NUMBER THEORY: HOMEWORK 6

TO BE HANDED IN BY THURSDAY 27TH FEBRUARY 2025 BY 6PM

1. Let p be an odd prime number, suppose that $h \geqslant 2$, and denote by g a primitive root modulo p^h.
(a) How many solutions does the congruence $x^p \equiv 1 \pmod{p^h}$ possess? List them all using the primitive root g modulo p^h.
(b) How many solutions does the congruence $x^{2p} \equiv 1 \pmod{p^h}$ possess? List them all using the primitive root g modulo p^h.

2. Let a and n be integers with $1 \leqslant a \leqslant n$ and $(a, n) = 1$.
(a) Suppose that the usual base 10 digital representation of a/n is a recurring decimal in the form

$$\begin{aligned} \frac{a}{n} &= 0 \cdot b_1 b_2 \cdots b_m b_1 b_2 \cdots b_m \cdots \\ &= 0 \cdot \overline{b_1 b_2 \cdots b_m}, \end{aligned}$$

where $b_i \in \{0, 1, \ldots, 9\}$ $(1 \leqslant i \leqslant m)$. Prove that $10^m \equiv 1 \pmod{n}$.
(b) Suppose that $(10, n) = 1$ and that the order of 10 modulo n is d. Show that a/n has a recurring decimal expansion with least period d, and show further that $d | \varphi(n)$.
(c) Show that a/n has a recurring decimal expansion with least period $n - 1$ if and only if n is prime and 10 is a primitive root modulo n.

3. Let $p_1, p_2, \ldots, p_r$ be distinct prime numbers. Show that an integer g exists satisfying the property that g is a primitive root modulo p_i for all indices i with $1 \leqslant i \leqslant r$.

4. (a) Let a be an integer with $a \geqslant 2$, and suppose that $q \in \mathbb{N}$. What is the smallest positive integer d satisfying the property that $a^d \equiv 1 \pmod{a^q - 1}$? Deduce that $q | \varphi(a^q - 1)$.
(b) Let q be a prime number. By considering the prime factorisation of the integer $N = a^q - 1$, show that either N is divisible by q, or else N is divisible by a prime number p with $p \equiv 1 \pmod{q}$.

5. Let q be a prime number. Prove that there are infinitely many prime numbers p with $p \equiv 1 \pmod{q}$.