Category A

We will go through the following definitions and lemmas in order on Lean, just like what we did in the natural number game.

1 Definition

1.1 Division

Definition 1. $\text{div}(a : \mathbb{N})(b : \mathbb{N}) := \exists c : \mathbb{N}, b = ac$

We denote div a b as $a|b$.
Now we can define what it means for a to be even:

Definition 2. $\text{is\_even}(a : \mathbb{N}) := 2|a$

1.2 Prime

Definition 3. $\text{is\_prime}(a : \mathbb{N}) := a \neq 1 \wedge (\forall b : \mathbb{N}, b|a \to (b = 1 \vee b = a))$

1.3 GCD

Definition 4. $\text{is\_gcd}(a : \mathbb{N})(b : \mathbb{N})(d : \mathbb{N}) := d|a \wedge d|b \wedge (\forall c : \mathbb{N}, c|a \wedge c|b \to c|d)$

It can be proved that the GCD of a, b is unique (See Lemma 25).
Now we can define what it means for a, b to be coprime:

Definition 5. $\text{is\_coprime}(a : \mathbb{N})(b : \mathbb{N}) := \text{is\_gcd}\ a\ b\ 1$

2 Lemma

2.1 Division Part

Lemma 6. $\forall a : \mathbb{N}, 1|a$

Lemma 7. $\forall a : \mathbb{N}, a|0$

Lemma 8. $\forall a : \mathbb{N}, a|a$

Lemma 9. $\forall a : \mathbb{N}, \forall b : \mathbb{N}, \forall c : \mathbb{N}, a|b \wedge b|c \to a|c$

Lemma 10. $\forall a : \mathbb{N}, \forall b : \mathbb{N}, \forall m : \mathbb{N}, a|b \to a|mb$

Lemma 11. $\forall a : \mathbb{N}, \forall b : \mathbb{N}, \forall c : \mathbb{N}, a|b \wedge a|c \to a|b + c$

Lemma 12. $\forall a : \mathbb{N}, \forall b : \mathbb{N}, \forall c : \mathbb{N}, \forall m : \mathbb{N}, \forall n : \mathbb{N}, a|b \wedge a|c \to a|mb + nc$

Proof. Use Lemma 10 and Lemma 11. □

Lemma 13. $\forall k : \mathbb{N}, k|1 \to k = 1$

Proof. There must be a lemma in the library for $1 = kj \to k = 1$. □

Lemma 14. $\forall b : \mathbb{N}, 0|b \to b = 0$

Lemma 15. $\forall a : \mathbb{N}, \forall b : \mathbb{N}, a|b \wedge b|a \to a = b$

Proof. We deduce $a = akj$ from $a = bk$, $b = aj$. For the case $a = 0$, use Lemma 14; for the other case, cancel a from both sides to derive $1 = kj$. Then $k = 1$ and hence $a = b$. □

Lemma 16. $\forall a : \mathbb{N}, \forall b : \mathbb{N}, b \neq 0 \wedge a|b \to a \leq b$

Proof. Let $b = ak$. Since $b \neq 0$, we can show that $k \neq 0$. So there is an n such that $k = \mathrm{succ}(n)$. We deduce $a \leq b = ak$ from $ak = a + an$. □

Lemma 17. $\forall a : \mathbb{N}, \forall b : \mathbb{N}, \forall c : \mathbb{N}, a \neq 0 \to (ab|ac \leftrightarrow b|c)$

Lemma 18. $\forall a : \mathbb{N}, \forall b : \mathbb{N}, \forall d : \mathbb{N}, d|a \wedge d|a + b \to d|b$

Proof. If $d = 0$, then $a = 0$ and $a + b = 0$ by Lemma 14. So $b = 0$ and hence $d|b$ by Lemma 7. If $d \neq 0$, we have $a = dk$ and $a + b = aj$ for some k, j. So $dk + b = dj$. So $dk \leq dj$ and hence $k \leq j$. So $j = k + n$ for some n. Thus, $dk + b = d(k + n)$ and hence $b = dn$. This implies $d|b$. □

2.2 Prime Part

Lemma 19. $\text{is\_prime}(0) \to \text{false}$

Proof. Consider $b = 2$ in Definition 3. □

Lemma 20. $\text{is\_prime}(1) \to \text{false}$

Lemma 21. $\text{is\_prime}(2) \to \text{true}$

Proof. For $b|2$, we have $b \neq 0$ by Lemma 14. We also have $b \leq 2$ by Lemma 16. So there is an a such that $a + b = 2$. Since $b \neq 0$, $b = \mathrm{succ}(n)$ for some n. Using the cancel law gives $a + n = 1$. If $n \neq 0$, then $n = \mathrm{succ}(m)$ for some m and $a + m = 0$. In this case, $m = 0$ and hence $n = 1$. So $n = 0 \vee n = 1$ and thus $b = 1 \vee b = 2$, which completes the proof. □

Lemma 22. $\forall a : \mathbb{N}, a \neq 2 \wedge \text{is\_even}(a) \wedge \text{is\_prime}(a) \to \text{false}$

Proof. $a = 2k$ for some k. We have $k \neq 0$ by Lemma 19 and $k \neq 1$ by the assumption $a \neq 2$. Furthermore, we can deduce $k \neq a$ from the fact that $a = 2k = k + k$ and $k \neq 0$. Since $k|a$ and a is prime, we know that $k = 1 \wedge k = a$. But we have already proved that $k \neq 1$ and $k \neq a$. $\square$

Lemma 23. $\forall a : \mathbb{N}, \forall b : \mathbb{N}, \text{is\_prime}(a) \wedge \text{is\_prime}(b) \wedge \text{is\_prime}(ab) \to \text{false}$

Proof. Since a, b are prime numbers, $a \neq 0$ $a \neq 1$, and $b \neq 1$ by Lemma 19 and 20. Thus, it can be argued that $a \neq ab$ (otherwise, $a = ab \to 1 = b$, contradiction!). Since ab is prime and $a|ab$ by Lemma 10, we have $a = 1 \vee a = ab$. But we have proved that $a \neq 1$ and $a \neq ab$. $\square$

Lemma 24. $\forall a : \mathbb{N}, \forall b : \mathbb{N}, \forall k : \mathbb{N}$,
$(a \neq 1 \to ((a|bk \to a|b \vee a|k) \to \text{is\_prime}(a)))$

Proof. For $b|a$, $a = bk$ for some k. We have $a|bk$ by Lemma 8. So $a|b \vee a|k$ by the condition. For the case $a|b$, we have $b = a$ by Lemma 15; for the other case, we have $k = a$ similarly and hence $a = ba$. If $a = 0$, we argue that $a|bk \to a|b \wedge a|k$ is false by considering $b = 1$; Otherwise, canceling a from $a = ba$ gives $b = 1$. So $b = 1 \vee b = a$, which completes the proof. $\square$

2.3 GCD Part

First we can show the uniqueness of the GCD.

Lemma 25. $\forall a : \mathbb{N}, \forall b : \mathbb{N}, \forall d_1 : \mathbb{N}, \forall d_2 : \mathbb{N}$,
$\text{is\_gcd}\ a\ b\ d_1 \wedge \text{is\_gcd}\ a\ b\ d_2 \to d_1 = d_2$

Proof. Try to prove $d_1|d_2$ and $d_2|d_1$ by Definition 4 and deduce $d_1 = d_2$ by Lemma 15. $\square$

Next, we list some basic properties of GCD.

Lemma 26. $\forall a : \mathbb{N}, \forall b : \mathbb{N}, \forall d : \mathbb{N}, \text{is\_gcd}\ a\ b\ d \leftrightarrow \text{is\_gcd}\ b\ a\ d$

Lemma 27. $\forall a : \mathbb{N}, \forall b : \mathbb{N}, a|b \to \text{is\_gcd}\ a\ b\ a$

Lemma 28. $\forall a : \mathbb{N}, \text{is\_gcd}\ a\ 0\ a$

Lemma 29. $\forall b : \mathbb{N}, \text{is\_gcd}\ 1\ b\ 1$

Lemma 30. $\forall a : \mathbb{N}, \forall b : \mathbb{N}, \forall c : \mathbb{N}, \forall d : \mathbb{N}$,
$a \neq 0 \to (\text{is\_gcd}\ ab\ ac\ ad \leftrightarrow \text{is\_gcd}\ b\ c\ d)$

Proof. Use Lemma 17. $\square$

Lemma 31. $\forall a : \mathbb{N}, \forall b : \mathbb{N}, \forall d : \mathbb{N}, \text{is\_gcd}\ a + b\ b\ d \leftrightarrow \text{is\_gcd}\ a\ b\ d$

Proof. Use Lemma 11 for "$\leftarrow$" and use Lemma 18 for "$\to$". $\square$

Lemma 32. $\forall b : \mathbb{N}, \text{is\_coprime } 1 + b\ b$

Proof. Use Lemma 29 and Lemma 31. □

Finally, the relation between "prime" and "coprime" can be demonstrated by the following lemma.

Lemma 33. $\forall a : \mathbb{N}, \forall p : \mathbb{N}, p \nmid a \to (\text{is\_prime}(p) \to \text{is\_coprime } a\ p)$

Proof. Just use Definition 3 and Definition 4. □

2.4 *Further Discussion

(Note: This part might not be covered if time is limited.)

Lemma 34. *Division Algorithm*

In most textbooks, the division algorithm is proved by the well-ordering theorem, which requires subtraction. However, we haven't defined the subtraction yet (unless we have integers rather than just natural numbers). I have no idea whether it can be proved by induction. We can have a try.

Lemma 35. *Bezout's Lemma*

Bezout's lemma can be shown by the division algorithm, but it might be complicated to prove the lemma on Lean.

The following lemmas are based on the Bezout's lemma.

Lemma 36. $\forall a : \mathbb{N}, \forall b : \mathbb{N}, \forall c : \mathbb{N}, \forall d : \mathbb{N}, \text{is\_gcd } a\ b\ d \to (d|c \leftrightarrow \exists x : \mathbb{N}, \exists y : \mathbb{N}, ax + by = c)$

Proof. See INT tutorial workshop 1, exercise 2. □

Lemma 37. $\forall a : \mathbb{N}, \forall b : \mathbb{N}, \forall c : \mathbb{N}, \text{is\_coprime } a\ b \to (a|bc \to a|c)$

Proof. a, b are coprime $\to as + bt = 1 \to cas + cbt = c \to a|c$ □

Lemma 38. $\forall a : \mathbb{N}, \forall b : \mathbb{N}, \forall k : \mathbb{N},$
$(a \neq 1 \to ((a|bk \to a|b \lor a|k) \leftrightarrow \text{is\_prime}(a)))$

(Don't confuse Lemma 38 with Lemma 24!)