Math 567, Assignment #8: Solutions

1. (a) Assume that a has order hk modulo n, so that $a^{hk} \equiv 1 \pmod{n}$ and $a^m \not\equiv 1 \pmod{n}$ for $0 < m < hk$. Since $(a^h)^k \equiv 1 \pmod{n}$, the element a^h has order less than or equal to k. If the order of a^h is r, with $0 < r < k$, then $a^{hr} = (a^h)^r \equiv 1 \pmod{n}$; this is impossible, since $0 < hr < hk$. Thus, a^h has order k modulo n.

The converse is false. E.g., 2^3 has order 4 mod 5, but 2 does not have order $3 \times 4 = 12$ modulo 5.

(b) Let a have order $2k$ modulo p, where p is an odd prime. Then $a^{2k} \equiv 1 \pmod{p}$ and $a^m \not\equiv 1 \pmod{p}$ for $0 < m < 2k$. Since $p|(a^k - 1)(a^k + 1)$, either $p|a^k - 1$ or $p|a^k + 1$; that is, either $a^k \equiv 1 \pmod{p}$ or $a^k \equiv -1 \pmod{p}$. The first case is impossible, since the order of a exceeds k. Hence $a^k \equiv 1 \pmod{p}$.

The converse is false. E.g., $4^3 \equiv (-1)^3 \equiv -1 \pmod{5}$, but 4 does not have order $2 \times 3 = 6$ modulo 5.

(c) Suppose a has order $n - 1$ modulo n. According to Theorem 8.1, $(n-1)|\phi(n)$. On the other hand, if the prime factors of n are $p_1, p_2, ...$, we have $\phi(n)/n = (1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \ldots < 1$, so that $\phi(n) \leq n$ (or we can just remember what $\phi(n)$ counts!). Thus $\phi(n) = n - 1$, from which it follows that n is prime.

The converse is true. If n is composite, it has some prime factor $p \leq \sqrt{n}$, so that $\phi(n)/n \leq 1 - \frac{1}{p} \leq 1 - \frac{1}{\sqrt{n}}$ and $\phi(n) \leq n - \sqrt{n} < n - 1$. This contradicts the fact that $n - 1$ divides $\phi(n)$.

2. Assume that a and b have orders h and k modulo n, respectively, and that ab has order r. Then

$$(ab)^{hk} = (a^h)^k (b^k)^h \equiv 1^k \cdot 1^h \pmod{n},$$

whence $r|hk$. Let $\gcd(h, k) = 1$. To see that $r = hk$, it suffices to show that $hk|r$. Now

$$a^{rk} \equiv a^{rk}(b^k)^r \equiv (ab)^{rk} \equiv 1 \pmod{n},$$

which implies that $h|rk$. Since $\gcd(h, k) = 1$, we get $h|r$. A similar argument gives $k|r$. Using the hypothesis $\gcd(h, k) = 1$ again, it follows that $hk|r$.

3. First we solve problem 8(a). Let p and q be odd primes with $q|a^p - 1$. Then $a^p \equiv 1 \pmod{q}$, so that the order of a modulo q is either 1 or p. If the

order of a is 1, then $a \equiv 1 \pmod{q}$ or $q|a-1$. On the other hand, if the order of a is p, then since the order divides $\phi(q) = q-1$, it follows that $q-1 = jp$ for some j; but $q-1$ is even, hence j is even, say $j = 2k$. Thus $q = 2kp+1$.

Proceeding: Let p be an odd prime. Assume that there are only a finite number of primes of the form $2kp+1$, say $q_1, q_2, \ldots, q_r$. Put $a = 2q_1q_2...q_r$ and consider the odd integer $a^{p-1}+a^{p-2}+\cdots+a+1$. If q is an odd prime divisor of this integer, then $a^p \equiv 1 \pmod{q}$. By the result of the preceding paragraph, either $q|a-1$ or q is of the form $2kp+1$. In the first case, $a \equiv 1 \pmod{q}$, so that $a^i \equiv 1 \pmod{q}$ for $i = 0$ through $p-1$, and $a^{p-1}+a^{p-2}+\cdots+a+1 \equiv p \pmod{q}$; but we already had $a^{p-1}+a^{p-2}+\cdots+a+1 \equiv 0 \pmod{q}$, so $p \equiv 0 \pmod{q}$, i.e., $q|p$. Since p and q are primes, we must have $p = q$. But then $1 \equiv a = 2q_1q_2...q_r \equiv 2 \pmod{p}$, a contradiction. Thus q is of the type $2kp+1$ and hence q must be one of the q_i. This means that $q|a^j$ for $1 \leq j \leq p-1$, and therefore q divides 1, which is impossible.

4. The integer 2 is a primitive root of 11. By the corollary to Theorem 8.4, the $\phi(10) = 4$ primitive roots of 11 are, modulo 11,

$$2^1 \equiv 2,\ 2^3 \equiv 8,\ 2^7 \equiv 7,\ 2^9 \equiv 6.$$

(If we'd used a different primitive root $r \neq 2$, then the primitive roots mod 11 would still be $r^1,\ r^3,\ r^7,\ r^9$.) The integer 2 is a primitive root of 19, so the $\phi(18) = 6$ primitive roots of 19 are, modulo 19,

$$2^1 \equiv 2,\ 2^5 \equiv 13,\ 2^7 \equiv 14,\ 2^{11} \equiv 15,\ 2^{13} \equiv 3,\ 2^{17} \equiv 10.$$

The integer 5 is a primitive root of 23, and the $\phi(22) = 10$ primitive roots of 23, are, modulo 23,

$$5^1 \equiv 5,\ 5^3 \equiv 10,\ 5^5 \equiv 20,\ 5^7 \equiv 17,\ 5^9 \equiv 11,$$

$$5^{13} \equiv 21,\ 5^{15} \equiv 19,\ 5^{17} \equiv 15,\ 5^{19} \equiv 7,\ 5^{21} \equiv 14.$$

5. Let r be a primitive root of the odd prime p. According to Theorem 8.4, the integers $1, 2, ..., p-1$ are congruent modulo p to $r, r^2, ..., r^{p-1}$ in some order. Thus,

$$\begin{aligned}(p-1)! &\equiv r \cdot r^2 \cdots r^{p-1} \equiv r^{1+2+\cdots+(p-1)} \\ &\equiv r^{p(p-1)/2} \equiv (-1)^p \equiv -1 \pmod{p},\end{aligned}$$

thereby proving Wilson's Theorem.