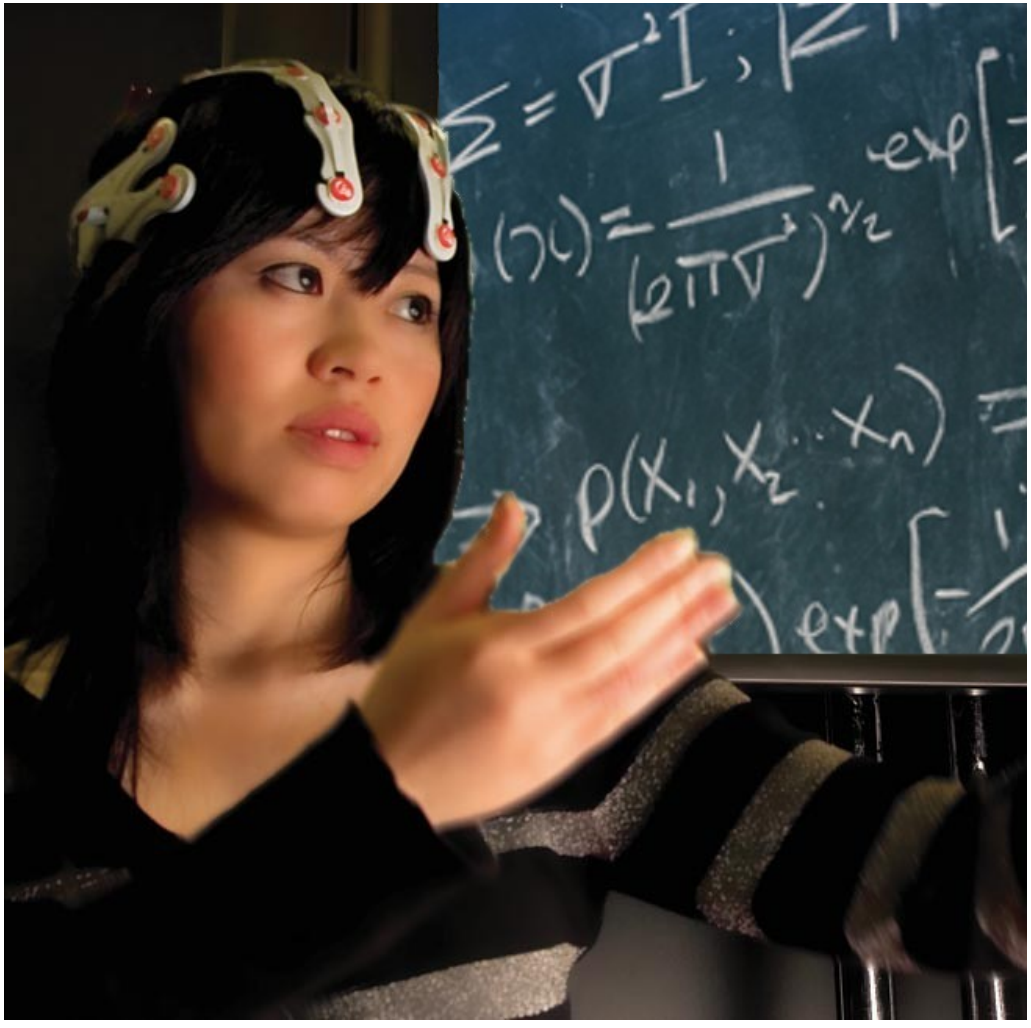
Data, Lucasian Professor of Mathematics

Knowledge Base for Robot Mathematicians?

"We are not scanning all those books to be read by people," explained one of my hosts after my talk. "We are scanning them to be read by an AI."

– George Dyson,
on his 2005 visit to Google (edge.org)

In the meantime...



Interface for human/computer symbiont mathematicians

Currently, formalization can be overwhelming.

Too much is missing

- The tools are good
- Not enough math yet

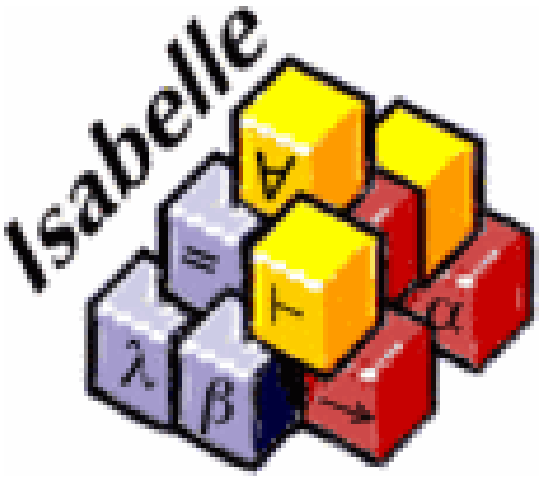
Why a *wiki?*

- Tons more contributors
- Top-down development (proof outlines)

Implementation

Isabelle/Isar:

- free software
- small trusted core
- human readable mathematics



Scrape web for mathematics

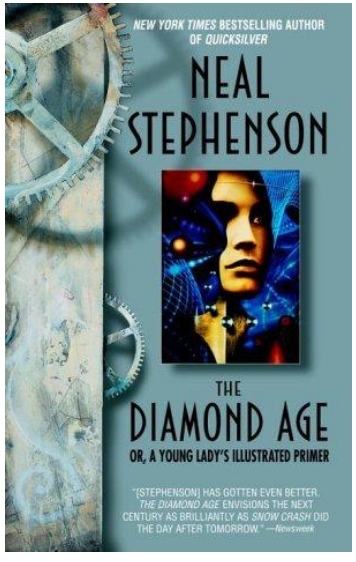
- arXMLiv, CiteSeer, other preprints
- open access journals

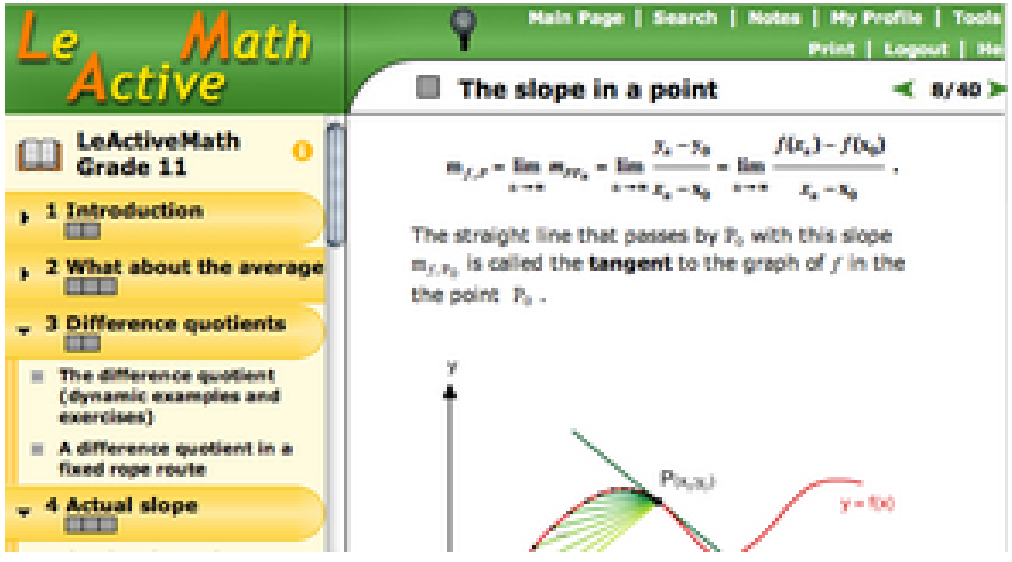
Connect to other sites

- Wikipedia, PlanetMath, MathWorld

Education

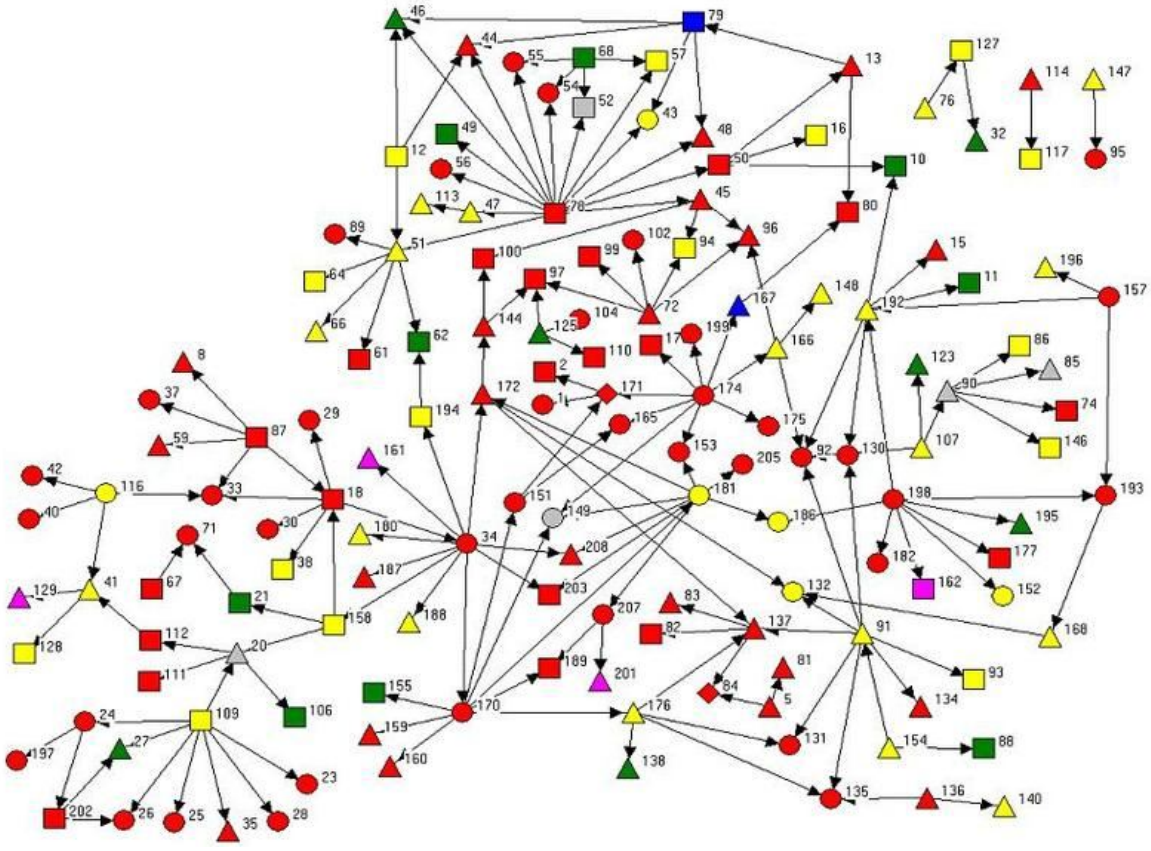
- interactive, open math textbooks
- "unfold" proofs all the way





The Theorome Project

visualize and browse interconnections within mathematics



Industrial applications

- hardware, software, and protocol verification
- Zero-Knowledge Proofs?

How you can help

- Contribute math to the wiki
- Back-end
- User Interface
- Connections (scrape, link)
- Organize challenge projects

Learn more or join the mailing list at `vdash.org`

Thanks!