Prove It or Lose It

Splash 2021

Li Xuan Tan, Kate Lu

Why?

How are math proofs “accepted”?

They are reviewed by people (might change with formal verification soon but not yet), so they have to be understandable

Why?

Not clear -> not believable -> basically equivalent to being unproved, since no one will use your result

Example: Dr. Shinichi Mochizuki claimed in 2012 to have solved the abc conjecture. To this day, his proof remains unverified and the problem is still considered open.

Structure of a typical paper

- **Lemmas** - smaller results not significant enough to be called theorems, usually is an intermediate step to proving theorems which is not reused outside of the proof of the theorem
    - If not reused, why do we need lemmas? Why not just put it together with the rest of the proof?
    - Sometimes, there are also "**claims**" within lemmas, which are even less significant results.
- **Theorems** - important results, typically the main part of a paper, will be built on and used
    - Often, theorems have names (eg Pythagoras' Theorem, four-squares theorem), but it is not a must. Also, names are weird sometimes.
- **Corollaries** - special cases, "follow-ups": results that can be deduced from the theorem and are significant enough to be mentioned

Organising your work

Separate things for readability

Label claims, lemmas, theorems etc. clearly

Number things when possible (equations that you will use, lemmas that you will reference)

Organising your work

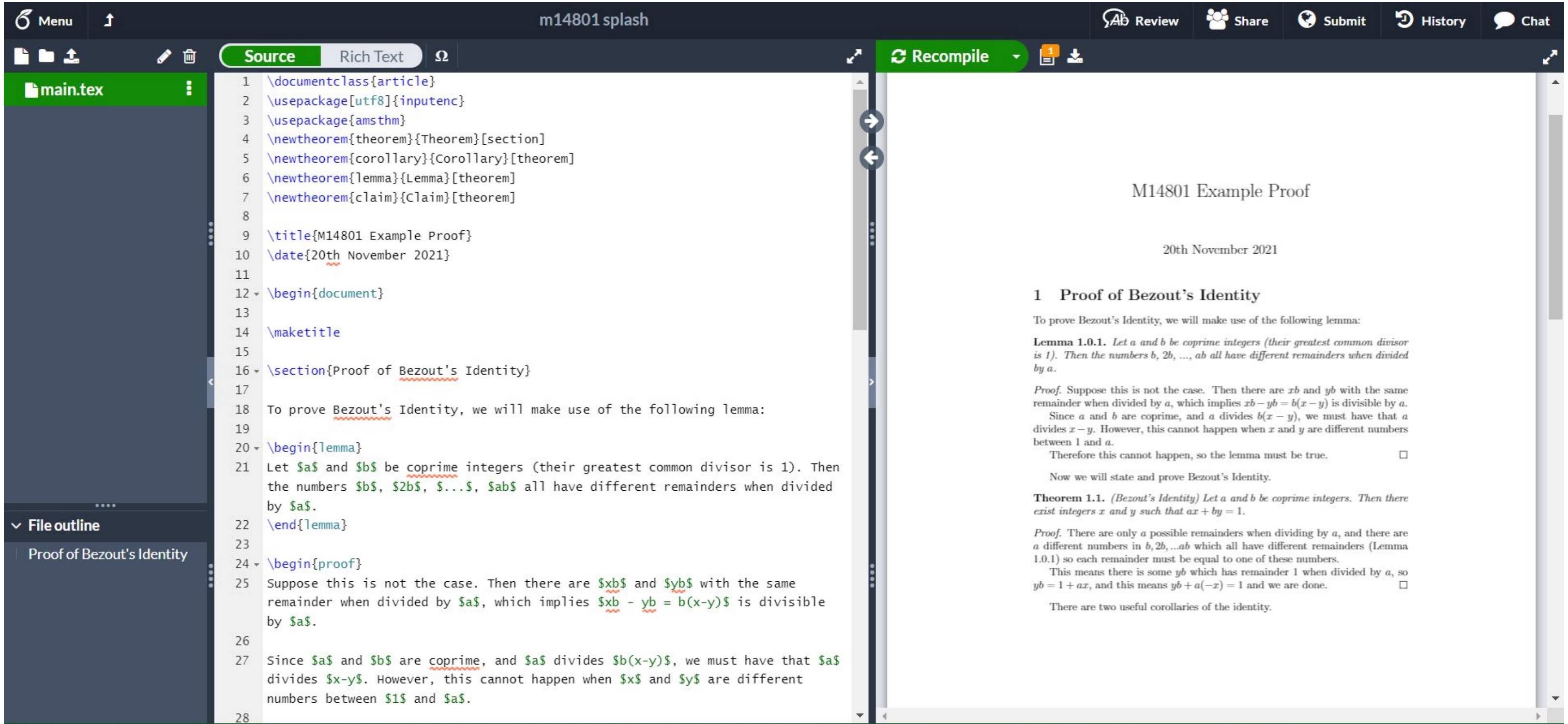
State what you aim to prove at the beginning of a proof or part of a proof, not later on

Scratch work should be organised as well

Variable naming conventions - a/b/c for constants, x/y/z for variables, if you must use subscripts then make sure they're related somehow

Other general tips

LaTeX is *much* more readable than handwriting (most of the time)



Other general tips

Convention for marking out important results:

Claim/Lemma/Theorem: (theorem name in brackets, if applicable)

(… theorem statement …)

Proof: (… proof …)

Examples!

Theorem: Bezout's Identity (also known as Bezout's Lemma - yes I know this name is terrible)

If a and b are coprime integers (their greatest common divisor is 1), then there exist integers x and y such that $ax + by = 1$.

Corollary: If d is the greatest common divisor of a and b, then there exist integers x and y such that $ax + by = d$.

Corollary: The numbers of the form $ax + by$ are exactly the multiples of d.

Try to reorganise this proof!

- If a, b are coprime, and b divides ac, then b divides c (why?)
- The numbers b, 2b … ab all have different remainders when divided by a
  - If not, then there are xb and yb with the same remainder, so (xb - yb) is divisible by a
  - Then b(x-y) is divisible by a, so (x-y) is divisible by a, but this cannot happens when x and y are both from 1 to a
- There are only a possible remainders for a numbers, so each remainder must match one of the multiples of b
- So, there must be some yb which has remainder 1 when divided by a
- This means yb = 1 + ax, so a(-x) + by = 1 and we are done

Try to reorganise this proof!

- In the previous proof, what should be a Lemma, or Theorem?

- The proofs of the Corollaries are as follows:
  - If d is the greatest common divisor of a and b, write b = db’ and a = da’, where a’ and b’ are coprime. Then apply the Theorem.
  - d divides a and b, so ax + by must be a multiple of d. Then, any multiple of d can be achieved by kd = k(ax + by) = a(xk) + b(yk), so ax + by can be every multiple of d.
- Reorganise these as well!

LaTeXed proof

1 Proof of Bezout's Identity

To prove Bezout's Identity, we will make use of the following lemma:

Lemma 1.0.1. *Let a and b be coprime integers (their greatest common divisor is 1). Then the numbers b, $2b$, ..., ab all have different remainders when divided by a.*

Proof. Suppose this is not the case. Then there are xb and yb with the same remainder when divided by a, which implies $xb - yb = b(x - y)$ is divisible by a.

Since a and b are coprime, and a divides $b(x - y)$, we must have that a divides $x - y$. However, this cannot happen when x and y are different numbers between 1 and a.

Therefore this cannot happen, so the lemma must be true. □

Now we will state and prove Bezout's Identity.

Theorem 1.1. *(Bezout's Identity) Let a and b be coprime integers. Then there exist integers x and y such that $ax + by = 1$.*

Proof. There are only a possible remainders when dividing by a, and there are a different numbers in $b, 2b, ...ab$ which all have different remainders (Lemma 1.0.1) so each remainder must be equal to one of these numbers.

This means there is some yb which has remainder 1 when divided by a, so $yb = 1 + ax$, and this means $yb + a(-x) = 1$ and we are done. □

There are two useful corollaries of the identity.

LaTeXed proof

Corollary 1.1.1. *If d is the greatest common divisor of a and b, then there exist integers x and y such that $ax + by = d$.*

Proof. Since d is the greatest common divisor, write $a = da'$ and $b = db'$ where a' and b' are coprime. Then by Bezout's Identity, there are integers x and y such that $a'x + b'y = 1$.

Multiply both sides by d to get $(a'd)x + (b'd)y = d$, so $ax + by = d$ and we are done. □

Corollary 1.1.2. *The numbers of the form $ax + by$ are exactly the multiples of d.*

Proof. d divides a and b, so d divides $ax + by$, meaning any number of the form $ax + by$ must be a multiple of d.

However, for any multiple of d, multiply $ax + by = d$ by k on both sides. Then we get $a(kx) + b(ky) = kd$, so any multiple of d is a number of the form $ax + by$. □

Additional resources

Advice for writing proofs (Evan Chen)

LaTeX in 30 minutes (Overleaf)

Thank you!

If you have more questions, let us know at
M14801s1-teachers@esp.mit.edu!