Math 465 - Spring 2021
Group Discussion 1
January 28th, 2021
That's all well and good in practice, but how does it work in theory?
— Shmuel Weinberger

---

(1) In your group, remind each other about tests for divisibility by 2, 4, and 5. Prove that these tests work.
(2) Let $a, b, c \in \mathbb{Z}$ with $c \neq 0$. Use the definition of divides to prove that if $c \mid a$ and $c \mid b$ then $c \mid (ax + by)$ for any $x, y \in \mathbb{Z}$.
(3) Prove that if $d = \gcd(a, b)$ and f is a common divisor of a and b, then $d \geq f$.

For the following problem we assume the following proposition:

> **Proposition:** (Least Integer Principle) *Every nonempty set of positive integers has a least element.*

This proposition may seem obvious, but would still need to be proved. (We could prove it using induction.) We will use it to prove the following.

> **Euclid's division lemma:** For any $a, b \in \mathbb{Z}$, with $b > 0$, there exists $q, r \in \mathbb{Z}$ with $a - bq = r$ and $0 \leq r < b$.

(4) Let $a, b \in \mathbb{Z}$ with $b > 0$.
  (a) Show that there exists some integer k such that $a - bk > 0$. (Hint: Try using two cases, one when $a > 0$ and one when $a \leq 0$.)
  (b) Set $S = \{k \in \mathbb{Z} \mid a - bk > 0\}$. Use the Least Integer Priciple and the previous problem to prove the existence of $q, r \in \mathbb{Z}$ satisfying the requirements of Euclids Lemma. (Namely, that $a - bq = r$ and $0 \leq r < b$.
  (c) Finally, give a proof by contradiction that q and r are the unique integers satisfying these two requirements. Suppose that q' and r' are another pair of integers with $a - bq' = r'$ and $0 \leq r' < b$.
    (i) Prove that $|r - r'| < b$.
    (ii) By subtracting the equation $a - bq = r$ from $a - bq' = r'$ use this to show that $|b(q - q')| < b$.
    (iii) Explain why this proves that $q = q'$ and then that $r = r'$.