Project 6.27: Finish your work on this project. Specifically, state and prove a proposition that characterizes the set of $n \geq 2$ such that $\mathbb{Z}_n$ satisfies the cancellation property (Axiom 1.5). You can opt to prove either Axiom 1.5 or its equivalent version Proposition 1.26.

Proposition 6.27: Let $n \in \mathbb{Z}_{\geq 2}$. Then $\mathbb{Z}_n$ satisfies Proposition 1.26 if and only if n is prime.

Proof. Suppose n is prime. Suppose $a, b \in \mathbb{Z}$ and

$$[a][b] = [0].$$

Recall that $[a][b] = [ab]$. Hence $[ab] = [0]$ and $ab \equiv 0 \pmod{n}$. Hence $n \mid ab$. Since n is prime, by Euclid's Lemma, either $n \mid a$ or $n \mid b$. Hence either $a \equiv 0 \pmod{n}$ or $b \equiv 0 \pmod{n}$. So either $[a] = [0]$ or $[b] = [0]$.

We prove the converse using the contrapositive. Suppose n is not prime; we will show that there are nonzero equivalence classes that have a product that is $[0]$. Since $n \geq 2$ is not prime, there exists $a \in \mathbb{Z}$ such that $2 \leq a \leq n-1$ and $a \mid n$. So there exists $b \in \mathbb{Z}$ such that $n = ab$. By Lemma 6.A proved below, it follows that $2 \leq b \leq n-1$ as well. Since $0 \leq a \leq n-1$ and $a \neq 0$, Proposition 6.24(ii) implies that $[a] \neq [0]$. Similarly, $[b] \neq [0]$. Nevertheless,

$$[a][b] = [ab] = [n] = [0],$$

so Proposition 1.26 fails. □

Lemma 6.B: Suppose $a, b \in \mathbb{Z}$, $g \in \mathbb{Z}_{\geq 0}$, and

(1) $g \mid a$ and $g \mid b$

(2) For all $d \in \mathbb{Z}$ such that $d \mid a$ and $d \mid b$, $d \mid g$.

Then $g = \gcd(a, b)$.

Proof. Your proof goes here. □

Proof. Suppose $a, b \in \mathbb{Z}$, $g \geq 0$, and g satisfies items (1) and (2).

Let $G = \gcd(a, b)$, and recall from Proposition 6.26 that G also satisfies conditions (1) and (2). Since $G \mid a$ and $G \mid b$, it follows from condition (2) that $G \mid g$. Since $g \mid a$ and $g \mid b$, it follows from condition (2) that $g \mid G$.

Now either $g = 0$ or $g > 0$. If $g = 0$, since $g \mid G$, $G = 0$ as well and $g = G = \gcd(a, b)$. Suppose $g > 0$. Since $G \mid g$, $G \neq 0$ and hence $G > 0$. Since $g, G \in \mathbb{N}$ and $g \mid G$, $g \leq G$. Similarly, $G \leq g$. So $g = G = \gcd(a, b)$. □

Lemma 6.C: Suppose p is prime and $a \in \mathbb{Z}$. Then either $p \mid a$ or $\gcd(p, a) = 1$.

Proof. Suppose p is prime and $a \in \mathbb{Z}$. Let $g = \gcd(p, a)$. Then $g \mid p$ and $g \mid a$. Note that $g \geq 0$ by definition, and $g \neq 0$ since $p \neq 0$. So $g \in \mathbb{N}$. Since p is prime, either $g = 1$ or $g = p$. If $g = 1$, then $\gcd(p, a) = 1$. If $g = p$ then, since $g \mid a$, $p \mid a$.

□

Lemma 6.30a: For all $a, b \in \mathbb{Z}$,

$$\gcd(a, b) = \gcd(-a, b) = \gcd(a, -b) = \gcd(-a, -b). \quad (1)$$

Proof. We will first prove that for all $a, b \in \mathbb{Z}$ that $\gcd(a, b) = \gcd(-a, b)$.

Let $a, b \in \mathbb{Z}$. If $a = b = 0$, the result is trivial since all expressions in equation (**??**) are zero. So suppose $a \neq 0$ or $b \neq 0$ so that $\gcd(a, b)$ is the least element of $S_{a,b}$ and $\gcd(-a, b)$ is the least element of $S_{-a,b}$. We will show that $S_{a,b} = S_{-a,b}$ to conclude, from the uniqueness of least elements, that $\gcd(a, b) = \gcd(-a, b)$.

Suppose $x =\in S_{a,b}$. Then $x \in \mathbb{N}$ and there exist integers i and j such that $x = ai + bj$. Hence $x = (-a)(-i) + bj$. This shows that $x \in S_{-a,b}$ as well. Hence $S_{a,b} \subseteq S_{-a,b}$. The proof that $S_{-a,b} \subseteq S_{a,b}$ is completely similar. Hence $S_{a,b} = S_{-a,b}$ as claimed.

We now establish the remaining equalities in (**??**). Let $a, b \in \mathbb{Z}$. Observe from the symmetry of gcd and the result we just proved (applied twice!) that

$$\gcd(a, b) = \gcd(b, a) = \gcd(-b, a) = \gcd(a, -b) = \gcd(-a, -b).$$

□

Proposition 6.30: For all $k, m, n \in \mathbb{Z}$,

$$\gcd(km, kn) = |k| \gcd(m, n)$$

Proof. Let k, m, and $n \in \mathbb{Z}$. If $k = 0$ or both $m = n = 0$, then

$$\gcd(km, kn) = |k| \gcd(m, n)$$

since both sides of this equation are zero. Hence we may assume that $k \neq 0$ and at least one of m or n is nonzero.

We first assume that $k > 0$. Let $g = \gcd(m, n)$ and let $G = \gcd(km, kn)$. We wish to show that $G = kg$. Since $g = \gcd(m, n)$, there exist integers a and b such that $g = am + bn$. Hence $kg = a(km) + b(kn)$. Since $g \in \mathbb{N}$ and $k \in \mathbb{N}$, $kg \in \mathbb{N}$ as well. Thus $kg \in S_{km,kn}$. Since G is the least element of $S_{km,kn}$ we conclude that $G \leq kg$. On the other hand, since $g \mid m$ and $g \mid n$, it follows that $kg \mid km$ and $kg \mid kn$ as well. But then $kg \mid G$ by Proposition 6.29(iii). Since kg and G are both natural numbers, we conclude that $kg \leq G$. Since $kg \geq G$ as well, $kg = G$.

Now suppose $k < 0$. Then $-k > 0$ and hence from Lemma 6.30a and the result we just proved,

$$\gcd(km, kn) = \gcd(-km, -kn) = (-k) \gcd(m, n) = |k| \gcd(m, n).$$

□