

Homework 19 – More Orders and Primitive Roots

- a) Suppose p is an odd prime. Prove that for all $n \geq 2$,

$$(1 + p)^{p^{n-2}} \equiv 1 + p^{n-1} \pmod{p^n}.$$

(Hint: use induction. You may use the binomial formula: for $n \geq 0$

$$(x + y)^n = \sum_{k=0}^n \binom{n}{k} x^{n-k} y^k$$

where $\binom{n}{k} = \frac{n(n-1)(n-2)\cdots(n-k+1)}{1 \cdot 2 \cdot 3 \cdots k} \in \mathbf{Z}$, and show that when $n = p$ a prime and $0 < k < p$, $\binom{p}{k}$ is a multiple of p .)

- b) Still with p an odd prime and $n \in \mathbf{Z}^+$, prove

$$(1 + p)^{p^{n-2}} \not\equiv 1 \pmod{p^n},$$

$$(1 + p)^{p^{n-1}} \equiv 1 \pmod{p^n},$$

and that $\text{ord}_{p^n}(1 + p) = p^{n-1}$.

- c) Suppose $m \in \mathbf{Z}^+$, $a, b \in \mathbf{Z}_m^*$. Prove $\text{ord}_m(ab) \leq \text{ord}_m(a)\text{ord}_m(b)$. Then give an example where $\text{ord}_m(ab) \neq \text{ord}_m(a)\text{ord}_m(b)$.
- d) Suppose $m \in \mathbf{Z}^+$, $a, b \in \mathbf{Z}_m^*$ where $\text{ord}_m(a)$ and $\text{ord}_m(b)$ are relatively prime. Prove that if $i, j \in \mathbf{Z}$ with $a^i \equiv b^j \pmod{m}$, then $a^i \equiv 1 \pmod{m}$. (Hint: show a^i has order 1.)
- e) Suppose $m_1, m_2 \in \mathbf{Z}^+$ and $a \in \mathbf{Z}_{m_1 m_2}^*$. Prove $\text{ord}_{m_1}(a) \mid \text{ord}_{m_1 m_2}(a)$.
- f) Suppose $m \in \mathbf{Z}^+$, $a \in \mathbf{Z}_m^*$, and $\text{ord}_m(a) = rs$ for some $r, s \in \mathbf{Z}^+$. Prove that $\text{ord}_m(a^r) = s$.
- g) Suppose p is an odd prime and $n \in \mathbf{Z}^+$. Use the previous parts to prove that there exists a primitive root modulo p^n . You may assume the existence of a primitive root modulo p . (Hint: construct an integer of order $p - 1$ and one of order p^{n-1} .)