Imperial College London

23 August 2023

UROP 2023

Archibald Browne

Imperial College London

What did I do?

The project focused around formalising exercises from Professor M. Liebeck's 'A Concise Introduction to Mathematics' in Lean. Specifically, those from Chapter 10 'The Integers'.

Imperial College London

What did I do?

The project focused around formalising exercises from Professor M. Liebeck's 'A Concise Introduction to Mathematics' in Lean. Specifically, those from Chapter 10 'The Integers'.

The questions were mainly focused around the following areas:

- Greatest Common Divisor
- Lowest Common Multiple
- Bézout's Identity
- Prime Numbers

Imperial College London

What did I do?

The project focused around formalising exercises from Professor M. Liebeck's 'A Concise Introduction to Mathematics' in Lean. Specifically, those from Chapter 10 'The Integers'.

The questions were mainly focused around the following areas:

- Greatest Common Divisor
- Lowest Common Multiple
- Bézout's Identity
- Prime Numbers

I will go over some of the highlights/difficulties I experienced over the project, and what I learnt.

Imperial College London

Highlights

Here I will look at a couple of my favourite questions:

Imperial College London

Highlights

Here I will look at a couple of my favourite questions:

Question 8

Let $n \geq 2$ be an Integer. Prove that n is prime if and only if $\forall a \in \mathbb{Z},\ \gcd(a, n) = 1 \vee n|a$

Imperial College London

Highlights

Here I will look at a couple of my favourite questions:

Question 8

Let $n \geq 2$ be an Integer. Prove that n is prime if and only if $\forall a \in \mathbb{Z},\ \gcd(a, n) = 1 \vee n|a$

- Like many of the questions, this was much harder to teach to Lean than it was to solve.
- The general idea is that prime numbers cannot have common factors with any numbers that aren't a multiple of that prime.

Imperial College London

Highlights

Question Statement in Lean:

```
lemma exercise08 (n : ℤ) (hn : 2 ≤ n) : Prime n ↔ ∀ (a : ℤ), Int.gcd a n = 1 ∨ n ∣ a := by
```

Imperial College London

Highlights

Question Statement in Lean:

```
lemma exercise08 (n : ℤ) (hn : 2 ≤ n) : Prime n ↔ ∀ (a : ℤ), Int.gcd a n = 1 ∨ n ∣ a := by
```

Lean is fussy about the distinction between integers and naturals, so even though we have declared $2 \leq n$ and $n \in \mathbb{Z}$, we still need to tell Lean that n is a natural number in order to use theorems about natural numbers.

Imperial College London

Highlights

Question Statement in Lean:

```
lemma exercise08 (n : ℤ) (hn : 2 ≤ n) : Prime n ↔ ∀ (a : ℤ), Int.gcd a n = 1 ∨ n ∣ a := by
```

Lean is fussy about the distinction between integers and naturals, so even though we have declared $2 \leq n$ and $n \in \mathbb{Z}$, we still need to tell Lean that n is a natural number in order to use theorems about natural numbers.

For the $\implies$ direction, we condition on whether $n|a$. If it does, we get the result immediately. If not, then $gcd(a, n) = 1$ because n is prime.

Imperial College London

Highlights

For the $\Longleftarrow$ direction, we use the theorem:

```
Nat.prime_def_lt'
```

Which says:

$$n \in \mathbb{N} \text{ is prime } \iff \forall d \in (1, n) \cap \mathbb{N}, d \nmid n$$

Imperial College London

Highlights

For the $\Longleftarrow$ direction, we use the theorem:

```
Nat.prime_def_lt'
```

Which says:

$$n \in \mathbb{N} \text{ is prime } \iff \forall d \in (1, n) \cap \mathbb{N}, d \nmid n$$

We then condition over our assumption specialized for some particular d value:

- If $gcd(d, n) = 1$ then clearly $d \nmid n$
- If $n|d$ then we have $d \geq n$, a contradiction.

Imperial College London

Highlights

Another of my favourite questions was question 9:

Question 9

Let a, b be coprime integers. Prove that for any integer n there exists integers s, t with $s > 0$ such that $sa + tb = n$.

Imperial College London

Highlights

Another of my favourite questions was question 9:

Question 9

Let a, b be coprime integers. Prove that for any integer n there exists integers s, t with $s > 0$ such that $sa + tb = n$.

The main steps are:

- By Bèzout, $\exists s', t', s'a + t'b = 1$ since a, b are coprime

Imperial College London

Highlights

Another of my favourite questions was question 9:

Question 9

Let a, b be coprime integers. Prove that for any integer n there exists integers s, t with $s > 0$ such that $sa + tb = n$.

The main steps are:

- By Bèzout, $\exists s', t', s'a + t'b = 1$ since a, b are coprime
- We don't know whether $s' > 0$, so we use a trick:

Imperial College London

Highlights

Another of my favourite questions was question 9:

Question 9

Let a, b be coprime integers. Prove that for any integer n there exists integers s, t with $s > 0$ such that $sa + tb = n$.

The main steps are:

- By Bèzout, $\exists s', t', s'a + t'b = 1$ since a, b are coprime
- We don't know whether $s' > 0$, so we use a trick:
- $(s' + kb)a + (t' - ka)b = 1)\ \forall k \in \mathbb{Z}$

Imperial College London

Highlights

Another of my favourite questions was question 9:

Question 9

Let a, b be coprime integers. Prove that for any integer n there exists integers s, t with $s > 0$ such that $sa + tb = n$.

The main steps are:

- By Bèzout, $\exists s', t', s'a + t'b = 1$ since a, b are coprime
- We don't know whether $s' > 0$, so we use a trick:
- $(s' + kb)a + (t' - ka)b = 1)\ \forall k \in \mathbb{Z}$
- Increase k until $s' + kb > 0$, multiply through by n and we get the result

Imperial College London

Highlights

Question statement in lean:

```
lemma exercise09 (a b : ℤ) (hb : b > 0) (hab : IsCoprime a b) :
  ∀ (n : ℤ), ∃ (s t : ℤ), 0 < s ∧ s * a + t * b = n := by
```

Imperial College London

Highlights

Question statement in lean:

```
lemma exercise09 (a b : ℤ) (hb : b > 0) (hab : IsCoprime a b) :
  ∀ (n : ℤ), ∃ (s t : ℤ), 0 < s ∧ s * a + t * b = n := by
```

To help, I used the following helper lemma:

```
lemma helper (a b n : ℤ) (hb : 0 < b) (hab : ∃ (s t : ℤ), s * a + t * b = n) :
    ∃ (s' t' : ℤ), 0 < s' ∧ s' * a + t' * b = n := by
```

This is the bulk of the question, and says that if we can find s, t with $sa + tb = n$, then there is s', t' with $s' > 0$ and $s'a + t'b = n$.

Imperial College London

Highlights

The following two lines impliment the trick described on the earlier slide:

```
set p := (b - s) / b with hp
use s + p * b, t - p * a
```

Imperial College London

Highlights

The following two lines impliment the trick described on the earlier slide:

```
set p := (b - s) / b with hp
use s + p * b, t - p * a
```

The rest of the proof of the helper proves that these are the correct choices of coefficients

Imperial College London

What did I Learn?

The project taught me quite a bit both about Lean, and undertaking a research project:

Imperial College London

What did I Learn?

The project taught me quite a bit both about Lean, and undertaking a research project:

- How to use Lean at a basic level

What did I Learn?

The project taught me quite a bit both about Lean, and undertaking a research project:

- How to use Lean at a basic level
- Developed interest in dependent type theory and functional programming (Curry-Howard Isomorphism etc.)

What did I Learn?

The project taught me quite a bit both about Lean, and undertaking a research project:

- How to use Lean at a basic level
- Developed interest in dependent type theory and functional programming (Curry-Howard Isomorphism etc.)
- How to contribute to open source projects

Imperial College London

What did I Learn?

I also learnt some more general things, unrelated to lean:

Imperial College London

What did I Learn?

I also learnt some more general things, unrelated to lean:

- What it is like to work on a project (almost) by yourself

Imperial College London

What did I Learn?

I also learnt some more general things, unrelated to lean:

- What it is like to work on a project (almost) by yourself
- Acknowledging when you are stuck, and when to ask for help

Imperial College London

What did I Learn?

I also learnt some more general things, unrelated to lean:

- What it is like to work on a project (almost) by yourself
- Acknowledging when you are stuck, and when to ask for help
- Informed my decision about whether to PhD or not

Imperial College London

Conclusion

Overall, huge thank you to Kevin for the opportunity, and everyone on the Xena discord for being so helpful!!!