NAME AND UCLA ID:

Task 1: Read Sections 7, 8, and 9.

Exercise 1: Let $a, b \in \mathbb{Z}^+$. Repeated use of the Division Algorithm gives the Euclidean Algorithm, that is, a system of equations

$$\begin{aligned}
a &= bq_1 + r_1, \quad 0 < r_1 < b \\
b &= r_1 q_2 + r_2, \quad 0 < r_2 < r_1 \\
r_1 &= r_2 q_3 + r_3, \quad 0 < r_3 < r_2 \\
&\vdots \\
r_{k-3} &= r_{k-2} q_{k-1} + r_{k-1}, \quad 0 < r_{k-1} < r_{k-2} \\
r_{k-2} &= r_{k-1} q_k + r_k, \quad 0 < r_k < r_{k-1} \\
r_{k-1} &= r_k q_{k+1} + 0.
\end{aligned}$$

Show this ends. Show that $r_k = \gcd(a, b)$. Plugging in backwards gives $r_k = ax + by$ for some $x, y \in \mathbb{Z}$. Do all of this for $a = 39493$ and $b = 19853$ (including finding an appropriate x and y).

Exercise 2: Let a, b, c be non-zero integers. Let $d = \gcd(a, b)$. Show that the equation $ax + by = c$ has a solution $x, y \in \mathbb{Z}$ if and only if d divides c. Moreover, show that if d divides c and $x_0, y_0 \in \mathbb{Z}$ is a solution, then the general integer solution is $x = x_0 + k(b/d)$ and $y = y_0 - k(a/d)$ for all $k \in \mathbb{Z}$.

Exercise 3: In the proof of the uniqueness of the Fundamental Theorem of Arithmetic, give two proofs to finish the argument after showing $p_1 = q_1$.

Exercise 4: Show the following.

1. Let R be an equivalence relation on A. Show that the equivalence classes $\overline{A}$ of this equivalence relation partitions A. Conversely, let $\mathcal{C}$ be a partition of A and define $\sim$ on $A \times A$ saying that $a \sim b$ whenever a and b belong to the same set in $\mathcal{C}$. Show that $\sim$ is an equivalence relation on A.

2. Through each integer point on the x-axis in the plane $\mathbb{R}^2$ draw a line perpendicular to the x-axis. Repeat this process with the y-axis. Define a (systematic) partition of the plane using this construction (being careful with points on various lines).

Exercise 5: Let $m \in \mathbb{Z}^+$, $m > 1$. Prove the following.

1. Congruence modulo m is an equivalence relation. In particular $\mathbb{Z} = \overline{0} \sqcup \overline{1} \sqcup \cdots \sqcup \overline{m-1}$, namely there are m equivalence classes. Let $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/\equiv = \{0, \ldots, m-1\}$.

2. Let $a, b, c, d \in \mathbb{Z}$ satisfy $a \equiv c \mod m$ and $b \equiv d \mod m$, then $a + b \equiv c + d \mod m$ and $ab \equiv cd \mod m$, namely $\overline{a+b} = \overline{c+d}$ and $\overline{ab} = \overline{cd}$.

3. Define $+$ and $\cdot$ on $\mathbb{Z}/m\mathbb{Z}$ by $\overline{a} + \overline{b} = \overline{a+b}$ and $\overline{a} \cdot \overline{b} = \overline{ab}$. Show that this is well-defined, namely if $\overline{a} = \overline{a'}$ and $\overline{b} = \overline{b'}$ then $\overline{a} + \overline{b} = \overline{a'} + \overline{b'}$ and $\overline{a} \cdot \overline{b} = \overline{a'} \cdot \overline{b'}$.

4. This $+$ and $\cdot$ make $\mathbb{Z}/m\mathbb{Z}$ into a commutative ring, namely they satisfy:
   (a) Associativity of the sum.
   (b) Commutativity of the sum.
   (c) Existence of zero.
   (d) Existence of additive inverses.
   (e) Associativity of the multiplication.
   (f) Commutativity of the multiplication.
   (g) Existence of one.
   (h) Right distributive law.
   (i) Left distributive law.

Exercise 6: Let $c_1, c_2, c_3 \in \mathbb{Z}$. Find $x \in \mathbb{Z}$ such that $x \equiv c_1 \mod 11$, $x \equiv c_2 \mod 12$, and $x \equiv c_3 \mod 13$. Find the smallest positive $x \in \mathbb{Z}$ satisfying these equations if $c_1 = 3$, $c_2 = 2$, and $c_3 = 1$.

Exercise 7: Prove that there exist infinitely many primes congruent to 3 modulo 4.

Exercise 8: Let p be a prime number. Show that $a^p \equiv a \mod p$ for all $a \in \mathbb{Z}$.