Theorems about the integers.

For these theorems you must use only the Axioms of the integers and the rules of logic; these are stated in the file AxiomsOfTheIntegers.

Definition: If $a \in \mathbb{R}$ then: $a^0 = 1$; $a^1 = a$; $a^{n+1} = a^n \cdot a$.

Definition: $2 = 1 + 1$. [Note that this is the definition of the symbol "2"; the symbols $3, 4, ...$ are defined inductively similarly.]

Theorem 2.1. Suppose that each of a, b and c is an integer.

a. $(a + b) \cdot c = a \cdot c + b \cdot c$.

b. $a + (b + c) = (c + a) + b$.

c. $a \cdot (b \cdot c) = (c \cdot a) \cdot b$.

Notational convention: By theorems similar to the above and the associativity and commutivity axioms, $a+b+c$ can now be defined as any of the following: $(a + b) + c$, $a + (b + c)$, $(a + c) + b$, $\ldots$. The quantity $a \cdot b \cdot c$ can be similarly defined.

Notational convention: ab means $a \cdot b$.

d. The additive and multiplicative identities are both unique. (i.e. no number other than 0 is the additive identity and similarly for the multiplicative identity.)

e. $(a + b)^2 = a^2 + 2ab + b^2$.

f. $0 \cdot a = 0$.

g. If $a + b = 0$ and $a + c = 0$ then $b = c$.

h. $(-1) \cdot a = -a$. [Hint: use f and g.]

i. $-(-a) = a$.

j. $(-a) \cdot b = -(ab) = a \cdot (-b)$.

k. $(-a) \cdot (-b) = a \cdot b$.

l. $-0 = 0$.

Theorem 2.2. Suppose that each of a, b and c is an integer.

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

b. If $a \neq 0$, then $a^2 > 0$.

c. If $ab = 0$ then either $a = 0$ or $b = 0$.

d. If $a > 0$ then $-a < 0$.

Theorem 2.3. There is no integer between 0 and 1.

Definition. If S is a subset of $\mathbb{Z}$ then ℓ is the least element of S means $\ell \in S$ and if $x \in S$ then $\ell \leq x$.

Theorem 2.4. If $S \subset \mathbb{N}$ and S is non-empty then S has a least element.

Note: From this point on you may assume all the algebraic facts about the integers that you have learned in your previous mathematics classes.

Divisibility.

Note: In this section you may not use fractions since they (and for that matter real numbers) have not yet been defined.

Definition. If a and b are integers then a is said to divide b if and only if there is an integer q so that b=aq. The standard notation is: $a|b$.

Theorem 2.5. If each of a, b, and c is an integer so that $a|b$ and $b|c$, then $a|c$.

Theorem 2.6. If each of a, b and c is an integer so that $a|b$ and $a|c$ then for arbitrary integers x and y, $a|(xb + yc)$.

Theorem 2.7. [The division algorithm.] If each of a and b is an integer with $0 < b$ then there exist unique integers q and r with $0 \leq r < b$ so that:

$$a = bq + r.$$

In the following exercises and theorems assume, as usual, that the quantities are appropriately defined.

Exercise 2.1. Find integers a, b, and c so that $a|bc$ but $a \nmid b$ and $a \nmid c$.

Theorem 2.8. If $c \neq 0$ then $a|b$ iff $ac|bc$.

Theorem 2.9. If $a > 0$, $b > 0$ and $a|b$ then $a \leq b$.