Elementary Number Theory in Type Theoretic Foundations

October 19, 2014

1 Introduction

One important set in mathematics is that of the natural numbers and number theory is the study of the properties that this set of natural numbers possesses. Here we examine the development of number theory in the language of a foundation of mathematics known as homotopy type theory differs in a few ways than in conventional mathematical foundations and one of the key features lies in how carefully we have to make derivations within this theory. Here we present an example of using only homotopy type theory to derive the well-known fact that there are an infinite number of prime numbers. Two facts of arithmetic that have been developed so far in homotopy type theory are the following which we will use here without proof. The first is the commutativity of addition:

$$add\_opp : \prod_{x,y:\mathbb{N}} x + y = y + x$$

and the functions that distinguish two members of $\mathbb{N}$ from each other known as encode and code, the latter which has been developed in the text Homotopy Type Theory: Univalent Foundations of Mathematics [1] in Chapter 2. Also, we will be using the projection functions on two types A and B: $pr_1 : A \times B \to A$ and $pr_2 : A \times B \to B$ and also the projections on the $\sum$-dependen type $pr_1(\sum_{x:A})B(x) \to A$ and $pr_2 : \prod_{p:\sum_{x:A} B(x)} B(pr_1(p))$, which have also been developed in [1] in Chapter 1. Finally, we will only be dealing with the realm of mere propositons, which is another concept that is developed in [1] in Chapter 3, and as such we will only be proving or pointing out when a statement is a mere proposition when it is not obvious that it is, i.e. when it contains the symbols $\sum$, $+$(as in the coproduct), or $<$ as in the ordering of members of $\mathbb{N}$. Here we define $(x < y)$ by induction on y by

$$(x < 0) :\equiv \mathbf{0}$$

and

$$x < succ(y) :\equiv (x < y) + (x = y).$$

We will start by deriving all the necessary properties on the $\mathbb{N}$ with respect to addition and ordering.

Note 1. *In all of the proofs $C(x, y)$ will stand for the proposition of which we are proving. We will also let 1 stand for $succ(0)$ and 2 stand for $succ(succ(0))$.*

2 Addition and Ordering

Lemma 1. *[1] in Chapter 1.*
We have

$$\prod_{x,y,z:\mathbb{N}} (x + y) + z = x + (y + z)$$

Proof. We perform induction on $x : \mathbb{N}$. For $y \equiv 0$, we have $(0 + y) + z \equiv y + z$ and $0 + (y + z) \equiv y + z$. Thus $\mathrm{refl}_{y+z} : (0 + y) + z = 0 + (y + z)$.

For the induction step, suppose we have an element $v : (x + y) + z = x + (y + z)$. We want to find an element of $(succ(x) + y) + z = succ(x) + (y + z)$. We have that $succ(x) + y \equiv succ(x + y)$ and so $(succ(x) + y) + z \equiv (succ(x + y)) + z \equiv succ((x + y) + z)$. Also $succ(x) + (y + z) \equiv succ(x + (y + z))$. Thus $\mathrm{ap}_{succ}(v) : (succ(x) + y) + z = succ(x) + (y + z)$. □

We will write $as\_add : \prod_{x,y,z}(x + y) + x = x + (y + z)$.

Lemma 2. *If A and B are mere propositions and $(A \times B) \to \mathbf{0}$, then $A + B$ is also a mere proposition.*

Proof. Let $p, q : A + B$. So by induction on p we have two cases: Either there is $p_1 : A$ with $inl(p_1) \equiv p$ or there is $p_2 : B$ with $inr(p_2) \equiv p$.

Take the first case of $p_1 : A$. By induction on q we again have two cases: Either there is $q_1 : A$ with $inl(q_1) \equiv q$ or there is $q_2 : B$ with $inr(q_2) \equiv q$. In the first case, we have $p_1 = q_1 : A$ since A is a mere proposition and thus $p = q : A + B$. In the second case, we have $(p_1, q_2) : A \times B$. Letting $v : (A \times B) \to \mathbf{0}$, we thus have $v((p_1, q_2)) : \mathbf{0}$ and so $p = q : A + B$ automatically.

The case of $p_2 : B$ is symmetical. □

Lemma 3. *We have*

$$\prod_{x:\mathbb{N}}((x < y) \to \mathbf{0}) \to ((succ(x) < y) \to \mathbf{0}).$$

Proof. We perform induction on y. For $y \equiv 0$, we have $succ(x) < 0 \equiv \mathbf{0}$ so it follows automatically that $C(x, 0)$.

Suppose $v : C(x, y)$. We wish to show $C(x, succ(y))$. Let $w_1 : (x < succ(y)) \to \mathbf{0}$ and $w_2 : succ(x) < succ(y)$. So $w_1 : ((x < y) + (x = y)) \to \mathbf{0}$ and $w_2 : (succ(x) < y) + (succ(x) = y)$. We may define a function $(x < y) \to \mathbf{0}$ by $\lambda a.w_1(inl(a))$, which we will denote by w_3. Also by induction on w_2, we have $w_4 : succ(x) < y$ or $w_5 : succ(x) = y$. In the first case, we have $v(w_3, w_4) : \mathbf{0}$. In the second case we note that $inr(\mathrm{refl}_x) : x < succ(x)$ and that by induction on w_5, we have $succ(x) \equiv y$ so that $x < y$. Thus again we may apply w_3. □

Lemma 4. *We have*

$$\prod_{x:\mathbb{N}}(succ(x) = x) \to \mathbf{0}.$$

Proof. We perform induction on $x : \mathbb{N}$. For $x \equiv 0$, let $v : 1 = 0$. We have $encode(v) : code(1, 0) \equiv \mathbf{0}$.

Suppose for $w : succ(x) = x$, we have $encode(w) : code(succ(x), x) \equiv \mathbf{0}$ for the induction step. Let $w_1 : succ(succ(x)) = succ(x)$. We have $encode(w_1) : code(succ(succ(x)), succ(x)) \equiv code(succ(x), x) \equiv \mathbf{0}$. □

Lemma 5. *The type $x < y$ is a mere proposition. Thus we have that Lemma 3 is a mere proposition. Also,*

$$\prod_{x,y:\mathbb{N}}((x < y) \times (x = y)) \to \mathbf{0},$$

which is a mere proposition from the first statement as well.

Proof. We perform induction on $y : \mathbb{N}$. If $y \equiv 0$, we have $x < 0 \equiv \mathbf{0}$ so $x < 0$ is a mere proposition.

Suppose $x < y$ is a mere proposition. We wish to show that $x < succ(y)$ is a mere proposition. We have $x < succ(y) \equiv (x < y) + (x = y)$. We know that $x < y$ is a mere proposition and by induction

on $x = y$ that if $p, q : x = y$, then $p \equiv \text{refl}_x$ and $q \equiv \text{refl}_x$ so that $p = q$ and so $x = y$ is a mere proposition.

By Lemma 2 it remains to show that $((x < y) \times (x = y)) \to \mathbf{0}$. First, we'll show that $(x < x) \to \mathbf{0}$. We'll perform induction on $x : \mathbb{N}$. We have $(0 < 0) : \mathbf{0}$ for the base case. Suppose $v : (x < x) \to \mathbf{0}$ for the induction step. We wish to show that $(succ(x) < succ(x)) \to \mathbf{0}$. Let $w : (succ(x) < succ(x)) \equiv (succ(x) < x) + (x < x)$. By induction, we have two cases: either $w_1 : succ(x) < x$ with $inl(w_1) \equiv w$ or $w_2 : x < x$ with $inr(w_2) \equiv w$. In the former case, we apply Lemma 3 to v to get an element of $\mathbf{0}$. In the latter case, apply the induction hypothesis to get an element of $\mathbf{0}$.

Having shown $(x < x) \to \mathbf{0}$, we can now show $((x < y) \times (x = y)) \to \mathbf{0}$. Let $w_3 : (x < y) \times (x = y)$. We have $pr_2(w_3)^{-1} : y = x$ and $pr_1(w_3) : x < y$. We then can use transport along the former to turn the latter into an element of $x < x$. □

Lemma 6. *We have*

$$\prod_{x,y:\mathbb{N}} (x < y) \to (succ(x) < succ(y)).$$

Proof. We perform induction on $y : \mathbb{N}$. For $y \equiv 0$, we have $(x < 0) \equiv \mathbf{0}$ so it automatically holds that $C(x, 0)$.

Suppose $v : C(x, y)$. We want to find an element of $C(x, succ(y))$. Let $v_1 : x < succ(y)$. By induction, we have two cases: $v_2 : x < y$ or $v_3 : x = y$. For the first case, we have $v(v_2) : succ(x) < succ(y)$ so that $inl(v(v_2)) : C(x, succ(y))$. For the second case, we have $\text{ap}_{succ}(v_3) : succ(x) = succ(y)$ so that $inr(\text{ap}_{succ}(v_3)) : C(x, succ(y)$. □

Write $\ll succ : \prod_{x,y:\mathbb{N}} (x < y) \to (succ(x) < succ(y))$.

Theorem 1. *We have*

$$\prod_{x,y:\mathbb{N}} (x = y) + ((x < y) + (y < x)).$$

Proof. We perform induction on $x : \mathbb{N}$. For $x \equiv 0$, we have the following. We perform induction on y. For $y \equiv 0$, we have $inl(\text{refl}_0) : (x = y) + ((x < y) + (y < x)$. Suppose we have $v : (0 = y) + ((0 < y) + (y < 0))$. By induction, we may split into three cases. We have $v_1 : 0 = y$, $v_2 : 0 < y$, or $v_3 : y < 0$. For the first case, we have $inr(v_1) : 0 < succ(y)$ and so $inr(inl(inr(v_1)) : C(0, succ(y))$. For the second case, we have $inl(v_2) : 0 < succ(y)$ and so $inr(inl(inl(v_2)) : C(0, succ(y)$. For the third case, we have $v_3 : \mathbf{0}$ and thus it follows there exists $v_4 : C(0, succ(y)$.

Suppose we have $w : C(x, y)$. We wish to show that there is an element in $C(succ(x), y)$. By induction, we have three cases: $w_1 : x = y$, $w_2 : x < y$, or $w_3 : y < x$. We repeat the above argument for w_1 and w_3 in place of v_1 and v_2 respectively and with x replaced by y and y replaced by 0 to get our respective elements in those two cases. We are then left with $w_2 : x < y$. Since $y \equiv 0$ gives us $w_3 : \mathbf{0}$, we may assume by induction that there exists $y' : \mathbb{N}$ with $succ(y') \equiv y$. Thus we have $w_3 : x < succ(y')$ so that $w_3 : (x < y') + (x = y')$. By induction, we have two cases, $w_4 : x < y'$ or $w_5 : x = y'$. For the first case, we have $\ll succ(x, y')(w_4) : succ(x) < y$ so that $inr(inl(\ll succ(x, y')(w_4))) : C(succ(x), y))$. For the second case, we have $app_{succ}(w_5)) : succ(x) = y$ so that $inr(inr(app_{succ}(w_5)))) : C(succ(x), y)$. □

Lemma 7. *The statement $(x < y) + (y < x)$ is a mere proposition.*

Proof. By Lemma 2, we need only prove that $((x < y) \times (y < x)) \to \mathbf{0}$. We perform induction on $y : \mathbb{N}$. For $y \equiv 0$, let $v : ((x < 0) \times (0 < x))$. Then $pr_1(v) : x < 0 \equiv \mathbf{0}$.

Suppose $v_1 : ((x < y) \times (y < x)) \to \mathbf{0}$. We wish to show $((x < succ(y)) \times (succ(y) < x)) \to \mathbf{0}$. Let $w : ((x < succ(y)) \times (succ(y) < x))$. We have $pr_1(w) : x < succ(y)$. By induction, we have two cases: $w_1 : x < y$ or $w_2 : x = y$. In the first case, we have a function $\lambda a.v_1((w_1, a)) : (y < x) \to \mathbf{0}$.

Thus by Lemma 3, we have a function $w_3 : (succ(y) < x) \to \mathbf{0}$. Thus $w_3(pr_2(w)) : \mathbf{0}$. In the second case, we have $pr_2(w) : succ(x) < x$. From the proof of Lemma 5, we have that there exists $w_4 : ((x < x) \times (x = x)) \to \mathbf{0}$. So we have a function $\lambda a.w_4((a, \mathrm{refl}_x)) : (x < x) \to \mathbf{0}$. Again by Lemma 3, there exists a function $w_5 : (succ(x) < x) \to \mathbf{0}$. Thus $w_5(pr_2(w)) : \mathbf{0}$. □

Theorem 2. *The statement in Theorem* 1 *is a mere proposition.*

Proof. Lemma 7 tells us that $(x < y)+(y < x)$ is a mere proposition. As well, in the proof of Lemma 5, we have shown that $x = y$ is a mere proposition. By Lemma 2 it suffices to prove $((x = y) \times ((x < y) + (y < x))) \to \mathbf{0}$. Let $v : (x = y) \times ((x < y) + (y < x))$. We have $pr_1(v) : x = y$ and $pr_2(v) : (x < y) + (y < x)$. We have two cases: either $v_1 : x < y$ or $v_2 : y < x$. In the first case, we get $(v_1, pr_1(v)) : (x < y) \times (x = y)$. From the proof of Lemma 5, we get $v_3 : ((x < y) \times (x = y)) \to \mathbf{0}$. Thus we obtain : $v_3((v_1, pr_1(v))) : \mathbf{0}$. The second case follows similarly. □

Lemma 8. *We have*

$$\prod_{x,y:\mathbb{N}} ((x < y) + (x = y)) \to \sum_{z:\mathbb{N}} z + x = y.$$

Proof. We perform induction on $y : \mathbb{N}$. For $y \equiv 0$, take $v : (x < 0) + (x = 0)$. We have two cases by induction: $v_1 : x < 0$ and $v_2 : x = 0$. In the first case, we have $v_1 : \mathbf{0}$ so it follows that there exists $v_4 : \sum_{z:\mathbb{N}} z + x = 0$. In the second case, we have $\mathrm{app}_{add(0)}(v_2) : 0 + x = 0 + 0$ so that $\mathrm{app}_{add(0)}(v_2) : 0 + x = 0$. Thus $(0, \mathrm{app}_{add(0)}(v_2)) : \sum_{z:\mathbb{N}} z + x = 0$.

Suppose $w : C(x, y)$. We want to find an element of $C(x, succ(y))$. Let $w_1 : (x < succ(y))+(x = succ(y))$. By induction, we have two cases: $w_2 : x < succ(y)$ and $w_3 : x = succ(y)$. In the first case, we have $w_2 : (x < y) + (x = y)$ and so we have $w(w_2) : \sum_{z:\mathbb{N}} z + x = y$. Thus we have $\mathrm{app}_{succ}(pr_2(w(w_2))) : succ(z) + x = succ(y)$. Let a be $\mathrm{app}_{succ}(pr_2(w(w_2)))$. Then $(succ(z), a) : C(x, succ(y))$ In the second case, we have $w_3 : 0 + x = succ(y)$ and so $(0, w_3) : \sum_{z:\mathbb{N}} z + x = succ(y)$. □

Lemma 9. *The statement in Lemma* 8 *is a mere proposition. We have*

$$\prod_{x,y,z} (x + y = z + y) \to (x = z).$$

In particular we have

$$\prod_{x,y:\mathbb{N}} (y + x = x) \to (y = 0),$$

which is a mere proposition.

Proof. Taking $a : z + x = y$, we can do induction to get that $z + x \equiv y$ so that $a : y = y$ and thus $a = \mathrm{refl}_y$ so that $z + x = y$ is a mere proposition. Let $v_1, v_2 : C(x, y)$. We wish to show $v_1 = v_2$. By function extentionality, it suffices to show $v_1(a) = v_2(a)$ for all $a : (x < y) + (x = y)$. Thus it suffices to show for all $x, y : \mathbb{N}$, we have for $w_1, w_2 : \sum_{z:\mathbb{N}} z + x = y$ that $w_1 = w_2$.

By induction, it suffices to show that $z_1 + x = y$ and $z_2 + x = y$ implies $z_1 = z_2$. Suppose $w_3 : z_1 + x = y$ and $w_4 : z_2 + x = y$. Then we have $w_3 \centerdot (w_4)^{-1} : z_1 + x = z_2 + x$. We will argue by induction on x that this implies $z_1 = z_2$. Let a stand for $w_3 \centerdot (w_4)^{-1}$.

For $x \equiv 0$, we have $a : z_1 + 0 = z_2 + 0$.. Thus we have $add\_opp(0, z_1) \centerdot a \centerdot add\_opp(0, z_1) : 0 + z_1 = 0 + z_2$. Thus $add\_opp(0, z_1) \centerdot a \centerdot add\_opp(0, z_1) : z_1 = z_2$.

Assume $z_1 + x = z_2 + x$ implies $z_1 = z_2$. We wish to show that $z_1 + succ(x) = z_2 + succ(x)$ implies $z_1 = z_2$. Let $w_5 : z_1 + succ(x) = z_2 + succ(x)$. We have $(add\_succ(z_1, x))^{-1} \centerdot w_5 \centerdot add\_succ(z_1, x) : succ(z_1 + x) = succ(z_2 + x)$. Let b be $(add\_succ(z_1, x))^{-1} \centerdot w_5 \centerdot add\_succ(z_1, x)$. Then we have $encode(b) :$

$code(succ(z_1 + x), succ(z_2 + x))$. Since $code(succ(z_1 + x), succ(z_2 + x)) \equiv code(z_1 + x, z_2 + x)$, we have there exists $c : z_1 + x = z_2 + x$. Thus there exists $d : z_1 = z_2$. As a special case, taking $z_2 \equiv 0$, we obtain

$$\prod_{x,y:\mathbb{N}} (y + x = x) \to (y = 0)$$

and since $y + x = x$ is a mere proposition, we thus have that the above is a mere proposition. □

Having derived all the necessary propositions related to addition and ordering, we now turn our attention to multiplication and deriving all the necessary facts related to multiplication.

3 Multiplication

Definition 1. *We define multiplication* $mult : \mathbb{N} \to \mathbb{N} \to \mathbb{N}$ *by induction as follows. We define*

$$mult(0) :\equiv \lambda n.0 : \mathbb{N} \to \mathbb{N}$$

and

$$mult(succ(n)) :\equiv \lambda m.add(m, mult(n, m)) : \mathbb{N} \to \mathbb{N}$$

, which by induction gives us a defined function.

Lemma 10. *We have*

$$\prod_{x,y:\mathbb{N}} y + y \cdot x = y \cdot succ(x).$$

Proof. We perform induction on $y : \mathbb{N}$. For $y \equiv 0$, we have $0 + 0 \cdot x \equiv 0 + 0 \equiv 0$ and $0 \cdot 1 \equiv 0$. Thus $\text{refl}_0 : 0 + 0 \cdot x = 0 \cdot succ(x)$.

For the induction step, suppose we have an element $v : y + y \cdot x = y \cdot succ(x)$. We want to find an element of $succ(y) + succ(y) \cdot x = succ(y) \cdot succ(x)$. We have $succ(x) + y \cdot succ(x) \equiv succ(y) \cdot succ(x)$ and so $\text{ap}_{add(succ(x))}(v) : succ(x) + (y + y \cdot x) = succ(y) \cdot succ(x)$. Also, we have that $succ(y) + succ(y) \cdot x \equiv succ(y) + (x + y \cdot x) \equiv succ(y + (x + y \cdot x)) = y + succ(x + y \cdot x) \equiv y + (succ(x) + y \cdot x)$.

By Lemma 1, there exists $w_1 : y + (succ(x) + y \cdot x) = (y + succ(x)) + y \cdot x$. Also, there exists $w_2 : y + succ(x) = succ(x) + y$ and so $\text{app}_{add(y \cdot x)}(w_2) : y \cdot x + (y + succ(x)) = y \cdot x + (succ(x) + y)$. Also, there exists $w_3 : (y + succ(x)) + y \cdot x = y \cdot x + (y + succ(x))$ and there exists $w_4 : y \cdot x + (succ(x) + y) = (succ(x) + y) + y \cdot x$. Thus $w_1 \centerdot w_3 \centerdot \text{app}_{add(y \cdot x)}(w_2) \centerdot w_4 : succ(y) + succ(y) \cdot x = (succ(x) + y) + y \cdot x$. Also, by Lemma 1, there exists $w_5 : (succ(x) + y) + y \cdot x = succ(x) + (y + y \cdot x)$. Thus we have

$$w_1 \centerdot w_3 \centerdot \text{app}_{add(y \cdot x)}(w_2) \centerdot w_4 \centerdot w_5 \centerdot \text{app}_{add(succ(x))} : succ(y) + succ(y) \cdot x = succ(y) \cdot succ(x).$$

□

We will write $mult\_succ : \prod_{x,y\mathbb{N}} y + y \cdot x = y \cdot succ(x)$.

Theorem 3. *We have*

$$\prod_{x,y:\mathbb{N}} x \cdot y = y \cdot x.$$

Proof. We perform induction on $x : \mathbb{N}$. For $x \equiv 0$, we have $0 \cdot y \equiv 0$, so we need to find an element of $y \cdot 0 = 0$ for each $y : \mathbb{N}$. We perform induction on y. For $y \equiv 0$, we have $\text{refl}_0 : 0 \cdot 0 = 0$. Suppose there exists $v : y \cdot 0 = 0$. We want to find an element of $succ(y) \cdot 0 = 0$. We have $succ(y) \cdot 0 \equiv 0 + y \cdot 0 \equiv y \cdot 0$. Thus $v : succ(y) \cdot 0 = 0$.

For the induction step on x, suppose $w : x \cdot y = y \cdot x$. We want to find an elment of $succ(x) \cdot y = y \cdot succ(x)$. We have $succ(x) \cdot y \equiv y + x \cdot y$ so that $\text{app}_{add(y)}(w) : succ(x) \cdot y = y + y \cdot x$. Thus we have $\text{app}_{add(y)}(w) \centerdot mult\_succ(x, y) : succ(x) \cdot y = y \cdot succ(x)$. □

Let $mult\_opp(x,y) : \prod_{x,y} x \cdot y = y \cdot x$.

Lemma 11. *We have*

$$\prod_{x,y,z\mathbb{N}} (x+y)\cdot z = x\cdot z + y\cdot z.$$

Proof. We perform induction on $x : \mathbb{N}$. For $x \equiv 0$, we have $(0+y)\cdot z \equiv y\cdot z$ and $0\cdot z + y\cdot z \equiv 0 + y\cdot z \equiv y\cdot z$. Thus $\mathrm{refl}_{y\cdot z} : (0+y)\cdot z = 0\cdot z + y\cdot z$.

For the induction step on x, suppose $v : (x+y)\cdot z = x\cdot z + y\cdot z$. We want to find an element of $(succ(x)+y)\cdot z = succ(x)\cdot z + y\cdot z$. We have $(succ(x)+y)\cdot z \equiv (succ(x+y))\cdot z \equiv z + (x+y)\cdot z$ and $succ(x)\cdot z + y\cdot z \equiv (z + x\cdot z) + y\cdot z$. Thus we have $as\_add(z, x\cdot z, y\cdot z) : succ(x)\cdot z + y\cdot z = z + (x\cdot z + y\cdot z)$. Thus $\mathrm{app}_{add(z)}(v) \centerdot (as\_add(z, x\cdot z, y\cdot z))^{-1} : (succ(x)+y)\cdot z = succ(x)\cdot z + y\cdot z$. □

We will write $dist(x,y,z) : \prod_{x,y:\mathbb{N}} (x+y)\cdot z = x\cdot z + y\cdot z$.

Theorem 4. *We have*

$$\prod_{x,y,z:\mathbb{N}} (x\cdot y)\cdot z = x\cdot(y\cdot z).$$

Proof. We perform induction on $x : \mathbb{N}$. For $x \equiv 0$, we have $(0\cdot y)\cdot z \equiv 0\cdot z \equiv 0$. Also, $0\cdot(y\cdot z) \equiv 0$. Thus $\mathrm{refl}_0 : (0\cdot y)\cdot z = 0\cdot(y\cdot z)$.

For the induction step on $x : \mathbb{N}$, suppose $v : (x\cdot y)\cdot z = x\cdot(y\cdot z)$. We want to find an element of $(succ(x)\cdot y)\cdot z = succ(x)\cdot(y\cdot z)$. We have $(succ(x)\cdot y)\cdot z \equiv (y + x\cdot y)\cdot z$ and $succ(x)\cdot(y\cdot z) \equiv y\cdot z + x\cdot(y\cdot z)$. Thus we have $dist(y, x\cdot y, z) \centerdot \mathrm{app}_{add(y\cdot z)}(v) : (succ(x)\cdot y)\cdot z = succ(x)\cdot(y\cdot z)$. □

Lemma 12. *We have*

$$\prod_{x,y:\mathbb{N}} (((x=0)\to\mathbf{0})\times((y=0)\to\mathbf{0}))\to((x\cdot y=0)\to\mathbf{0}).$$

Proof. Let $v : ((x=0)\to\mathbf{0})\times((y=0)\to\mathbf{0})$. By induction, we have $v_1 : (x=0)\to\mathbf{0}$ and $v_2 : (y=0)\to\mathbf{0}$. By induction on $\mathbb{N}$, we have either $x \equiv 0$ or $x \equiv succ(x')$ for some $x' : \mathbb{N}$. In the first case, we have the following. For $x \equiv 0$, we have $v_2(\mathrm{refl}_0) : \mathbf{0}$ and so automatically there exists $v_3 : ((x\cdot y=0)\to\mathbf{0})$.

In the second case, let $w_1 : succ(x')\cdot y = 0$. We wish to construct an element of $\mathbf{0}$. We have $w_1 : y + x'\cdot y = 0$. Either $y \equiv 0$ or there exists $y' : \mathbb{N}$ such that $y \equiv succ(y')$. In the second case, we have $w_1 : succ(y' + x'\cdot y) = 0$. But then we have $encode(w_1) : \mathbf{0}$. In the first case, we have $\mathrm{refl}_0 : y = 0$ and so $v_2(\mathrm{refl}_0) : \mathbf{0}$. □

Having derived all the necessary facts related to multiplication, we will now define and derive the propositions related to divisibility and prime numbers that lead up to our proof of the infinitude of the primes.

4 Divisibility and Primes

Definition 2. *We will define the type $x \mid y$ as $((x=0)\to\mathbf{0})\times\sum_{z:\mathbb{N}} y = z\cdot x$. We will also define the type (y is prime) as $((y=1)\to\mathbf{0})\times\prod_{x:\mathbb{N}}((x\mid y)\times((x=1)\to\mathbf{0}))\to(x=y)$.*

Lemma 13. *The type $x \mid y$ is a mere proposition.*

Proof. Let $v_1, v_2 : x \mid y$. We have $pr_2(pr_2(v_1)) : y = pr_1(pr_2(v_1)) \cdot x$ and $pr_2(pr_2(v_2)) : y = pr_1(pr_2(v_2)) \cdot x$. So we have $(pr_2(v_1))^{-1} \centerdot pr_2(v_2) : pr_1(v_1) \cdot x = pr_1(v_2) \cdot x$. Abbreviate $(pr_2(v_1))^{-1} \centerdot pr_2(v_2)$ to a, $pr_1(pr_2(v_1))$ to b and $pr_1(pr_2(v_2))$ to c so we have $a : b \cdot x = c \cdot x$. By Theorem 1, we have three cases: $b = c$, $b < c$, or $c < b$. By Lemma 8, we thus derive two cases: there is some $z_1 : \mathbb{N}$ such that $z_1 + b = c$ or there exists $z_2 : \mathbb{N}$ such that $z_2 + c = b$.

Suppose the first case holds and let $d_1 : z_1 + b = c$. Then $\mathrm{ap}_{mult(x)}(d_1) : x \cdot (z_1 + b) = x \cdot c$. So we have $mult\_(z_1 + b, x) \centerdot \mathrm{ap}_{mult(x)}(d_1) \centerdot mult\_opp(x, c) : (z_1 + b) \cdot x = c \cdot x$. Thus we have an element $d_2 : c \cdot x = (z_1 + b) \cdot x$. So we have $a \centerdot d_2 : b \cdot x = (z_1 + b) \cdot x$. So we have $a \centerdot d_2 \centerdot dist(z_1, b, x) : b \cdot x = z_1 \cdot x + b \cdot x$. We have $\mathrm{refl}_{b \cdot x} : b \cdot x = b \cdot x$ and so by Lemmas 8 and 9, we have that $z_1 \cdot x \equiv 0$. By Theorem 1, we have by induction three cases: $z_1 < 0$, $0 < z_1$, and $z_1 = 0$. In the first case, we have $z_1 < 0 : \mathbf{0}$ so $v_1 = v_2$ follows automatically. For the second case, let $d_3 : 0 < z_1$. From the proof of Lemma 5, we have $d_4 : ((0 < z_1) \times (0 = z_1)) \to \mathbf{0}$. Thus we have $\lambda e.d_4((d_3, e) \times (e)) : (0 = z_1) \to \mathbf{0}$. Thus we have a function $d_5 : (z_1 = 0) \to \mathbf{0}$. As well, let $d_6 : x = 0$. By induction, we have $x \equiv 0$. Thus $pr_2(pr_2(v_1)) \centerdot mult\_opp(pr_1(pr_2(v_1)), x) : y = x \cdot pr_1(pr_2(v_1)) \equiv 0 \cdot pr_1(pr_2(v_1)) \equiv 0$. Thus we have $d_7 : y = 0$. But then $pr_1(v_1)((d_6, d_7)) : \mathbf{0}$. So again we have $v_1 = v_2$ automatically. The third case of $d_8 : z_1 = 0$ gives us $(d_8)^{-1} : 0 = z_1$. Also $add\_opp(b, z_1) \centerdot d_1 : b + z_1 = c$. So $\mathrm{app}_{add(b)}(d_8)^{-1} \centerdot add\_opp(b, z_1) \centerdot d_1 : b + 0 = c$. Let $d_9 : b + 0 = c$. Then $add\_opp(0, b) \centerdot d_9 : b \equiv 0 + b = c$. So there exists $d_{10} : pr_1(pr_2(v_1)) = pr_1(pr_2(v_2))$. By induction, we have that $pr_1(pr_2(v_1)) \equiv pr_1(pr_2(v_2))$ so that $pr_2(pr_2(v_2)), pr_2(pr_2(v_1)) : y = pr_1(pr_2(v_1)) \cdot x$. Then as in the proof of Lemma 5, we deduce that $pr_2(pr_2(v_2)) = pr_2(pr_2(v_1))$ and so by induction we have $pr_2(pr_2(v_2)) \equiv pr_2(pr_2(v_1))$. Thus we have $v_1 \equiv v_2$ so that $v_1 = v_2$.

The case of $z_2 + c = b$ is similar. □

Lemma 14. *We have*

$$\prod_{x,y,z} ((x \mid y) \times (x \mid (y + z))) \to (x \mid z).$$

Proof. Let $v : (x \mid y) \times (x \mid (y + z))$. We have $pr_1(v) : x \mid y$ and $pr_2(v) : x \mid (y + z)$. So we obtain $v_1 : y = a \cdot x$ and $v_2 : y + z = b \cdot x$. We have $add\_opp(z, y) \centerdot v_2 : z + y = b \cdot x$. So we have $(\mathrm{ap}_{add(z)}(v_1))^{-1} \centerdot add\_opp(z, y) \centerdot v_2 : z + a \cdot x = b \cdot x$. Abbreviate to $v_3 : z + a \cdot x = b \cdot x$. By induction on Theorem 1, we have three cases: $b < a$, $a = b$, and $a < b$. For the first case, we have by Lemma 8, there exists $z_1 : \mathbb{N}$ such that there exists $v_4 : z_1 + b = a$. So we have $(dist(z_1, b, x))^{-1} \centerdot mult\_opp(z_1 + b, x)\mathrm{ap}_{mult(x)}(v_4) \centerdot mult\_opp(x, a) : z_1 \cdot x + b \cdot x = a \cdot x$. Abbreviate to $v_5 : z_1 \cdot x + b \cdot x = a \cdot x$. We have $as\_as(z, z_1 \cdot z, b \cdot x) \centerdot \mathrm{ap}_{add(z)}(v_5) \centerdot v_3 : (z + z_1 \cdot x) + b \cdot x = b \cdot x$. By Lemmas 8 and 9, we can dervive that $z + z_1 \cdot x = 0$. We perform induction on $z : \mathbb{N}$. If $z \equiv 0$, then we have $\mathrm{refl}_0 : z = 0 \cdot x$. Thus $(pr_1(pr_1(v)), (0, \mathrm{refl}_0)) : (x \mid z)$. Otherwise, there exists $z' : \mathbb{N}$ such that $succ(z') \equiv z$. Thus we have $succ(z' + z_1 \cdot x) \equiv succ(z') + z_1 \cdot x = 0$. Thus $encode(succ(z' + z_1 \cdot x) \equiv succ(z') + z_1 \cdot x = 0) : \mathbf{0}$ so we have our result automatically.

For the other two cases, we have in both cases by Lemma 8 there exists $z_2 : \mathbb{N}$ such that there exists $v_6 : z_2 + a = b$. We have $(dist(z_2, a, x))^{-1} \centerdot mult\_opp(z_2 + a, x) \centerdot \mathrm{ap}_{mult(x)}(v_6) \centerdot mult\_opp(x, b) : z_2 \cdot x + a \cdot x = b \cdot x$. By Lemma 9 and $v_3 : z + a \cdot x = b \cdot x$, we thus have $z_2 \cdot x = z$. So we have $\mathrm{refl}_z : z = z_2 \cdot x$. Thus $(pr_1(pr_1(v)), (z_2, \mathrm{refl}_z)) : (x \mid z)$. □

Proposition 1. *We have*

$$\prod_{x,y:\mathbb{N}} ((x|y) \times ((y = 0) \to \mathbf{0})) \to ((x < y) + (x = y)),$$

which is a mere proposition.

Proof. Let $v : (x|y) \times ((y = 0) \to \mathbf{0})$. We have $pr_1(v) : x \mid y$ and $pr_2(v) : (y = 0) \to \mathbf{0}$. So we obtain $v_1 : y = a \cdot x$ and $v_2 : (x = 0) \to \mathbf{0}$. We have two cases: either $a \equiv 0$ or $a = succ(a')$ for

some $a' : \mathbb{N}$. In the first case, we obtain $v_1 : y = 0 \cdot x \equiv 0$ so that $pr_2(v)(v_1) : \mathbf{0}$. Thus we have automatically that $(x < y) + (x = y)$. In the second case, we obtain $v_1 : y = succ(a') \cdot x$ so that $v_1 : y = x + a' \cdot x$. By Theorem 1, we have by induction three cases: $y < x$, $x < y$, and $x = y$. Since the second and third cases give the result directly, we need only deal with the first case so assume $y < x$. By Lemma 8, there exists $z : \mathbb{N}$ such that there exists $w : z + y = x$. So we have $w^{-1} \centerdot \mathrm{ap}_{add(z)}(v_1) \centerdot add\_opp(z, x + a' \cdot x) \centerdot as\_add(x, a' \cdot x, z) \centerdot add\_opp(x, a' \cdot x + z) : x = (a' \cdot x + z) + x$. Thus we have $(a' \cdot x + z) + x = x$ from which it follows by induction that $0 \equiv a' \cdot x + z$ by Lemma 9. By induction, we have two cases: $z \equiv 0$ or $z = succ(z')$ for some $z' : \mathbb{N}$. In the first case, we have $w : y \equiv 0 + y = x$ so we have $(y < x) \times (y = x)$, which gives an element of $\mathbf{0}$ from Lemma 5. Thus we have $(x < y) + (x = y)$ automatically. In the second case, we have $add\_succ(z', a' \cdot x) : 0 = succ(a' \cdot x + z')$. But then $encode(add\_succ(z', a' \cdot x) : \mathbf{0}$. So again we have $(x < y) + (x = y)$ automatically.

From Lemma 5 again, we have that $((x < y) \times (x = y)) \to \mathbf{0}$. Thus by Lemma 2, Proposition 1 is a mere proposition. □

For the proof of the next proposition, we require the following lemma:

Lemma 15. *We have*

$$\prod_{x,y,z} ((x < y) \times (y < z)) \to (x < z).$$

Proof. Let $v : (x < y) \times (y < z)$. Then $pr_1(v) : x < y$ and $pr_2(v) : y < z$. So by Lemma 8 there exists $w_1 : \mathbb{N}$ such that there exists $w_2 : w_1 + y = z$ and there exists $w_3 : \mathbb{N}$ such that there exists $w_4 : w_3 + x = y$ by Lemma 8. Thus $as\_add(w_1, w_3, x) \centerdot \mathrm{ap}_{add(w_1)}(w_4) \centerdot w_2 : (w_1 + w_3) + x = z$. Abbreviate to $a : (w_1 + w_3) + x = z$. We have three cases by Theorem 1: $z < x$, $z = x$, and $x < z$. In the first two cases, we have there exists $b : \mathbb{N}$ such that there exists $c : b + z = x$. So we have $as\_add(b, w_1 + w_3, x) \centerdot \mathrm{ap}_{add(b)}(a) \centerdot c : (b + (w_1 + w_3)) + x = x$. By Lemma 9, we have there exists $d : b + (w_1 + w_3) = 0$. So we have $(as\_add(w_1, w_3, b))^{-1} \centerdot add\_opp(w_1 + w_3, b) \centerdot d : w_1 + (w_3 + b) = 0$. Either $w_1 \equiv 0$ or $w_1 = succ(w_4)$ for some $w_4 : \mathbb{N}$. In the first case, we have $w_2 : y = z$ which with $y < z$ gives an element of $\mathbf{0}$ by the proof of Lemma 5. So we have our result automatically. In the second case, we have $succ(w_4 + (w_3 + b)) = 0$, but $code(succ(w_4 + (w_3 + b)) = 0) : \mathbf{0}$ so again, we have our result automatically. Thus $x < z$. □

Proposition 2. *If $C(x, y)$ is decidable for $x, y : \mathbb{N}$ and*

$$\sum_{y:\mathbb{N}} C(x, y)$$

is decidable for $x : \mathbb{N}$, then

$$D(x) :\equiv \sum_{y:\mathbb{N}} (C(x, y)) \times \left(\prod_{z:\mathbb{N}} (z < y) \to (C(x, z) \to \mathbf{0}) \right)$$

is decidable and is a mere proposition, assuming $C(x, y)$ is a mere proposition. Moreover, we have that

$$\prod_{x:\mathbb{N}} \left(\sum_{y:\mathbb{N}} C(x, y) \right) \to D(x),$$

which is a mere propositon, assuming $D(x)$ is a mere proposition.

Proof. It's clear that

$$\prod_{x:\mathbb{N}} D(x) \to \sum_{y:\mathbb{N}} C(x, y),$$

from which we can derive $D(x) \to \mathbf{0}$ from $C(x,y) \to \mathbf{0}$ from the decidability of $C(x,y)$. We will prove that

$$\prod_{x:\mathbb{N}} \left(\sum_{y:\mathbb{N}} C(x,y) \right) \to D(x).$$

To prove this, we first prove the decidability of the following statement:

$$E(x,y') :\equiv \sum_{y:\mathbb{N}} ((y < y') \times (C(x,y))) \times \left(\prod_{z:\mathbb{N}} (z < y) \to (C(x,z) \to \mathbf{0}) \right)$$

We prove by induction on y'. For $y' \equiv 0$, we have $y < 0 : \mathbf{0}$ and so $E(x,0) \to \mathbf{0}$.

Suppose $v : E(x,y') + (E(x,y') \to \mathbf{0})$. We wish to show that $E(x, succ(y')) + (E(x, succ(y')) \to \mathbf{0})$. By induction, we have two cases: $v_1 : E(x,y')$ or $v_2 : E(x,y') \to \mathbf{0}$.

Suppose the first case holds. By induction, we have $v_3 : y < y'$, $v_4 : C(x,y)$, and $v_5 : (\prod_{z:\mathbb{N}} (z < y) \to (C(x,z) \to \mathbf{0}))$. We have $y < succ(y')$. Thus $E(x, succ(y'))$ holds.

Suppose the second case holds. Let $m : \mathbb{N}$ and for every $n : \mathbb{N}$ let $G(n) :\equiv (n < y') \to (C(x,n) \to \mathbf{0})$. We wish to show that $G(n)$ holds for every $n : \mathbb{N}$, which we will prove by strong induction.

To prove $G(n)$ holds for every $n : \mathbb{N}$ by strong induction, we first thus suppose that $v_4 : \prod_{z:\mathbb{N}} (z < m) \to (G(z))$ and derive $G(m)$. We have three cases by Theorem 1: $y' < m$, $y' = m$, or $m < y'$. If the first case holds, then we have $(y' < m) \times (m < y')$, which gives an element of $\mathbf{0}$ from Lemma 6. If the second case holds, then we have $(m < y') \times (m = y')$, which gives an element of $\mathbf{0}$ from Lemma 5. In both these cases we thus obtain $G(m)$ immediately.

In the third case let $v_6 : m < y'$. Suppose $v_7 : z < m$. Then by Lemma 15, we have $v_8 : z < y'$. Also, we have $v_4(v_7) : G(z) \equiv (z < y') \to (C(x,z) \to \mathbf{0})$. Thus we have $v_4(v_7(v_8)) : C(x,z) \to \mathbf{0}$. Thus

$$\prod_{z:\mathbb{N}} (z < m) \to (C(x,z) \to \mathbf{0}).$$

But we have $E(x,y') \to \mathbf{0}$ and thus $C(x,m) \to \mathbf{0}$. Thus $G(m)$ holds and so we have

$$\prod_{n:\mathbb{N}} (n < y') \to (C(x,n) \to \mathbf{0}).$$

We have two cases: either $C(x,y') \to \mathbf{0}$ or $C(x,y')$. In the first case, we have $\prod_{n:\mathbb{N}} (n < succ(y')) \to (C(x,n) \to \mathbf{0})$ and thus we can derive $(y < succ(y')) \times (C(x,y))) \to \mathbf{0}$ so that $E(x, succ(y')) \to \mathbf{0}$. In the second case, we have $y' < succ(y')$ and $E(x, succ(y'))$. Thus $E(x,y')$ is decidable.

We now use the decidability of $E(x,y')$ to prove that

$$\prod_{x:\mathbb{N}} \prod_{y:\mathbb{N}} C(x,y) \to E(x, succ(y)).$$

We prove by strong induction on y. Let $m : \mathbb{N}$ and suppose

$$\prod_{k:\mathbb{N}} (k < m) \to (C(x,k) \to E(x, succ(k))).$$

We want to show that $C(x,m) \to E(x, succ(m))$. Suppose $E(x, succ(m)) \to \mathbf{0}$ and that $C(x,m)$. Let $k < m$. Then by Lemma 6, we have $succ(k) < succ(m)$. We can easily derive that $E(x, succ(k)) \to$

$E(x, succ(m))$. By the decidability of $E(x, y')$, we therefore have $E(x, succ(k)) \to \mathbf{0}$. By the decidability of $C(x, y)$ and the inductive hypothesis, we therefore have $C(x, k) \to \mathbf{0}$. Thus we have that

$$\prod_{k:\mathbb{N}} (k < m) \to (C(x, k) \to \mathbf{0}).$$

Thus we obtain $E(x, succ(m))$, so we get an element of $\mathbf{0}$. Thus by the decidability of $E(x, y')$, we obtain $C(x, m) \to E(x, succ(m))$.

We now note that

$$\prod_{y':\mathbb{N}} E(x, y') \to D(x)$$

to get our desired result of

$$\prod_{x:\mathbb{N}} \left(\sum_{y:\mathbb{N}} C(x, y) \right) \to D(x),$$

and in particular that $D(x)$ is decidable.

Assuming that $C(x)$ is a mere proposition, we have that

$$((y < x) \times (C(y))) \times \left(\prod_{z:\mathbb{N}} (z < y) \to (C(z) \to \mathbf{0}) \right)$$

is a mere proposition from Lemma 5. So we only have to show there exists only one $y : \mathbb{N}$ that satisfies $D(x)$. Suppose we have $y_1, y_2 : \mathbb{N}$ both satisfy $D(x)$. If $y_1 = y_2$, then there is nothing to prove so by Theorem 1, we may assume that $y_1 < y_2$. But then from $D(x)$, we have $C(y_1) \to \mathbf{0}$ and $C(y_1)$ thus obtaining an element of $\mathbf{0}$. Thus $D(x)$ is a mere proposition. □

Proposition 3. *We have*

$$\prod_{x:\mathbb{N}} ((x = 0) \to \mathbf{0}) \to (x \mid x).$$

Proof. Let $v : (x = 0) \to \mathbf{0}$. Then we have $1 \cdot x \equiv x + 0 \cdot x \equiv x + 0$. So we have $add\_opp(0, x) : 1 \cdot x = x$. So $(v, (1, add\_opp(0, x))) : (x \mid x)$. □

Proposition 4. $(y \mid x) \times ((y = 1) \to \mathbf{0})$ *is decidable.*

Proof. We will prove $y \mid x$ and $(y = 1) \to \mathbf{0}$ are each decidable. We have that $y = 1$ is decidable by Theorems 1 and 2. Thus $(y = 1) \to \mathbf{0}$ is decidable.

To prove it for $y \mid x$, we use strong induction. Let $m \in \mathbb{N}$ and suppose $v : \prod_{k:\mathbb{N}} (k < m) \to ((y \mid k) + ((y \mid k) \to \mathbf{0}))$. By Theorem 1, we have three cases: $m = y$, $m < y$, and $y < m$. In the first case, we use induction to get $m \equiv y$ and so applying Proposition 3 gives us $y \mid m$ if $(y = 0) \to \mathbf{0}$ and $(y \mid m) \to \mathbf{0}$ if $y = 0$. In the second case, we have two subcases: $v_1 : m = 0$ and $v_2 : (m = 0) \to \mathbf{0}$. In the first instance, we have $v_1 \cdot mult\_opp(0, y) : m = y \cdot 0$ so thus $y \mid m$ if $(y = 0) \to \mathbf{0}$ and $(y \mid m) \to \mathbf{0}$ if $y = 0$. In the second instance, assume $v_3 : y \mid m$. We apply Proposition 1 to obtain $v_4 : (y < m) + (y = m)$. We apply induction to obtain $v_5 : y < m$ or $v_6 : y = m$. We then use Theorem 2 or follow the proof of Lemma 5 to obtain an element of $\mathbf{0}$. Thus $(y \mid m) \to \mathbf{0}$. In the third case, we have $v_6 : y < m$. By Lemma 8 there exists $m' : \mathbb{N}$ such that there exists $v_7 : m' + y = m$. We have $add\_opp(y, m') \cdot v_7 : y + m' = m$. By Theorem 1, we have three cases: $m < m'$, $m = m'$, and $m' < m$. In the first two cases, we have there exists $t : \mathbb{N}$ such that there exists $v_8 : t + m = m'$. Thus $\_add(t, y, m') \cdot \mathrm{ap}_{add(y)}(v_8) : (t + y) + m' = m'$. By Lemma 9, we have $t + y = 0$. Either $t \equiv 0$ or $t = succ(t')$ for some $t' : \mathbb{N}$. So we have $succ(t' + y) = 0$, but then $encode(succ(t' + y) = 0) \equiv \mathbf{0}$, which gives $(t \mid y)$ is decidable automatically. So $t \equiv 0$ so there exists $v_9 : y = 0$ and thus $pr_1(y \mid x)(v_9) : \mathbf{0}$ so that $(y \mid x) \to \mathbf{0}$. In the third case that $m' < m$, we apply the

induction hypothesis so that $(y \mid m')$ or $(y \mid m') \to \mathbf{0}$. In the first case, we have that there exists $w_1 : \mathbb{N}$ such that there exists $w_2 : m' = w_1 \cdot y$. So we obtain $(v_7)^{-1}{\cdot}add\_opp(m', y){\cdot}\mathrm{ap}_{add(y)}(w_2) : m = succ(w_1) \cdot y$ so we have $y \mid m$. In the second case, suppose $w_3 : y \mid m$. Then there exists $w_4 : \mathbb{N}$ such that there exists $w_5 : m = w_4 \cdot y$. Either $w_4 \equiv 0$ or there exists $w' : \mathbb{N}$ such that $w_4 \equiv succ(w')$. In the former case, we have $w_5 : m = 0 \equiv 0 \cdot y$ so that $y \mid m$ so we get an element of $\mathbf{0}$ so we get $(y \mid m)$ is decidable automatically. In the second instance, we get $w_5 : m = y + w' \cdot y$. Applying *add_opp*, we obtain $w' \cdot y + y = m$. Since $m' + y = m$, Lemma 9 gives us $m' = w' \cdot y$ so that $y \mid m'$ and thus we get an element of $\mathbf{0}$. Thus $(y \mid m) \to \mathbf{0}$. □

Proposition 5. *Let* $F(x, y) :\equiv (((y = 1) \to \mathbf{0}) \times (y \mid x)$ *We have*

$$\prod_{x:\mathbb{N}} (1 < x) \to \sum_{y:\mathbb{N}} \left(F(x, y) \times \left(\prod_{z:\mathbb{N}} (z < y) \to ((F(x, z)) \to \mathbf{0}) \right) \right).$$

Proof. Let $v : 1 < x$. By Proposition 4, we have there exists $v_1 : x \mid x$ for since $1 < x$, we have that $(x = 1) \to \mathbf{0}$. By Proposition 1 it suffices to prove

$$\prod_{x:\mathbb{N}} (1 < x) \to \sum_{y:\mathbb{N}} \left(((y < succ(x)) \times (F(x, y)) \times \left(\prod_{z:\mathbb{N}} (z < y) \to ((F(x, z)) \to \mathbf{0}) \right) \right).$$

By Proposition 4, $F(x, y)$ is decidable. Since we have $F(x, x)$, we thus have

$$\sum_{y:\mathbb{N}} F(x, y).$$

By Proposition 2, we thus have

$$\sum_{y:\mathbb{N}} F(x, y) \times \left(\prod_{z:\mathbb{N}} (z < y) \to ((F(x, z)) \to \mathbf{0}) \right).$$

□

Proposition 6. *The* $y : \mathbb{N}$ *in Proposition* 5 *from any* $x : \mathbb{N}$ *satisfies* (y *is prime*).

Proof. Let $x : \mathbb{N}$ and let $y : \mathbb{N}$ follow from Proposition 5. We have $F(x, y)$ so that $(y = 1) \to \mathbf{0}$. Let $z : \mathbb{N}$ and suppose $v : ((z \mid y) \times ((z = 1) \to \mathbf{0}))$. By Proposition 1, we have by induction two cases: $z < y$ and $z = y$. Since $z = y$ gives us our desired result, let us assume $w : z < y$. By Proposition 5, we have $(F(x, z)) \to \mathbf{0}$. Since $z \mid y$, we have there exists $w_1 : \mathbb{N}$ such that there exists $w_2 : y = w_1 \cdot z$. Also since $y \mid x$, we have there exists $w_3 : \mathbb{N}$ such that there exists $w_4 : x = w_3 \cdot y$. We have $w_4 \cdot \mathrm{ap}_{mult(w_1)} \cdot (as\_mult(w_3, w_1, z))^{-1} : x = (w_3 \cdot w_1) \cdot z$. So we have $z \mid x$. But we also have $((z = 1) \to \mathbf{0}$ so that $F(x, z)$. Thus we get an element of 0 so that we get (y is prime) automatically. □

Proposition 7. *We have* (x *is prime*) *is decidable.*

Proof. Let $x : \mathbb{N}$. We have three cases: $x < 1$, $x = 1$, and $1 < x$. We will first prove that in the first two cases x is not prime. We'll assume that $v : ((x = 1) \to \mathbf{0}) \times \prod_{z:\mathbb{N}} ((z \mid x) \times ((z = 1) \to \mathbf{0})) \to (z = x)$ and derive an element of $\mathbf{0}$. If $x < 1$, we can deduce that $x = 0$. We have $0 \equiv 0 \cdot 2$ so that $2 \mid 0$. Also $(2 = 1) \to \mathbf{0}$ from Lemma 4. From $pr_2(v)$, we obtain an element of $\mathbf{0}$. Thus (0 is prime) $\to \mathbf{0}$. In the second case, $pr_1(v)$ gives an element of $\mathbf{0}$ so that (1 is prime) $\to \mathbf{0}$.

We turn to the last case of $1 < x$. We let $y : \mathbb{N}$ be obtained from x by Proposition 5. Since $y \mid x$, we have by Proposition 1, two cases: either $y < x$ or $y = x$. Let the first case hold. We'll again take our element v above and derive an element of $\mathbf{0}$ showing again that x is not prime. We have $F(x, y)$ so that $(y = 1) \to \mathbf{0}$. From $pr_2(v)$, we have $y = x$, but $((y < x) \times (y = x)) \to \mathbf{0}$ so we have (y is prime) $\to \mathbf{0}$. In the second case, we perform induction to get that $y \equiv x$ so that (x is prime). □

Proposition 8. *If $C(x)$ for $x : \mathbb{N}$ is decidable, that is,*

$$\prod_{x:\mathbb{N}}(C(x)) + (C(x) \to \mathbf{0}),$$

(which is a mere proposition from Lemma 2), then for any $y : \mathbb{N}$, $(x < y) \to C(x)$ is decidable, that is

$$\prod_{y,x:\mathbb{N}} ((x < y) \to C(x)) + (((x < y) \to C(x)) \to \mathbf{0}),$$

which is a mere proposition.

Proof. We prove by induction on $y : \mathbb{N}$. For $y \equiv 0$, we have $x < 0 : \mathbf{0}$ so that $(x < 0) \to C(x)$ follows automatically.

Suppose the claim holds for $y : \mathbb{N}$. We want to show it holds for $succ(y) : \mathbb{N}$. By induction we have two cases: $v_1 : (x < y) \to C(x)$ and $v_2 : ((x < y) \to C(x)) \to \mathbf{0}$.

Suppose the first case holds. Let $v_2 : x < succ(y)$. We have two cases $v_3 : x < y$ and $v_4 : x = y$. In the first case, we have $v_1(v_3) : C(x)$. In the second case, we have either $C(y)$ or $C(y) \to \mathbf{0}$. If $C(y)$ holds, then we have $(x < succ(y)) \to C(x)$. Otherwise $C(y) \to \mathbf{0}$. We'll show that we can derive an element of $\mathbf{0}$ from $v : (x < succ(y)) \to C(x)$. We have $x < succ(y) \equiv (x < y) + (x = y)$ and thus $v(inr(\mathrm{refl}_y)) : C(y)$. Thus we have an element of $\mathbf{0}$.

Suppose the second case holds. Let $v_6 : (x < succ(y)) \to C(x)$. So $\lambda a.v_6(inl(a)) : (x < y) \to C(x)$. Applying v_2, we get an element of $\mathbf{0}$. □

Proposition 9. *Let*

$$M(x, y) :\equiv \prod_{z:\mathbb{N}}(z < x) \to ((z \text{ is prime}) \to (z \mid y)),$$

which is a mere proposition. We have

$$\prod_{x:\mathbb{N}} \left(\sum_{y:\mathbb{N}}((M(x, y)) \times (0 < y)) \times \left(\prod_{n:\mathbb{N}}(n < y) \to (((M(x, n)) \times (0 < n)) \to \mathbf{0}) \right) \right),$$

which again is a mere proposition from Proposition 2.

Proof. By Proposition 2, it suffices to prove that $M(x, y)$ is decidable and is a mere proposition and that

$$\prod_{x:\mathbb{N}} \left(\sum_{y:\mathbb{N}}((M(x, y)) \times (0 < y)) \right).$$

We perform induction on x to first prove the latter statement. For $x \equiv 0$, take $y \equiv 1$. Then $z < 0 \equiv \mathbf{0}$ so $M(0, 1)$ holds trivially. Also, from $n < 1$, we get $n = 0$, but $0 < 0 : \mathbf{0}$ so the claim holds trivially.

Suppose the claim holds for $x : \mathbb{N}$. We want to show it holds for $succ(x)$. Let $y : \mathbb{N}$ be the output on x given by the claim. By Proposition 7, we have either (x is prime) or (x is prime) $\to \mathbf{0}$. In the latter case, we have $z < succ(x) :\equiv (z < x) + (z = x)$ so that $((z < succ(x)) \to ((z \text{ is prime}) \to (z \mid y))) \to ((z < x) \to ((z \text{ is prime}) \to (z \mid y)))$ and $((z < x) \to ((z \text{ is prime}) \to (z \mid y))) \to ((z < succ(x)) \to ((z \text{ is prime}) \to (z \mid y)))$. Thus for all $n : \mathbb{N}$ $M(x, n) \to M(succ(x), n)$ and $M(succ(x), n) \to M(x, n)$. Thus the claim holds for $succ(x)$ with y.

Suppose we have (x is prime). Consider $x \cdot y$. Suppose we have $(z < succ(x))$ and (z is prime). Either $z < x$ or $x = z$. In the first case, we have $(z \mid y)$ by $M(x, y)$. So there exists $v_1 : \mathbb{N}$ such that there

exists $v_2 : y = v_1 \cdot z$. So we have $\mathrm{ap}_{mult(x)}(v_2) \centerdot (x, v_1, z)^{-1} : x \cdot y = (x \cdot v_1) \cdot z$ so $z \mid (x \cdot y)$. In the second case, let $v_3 : x = z$. We have $mult\_opp(x, y) \centerdot \mathrm{ap}_{mult(y)}(v_3) : x \cdot y = y \cdot z$. Thus again $z \mid (x \cdot y)$. Thus $M(succ(x), x \cdot y)$.

It remains to prove that $M(x, y)) \times (0 < y)$ is decidable and is a mere proposition. Since (z is prime) and ($z \mid y$) are both decidable, we have (z is prime) $\to$ ($z \mid y$) is decidable. Thus by Proposition 8, $M(x, y)$ is decidable. As well, by Theorems 1 and 2, $(0 < y)$ is decidable. Thus $(M(x, y)) \times (0 < y)$ is decidable. Also, $(z \mid y)$ is a mere proposition so $M(x, y)$ is a mere proposition. □

Theorem 5. *(Infinitude of the Prime Numbers) Let* $P(x, y) :\equiv ((x = y) + (x < y)) \times (y$ *is prime), which is a mere proposition from Lemma* 5*. We have*

$$\prod_{x:\mathbb{N}} \left(\sum_{y:\mathbb{N}} (P(x, y)) \times \left(\prod_{z:\mathbb{N}} (z < y) \to (P(x, z) \to \mathbf{0}) \right) \right),$$

which is again a mere proposition from Lemma 5*.*

Proof. By Proposition 2, it suffices to prove that $P(x, y)$ is decidable and that

$$\prod_{x:\mathbb{N}} \left(\sum_{y:\mathbb{N}} (P(x, y)) \right).$$

By Theorems 1 and 2, we see that $(x = y)$, $(x < y)$, and (y is prime) are all decidable. Thus $P(x, y)$ is decidable. For the latter claim, we argue as follows.

Let $x : \mathbb{N}$. Pick $a : \mathbb{N}$ satisfying y in Proposition 9 and consider $a + 1$. Apply Propositions 5 and 6 to get that there exists $p : \mathbb{N}$ satisfying (p is prime) and $p \mid (a + 1)$. We first wish to show that $P(x, p)$. We have by induction and Theorem 1, three cases: $p < x$, $p = x$, or $x < p$. The last two cases give us $P(x, p)$ so assume $p < x$. Then by the statement in Proposition 9, we have $M(x, a)$ so that $p \mid a$. By Lemma 14, we thus have $p \mid 1$. Since $(1 = 0) \to \mathbf{0}$ by Lemma 4, we have by Proposition 1 that $p < 1$ or $p = 1$. In the former case, we get $p = 0$ and as was shown in Proposition 7, this leads to an element of $\mathbf{0}$ so $P(x, p)$ follows automatically. In the latter case, we also get that $p = 1$ leads to an element of $\mathbf{0}$ so again we get $P(x, p)$ automatically. □

5 Observations and Conclusions

Deriving number theoretic results within the realm of homotopy type theory can certainly prove to be an enlightening experience. One thing in particular that is worth pointing out is how the theory takes little for granted. For example, it does not even assume the law of the excluded middle, which we did not use in our development of the proof of the infinitude of the primes. Instead, a lot of the time the theory works is to split a problem up into various cases by the rules of its type operations, have some of these cases possibly ultimately giving an element of the type $\mathbf{0}$ and following the rule that you can derive anything from an element of $\mathbf{0}$, which is logically sound since the type $\mathbf{0}$ conceptually has no elements. As well, for any statements where we had to use the law of the excluded middle we were able to derive it ourselves, which happens when we prove a given proposition is decidable, from the rules of homotopy type theory.

There are two remarkable examples in our proof of the infinitude of primes that illustrate type theory's tendency to not let us use facts that we do not really need to derive a specific theorem. For one, no where in our proof. We showed how to decide whether a given number is prime and how to derive a prime from a given number, but no where did we explicitly give a solid example of a prime. Another is the use of the fact that there exists a least natural number that is divisible by all the primes

up to a given number x. In conventional foundations, we know that a number that is divisible by all these primes is the product of them all, but we did not need to prove this. All we needed was the existence of such an element and pickout out the least of them made our statement into a mere proposition.

On the other hand, the basic inution of how to develop number theory is the same and it still is possible to view our methods as an algorithm or a program. In our proof of the infinitude of primes, for example, we start with a given number x. We go through all the numbers in increasing order up to x, keeping track of our "a" value that is the least value that is divisible by all the primes less than y. If y turns out to be prime we multiply our "a" value by y to get an upperbound for our new value of a so that we get pick out the least value that works. We repeat this procedure until we hit x at which time we add 1 to it. Then we go up the chain of natural numbers again until we hit a number greater than the 1 that divides it and this new number has to a prime p that is at least x. Then we go up the chain of numbers from x to p to pick out the least one.

We end here with a specific example of a prime (in this case the prime corresponding to 2) and prove it is a prime using our derived propositions.

Proposition 10. *We have* 2 *is prime.*

Proof. We have there exists $v : (2 = 1) \to \mathbf{0}$ by Lemma 4. Suppose $v_1 : x|2$ and $v_2 : (x = 1) \to \mathbf{0}$. Also, we have $encode(2 = 0) \equiv \mathbf{0}$ so we have a function $v_3 : (2 = 0) \to \mathbf{0}$. Thus by Proposition 1 $x < 2$ or $x = 2$. Since the latter case is exactly what we want, we need only deal with the former case. That case gives us the two cases $x < 1$ and $x = 1$. Applying v_2 to the latter case gives us an element of $\mathbf{0}$ so we get $x = y$ automatically. Again, the other case can be split into two cases: $x < 0$ and $x = 0$. If $x < 0$ holds, we have $x < 0 : \mathbf{0}$ so $x = y$ automatically. If $x = 0$ holds, then $pr_1(v_1) : (x = 0) \to \mathbf{0}$ so again $x = y$ automatically. □

References

[1] *The Univalent Foundations Program*, Homotopy Type Theory: Univalent Foundations of Mathematics, http://homotopytypetheory.org/book, Institute for Advance Study 2013.