Homework 7—Solutions

1. (a) $\mathbb{Z}_{24} = \{0, 1, 2, 3, \ldots, 23\}$.
   (b) Yes, it is cyclic; 1 is a generator.
   (c) $\langle 18 \rangle = \{0, 18, 12\}$, so 18 is not a generator.
   (d) $\langle 5 \rangle = \{0, 5, 10, 15, 20, 25, 6, 11, 16, 21, 2, 7, 12, 17, 22, 3, 8, 13, 18, 23, 4, 9, 14, 19\}$, so 5 is a generator.

2. (a) $\mathbb{Z}_{21}^* = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$.
   (b) There are 12 elements in the group.
   (c) Since $21 = 3 \cdot 7$, we have $\phi(21) = (3 - 1) \cdot (7 - 1) = 12 = |\mathbb{Z}_{21}^*|$.
   (d) This can be computed using the extended Euclidean algorithm, or by (guided) trial-and-error. One can verify that $2 = [11^{-1} \mod 21]$ since
   
   $$2 \cdot 11 = 22 = 1 \mod 21.$$

   (e) $[2^{2403} \mod 21] = [2^{[2^{2403} \mod \phi(21)} \mod 21}] = [2^3 \mod 21] = 8$.

3. (a) Since $55 = 5 \cdot 11$, we have $\phi(55) = 40$.
   (b) Since gcd($3, 40$) = 1, exponentiating to the 3rd power is a permutation.
   (c) Since $3 \cdot 27 = 1 \mod 40$, we can compute 3rd roots modulo 55 by raising to the 27th power. In particular, the 3rd root of 2 modulo 55 is 18 since

   $$2^{1/3} = 2^{27} = (2^6)^4 \cdot 2^3 = 9^4 \cdot 8 = 26^2 \cdot 8 = 13^2 \cdot 2^2 \cdot 8 = 4 \cdot 4 \cdot 8 = 1 \mod 55.$$

   (d) Since gcd($5, 40$) $\neq 1$, exponentiating to the 5th power is not a permutation.

4. $[1014.800,000,002 \mod 35] = (-4)^{[4.800,000,002 \mod \phi(35)]} \mod 35] = [(-4)^2 \mod 35] = 16$.

5. Since $p$ is prime, $\phi(p) = p - 1$ and so $\phi(p)$ is easily computed from $p$. Computing roots modulo $p$ is not hard when $\phi(p)$ is known. In particular, just compute $d = [x^{-1} \mod \phi(p)];$ then $g = y^d \mod p$. 
