

Q4i: We claim that  $[1], [5], [7], [11]$  generate  $C_{12}$  and no other elements do. We can verify using the group operation that indeed

$$\begin{aligned}\langle 1 \rangle &= \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 0\} \\ \langle 5 \rangle &= \{5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7, 0\} \\ \langle 7 \rangle &= \{7, 2, 9, 4, 11, 6, 1, 8, 3, 10, 5, 0\} \\ \langle 11 \rangle &= \{11, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1, 0\}\end{aligned}$$

We claim that any other element of  $C_{12}$  will not generate  $C_{12}$ . Note that 1, 5, 7, 11 are the only integers less than 12 which are coprime to 12. Assume that  $n$  is not coprime to 12. We will show that  $|\langle n \rangle| < 12$ . Since  $n < 12$  and not coprime, for some integer  $k < 12$  we have that  $nk = 12$ . We see that

$$\langle n \rangle = \{n, 2n \dots kn\}$$

We see that  $|\langle n \rangle| = k$  which is strictly less than 12. Hence any element of  $C_{12}$  which is not coprime to 12 will not generate  $C_{12}$

Q4ii: We claim that every  $k < n$  that is coprime to  $n$  generates  $C_n$ . By bezouts identity we have that there exists integers  $a, b$  such that  $ak + nb = 1$ . If we had any  $c \in C_n$ , we can write  $c = (ac)k + n(bc)$ . Therefore we see that

$$[c]_n = [(ac)k + n(bc)]_n = [(ac)k]_n + [nbc]_n = [(ac)k]$$

Thus  $k$  generates  $C_n$