Your Name: ____________ Group Members: ____________ ____________

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

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

In-class 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 2. Let $r, m \in \mathbb{Z}$ with $m > 0$ and r a primitive root modulo m. If i is a positive integer, then

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

Solution: Let r be a primitive root modulo m. Then by Proposition 5.3, $\{r, r^2, \ldots, r^{\phi(m)}\}$ is a complete residue system modulo m. By Proposition 5.1, $\operatorname{ord}_m(r^i) \mid \phi(m)$ and by Proposition 5.3, $r, r^2, \ldots, r^{\phi(m)}$ is a complete residue system modulo m

---

In-class Problem 2 Prove

Proposition 3 (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.

Solution: Let p be prime, and let m be a positive integer. By Fermat's Little Theorem, $a^{p-1} \equiv 1 \pmod{p}$.

(a) If $m \mid p-1$, then there exists $k \in \mathbb{Z}$ such that $mk = p-1$. If $a^m \equiv 1 \pmod{p}$

In-class 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.

Solution: Let p be prime, and let $a \in \mathbb{Z}$ such that every integer $b \in \mathbb{Z}$ where $p \nmid b$ is congruent to a^i modulo p for some positive integer i. Thus, $(a, p) = 1$, otherwise 1 would not be congruent to a power of a. ByProposition 5.2, $a^i \equiv a^j \pmod{p}$ if and only if $i \equiv j \pmod{p-1}$. Thus, $a^1, a^2, \ldots, a^{p-1}$ are distinct congruence classes and only one of $a^1, a^2, \ldots, a^{p-1}$ is congruent to 1 modulo p. By Fermat's Little Theorem, $a^{p-1} \equiv 1 \pmod{p}$, so $\operatorname{ord}_p a = p - 1$.

In-class Problem 4 Prove the following generalization of Reading Lemma 10.3.5

Lemma 1. 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

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

Learning outcomes:

Author(s): Claire Merriman