Fall 2019 – Math 328K – Florian Stecker

Homework 11

due Thursday, November 21, 11:00

Problem 1. Let $m, k \in \mathbb{N}$ and $a \in \mathbb{Z}_m^\times$. Show that

$$\operatorname{ord}(a^k) = \frac{\operatorname{ord}(a)}{(\operatorname{ord}(a), k)}.$$

Problem 2. Let $m \in \mathbb{N}$ so that $\mathbb{Z}_m$ has a primitive root. Show that it has exactly $\phi(\phi(m))$ primitive roots.

Hint: Which powers of the primitive root are primitive roots?

Problem 3. Let $k \geq 3$ be an integer. Show by induction that $x^{2^{k-2}} = \overline{1}$ for every $x \in \mathbb{Z}_{2^k}^\times$. Conclude that $\mathbb{Z}_{2^k}$ has no primitive roots.

Problem 4. Let $m \in \mathbb{N}$ be a positive integer such that $\mathbb{Z}_m$ has a primitive root. Show the following generalization of Wilson's Theorem:

$$\prod_{x \in \mathbb{Z}_m^\times} x = -1.$$

Find a counterexample of this statement for some $\mathbb{Z}_m$ which does not have a primitive root.