Section 1.2: The Division Algorithm and consequences

Theorem 1.3 The Division Algorithm [DA] Let a and b be integers with $b > 0$. Then there are unique integers q and r which satisfy

$$a = bq + r \quad \text{and} \quad 0 \leq r < b.$$

Definition 1.4 Let a and b be integers that are not both zero and let d be in $\mathbf{N}$. We say d is the <u>greatest common divisor</u> of a and b if

(i) $d|a$ and $d|b$ and,
(ii) given any c in $\mathbf{N}$ for which $c|a$ and $c|b$, $c \leq d$.

We write (a, b) for the greatest common divisor of a and b.

NB. The concept of greatest common divisor can be extended to any [finite] collection of integers $a_1, a_2, \ldots, a_n$ that are not all zero. The precise definition of $(a_1, a_2, \ldots, a_n)$ is left as an exercise.

Definition 1.5 We say that integers a and b are <u>relatively prime</u> if $(a, b) = 1$.

Theorem 1.6 Let a and b be integers that are not both zero. Then there are integers x and y for which $(a, b) = ax + by$.

NB. Theorem 1.6 guarantees that (a, b) can always be expressed as an integral linear combination of a and b. This is a very useful idea when proving statements that involve gcd's.

Theorem 1.7 For a and b integers, not both zero, $(a, b) = 1$ if and only if $ax + by = 1$ for some choice of integers x and y.

NB. The statement of this theorem is based on a bi-conditional form. Establishing the statement is true involves proving two separate conditional statements [using whatever methodology you choose].

Proposition 1.8 Let $d = (a, b)$ and write $a = dm$ and $b = dn$. Then $(m, n) = 1$.

Proposition 1.9 Let a and b be integers with $b > 0$. Using the Division Algorithm, fix q and r in $\mathbf{Z}$ with $a = bq + r$ and $0 \leq r < b$. Then $(a, b) = (b, r)$.

Result 1.10 The Euclidean Algorithm

Definition 1.11 Let a and b be non-zero integers and m a natural number. We say that m is the <u>least common multiple</u> of a and b if

(i) $a|m$ and $b|m$ and,
(ii) given any n in $\mathbf{N}$ for which $a|n$ and $b|n$, $n \geq m$.

We write $\mathrm{lcm}(a, b)$ or $[a, b]$ for the least common multiple.