Basic Number Theory

Let a and b be nonzero integers. Then there exist unique inetegrs q and r, $0 \leq r < |b|$, where $q = \text{floor}(ab)$ if $b > 0$ and $q = \text{ceil}(ab)$ if $b < 0$. q is called the *quotient* and r is called the *remainder*.

EXAMPLE 1. If $a = 102$ and $b = -25$, then $q = -4$ and $r = 2$.

If $a = -102$ and $b = 25$, then $q = -5$ and $r = 23$.

Note: The following are equivalent:

(1) $m|n$ (read as m divides n).
(2) n is divisible by m.
(3) n is a multiple of m.

Facts:

(1) Let a, b, and c be nonzero integers. If c divides both a and b, then c divides $ma + nb$, for any integers m and n.
(2) Let p be prime and a and b be integers. If p divides $a \cdot b$, then either p divides a or p divides b.

Notation: Let a and b be nonzero integers. Then the greatest common divisor of a and b is denoted $\gcd(a, b)$ and the least common multiple of a and b is denoted $\text{lcm}(a, b)$.

Note: If $g = gcd(a, b)$, then g can be written as a linear combination of a and b using the Eucildean algorithm.

Note: If $gcd(a, b) = 1$, then a and b are said to be *relatively prime*.

Fact: Let a, b, and x be integers. If x divides $a \cdot b$ and a and x are relatively prime, then x divides b.

Note: If $a = qb + r$, where q is the quotient when a is divided by b and r is the remainder, then $gcd(a, b) = gcd(b, r)$.

Note: If a and b are nonzero integers, then

$$gcd(a, b) = gcd(a, -b) = gcd(-a, b) = gcd(-a, -b).$$

Note: Let a and b be nonzero integers. Then

$$gcd(a, b) \cdot lcm(a, b) = |a \cdot b|.$$