STEP III, 2010 Q3 MS

3. The two primitive 4th roots of unity are $\pm i$ so $C_4(x) = (x-i)(x+i) = x^2+1$

$C_1(x) = x-1$, $x^2-1 = (x-1)(x+1)$ so $C_2(x) = x+1$,
$x^3-1 = (x-1)(x^2+x+1)$ so $C_3(x) = x^2+x+1$
$x^5-1 = (x-1)(x^4+x^3+x^2+x+1)$ so $C_5(x) = x^4+x^3+x^2+x+1$
$x^6-1 = (x^3-1)(x^3+1) = (x^3-1)(x+1)(x^2-x+1)$ so $C_6(x) = x^2-x+1$

In part (ii), $C_n(x) = 0 \Rightarrow x^4 = -1 \Rightarrow x^8 = 1$ so n is a multiple of 8, and as there are 4 primitive 8th roots of unity, n must be 8.

$x^p = 1 \Rightarrow x^p - 1 = 0 \Rightarrow (x-1)(x^{p-1}+x^{p-2}+x^{p-3}+\cdots+1)$
1 is the only non-primitive root as no power of any other root less than the pth equals unity, because p is prime, so $C_p(x) = x^{p-1}+x^{p-2}+x^{p-3}+\cdots+1$

No root of $C_n(x) = 0$ is a root of $C_t(x) = 0$ for any $t \neq n$. (For if $t < n$, by the definition of $C_n(x)$, there is no integer t such that $a^t = 1$ when $a^n = 1$. Similarly, if $t > n$.)
Thus if $C_q(x) \equiv C_r(x)C_s(x)$, and if $C_q(x) = 0$, then $C_r(x) = 0$ or $C_s(x) = 0$, so $q = r$ or $q = s$.

If $q = r$, then $C_q(x) \equiv C_r(x)$, and so $C_s(x) \equiv 1$ which is not possible for positive s, and likewise in the alternative case.