

9 The Theory of Numbers

At this point now, having covered the material from the previous set of notes, we can take for granted all of the “grade school” arithmetic and algebraic properties of $\mathbb{N}$ and $\mathbb{Z}$.

Theorem 9.1: Strong Induction.

For any wff φ with at most one free variable, the following equivalence holds.

$$\begin{aligned} (\forall n \in \mathbb{N})(\varphi(n)) &\Leftrightarrow \varphi(0) \wedge (\forall k \in \mathbb{N})((\forall \ell \in \mathbb{N})(\ell < k \Rightarrow \varphi(\ell)) \Rightarrow \varphi(k)) \\ &\Leftrightarrow \varphi(0) \wedge (\forall k \in \mathbb{N})((\forall \ell \in \mathbb{N})(\ell \leq k \Rightarrow \varphi(\ell)) \Rightarrow \varphi(k+1)) \end{aligned}$$

9.1 The Fundamentals

Definition 9.1: Divisibility.

Given two integers $x, y \in \mathbb{Z}$, we say that x *divides* y when y is an integer multiple of x .¹

divides

$x \mid y$

$$x \mid y :\Leftrightarrow (\exists z \in \mathbb{Z})(x \cdot z = y)$$

¹It is important to note $x \mid y$ is a *sentence*, as opposed to an *object* like the quotient $\frac{x}{y}$.

When $x \mid y$, we typically call x the *divisor* and y the *dividend* in the relationship.

It should be clear that $x \mid y \Rightarrow -x \mid y$ and $x \mid y \Rightarrow x \mid -y$ for any $x, y \in \mathbb{Z}$, so sign does not impact divisibility relationships. Further, the integer 1 divides every other integer.

Lemma 9.1: One is a Universal Divisor.

$(\forall x \in \mathbb{Z})(1 \mid x)$.

Proof. Let $x \in \mathbb{Z}$ and notice $1 \cdot x = x$. Since $x \in \mathbb{Z}$, we can conclude $1 \mid x$ by definition.

QED

This establishes 1 as a *universal divisor* in $\mathbb{Z}$.² The integer 0 plays a role “dual” to 1 with respect to divisibility; whereas 1 is a universal divisor, 0 is a *universal dividend*.³

Lemma 9.2: Zero is a Universal Dividend.

$(\forall x \in \mathbb{Z})(x \mid 0)$.

Proof. Let $x \in \mathbb{Z}$ and observe that $x \cdot 0 = 0$. Since $0 \in \mathbb{Z}$, we have that $x \mid 0$ by definition.

QED

We will soon see that the relation established by divisibility on $\mathbb{N}$ has all of the same properties that the $\leq$ ordering on $\mathbb{N}$ did. Divisibility gives us a different perspective from which we can think about *ordering* the integers.

Theorem 9.2: Divisibility is Absolutely Monotonic.

$(\forall x, y \in \mathbb{Z})((x \mid y \wedge y \neq 0) \Rightarrow |x| \leq |y|)$.

As a consequence of this theorem, whenever $x, y \in \mathbb{N}_+$ such that $x \mid y$, we know $x < y$. This is an incredibly useful fact to keep in mind as we develop our understanding of divisibility—we don’t yet know too much about what $x \mid y$ means, but we know a few things about what $x \leq y$ means by this point. Let’s learn some more about divisibility.

Lemma 9.3.

$(\forall x \in \mathbb{Z})(0 \mid x \Rightarrow x = 0)$.

Proof. Let $x \in \mathbb{Z}$ and assume $0 \mid x$. By definition, this means $0 \cdot k = x$ for some $k \in \mathbb{Z}$. Since $0 = 0 \cdot k$, this implies $0 = 0 \cdot k = x$ as desired.

QED

²In the language of category theory, this property makes 1 an *initial object*.

³In the language of category theory, this property makes 0 a *terminal object*.

Lemma 9.4.

$$(\forall x \in \mathbb{Z})(x \mid 1 \Rightarrow |x| = 1).$$

Proof. Let $x \in \mathbb{Z}$ and assume $x \mid 1$. This implies $|x| \leq |1| = 1$ by the absolute monotonicity of divisibility. $|x| \leq 1$ implies that either $x \leq 1$ or $-x \leq 1$,⁴ and we can see that $-x \leq 1 \Leftrightarrow -1 \leq x$. Thus, we have $x \in \{-1, 0, 1\}$. Now, towards a contradiction, assume that $x = 0$. Then, $0 \mid 1$, which implies $1 = 0$ by Lemma 9.3, contradicting the fact that we know $1 \neq 0$. $\nexists$ Therefore, $x \neq 0$, implying $x \in \{-1, 1\}$, so that $|x| = 1$.

⁴This follows from the definition of the absolute value function.

QED

Lemma 9.5.

$$(\forall n, x, y, a, b \in \mathbb{Z})((n \mid x \wedge n \mid y) \Rightarrow n \mid ax + by).$$

Proof. This proof is left as an exercise to the reader. $\square$

The next three theorems establish that divisibility is *almost* a partial order on the integers. In fact, if we restated the next three theorems for $\mathbb{N}$ instead of for $\mathbb{Z}$, then we would see that divisibility is a partial order on the *natural numbers*.

Lemma 9.6: Divisibility is Almost a Partial Order on the Integers.

The following three statements are *true*.

1. $(\forall x \in \mathbb{Z})(x \mid x)$.
2. $(\forall x, y \in \mathbb{Z})(x \mid y \wedge y \mid x \Rightarrow |x| = |y|)$.
3. $(\forall x, y, z \in \mathbb{Z})((x \mid y \wedge y \mid z) \Rightarrow x \mid z)$.

Reflexivity

Antisymmetry (almost)

Transitivity

Proof.

1. Let $x \in \mathbb{Z}$ and recall that $x \cdot 1 = x$. Since $1 \in \mathbb{Z}$, we know $x \mid x$ by definition.
2. Let $x, y \in \mathbb{Z}$. Assume $x \mid y$ and $y \mid x$. We can see that $x \mid y$ implies $|x| \leq |y|$. Similarly, since $y \mid x$, we know $|y| \leq |x|$. We can then conclude that $|x| = |y|$.
3. Let $x, y, z \in \mathbb{Z}$. Assume $x \mid y$ and $y \mid z$. Then, we know there exist $k_1 \in \mathbb{Z}$ and $k_2 \in \mathbb{Z}$ such that $x \cdot k_1 = y$ and $y \cdot k_2 = z$ by definition. We can then observe.

$$y \cdot k_2 = (x \cdot k_1) \cdot k_2 = x \cdot (k_1 \cdot k_2) = z$$

Since $k_1 \in \mathbb{Z}$ and $k_2 \in \mathbb{Z}$, we know $k_1 \cdot k_2 \in \mathbb{Z}$, so that $x \mid z$ by definition.

QED

Definition 9.2: Primality.

prime

We call a natural number $n \in \mathbb{N}$ *prime* when $n > 1$ and n has as few divisors as possible.

$$n \text{ is prime} :\Leftrightarrow (n > 1) \wedge (\forall p \in \mathbb{N})(p \mid n \Rightarrow p \in \{1, n\})$$

If n is not prime, then we usually say that n is *composite*.

Theorem 9.3: Fundamental Lemma of Arithmetic.

$$(\forall n \in \mathbb{N})(n \geq 2 \Rightarrow (\exists p \in \mathbb{N})(p \text{ is prime} \wedge p \mid n)).$$

Proof. We show every natural number after 1 has a prime divisor by *strong induction*.

Basis Step:

Let $x \in \mathbb{N}$ such that $x \mid 2$. This implies $|x| \leq |2|$, so that $x \leq 2$, meaning $x \in \{0, 1, 2\}$.

Towards a contradiction, suppose $x = 0$; then, since $x \mid 2$, we know $0 \mid 2$, so that $2 = 0$, contradicting the fact that $2 \neq 0$. $\nexists$ Thus, $x \neq 0$, so that $x \in \{1, 2\}$. From all of this, we now know that 2 is prime by definition. We conclude by recalling $2 \mid 2$.

Inductive Step:

Let $k \in \mathbb{N} \setminus \{0, 1\}$. Assume $(\forall \ell \in \mathbb{N})(\ell < k \Rightarrow (\exists p \in \mathbb{N})(p \text{ is prime} \wedge p \mid \ell))$.⁵

We now take two cases based on whether or not k is prime.

Case 1:

Suppose that k is prime. Recalling $k \mid k$ since $(\forall x \in \mathbb{Z})(x \mid x)$, we are done.

Case 2:

Suppose that k is composite. By definition, this means that there exists $m \in \mathbb{N}$ such that $m \mid k$ and $m \neq 1$ and $m \neq k$ by definition.

Towards a contradiction, suppose that $m = 0$; this would imply $0 \mid k$, so that $k = 0$, contradicting the fact that $k > 1$. $\nexists$ Thus, we also know $m \neq 0$; recalling that $m \neq 1$, we can then deduce $m > 1$.

Now, remembering $m \mid k$, we can see that $|m| \leq |k|$, so that $m \leq k$. Combined with the fact that $m \neq k$, we now know $m < k$.

This all means that we can apply our *inductive hypothesis* to realize there exists $p \in \mathbb{N}$ such that p is prime and $p \mid m$. If we recall that $m \mid k$ by assumption, then transitivity of divisibility yields $p \mid k$ as we wanted.

Therefore, $(\forall n \in \mathbb{N})(n > 1 \Rightarrow (\exists p \in \mathbb{N})(p \text{ is prime} \wedge p \mid n))$.

QED

Theorem 9.4: Fundamental Theorem of Arithmetic.

For every $n \in \mathbb{N}$ such that $n \geq 2$, there exists a *unique* $k \in \mathbb{N}$, and there exist *unique* $p_0, \dots, p_k \in \mathbb{N}$, and there exist *unique* $\alpha_0, \dots, \alpha_k \in \mathbb{N}_+$ such that the following hold.

- $(\forall i, j \in k)(i \neq j \Rightarrow p_i \neq p_j)$.
- $(\forall i \in k)(p_i \text{ is prime})$.
- $n = \prod_{i=1}^k p_i^{\alpha_i}$

Theorem 9.5: Euclid's Division Lemma.

$(\forall x, y \in \mathbb{Z})(y \neq 0 \Rightarrow (\exists! q, r \in \mathbb{Z})(x = qy + r \wedge 0 \leq r < |y|))$.

Proof. We first prove existence and then uniqueness. Let $x, y \in \mathbb{Z}$ such that $y \neq 0$.

Case 1:

Suppose $y > 0$ and observe the following deductions.

$$\begin{aligned} x \geq 0 &\Rightarrow x = 0 \cdot y + x \\ x < 0 &\Rightarrow x = x \cdot y + (x - x \cdot y) \end{aligned}$$

Thus, in either case, we know $(\exists q, r \in \mathbb{Z})(x = q \cdot y + r \wedge r \geq 0)$. Now, consider $R := \{r \in \mathbb{N} \mid (\exists q \in \mathbb{Z})(x = q \cdot y + r)\}$. As we just saw, $R \neq \emptyset$, and we can also clearly see $R \subseteq \mathbb{N}$. Therefore, there exists $r_0 \in R$ such that $(\forall s \in R)(r_0 \leq s)$.

Towards a contradiction, assume $r_0 < |y|$, so that $r_0 \geq |y|$, implying $r_0 - |y| \geq 0$. Since $r_0 \in R$, we know there exists $q_0 \in \mathbb{Z}$ such that $x = q_0 \cdot y + r_0$ by definition.

⁵This sentence is our *strong inductive hypothesis*.

$$\begin{aligned}
x &= q_0 \cdot y + r_0 \\
&= q_0 \cdot y + (r_0 - |y| + |y|) \\
&= (q_0 \cdot y + |y|) + (r_0 - |y|) \\
&= (q_0 \cdot y + y) + (r_0 - y) \quad \text{since we assumed } y > 0 \\
&= (q_0 + 1) \cdot y + (r_0 - y)
\end{aligned}$$

Now, notice $q_0 + 1 \in \mathbb{Z}$. Since we assumed $r_0 \geq |y|$, and $|y| = y$ because $y > 0$, we also now know $0 \leq r_0 - y < r_0$. All this means that $r_0 - y \in R$ by definition; however, $r_0 - y < r$ contradicts the fact that $(\forall s \in R)(r_0 \leq s)$. $\nexists$ Thus, $r_0 < |y|$. We therefore conclude $(\exists q, r \in \mathbb{Z})(x = q \cdot y + r \wedge 0 \leq r < |y|)$. This proves existence.

To prove uniqueness, suppose that $x = q_1 \cdot y + r_1$ and $x = q_2 \cdot y + r_2$ for some $q_1, r_1, q_2, r_2 \in \mathbb{Z}$ such that $0 \leq r_1 < |y|$ and $0 \leq r_2 < |y|$. Combining information from these two inequalities and recalling $y > 0$ shows us the following.

$$\begin{aligned}
0 \leq r_1 < |y| &\Rightarrow r_1 < y \\
&\Rightarrow r_1 - r_2 < y - r_2 \\
&\Rightarrow r_1 - r_2 < y - r_2 \leq y \\
&\Rightarrow r_1 - r_2 < y \\
0 \leq r_2 < |y| &\Rightarrow r_2 < y \\
&\Rightarrow r_2 - r_1 < y - r_1 \\
&\Rightarrow r_2 - r_1 < y - r_1 \leq y \\
&\Rightarrow r_2 - r_1 < y \\
&\Rightarrow -(r_1 - r_2) < y
\end{aligned}$$

From our results $r_1 - r_2 < y$ and $-(r_1 - r_2) < y$ above, we can see $|r_1 - r_2| < y$. Now, towards a contradiction, suppose $r_1 \neq r_2$, so that $r_1 - r_2 \neq 0$. By subtracting one equation from the other, we can infer that y divides $|r_1 - r_2|$ as shown below.

$$\begin{aligned}
x - x &= (q_1 - q_2) \cdot y + (r_1 - r_2) \Rightarrow 0 = (q_1 - q_2) \cdot y + (r_1 - r_2) \\
&\Rightarrow -(q_1 - q_2) \cdot y = r_1 - r_2 \\
&\Rightarrow |q_1 - q_2| \cdot y = |r_1 - r_2| \\
&\Rightarrow y \mid |r_1 - r_2| \\
&\Rightarrow |y| \leq |r_1 - r_2| \quad \dots \text{ since } r_1 - r_2 \neq 0. \\
&\Rightarrow y \leq |r_1 - r_2|
\end{aligned}$$

However, $y \leq |r_1 - r_2|$ contradicts our earlier result $|r_1 - r_2| < y$. $\nexists$ Thus, $r_1 = r_2$. Knowing this, we can return to our earlier equation and prove $q_1 = q_2$ as follows.

$$\begin{aligned}
0 &= (q_1 - q_2) \cdot y + (r_1 - r_2) \Rightarrow 0 = (q_1 - q_2) \cdot y + 0 \\
&\Rightarrow 0 = (q_1 - q_2) \cdot y \\
&\Rightarrow q_1 - q_2 \mid 0 \\
&\Rightarrow q_1 - q_2 = 0
\end{aligned}$$

Therefore, $q_1 = q_2$ and $r_1 = r_2$, so the claimed integers are unique.

Case 2:

Suppose $y < 0$. This case is left as an exercise for the reader.

QED

Definition 9.3: Greatest Common Divisor.

Given $x, y \in \mathbb{Z}$, we say that $d \in \mathbb{N}$ is the *greatest common divisor* of x and y iff the following three conditions hold.

1. $d \mid x$.
2. $d \mid y$.
3. $(\forall z \in \mathbb{Z})(z \mid x \wedge z \mid y \Rightarrow z \mid d)$.

It is a theorem that such a number always exists and is unique for any given $x, y \in \mathbb{Z}$.

$\gcd(\square, \square)$ We denote this number—the greatest common divisor of x and y —by $\gcd(x, y)$.

Definition 9.4: Least Common Multiple.

Given $x, y \in \mathbb{Z}$, we say that $m \in \mathbb{N}$ is the *least common multiple* of x and y iff the following three conditions hold.

1. $x \mid m$.
2. $y \mid m$.
3. $(\forall z \in \mathbb{Z})(x \mid z \wedge y \mid z \Rightarrow m \mid z)$.

It is a theorem that such a number always exists and is unique for any given $x, y \in \mathbb{Z}$.

$\text{lcm}(\square, \square)$ We denote this number—the least common multiple of x and y —by $\text{lcm}(x, y)$.

Exercise 9.1. For any $x \in \mathbb{Z}$, we have $\gcd(x, 0) = |x|$ and $\gcd(x, 1) = 1$.

Exercise 9.2. $(\forall x, y \in \mathbb{Z})(x = 0 \wedge y = 0 \Leftrightarrow \gcd(x, y) = 0)$.

Exercise 9.3. $(\forall x, y \in \mathbb{Z})(x \neq 0 \vee y \neq 0 \Leftrightarrow \gcd(x, y) \geq 1)$

Definition 9.5: Coprimality.

We say two integers $x, y \in \mathbb{Z}$ are *coprime* iff $\gcd(x, y) = 1$.

Theorem 9.6.

$(\forall x, y \in \mathbb{Z})(\gcd(x, y) = 1 \Leftrightarrow (\forall p \in \mathbb{N})(p \text{ is prime} \Rightarrow (p \nmid x \vee p \nmid y)))$.

Exercise 9.4. $(\forall a, b, c \in \mathbb{Z})(a = b + c \Rightarrow \gcd(a, b) = \gcd(b, c) = \gcd(a, c))$.

Algorithm 9.1: Euclid's Division Algorithm.

$$\gcd(x, y) = \begin{cases} x & \text{if } y = 0 \\ \gcd(y, r) & \text{if } y \neq 0, \text{ where } r \in \mathbb{Z} \text{ such that} \\ & 0 \leq r < |y| \text{ and } (\exists q \in \mathbb{Z})(x = qy + r) \end{cases}$$

Theorem 9.7.

For any $x, y \in \mathbb{Z}$, we have $|x \cdot y| = \gcd(x, y) \cdot \text{lcm}(x, y)$.

Theorem 9.8: Bezout's Identity.

$(\forall x, y \in \mathbb{Z})(\exists a, b \in \mathbb{Z})(\gcd(x, y) = ax + by)$.

Theorem 9.9: Euclid's Lemma.

$(\forall p \in \mathbb{N})(\forall x, y \in \mathbb{N})(p \text{ is prime} \wedge p \mid a \cdot b \Rightarrow (p \mid a \vee p \mid b))$.

Corollary 9.1.

$(\forall x, y, z \in \mathbb{Z})(\gcd(x, y) = 1 \wedge x \mid y \cdot z \Rightarrow x \mid z)$.

For any integers x and y , we can clearly see that $\gcd(x, y) = \gcd(y, x)$ and $\text{lcm}(x, y) = \text{lcm}(y, x)$.

coprime