Divisibility of integers.

If m, n are integers then we say that m *divides* n if $n = km$ for some integer k. We write: $m|n$.

Some properties of divisibility:

- For every n we have $1|n$.
- For every $m \neq 0$ we have $m|0$
- If $k|m$ and $m|n$ then $k|n$
- If $m|n$ and $n|m$ then either $m = n$ or $m = -n$

The Greatest Common Divisor

The *greatest common divisor* of integers $n_1, \ldots, n_k$ is the greatest integer m such that $m|n_i$ for $i = 1, \ldots, k$. We denote this integer by $\gcd(n_1, \ldots, n_k)$.

Some properties of gcd:

- If $m|n_i$ for $i = 1, \ldots, k$ then $m|gcd(n_1, \ldots, n_k)$.
- If $n > 0$ then $\gcd(0, n) = n$
- $\gcd(m, n) = \gcd(m, n - m)$
- If m, n are non-zero integers that there exists integers a, b such that

$$\gcd(m, n) = am + bn$$

  Moreover, $\gcd(m, n)$ is the smallest positive integer of such form.

If $\gcd(m, n) = 1$ then we say that m and n are *relatively prime*.

The Least Common Multiple

The *least common multiple* of integers $n_1, \ldots, n_k$ is the smallest positive integer m such that $n_i | m$ for $i = 1, \ldots, k$. We denote this integer by $\mathrm{lcm}(n_1, \ldots, n_k)$.

Some properties of lcm:

- If m is an integer such that $n_i | m$ for $i = 1, \ldots, k$ then $\mathrm{lcm}(n_1, \ldots, n_k) | m$.
- $\mathrm{lcm}(n_1, \ldots, n_k) = \dfrac{n_1 \cdot \ldots \cdot n_k}{\gcd(n_1, \ldots, n_k)}$

Prime numbers.

An integer $p > 1$ is prime if the only positive integers dividing p are p and 1.

Some properties of primes:

- If p is a prime and $p | mn$ then either $p | m$ or $p | n$.
- If $n > 1$ is any integer then there is a unique way of writing n as a product of primes:
$$n = p_1 p_2 \cdot \ldots \cdot p_k$$
such that $p_1 \geq p_2 \geq \ldots \geq p_k$.