Math 406 Section 1.5: Divisibility

---

1. **Introduction:** One of the primary starting points in number theory is the concept of divisibility and what stems from it.

2. **Definition:** If $a, b \in \mathbb{Z}$ with $a \neq 0$ we say that a *divides* b, written $a \mid b$, if there is some $c \in \mathbb{Z}$ such that $ac = b$. If not, then $a \nmid b$.

3. **Properties and Warnings:**

   (a) **Note:** Note that all nonzero numbers divide 0, so $10 \mid 0$ and $3498238402 \mid 0$. However we can't even talk about 0 dividing or not dividing things, so both $0 \mid 3$ and $0 \nmid 3$ are nonsensical.

   (b) **Theorem:** If $a \mid b$ and $b \mid c$ then $a \mid c$.
   Proof: $\mathcal{QED}$

   (c) **Useful Note:** Loosely speaking, ignoring negatives, a number can't divide a smaller number unless that smaller number is zero. For example if $5 \mid b$ and $b \geq 0$ then either $b \geq 5$ or $b = 0$. If we include negatives then we can say things like if $5 \mid b$ then either $b \geq 5$, $b \leq -5$ or $b = 0$. Paying attention to this can help clarify some proofs.

   (d) **Warning:** If $a \mid bc$ we cannot conclude that $a \mid b$ or $a \mid c$. For example $10 \mid (2)(5)$.

   (e) **Warning:** If $a \mid (b + c)$ we cannot conclude that $a \mid b$ or $a \mid c$. For example $10 \mid (3 + 7)$.

4. **Theorem (The Division Algorithm):** If $a, b \in \mathbb{Z}$ with $b > 0$ then there are unique $q, r \in \mathbb{Z}$ such that $a = bq + r$ with $0 \leq r < b$.
   Proof: Define the set:
   $$S = \{a - bk \mid k \in \mathbb{Z} \wedge a - bk \in \mathbb{Z} \wedge a - bk \geq 0\}$$
   Note that for any integer $k < a/b$ we have $a - bk > a - b(a/b) = 0$ so S is nonempty and therefore by well-ordering has a least element. Call this element r, so that $r \geq 0$ and $r = a - bq$ for some $q \in \mathbb{Z}$.
   To ascertain that $r < b$ observe that if $r \geq b$ then consider $r - b$:

   - We have $r - b \geq 0$.
   - We have $r - b < r$.
   - We have $0 \leq r - b = (a - bq) - b = a - b(q + 1)$.

   But then $r - b \in S$, a contradiction.
   To verify that these q and r are unique assume we have two such pairs q_1, r_1 and q_2, r_2. Then we have $a = bq_1 + r_1$ and $a = bq_2 + r_2$ and subtracting yields:
   $$0 = b(q_1 - q_2) + (r_1 - r_2)$$
   Equivalently:
   $$b(q_1 - q_2) = -(r_1 - r_2)$$
   But then this tells us that $b \mid (r_1 - r_2)$. However $0 \leq r_1 < b$ and $0 \leq r_2 < b$ so that $-b < r_1 - r_2 < b$. In order to have $b \mid (r_1 - r_2)$ we then must have $r_1 - r_2 = 0$. and then $0 = b(q_1 - q_2)$ and $b \neq 0$ yields $q_1 - q_2 = 0$. $\mathcal{QED}$

5. **Greatest Common Divisors and Relative Primality**

   (a) **Definition:** Suppose $a, b \in \mathbb{Z}$ such that at least one of them is nonzero. Then we define the *greatest common divisor* $\gcd(a, b)$ to be the largest integer that divides both.

   (b) **Definition:** We say that $a, b \in \mathbb{Z}$ are *relatively prime* or *coprime* if $\gcd(a, b) = 1$.