Solutions to the homework exercises

Homework 9

Question 4:

First we need to factorize $851 = 23 \cdot 37$. Using the fact that if $\gcd(a, b) = 1$, then $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$, we get $\phi(851) = \phi(23 \cdot 37) = \phi(23) \cdot \phi(37)$. As factors are prime numbers we can use the fact that for p-prime $\phi(p) = p - 1$. Finally $\phi(851) = (23 - 1) \cdot (37 - 1) = 792$.

Question 5:

A generator of a group $\mathbb{G}$ is a group element g for which $\langle g \rangle = \mathbb{G}$, where $\langle g \rangle := \{g^0, g^1, g^2, \ldots\}$. Note that for some power i: $g^i = 1 = g^0$, so $\langle g \rangle$ is of size at most $|\mathbb{G}|$. Exponentiation is just performing the group operation multiple times, in our case of $\mathbb{Z}_{11}^*$ the group operation is multiplication modulo 11. The subsets generated by elements of $\mathbb{Z}_{11}^*$ are

$$\begin{aligned}
\langle 1 \rangle &= \{1\} \\
\langle 2 \rangle &= \{1, 2, 4, 8, 5, 10, 9, 7, 3, 6\} \\
\langle 3 \rangle &= \{1, 3, 9, 5, 4\} \\
\langle 4 \rangle &= \{1, 4, 5, 9, 3\} \\
\langle 5 \rangle &= \{1, 5, 3, 4, 9\} \\
\langle 6 \rangle &= \{1, 6, 3, 7, 9, 10, 5, 8, 4, 2\} \\
\langle 7 \rangle &= \{1, 7, 5, 2, 3, 10, 4, 6, 9, 8\} \\
\langle 8 \rangle &= \{1, 8, 9, 6, 4, 10, 3, 2, 5, 7\} \\
\langle 9 \rangle &= \{1, 9, 4, 3, 5\} \\
\langle 10 \rangle &= \{1, 10\}.
\end{aligned}$$

The elements which generate the whole $\mathbb{Z}_{11}^*$ are then 2, 6, 7, and 8.