Improving my pen-and-paper proofs in introductory number theory using Lean

– SSFM –

Alexander Brodbelt

University of Edinburgh

February 6th, 2024

Introduction

- Today I will discuss the impact that formalisation in Lean had on my mathematical understanding (subsequently, on my pen-and-paper proofs).
- This will be a brief and short talk.

Outline

1. Why did I formalise my course homework? Isn't that a waste of time and effort?
2. The challenges I faced during the formalisation.
3. The transformation of my pen-and-paper proofs (post-formalisation).

Why?

Why did I formalise my course homework, after having done it?

- I was not sure if I was:
  - contraposing statements correctly
  - carrying out the proof by contradiction correctly

  I was concerned with what happened to the assumptions, which of the assumptions are modified?
- Provided the previous question could be used to solve the next one, I wanted to be sure I used the results correctly and all the conditions required by the theorem were satisfied.
- It was fun!
- A 10/10 on my homework should now be guaranteed!

The challenges

Let's take a look at one of the questions:

Theorem

If n is non-prime, then $2^n - 1$ is non-prime.

In Lean this is:

```
theorem (n : ℕ) (hn : ¬ Prime n) : ¬ Prime (2 ^ n - 1)
  := sorry
```

The challenges (cont.)

- Proving intermediate and trivial results such as the following,

$$x^n - 1 = (x-1)(1 + x + \cdots + x^{n-1}).$$

- As you would expect, the equation above cannot quite be understood by Lean (or not that I know of), so this has to be stated more precisely as

$$x^n - 1 = (x-1)\sum_{k=0}^{n-1} x^k,$$

which then can be proved by induction on n (with a bit more effort than simply saying the result follows trivially ...).

The challenges (cont.)

- Proving statements about the natural numbers, especially whenever subtraction is involved is finicky, very finicky. Try proving this in Lean:

$$x^{n+1} - 1 = (x^{n+1} - x^n) + (x^n - 1).$$

- I learned that the natural numbers (with 0) are:
  1. not a field (that was a quick to find out)
  2. not a ring
  3. not even an additive group!
  4. but an additive commutative semigroup! or that's what `tsub_tsub` told me...

  This is not new to most of you, but the point is I learned about mathematics in the process, thanks to VSCode's F12 command. Which, is less effort than following a rabbit hole of references at the appendix of a text book...

Conclusion

- My proofs were simplified, I realised what was required for the proof and what was added fluff.
- All the i's were dotted and all the t's were crossed. I could now sleep at night.
- I learned about the generality of certain theorems and how this generality leads on to more engaging and deeper questions. Learned about the existence of Filters, and why the definition exists
- The impact Lean had on my mathematical proofs and comprehension **reverberates** the potential that the ForMaL course says it does with making the teaching of advanced mathematics more <u>inclusive</u> and more <u>engaging</u>.

References

1. github.com/AlexBrodbelt/LeanIntroToNumberTheory