STEP 2010, Paper 3, Q3 – Solution (4 pages; 10/6/18)

The two primitive 4th roots of unity are i & $-i$

$C_4(x) = (x - i)(x + i) = x^2 - i^2 = x^2 + 1$

(i) $C_1(x) = x - 1$; $C_2(x) = x + 1$

$C_3(x) = \left(x - e^{\frac{2\pi i}{3}}\right)\left(x - e^{\frac{4\pi i}{3}}\right) = x^2 - \left(e^{\frac{2\pi i}{3}} + e^{\frac{4\pi i}{3}}\right)x + e^{\frac{6\pi i}{3}}$

$= x^2 - e^{\frac{3\pi i}{3}}\left(e^{\frac{-\pi i}{3}} + e^{\frac{\pi i}{3}}\right)x + 1 = x^2 - (-1)(2cos\left(\frac{\pi}{3}\right))x + 1$

$= x^2 + x + 1$

$C_5(x)$ & $C_6(x)$ can be obtained in a similar way (though this is quite time-consuming for $C_5(x)$)

However, as indicated in the official sol'ns, there is an alternative approach:

The roots of $x^n = 1$ are those of $x^n - 1 = 0$

Then $x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1)$

[Note that $x^4 + x^3 + x^2 + x + 1 = \frac{x^5-1}{x-1}$]

We need to exclude from the factorisation any linear factor (including those involving complex numbers) that appears within an earlier $C_n(x)$ - since any non-primitive root will be a root of $C_m(x) = 0$ for some $m < n$.

Thus, for $x^5 - 1$, $x - 1$ appears in $C_1(x)$. As far as

$x^4 + x^3 + x^2 + x + 1$ is concerned, we should in theory confirm that it contains none of the linear factors of $C_2(x), C_3(x)$ & $C_4(x)$.

This is straightforward for the factors $x+1, x-i$ & $x+i$, but not so clear for x^2+x+1 [This seems to be glossed over in the official sol'ns.]

However, on the assumption that $x^4+x^3+x^2+x+1$

and x^2+x+1 share no common linear factors (involving complex numbers), we conclude that

$C_5(x) = x^4+x^3+x^2+x+1$

For $C_6(x)$ we consider $x^6-1 = (x^3-1)(x^3+1)$

$= (x-1)(x^2+x+1)(x+1)(x^2-x+1)$,

and all but x^2-x+1 is rejected, as appearing in an earlier $C_n(x)$; ie $C_6(x) = x^2-x+1$

(ii) $x^4+1 = (x^2)^2 - i^2 = (x^2-i)(x^2+i)$

$= (x-\sqrt{i})(x+\sqrt{i})(x-\sqrt{-i})(x+\sqrt{-i})$

Now $\left(\pm\sqrt{i}\right)^8 = \left(\pm\sqrt{-i}\right)^8 = 1$, whilst $\left(\pm\sqrt{i}\right)^4 = \left(\pm\sqrt{-i}\right)^4 = -1$

and other powers less than 8 will not give 1

Also, the other 8th roots of unity are ± 1 and $\pm i$, and these are not primitive.

So $n = 8$

(iii) First of all, 1 isn't a primitive root of $x^p = 1$, as $1^1 = 1$ (ie $m = 1$).

And there are no other non-primitive roots y, as if $y^p = 1$ and $y^m = 1$, where $p = qm + r$ (the remainder r ($< m$) being non-zero, as p is prime) and assuming that $m \neq 1$ is the smallest such integer), then

$y^p = y^{qm+r} = (y^m)^q y^r = y^r \neq 1$ (as m is the smallest integer, other than 1, for which $y^m = 1$); ie contradicting the fact that $y^p = 1$

Thus, all the roots of $x^p = 1$ are primitive except 1.

and as $x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \cdots + x + 1)$,

it follows that $C_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$

(iv) First of all, $r = s$ is not possible, as otherwise $C_q(x) = 0$ would have repeated roots. Assume then, without loss of generality, that $r < s$.

Suppose that $q > s$. Then if x is a primitive qth root of unity, $C_q(x) = C_r(x)C_s(x) \Rightarrow x$ is either a primitive rth root or a primitive sth root. But each of these contradicts the fact that x is a primitive qth root.

Suppose instead that $q = s$. Then $C_r(x) \equiv 1$, which is not possible.

[The reason for this is skipped over in the official sol'ns:

Suppose that the prime factorisation of r is $p_1 p_2 \dots p_k$. Then

$x^r = (x^{p_1})^{p_2 \dots p_k}$, and we saw in (iii) that $x^{p_1} = 1$ has $p - 1$ (complex) roots. So $x^r = 1$ has at least one root, and hence $C_r(x) \not\equiv 1$]

Finally, suppose that $q < s$. Then if x is a primitive sth root of unity, $C_q(x) = C_r(x)C_s(x) \Rightarrow x$ is also a primitive qth root of unity, which is a contradiction, as $q < s$.

Thus there are no possibilities for which $C_q(x) = C_r(x)C_s(x)$.