CMSC 27100 Practice Problems
Week #3

Division Theorem

Theorem 1 (Division Algorithm)**.** *For every integer n and every integer $d > 0$, there exist unique integers q and r such that*

$$n = dq + r \quad \text{and} \quad 0 \leq r < d.$$

Proof. **Existance**
Consider the set $A = \{n - dq | q \in \mathbf{Z}\}$. Since $d \neq 0$, A must have a non-negative number. By ordering, we know there must exist a smallest non-negative number, We call this r. $r < d$ becuase otherwise, $r = n - dq = d + m$ and so $m = n - d(q+1)$ so $m \in A,\ m < r$, a contradiction.

Uniqueness

$$\begin{aligned} n &= dq_1 + r_1 = dq_2 + r_2 \\ 0 &= d(q_1 - q_2) + (r_1 - r_2) \\ r_2 - r_1 &= d(q_1 - q_2) \end{aligned}$$

$$d | r_2 - r_1,\ 0 \leq r_2 < d \ \Rightarrow\ r_2 - r_1 = 0 \ \Rightarrow\ r_2 = r_1 \ \Rightarrow\ q_2 = q_1$$ □

1. Prove $\forall n \in \mathbf{Z}$, let r be the remainder of n divided by d, prove that $n = r \pmod d$
2. Let $d > 0$, prove $d|(n - m) \iff n$ and m have the same remainder divided by d

Euclid's Algorithm

If $d = gcd(a, b), b \neq 0$ and $r = a \mod b,$ then $d = gcd(b, r)$

1. Compute $gcd(105, 252)$
2. Prove $gcd(a, b) = gcd(a, b - ka)$ for any integer k. Use this fact to compute $gcd(98765, 43210)$

Modular Arthemtic

1. Find x s.t $35x = 10 \pmod{50}$