M328K Homework 12

Joshua Dong

April 21, 2014

0.1   9.1.12

Show that if $n \in \mathbb{Z}^+$, $a, b \perp n$ such that $ord_n a \perp ord_n b$, then $ord_n(ab) = ord_n a \cdot ord_n b$.

0.2   9.1.16

Show that if $a, m \in \mathbb{Z}^+$, $a \perp m$ such that $ord_m a = m - 1$, then $m \in \mathbf{P}$.

0.3   9.2.8

Let r be a primitive root of the prime p with $p \equiv 1 \pmod 4$. Show that $-r$ is also a primitive root.

0.4   9.2.12

Find the least positive residue of the product of a set of $\varphi(p-1)$ incongruent primitive roots modulo some prime p.