Your Name: ______________ Group Members: ______________ ______________

Proposition (Proposition 5.4)**.** *Let $a, m \in \mathbb{Z}$ with $m > 0$ and $(a, m) = 1$. If i is a positive integer, then*

$$\operatorname{ord}_m(a^i) = \frac{\operatorname{ord}_m a}{\gcd(\operatorname{ord}_m a, i)}.$$

Problem 1 *Use only the results through Proposition 5.3/Reading Lemma 10.3.5 (ie, not Proposition 5.4) to prove the primitive root version:*

Proposition. *Let $r, m \in \mathbb{Z}$ with $m > 0$ and r a primitive root modulo m. If i is a positive integer, then*

$$\operatorname{ord}_m(r^i) = \frac{\phi(m)}{\gcd(\phi(m), i)}.$$

Problem 2 *Prove*

Proposition (Proposition 10.2.2)**.** *Let p be prime, and let m be a positive integer. Consider*

$$x^m \equiv 1 \pmod{p}.$$

(a) *If $m \mid p-1$, then there are exactly m incongruent solutions modulo p.*

(b) *For any positive integer m, there are $\gcd(m, p-1)$ incongruent solutions modulo p.*

Problem 3 *Prove the following statement, which is the converse of Reading Proposition 10.3.2:*

Let p be prime, and let $a \in \mathbb{Z}$. If every $b \in \mathbb{Z}$ such that $p \nmid b$ is congruent to a power of a modulo p, then a is a primitive root modulo p.

Problem 4 *Prove the following generalization of Reading Lemma 10.3.5*

Lemma. *Let $n \in \mathbb{Z}$ and let $x_1, x_2, \ldots, x_m$ be reduced residues modulo n. Suppose that for all $i \neq j$, $\operatorname{ord}_n(x_i)$ and $\operatorname{ord}_n(x_j)$ are relatively prime. Then*

$$\operatorname{ord}_n(x_1 x_2 \cdots x_m) = (\operatorname{ord}_n x_1)(\operatorname{ord}_n x_2) \cdots (\operatorname{ord}_n x_m).$$