Math 109 – Homework Assignment 9
Due Friday, June 8

1. Exercise 18.1. Solve the Diophantine equation

$$7684m + 4148n = 272.$$

2. Exercise 18.3. Solve the Diophantine equation

$$516m + 564n = 6432$$

   Prove that there are unique positive integers satisfying this equation and find these integers.

3. Solve the Diophantine equation

$$38x + 57y = 133.$$

4. Let p be a prime number. Prove that if $a \in \{1, \ldots, p-1\}$ then there is a unique $x \in \{1, \ldots, p-1\}$ such that

$$ax \equiv 1 \bmod p.$$

   Hint: Note that by definition $ax \equiv 1 \bmod p$ just means that there exists $y \in \mathbb{Z}$ such that $ax + py = 1$. Find all solutions $(x, y) \in \mathbb{Z}^2$ to $ax + py = 1$ and prove that there is only one such solution where $x \in \{0, 1, \ldots, p-1\}$. Then prove that for any solution $(x, y) \in \mathbb{Z}^2$ to $ax + py = 1$, $x \neq 0$.

Definition: Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{N}$. We say that *a is congruent to b modulo m*, written $a \equiv b \bmod m$, if a and b have the same remainder when divided by m. (That is, if $a = qm + r$ and $b = q'm + r'$ with $q, q' \in \mathbb{Z}$ and $r, r' \in \{0, 1, \ldots, m-1\}$, then $a \equiv b \bmod m$ just means $r = r'$.) Equivalently, $a \equiv b \bmod m$ means that $a - b$ is an integer multiple of m, i.e. m divides $a - b$.