1. The Natural Numbers

Definition 1.1. Given sets a and b, the *order pair* of a and b is defined as the set

$$(a, b) = \{\{a\}, \{a, b\}\}.$$

For two sets A and B we define the *Cartesian product* of A and B as

$$A \times B = \{(a, b) : a \in A, b \in B\}.$$

We often write A^2 instead of $A \times A$.

Definition 1.2. Suppose A is a set. A *binary relation* on A is a subset of $A \times A$. Let R be a relation on A. We say that R is

- *reflexive* if for all $a \in A$, $(a, a) \in R$,
- *symmetric* if for all $a, b \in A$, $[(a, b) \in R \to (b, a) \in R]$,
- *antisymmetric* if for all $a, b \in A$, $[\ [(a, b) \in R \text{ and } (b, a) \in R] \to a = b]$,
- *transitive* if for all $a, b, c \in A$, $[\ [(a, b) \in R \text{ and } (b, c) \in R] \to (a, c) \in R]$.

A relation which is reflexive, symmetric, and transitive is called an *equivalence relation*. On the other hand if a relation is reflexive, antisymmetric, and transitive, then the relation is called a *partial order*. We shall often denote a partial order by the symbol $\leq$ and say that $(A, \leq)$ is a partially ordered set. A partial order which satisfies the following property is called a *linear order*:

- for all $a, b \in A$, $(a, b) \in R$ or $(b, a) \in R$.

We shall often say that $(A, \leq)$ is linearly ordered to mean that A is a set equipped with a partial order $\leq$ which is also a linear order.

Definition 1.3. Recall that for a set x we define its *successor* as $x^+ = x \cup \{x\}$. A set I is called *inductive* if it satisfies the following two properties: (1) $\emptyset \in I$ and (2) whenever $x \in I$, then so is x^+. We leave it as an exercise to show that assuming there is an inductive set then the intersection of all inductive sets is again inductive. Thus, there is a smallest inductive set. We denote the smallest inductive set by $\mathbb{N}$ and call this set the *set of natural numbers*.

Theorem 1.4 (The Principle of Mathematical Induction)**.** *Suppose S is a set of natural numbers satisfying the following two properties:*

(1) $0 \in S$,
(2) *if* $n \in S$, *then so is* $n + 1 \in S$.

Then $S = \mathbb{N}$.

Corollary 1.5. *Let $P(x)$ be a property of natural numbers. If*

$$S = \{n \in \mathbb{N} : P(n) \text{ is true } \},$$

and S satisfies the following properties:

(1) $0 \in S$,
(2) *if* $n \in S$, *then so is* $n + 1 \in S$,

then $S = \mathbb{N}$.

Definition 1.6. On the set of natural numbers define the relation $\leq$ as follows

$$n \leq m \text{ iff either } n \in m \text{ or } n = m.$$

We will show that this is a partial order on $\mathbb{N}$.

Theorem 1.7. *The set $(\mathbb{N}, \leq)$ is a linearly ordered set.*

Proof. (Reflexive) Since in the definition of the order we have the possibility that $n = m$, we get that for all $n \in N$, $n \leq n$.

(Transitive) Suppose $n \leq m$ and $m \leq k$. This means that ($n \in m$ or $n = m$) or ($m \in k$ or $m = k$). This yields four cases: 1) $n \in m$ and $m \in k$, 2) $n \in m$ and $m = k$, 3) $n = m$ and $m \in k$, 4) $n = m$ and $m = k$. For case 2) use substitution to get that $n \in k$ and so $n \leq k$. For case 3) use substitution to get that $n \in k$ and so $n \leq k$. For case 4) $n = k$ by the fact that we assume $=$ is transitive. Thus, $n \leq k$. This just leaves us with the first case.

Suppose that $n \in m$ and $m \in k$. We proceed by induction on the property $P(x) := \forall y, z \in N\ [(y \in z \text{ and } z \in x) \rightarrow y \in x]$.

(1) $P(0)$: Let $y, z \in \mathbb{N}$ and consider the implication: If $y \in Z$ and $z \in 0$, then $y \in 0$. Since the hypothesis of the conditional is always false (there is no $z \in 0$) it follows that the conditional is true. Since y, z are arbitrary it follows that $P(0)$ is true.

(2) Suppose $P(k)$. We want to show that $P(k+1)$ is true. $P(k)$ true means that for $\forall y, z \in N\ [(y \in z \text{ and } z \in k) \rightarrow y \in k]$. To show that $P(k+1)$ is true let $y, z \in \mathbb{N}$ and suppose that $y \in z$ and $z \in k+1$. We need to argue that $y \in k+1$. Now, $z \in k+1$ means that $z \in k$ or $z = k$; so we consider the two cases. Suppose $z \in k$. Then by $P(k)$ we have that $y \in z$ and $z \in k$, therefore $y \in k$. In the second case $z = k$, by substitution, $y \in k$. In either case $y \in k$.

By the Principle of Mathematical Induction, $P(k)$ is true for all natural numbers k. Therefore, $n \in m$ and $m \in k$ implies that $n \in k$ and so $\leq$ is transitive.

(Anti-symmetric) Suppose that $n, m \in \mathbb{N}$ and that both $n \leq m$ and $m \leq n$. We have a total of four choices given by ($n \in m$ or $n = m$) and ($m \in n$ or $m = n$). The cases are 1) $n \in m$ and $m \in n$, 2) $n \in m$ and $m = n$, 3) $n = m$ and $m \in n$, 4) $n = m$ and $m = n$. By Well-Foundedness the cases 2) and 3) lead to $n \in n$ or $m \in m$ which is a contradiction. Case 4) is what we would like to conclude. So this just leaves the first case. Suppose $n \in m$ and $m \in n$. By the proof of case 1) in (Transitive) it follows that $n \in n$, a contradiction.

Before we proceed in showing that $\leq$ is a linear order our next lemma will be very useful.

Lemma 1.8. *a) For all $n \in \mathbb{N}$, either $0 = n$ or $0 \in n$.*
b) For all $n \in \mathbb{N}$, the statement: $\forall y \in M[n \in y \rightarrow [n+1 \in y \text{ or } n+1 = y]]$.

Proof. a) Let $Q(x)$ be the property that either $0 = x$ or $0 \in x$. We proceed by induction. $Q(0)$ is true since $0 = 0$. Suppose $Q(n)$ is true. This means that either $0 = n$ or $0 \in n$. If $0 = n$, then since $n \in n+1$ it follows that $0 \in n+1$. In the other case, $0 \in n$. Since $n+1 = n \cup \{n\}$ it follows that $0 \in n+1$. Therefore, by induction $0 \in n$ for all $n \in \mathbb{N}$.

b) Let $Q(x)$ be the property that $\forall y \in M[y \in x \rightarrow [y+1 \in x \text{ or } y+1 = x]]$ and proceed by induction. $Q(0)$ is trivially true (since the hypothesis of the conditional is false). So assume that $Q(n)$ is true. Also suppose that $y \in \mathbb{N}$ and that $y \in n+1$. Then by definition of $n+1$ it follows that either $y \in n$ or $y = n$. In the first case we have that $y \in n$. But we are assuming that $Q(n)$ is true and so either $y+1 \in n$ or $y+1 = n$. In the first case $y+1 \in n$ and so by the definition of $n+1$ we gather that $y+1 \in n+1$. In the other csae $y+1 = n$ which also is a member of $n+1$.

Thus, $y+1 \in n+1$ or $y+1 = n+1$. By the Principle of Mathematical Induction, $Q(n)$ holds for all $n \in \mathbb{N}$. □

(Linear order). Let $n, m \in \mathbb{N}$. We want to show that either $n \leq m$ or $m \leq n$. Consider the property $P(x) := \forall y \in \mathbb{N}$, [$y \in x$ or $x \in y$ or $x = y$; we proceed by induction. First a useful lemma.

(1) $P(0)$: Let $y \in \mathbb{N}$. By a) of the lemma $0 = y$ or $0 \in y$ and so $P(0)$ is true.

(2) Suppose $P(n)$ is true. Let $y \in \mathbb{N}$ and we would like to show that either $y \in n+1$ or $n+1 \in y$ or $y = n$. Since $P(n)$ is true it follows that either $y \in n$ or $n \in y$ or $y = n$. In the first case, $y \in n$ and since $n \in n+1$ we have that, by transitivity, $y \in n+1$. In the third case, $y = n$ and so $y \in n+1$. Thus, for the last case assume that $n \in y$. Then $n+1 \in y$ or $n+1 = y$ by 2) of the lemma. Thus, $P(n+1)$ is true. By the Principle of Mathematical Induction, $P(n)$ holds for all $n \in \mathbb{N}$. Consequently, $\leq$ is a linear order on $\mathbb{N}$. □

Theorem 1.9 (The Second Principle of Mathematical Induction)**.** *Let $P(x)$ be a property of natural numbers and let $k \in \mathbb{N}$ be a fixed natural number. Suppose that $P(k)$ is true and that whenever $k \leq n$, if $P(n)$ is true, then so is $P(n+1)$. Then $P(n)$ is true for all $k \leq n$.*

Definition 1.10. Suppose $(A, \leq)$ is a linearly-ordered set and let S be a nonempty subset of A. We say that S has a *minimum element* if there is an element $s \in S$ such that for every $t \in S$, $s \leq t$. Whenever a linearly-ordered set has the property that every nonempty subset of it has a minimum element then A is said to be a *well-ordered* set.

Theorem 1.11. *The set $(\mathbb{N}, \leq)$ is a well-ordered set.*

2. Divisibility Properties of the Naturals

In this section we look at some nice divisibility properties of the natural numbers. Our first result is the most useful Division Algorithm.

Theorem 2.1 (The Division Algorithm)**.** *Given integers a, b with $b > 0$, there exist unique integers q, r such that*

$$a = bq + r, \text{ with } 0 \leq r < b.$$

q is called the quotient *and r is called the* remainder.

Proof. Let S be the set of natural numbers given by

$$S = \{y \in \mathbb{Z}^+ : y = a - bx, \text{ where } x \in \mathbb{Z}\}$$

This is a nonempty set of natural numbers. To see this observe that if $a \geq 0$, then $a \in S$. Otherwise, we may choose an integer x such that $a \geq bx$, from which it follows that $a - bx \geq 0$ and hence lies in S. By the Well-Ordering Principle of the naturals S contains a least element $r = a - bq$. So $a = bq + r$ where $r \geq 0$.

If $b \leq r$, then $0 \leq r - b < r$, where $r - b = a - bq - b = a - b(q+1)$. But then $r - b \in S$ contradicting our choice of least element r. Thus, $0 \leq r < b$.

As for uniqueness, suppose $a = bq + r = bq' + r'$, where both $0 \leq r, r' < b$. Then $b(q - q') = r - r'$. If $q' \neq q$, then $b \leq |r' - r|$ since $b \geq 1$. But this is not possible since $|r' - r| < b$. Hence, we obtain that $q' = q$ and $r' = r$. □

Example 2.2. By the Division Algorithm, for each natural number n there are $r, q \in \mathbb{N}$ such that $n = 2q + r$ where $r < 2$. it follows that every natural number has an expression as either $2q$ or $2q+1$ for some q. Similarly, every natural number may be written as either $3q, 3q + 1$, or $3q + 2$.

Definition 2.3. Let $n, m \in \mathbb{N}$. We say that n *divides* m if there exists a natural number k such that $nk = m$. We also say that n is a *factor* of m, or that m is a *multiple* of n. We write

$$n \mid m$$

to mean that n divides m.

Proposition 2.4. *Divisibility has the following properties. The proofs are left for the reader.*

(i)	$n\|n$	(reflexive property)
(ii)	If $d\|n$ and $n\|m$, then $d\|m$.	(transitive property)
(iii)	If $d\|m$, then $ad\|am$ for all $a \in \mathbb{N}$.	(multiplication property)
(iv)	If $ad\|am$ and $a \neq 0$, then $d\|m$.	(cancellation)
(v)	$d\|m$ implies $d \leq m.\|$	(comparison property)
(vi)	If $d\|a$ and $d\|b$, then $d\|na + mb$ for any integers n, m.	(linear combination)

Definition 2.5. Because of the comparison property in the previous proposition it follows that given two integers a, b there exists a greatest common divisor. In other words, each nonzero natural number has only a finite number of divisors. If we define D_a to be the set of divisors of an arbitrary nonzero integer a, then the gcd of a and b is precisely the largest element in $D_a \cap D_b$.

Alternatively, the element d is called *the greatest common divisor of a and b (or simply the gcd)* if d divides both a and b and it is the largest such natural number with this property. The gcd of a and b is often written as $gcd(a, b)$.

Remark 2.6. Everything above can be translated into an appropriate statement involving integers. We let $\mathbb{Z}$ denote the set of integers.

Proposition 2.7. *Let $a, b \in \mathbb{N}$ and set $d = (a, b)$, Then*

(a) $d \geq 1$
(b) $d|a$ *and* $d|b$
(c) *If* $e|a$ *and* $e|b$, *then* $e|d$.

Conversely, any natural number satisfying the above three conditions is necessarily equal to $gcd(a, b)$.

Theorem 2.8. *Let a and b be integers. Then the gcd of a and b is the least positive linear combination of a and b, i.e., it is the least natural number (greater than 0) having the form $ax + by$.*

Proof. Let $S = \{x \in \mathbb{N} : x = na + mb \text{ for some } n, m \in \mathbb{Z}\}$. Since $a^2 + b^2 \in S$ it follows that S is nonempty and hence by the Well Ordering principle has a least element. Call this element $d = na + mb$.

We would like to show that $d = (a, b)$. By the division algorithm, we have

$$a = dq + r, \qquad 0 \leq r < d.$$

By substitution we obtain

$$r = a - dq = a - q(na + mb) = (1 - qn)a - qmb$$

Since r is non-negative, a linear combination of both a and b, and $r < d$ it follows that $r = 0$, whence $d|a$. Similarly, $d|b$.

Now, if $e|a$ and $e|b$, then $e|d$ by (vi) of Proposition 2.4. □

Theorem 2.9. *If $a|(bc)$ and $gcd(a, b) = 1$, then $a|c$.*