SOLUTIONS: PROBLEM SET 23 FROM SECTION 9.6

2.

- (a) Only $\lambda(2)$ takes the value 1.
- (b) If $p > 3$ is an odd prime, then $\phi(p)$ is divisible eitner by 4 or by an odd prime. Moreover $\phi(9)$ is divisible by 3, and $\phi(16)$ by 4. It follows that the only possibilities are 2^k for $k = 2, 3$ and $3 \cdot 2^k$ for $0 \leq k \leq 3$.
- (c),(e) $\phi(n)$ does not take any odd value except 1.
- (d) 5 is now a possible prime factor for n. The possibilities are now $5 \cdot 2^k$ and $15 \cdot 2^k$ for $0 \leq k \leq 4$ and also 16 and 48.
- (f) 5 is not possible as a factor since $\phi(5) = 4$. The possible odd factors are now 7,9,21 and 63. Each of these can be multiplied by 2^k for $k \leq 3$.

4.

- (a) $\lambda(12) = [\lambda(4), \phi] = [2, 2] = 2$. In this case, any residue relatively prime to 12 has order 2 except for 1. 5,7,and 11 are all acceptable.
- (b) $\lambda(15) = [\phi(3), \phi(5)] = [2, 4] = 4$ any primitive root $\pmod 5$ that is relatively prime to 15 will do. Acceptable answers are 2,7,8 and 13.
- (c) $\lambda(20) = [\lambda(4), \phi(5)] = [2, 4] = 4$. Any odd primitive root $\pmod 5$ will do. Acceptable answers are 3,13,7 and 17.
- (d) $\lambda(36) = [\lambda(4), \phi(9)] = [2, 6] = 6$. In this case, any odd primitive root $\pmod 9$ will do. Acceptable answers are 7,25,5 and 23.
- (e) $\lambda(40) = [\lambda(8), \phi(5)] = [2, 4] = 4$. Any odd primitive root $\pmod 5$ will do. Acceptable answers are 3,13,23,33,7,17,27 and 37.
- (f) $\lambda(63) = [\phi(7), \phi(9)] = [6, 6] = 6$. In this case, there are many correct answers, of which the smallest is 2. In fact $\mathrm{ord}_{63} a = 6$ provided $[\mathrm{ord}_9 a, \mathrm{ord}_7 a] = 6$. Assuming a is relatively prime to 63, a can be a primitive root either $\pmod 9$ or $\pmod 7$ (or both) but it need not be. An example is 44, for which $\mathrm{ord}_7 44 = 3$ and $\mathrm{ord}_9 44 = 2$.

6. This was essentially proved in class when we first discussed primitive roots.