Solutions for CS174 HW9

1. $\mathcal{Z}_N^*$ is a multiplicative group is cyclic iff n is either: $1, 2, 4, p^k$, or $2p^k$ where p is an odd prime. $\phi(2) = 1$. If $n = 4$, $\phi(n) = 2$. If $n = p^k$, $\phi(n) = p^{k-1}(p-1)$, so set $p^{k-1}(p-1) = 2^m$, we get p needs to have the form $2^m + 1$ and $k = 1$. If $n = 2p^k$, $\phi(n) = p^{k-1}(p-1)$ which is the same as for a prime power. So n needs to be either $1, 4$, or $2^m + 1$ or $2(2^m + 1)$ for some m where $2^m + 1$ is an odd prime.

2. $\phi(\phi(5^k)) = \phi(5^{k-1}2^2) = 2 \times 5^{k-2} \times 4 = 5^{k-2} \times 8$. So the fraction of generators is $8/25$.

3. Given $\gcd(e_1, e_2) = 1$, we can find x_1 and x_2 using Euclid's algorithm such that $e_1x_1 + e_2x_2 = 1$. So $C_1^{x_1}C_2^{x_2} = M(\mod n)$.

4. $\phi(\phi(p)) = q - 1$. So the fraction of generators is $(q-1)/(2q+1)$.