Imperial College London

21 August 2023

UROP 2023

Archibald Browne

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'.

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

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.

Highlights

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

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
$\forall a \in \mathbb{Z},\ \gcd(a, n) = 1 \vee n|a$

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.

Highlights

Question Statement in Lean:

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

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:

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

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 $d|n$ then we have $d \geq n \vee d = 1$, a contradiction

What did I Learn?

Specific

What did I Learn?

General

Imperial College London

Conclusion