SOLUTIONS TO HOMEWORK 6

1. (a) Let g be a primitive root modulo p^h. Then every reduced residue x modulo p^h can be written uniquely in the form $x \equiv g^u \pmod{p^h}$ for some integer u with $0 \leqslant u \leqslant p^{h-1}(p-1)$. Consequently, one has $x^p \equiv 1 \pmod{p^h}$ if and only if $g^{up} \equiv 1 \pmod{p^h}$, and this is possible if and only if $p^{h-1}(p-1)|up$. Since the latter condition is equivalent to requiring $p^{h-2}(p-1)|u$, we see that the solutions of $x^p \equiv 1 \pmod{p^h}$ are given by $x \equiv g^{kp^{h-2}(p-1)} \pmod{p^h}$, with $0 \leqslant k < p$. Hence the congruence in question has precisely p solutions.
(b) Proceeding as in (a), we find that $x^{2p} \equiv 1 \pmod{p^h}$ if and only if one has $g^{2up} \equiv 1 \pmod{p^h}$, and this is possible if and only if $p^{h-1}(p-1)|2up$. Since the latter condition is equivalent to requiring $\frac{1}{2}p^{h-2}(p-1)|u$, we see that the solutions of $x^{2p} \equiv 1 \pmod{p^h}$ are given by $x \equiv g^{kp^{h-2}(p-1)/2} \pmod{p^h}$, with $0 \leqslant k < 2p$. Hence the congruence in question has precisely $2p$ solutions.

2. (a) Put $B = b_m + 10b_{m-1} + \ldots + 10^{m-1}b_1$. Then, if the usual base 10 digital representation of a/n is a recurring decimal in the specified form, one has

$$\frac{a}{n} = 10^{-m}B\sum_{h=0}^{\infty}(10^{-m})^h = \frac{B}{10^m - 1}.$$

Then $a(10^m - 1) = Bn$, whence $a(10^m - 1) \equiv 0 \pmod{n}$. But $(a, n) = 1$, and thus $10^m \equiv 1 \pmod{n}$.
(b) When $(10, n) = 1$ and the order of 10 modulo n is d, it follows at once that $d|\varphi(n)$ (as a consequence of Euler's theorem). Moreover, we have $10^d \equiv 1 \pmod{n}$, and thus $10^d - 1 = Cn$, for some positive integer C. Write $B = aC$ in the shape $b_1b_2\cdots b_d$ as a base 10 integer, where $b_i \in \{0, 1, 2, \ldots, 9\}$. Then we have

$$\frac{a}{n} = \frac{aC}{10^d - 1} = \frac{B}{10^d - 1} = 10^{-d}B\sum_{h=0}^{\infty}(10^{-d})^h,$$

whence $a/n = 0 \cdot \overline{b_1b_2\cdots b_d}$. So a/n has a recurring decimal expansion with period d. Moreover, since $10^k \not\equiv 1 \pmod{n}$ whenever $0 \leqslant k < d$, it follows from part (a) that d is the least period of this recurring decimal.
(c) The largest possible order of 10 modulo n is $\varphi(n)$, and this can occur only when 10 is a primitive root modulo n. Moreover, we have $\varphi(n) = n - 1$ if and only if n is prime. The desired conclusion follows.

3. For each prime p_i, there exists a primitive root g_i. Moreover, since $(p_i, p_j) = 1$ for $1 \leqslant i < j \leqslant r$, it follows from the Chinese Remainder Theorem that there exists an integer g with $g \equiv g_i \pmod{p_i}$ for $1 \leqslant i \leqslant r$. This integer g has the property that for each integer d and each index i, one has $g^d \equiv g_i^d \pmod{p_i}$, and thus g is primitive modulo p_i for $1 \leqslant i \leqslant r$.

4. (a) Since $0 < a^d - 1 < a^q - 1$ whenever $1 \leqslant d < q$, the smallest integer d with $a^d \equiv 1 \pmod{a^q - 1}$ is q. This integer $d = q$ is the order of a modulo $a^q - 1$, and consequently divides $\varphi(a^q - 1)$.
(b) Suppose that $N = a^q - 1 = \prod_{p^r \| N} p^r$, where the exponents r are positive integers and the primes p are distinct. Hence $\varphi(N) = \prod_{p^r \| N} p^{r-1}(p-1)$. From part (a) we have $q | \varphi(N)$, so for some prime p dividing N, we have $q | p^{r-1}(p-1)$. The latter implies that $q = p$ or $p \equiv 1 \pmod{q}$. Thus we conclude that either N is divisible by q, or else N is divisible by a prime number p with $p \equiv 1 \pmod{q}$.

5. Suppose that there are only finitely many prime numbers p with $p \equiv 1 \pmod{q}$, and let these primes be $p_1, p_2, \dots, p_n$. Put $a = qp_1 \cdots p_n$, and consider the integer $N = a^q - 1$. Since a is divisible by q, we find that $(N, q) = (a^q - 1, q) = 1$, so that $q \nmid N$. Then it follows from Q4(b) that N must be divisible by a prime number p with $p \equiv 1 \pmod{q}$. But for $1 \leqslant i \leqslant n$, we have $p_i | a$ and hence $(N, p_i) = (a^q - 1, p_i) = 1$, and thus $p_i \nmid N$. Then p is a prime congruent to 1 modulo q that is different from $p_1, \dots, p_n$, contradicting our initial hypothesis. Therefore, there are infinitely many primes p with $p \equiv 1 \pmod{q}$.