MATH 3070 – THEORY OF NUMBERS

Homework 3

Due: Thursday, Oct 13, 2022 (in class)

1.

(i). Prove that for $m \geq 3$ an integer, $\mathrm{ord}_m(m-1) = 2$.

(ii). Prove that for $p \geq 3$ a prime, there is only one integer among $\{1, 2, \ldots, p\}$ of order 2 modulo p, and this integer is $p - 1$.

2. Let $p \geq 5$ be a prime. Let g be a primitive root of p.

(i). If $g^{-1} \bmod p$ is the modular inverse of g, prove that g^{-1} is also a primitive root of p.

(ii). Prove that $g \not\equiv g^{-1} \pmod p$. (Hint: Prove first that $g \equiv g^{-1} \pmod p$ implies that $g^2 \equiv 1 \pmod p$.)

(iii). Recall that there are $\phi(\phi(p)) = \phi(p-1)$ primitive roots of p among $\{1, 2, \ldots, p\}$. We denote them by $g_1, g_2, \ldots, g_{\phi(p-1)}$. Prove that

$$\prod_{i=1}^{\phi(p-1)} g_i \equiv 1 \pmod p.$$

(Hint: Pair the primitive roots g and g^{-1}.)

3. Let m and n be positive integers with $m \mid n$.

(i). For a with $(a, m) = 1$, if a is not a primitive root of m, prove that there exists an integer b with $(b, m) = 1$ such that $b \not\equiv a^k \pmod m$ for any integer k.

(ii). Let x be such that $(x, m) = 1$. Prove that there exists an integer y such that $(y, n) = 1$ and $y \equiv x \pmod m$.

(This result, although looking trivial, is surprisingly *not* easy. So I give more clues. Write n in the canonical form $n = \prod_i p_i^{\alpha_i} \prod_j q_j^{\beta_j}$ with $p_i \mid m$ and $q_j \nmid m$. Consider the linear congruence system: $y \equiv x \pmod{p_i^{\alpha_i}}$ for each i, and $y \equiv 1 \pmod{q_j^{\beta_j}}$ for each j. Is this system solvable? By which theorem? Is it true that $(y, n) = 1$? Is it true that $y \equiv x \pmod m$?)

(iii). Prove through the previous two parts that if g is a primitive root of n, then g is also a primitive root of m.