M328K Homework 12

Joshua Dong

April 23, 2014

0.1 9.1.12

Show that if $n \in \mathbb{Z}^+$, for some $a, b \perp n$ 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 $m \in \mathbf{P}$.

In the previous problem, 9.1.12, we showed that the order function modulo some integer power is multiplicative across coprime factors.
Let $ord_m a = g(a)$ for convinience.
$g(a) = g(p_1^{a_1} p_2^{a_2} ... p_{\omega(n)}^{a_{\omega(n)}}) = g(p_1^{a_1}) g(p_2^{a_2}) ... g(p_{\omega(n)}^{a_{\omega(n)}})$ (by the fundamental theorem of arithmetic and the multiplicative property of the order function across coprime factors)
The order of prime powers is known. $g(p_i^{a_i}) = (a_i) g(p_i)$, if $\exists g(p_1)$.
If $a \notin \mathbf{P}$, then the product derived from the fundamental theorem of arithmetic is not equal to a-1.
Therefore, if $a, m \in \mathbb{Z}^+$, $a \perp m$ such that $ord_m a = m - 1$, then $m \in \mathbf{P}$.
We can also observe that if m is prime, then the product derived from the fundamental theorem of arithmetic is always equal to $g(p_i)$, which is always $\varphi(m) = m - 1$ when m is prime, by Fermat's little theorem.

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.

We observe that r must be odd, because if $2 \perp r$, then $r \not\perp 4$ and thus r cannot be a primitive root. Also, $p > 2$, so we do not have to worry about edge cases.
If we can prove that the order of $-r$ modulo p exists, then that is sufficent to prove that $-r$ is a primitive root.
By 9.1.12, we have that if $r \perp ord_n - 1$, then $ord_n(-r) = ord_n(r) \cdot ord_n(-1)$.

$ord_n(-1) = 2$, because $-1 \cdot -1 = 1$. We do not have to worry about moduli less than or equal to 2.
r is a primitive root, $\therefore \exists ord_n(r)$.
$\therefore \exists k \in \mathbb{Z}$ such that $k = ord_n(-r) = ord_n(r) \cdot ord_n(-1)$.
Therefore $-r$ is 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.