## Section 1.1: Basic notation, axioms, definitions, propositions and an important theorem

**Set notation** The following notation will be used to denote sets of numbers that feature in the course

**N** = { 1, 2, 3, ... } is the set of natural numbers (or the set of positive integers)

**N***  = { 0, 1, 2, 3, ... } is the set of non-negative integers

**Z** = { ... , -3, -2, -1, 0, 1, 2, 3, ... } is the set of integers

Note, in particular, that 0 is not a natural number, nor is it considered either positive or negative as an integer.

**Basic axioms** The following are the basic axioms and properties of integer arithmetic. In the following statements, $a$, $b$, $c$, and $d$ represent arbitrary integers.

<u>Axioms of Equality</u>

Reflexive: $a = a$.

Symmetric: If $a = b$, then $b = a$.

Transitive: If $a = b$ and $b = c$, then $a = c$.

<u>Axioms of Addition and Multiplication</u>

Well-defined operations: If $a = b$ and $c = d$, then $a + c = b + d$ and $ac = bd$.

Closure: $a + b$ and $ab$ are integers.

Commutative: $a + b = b + a$ and $ab = ba$.

Associative: $(a + b) + c = a + (b + c)$ and $(ab)c = a(bc)$.

Identities: $a + 0 = a$ and $a(1) = a$.

Additive inverse: There is an integer $-a$ such that $a + (-a) = 0$.

Cancellation: If $ac = bc$ and $c \neq 0$, then $a = b$.

Distributive: $a(b + c) = ab + ac$.

<u>Axioms of Inequality</u> [NB $a < b$ is equivalent to $b > a$]

Tricohotomy: For any pair of integers, exactly one of the following is true:

$$a < b, \quad a = b, \quad \text{or} \quad b < a.$$

Addition: If $a < b$, then $a + c < b + c$.

Multiplication: If $a < b$ and $c > 0$, then $ac < bc$.

Transitive: If $a < b$ and $b < c$, then $a < c$.

<u>Axiom of Well-Ordering</u> [also known as the <u>Principle of Well-Ordering</u>]

If S is a non-empty collection of non-negative integers, then S has a smallest element.

**Proposition 1.1** The following are basic properties of integral arithmetic.

(1) Zero property of multiplication: For any $a$, $a(0) = 0$.

(2) Inequality property of inverses: If $0 < a$, then $-a < 0$.

(3) Multiplication property of inverses: For any $a$, $a(-1) = -a$.

(4) Zero-product: If $ab = 0$, then $a = 0$ or $b = 0$.

(5) Cancellation property of addition for order: If $a + c < b + c$, then $a < b$.

(6) Cancellation property of multiplication for order: If $ac < bc$ and $c > 0$, then $a < b$.

**Definition 1.2** Let $a$ and $b$ be integers. To say that $b$ <u>divides</u> $a$ means that $a = bc$ for some choice of integer, $c$.

NB. Although tempting, we <u>do not</u> define $b$ divides $a$ to mean that the fraction represented by $a/b$ is a whole number. As you'll see when you begin to construct proofs, it is easier to think of "divides" as a statement about multiplication, an operation that you have axioms to work with. A natural extension of this idea is the very important theorem [which we will prove later] known as the Division Algorithm.

**Theorem 1.3 [The Division Algorithm]** Let $a$ and $b$ be integers with $b > 0$. Then there are unique integers $q$ and $r$ satisfying the conditions $a = qb + r$ and $0 \leq r < b$.