Proposition HW10.1: Let A be a set, and let $\sim$ be an equivalence relation on A. Then the equivalence classes of $\sim$ form a partition of A.

Proof. We need to prove the following:

1. For all $a \in A$, there exists $x \in A$ such that $a \in [x]$
2. For all $a, b \in A$, if $[a] \neq [b]$, then $[a] \cap [b] = \emptyset$.

1) Let $a \in A$. Since $a \sim a$, $a \in [a]$.

2) Let $a, b \in A$, and suppose $[a] \cap [b] \neq \emptyset$. Then there exists $c \in [a] \cap [b]$. Since $c \in [a]$, $c \sim a$. Similarly, $c \sim b$. But then $a \sim b$ and $[a] = [b]$ by Proposition 6.4 (ii). □

Proposition HW10.2: Let A and B be sets. Then

$$(A \cup B) \setminus B \subseteq A.$$

Proof. Suppose $a \in (A \cup B) \setminus B$. The $a \in (A \cup B)$ and $a \notin B$. Since $a \in (A \cup B)$, either $a \in A$ or $a \in B$. Since $a \notin B$, we conclude $a \in A$. Hence $(A \cup B) \setminus B \subseteq A$. □

Lemma 6.13c: Let $n \in \mathbb{N}$. Suppose that q and r are integers such that $0 \leq r \leq n - 1$ and

$$qn + r = 0.$$

Then $q = 0$ and $r = 0$.

Proof. Let $n \in \mathbb{Z}$. Suppose $q, r \in \mathbb{Z}$, $0 \leq r \leq n - 1$, and $nq + r = 0$. Hence $r = -qn$ and in particular $n \mid r$. Suppose to produce a contradiction that $n \neq 0$. Then, since $0 \leq r$, we conclude that $r \in \mathbb{N}$. Since $n \in \mathbb{N}$ and $n \mid r$, Proposition 2.33 implies $n \leq r$. But $r \leq n - 1 < n$. This is a contradiction. Hence $r = 0$. But then

$$0 = qn + r = qn + 0 = qn.$$

Proposition 1.26 then implies either $q = 0$ or $n = 0$. Since $n \in \mathbb{N}$, we conclude that $q = 0$. □

Proposition 6.25: If $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$ then

$$a + b \equiv a' + b' \pmod{n}$$

and

$$ab \equiv a'b' \pmod{n}.$$

Proof. Suppose $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$. Then $n \mid (a - a')$ and $n \mid (b - b')$. So there exists integers j and k such that $a - a' = nj$ and $b - b' = nk$. Note that

$$(a + b) - (a' + b') = (a - a') + (b - b') = nj + nk = n(j + k).$$

Hence $n \mid (a + b) - (a' + b')$ and

$$a + b \equiv a' + b' \pmod{n}.$$

Moreover,

$$\begin{aligned} ab - a'b' &= ab - ab' + ab' - a'b' \\ &= a(b - b') + (a - a')b' \\ &= ank + njb' \\ &= (ak + jb')n. \end{aligned}$$

So $n \mid (ab - a'b')$ and $ab \equiv a'b' \pmod{n}$. □

Lemma HW10.3: Suppose $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$, $2 \leq a \leq n - 1$, and $ab = n$. Then

$$2 \leq b \leq n - 1.$$

Proof. Since $ab = n$ and since $a, n \in \mathbb{N}$, it follows that $b \in \mathbb{N}$. Since $b \in \mathbb{N}$ and $b \mid n$, $b \leq n$. So $1 \leq b \leq n$. We will show that $b \neq 1$ and $b \neq n$, from which it follows that $2 \leq b \leq n - 1$.

Suppose to the contrary that $b = 1$. Then

$$n = ab = a1 = a.$$

So $a = n$, which is a contradiction.

Suppose to the contrary that $b = n$. Then

$$1 \cdot n = n = ab = an.$$

Since $n \neq$, by multiplicative cancellation, $a = 1$. But $a \neq 1$, so this is also a contradiction. □

Proposition 6.28: Every integer greater than or equal to 2 can be factored in to primes.

Proof. We will prove by strong induction that every integer $n \geq 2$ admits a prime factorization. Suppose for some $n \geq 2$ that every integer k such that $2 \leq k < n - 1$ admits a prime factorization. We wish to show that n also admits a prime factorization. If n is prime then it admits a trivial factorization. Suppose n is composite. Then there exists $a \in \mathbb{Z}$ such that $2 \leq a \leq n - 1$ and $a \mid n$. Since $a \mid n$ there exists $b \in \mathbb{Z}$ such that $ab = n$. Lemma 6.A implies $2 \leq b \leq n - 1$. By the induction hypothesis, both a and b admit prime factorizations. But then so does n: it is the product of the prime factorizations of a and b. □