Math 309 **Summer B 2018**
Homework 4 **Drew Armstrong**

---

1. Squares Mod 4. Every integer $n \in \mathbb{Z}$ has a unique "remainder mod 4." Let us use the notation $(n \bmod 4) \in \{0,1,2,3\}$ to denote this remainder.

(a) For all $x \in \mathbb{Z}$, show that $(x^2 \bmod 4) \in \{0,1\}$. [Hint: There are four kinds of integers. Square them all and see what you get.]

(b) Let $x, y, z \in \mathbb{Z}$ be integers satisfying the equation

$$x^2 + y^2 = z^2.$$

Prove that at least one of x, y must be even. [Hint: Assume for contradiction that x and y are both odd, which implies that x^2 and y^2 are both odd. Now use part (a) to get a contradiction.]

2. Euclidean Algorithm.

(a) Apply the Euclidean Algorithm to compute the greatest common divisor of 62 and 24.

(b) Apply the Extended Euclidean Algorithm to find all **integer** solutions $x, y \in \mathbb{Z}$ to the linear equation

$$62x + 24y = 4.$$

Hint: You need to find the complete solution of the "homogeneous" equation

$$62x_0 + 24y_0 = 0,$$

and one particular solution of the "non-homogeneous" equation

$$62x' + 24y' = 4.$$

Then the complete solution is $x = x_0 + x'$ and $y = y_0 + y'$.

3. Divisibility. For all integers $a, b \in \mathbb{Z}$ we define the divisibility relation as follows:

$$\text{"}a \text{ divides } b\text{"} = \text{"}a|b\text{"} = \text{"}\exists k \in \mathbb{Z}, ak = b.\text{"}$$

Let $a, b, c \in \mathbb{Z}$ and prove the following properties of divisibility.

(a) If $a|b$ and $b|c$ then $a|c$.

(b) If $a|b$ and $a|c$ then $a|(bx + cy)$ for all $x, y \in \mathbb{Z}$.

(c) If $a|b$ and $b|a$ then $a = \pm b$.

4. Euclid's Lemma. Let $a, b, c \in \mathbb{Z}$ and prove the following:

$$\text{if } a|bc \text{ and } \gcd(a,b) = 1 \text{ then } a|c.$$

Hint: If $\gcd(a,b) = 1$ then one may use the Extended Euclidean Algorithm to find some integers $x, y \in \mathbb{Z}$ satisfying

$$ax + by = 1.$$

Multiply both sides of this equation by c and see what happens.