Your Name: ____________ Group Members: ____________ ____________

Previous Results

Lemma 1. *Let $a, b \in \mathbb{Z}$, not both zero. Then any common divisor of a and b divides the greatest common divisor.*

Lemma 2. *Let $a, b \in \mathbb{Z}$, not both zero. Then any divisor of (a, b) is a common divisor of a and b.*

Proposition (Proposition 5.1)**.** *Let $a, m \in \mathbb{Z}$ with $m > 0$ and $(a, m) = 1$. Then $a^n \equiv 1 \pmod{m}$ for some positive integer n if and only if $\operatorname{ord}_m a \mid n$. In particular, $\operatorname{ord}_m a \mid \phi(m)$.*

Problems

Problem 1 *Let p be prime, m a positive integer, and $d = (m, p-1)$. Prove that $a^m \equiv 1 \pmod{p}$ if and only if $a^d \equiv 1 \pmod{p}$.*

Proof *Let p be prime, m a positive integer, and $d = (m, p-1)$. Let $a \in \mathbb{Z}$. If $p \mid a$, then $a^i \equiv$ ____________ for all positive integers. Otherwise, $a^{p-1} \equiv 1 \pmod{p}$ by ____________.*

By Proposition 5.1, $a^m \equiv 1 \pmod{p}$ if and only if ____________. Similarly, ____________ if and only if ____________. Thus, ____________ is a common divisor of ____________ and ____________. Combining Lemmas 1 and 2 gives $\operatorname{ord}_p a$ is a common divisor of ____________ and ____________ if and only if $\operatorname{ord}_p a \mid d$. One final application of Proposition 5.1 gives ____________ if and only if ____________. ■

Problem 2 on back page

Problem 2 *Let p be prime and m a positive integer. Prove that*

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

has exactly $(m, p-1)$ incongruent solutions modulo p.

Proof *Let p be prime, m a positive integer, and $d = (m, p-1)$. From Problem 1,*

Now find a result that allows you to finish the proof in 1-2 sentences.

■

If you have time, start working on this problem from the homework.

Problem 3 *Prove the following statement, which is the converse of Proposition 5.4 (for a prime):*

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.
