Practice questions:

1. Draw out the multiplication table for integers mod 6.

2. Let p be a prime number and assume $a, b \in \mathbb{Z}$. Prove that if $p \mid ab$, then $p \mid a$ or $p \mid b$.

3. Prove that for all $n \in \mathbb{Z}$, n and $n+1$ are coprime.

4. Let $m, n \in \mathbb{Z}$, and let r be the remainder of m under division by n. Prove that $\gcd(m, n) = \gcd(n, r)$.

5. Prove that for all odd $a, b, c \in \mathbb{Z}$, there exists no rational solutions to $ax^2 + bx + c = 0$. (Hint: Proof by contradiction under mod 2)

6. Let $\mathbb{Z}_p$ be the set $\{[0], [1], [2], [3], \ldots, [p-1]\}$ with the usual modular arithmetic. Prove that if p is prime, then for all $[a] \neq [0] \in \mathbb{Z}_p$, there exists $[a]^{-1}$ such that $[a] \cdot [a]^{-1} = [1]$ (Note that $\cdot$ is multiplication in modular arithmetic; Hint: Bézout's identity)

7. Let $\mathbb{Z}_n$ be the set $\{[0], [1], [2], [3], \ldots, [n-1]\}$ under addition mod n and suppose $M \subseteq \mathbb{Z}_n$ is a non-empty subset such that for all $[a], [b] \in M$, $[a] + [n-b] \in M$ (Note that $+$ denotes addition mod n).

   (a) Prove that $[0] \in M$.

   (b) Prove that for all $[a] \in M$, $[n-a] \in M$.

   (c) Prove that $|M|$ divides n. (Hint: consider equivalence classes under the relation where for all $[a], [b] \in \mathbb{Z}_n$, $[a] \sim [b]$ if and only if $[a] + [n-b] \in M$)

8. We will prove Fermat's little theorem, i.e. for all $a, p \in \mathbb{Z}$ such that p is prime, $a^{p-1} \equiv 1 \mod p$. Let $\mathbb{Z}_p$ be the set $\{[0], [1], [2], [3], \ldots, [p-1]\}$ with the usual modular arithmetic. By Q6, we know every element in the set $\mathbb{Z}_p \setminus \{[0]\}$ is invertible under multiplication.

   (a) Assume k is the smallest natural number such that $a^k \equiv 1 \mod p$ for some $a \in \mathbb{Z}$ such that $1 \leq a \leq p-1$. Let $S \subseteq \mathbb{Z}_p \setminus \{[0]\}$ be a non-empty subset such that $S = \left\{[1], [a], [a]^2, \ldots, [a]^{k-1}\right\}$. Similarly to Q7c, prove that $|S| = k$ divides $|\mathbb{Z}_p \setminus \{[0]\}| = p-1$.

   (b) Hence, prove that $a^{p-1} \equiv 1 \mod p$.