2010.3 Question 3

An n-th root of unity takes the form $\exp(\frac{k}{n} \cdot 2\pi I)$ for $k = 0, \ldots, n-1$, and specially, it is a primitive nth root of unity, if and only if the fraction $\frac{k}{n}$ is irreducible (being reducible is equivalent to it being another mth root of unity where $0 < m < n$), and this is equivalent to $\gcd(k, n) = 1$.

The two primitive 4th roots of unity are when $k = 1$ or 3, which gives i and $-i$ as the two primitive roots.

Hence,

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

1. For $n = 1$, $k = 0$, and $\gcd(0, 1) = 1$. So the only 1st root of unity is primitive, and hence

   $$C_1(x) = x - 1.$$

   For $n = 2$, $k = 0$ or 1, and only $\gcd(1, 2) = 1$. So the only primitive 2nd root of unity is $\exp\left(\frac{1}{2} \cdot 2\pi i\right) = -1$, and hence

   $$C_2(x) = x + 1.$$

   For $n = 3$, $k = 1$ or 2 gives $\gcd(k, n) = 1$. Hence, the primitive 3rd roots of unity are all 3rd roots of unity apart from $x = 1$. Hence,

   $$C_3(x) = \frac{x^3 - 1}{x - 1} = x^2 + x + 1.$$

   For $n = 5$, $k = 1, 2, 3, 4$ or 5 gives $\gcd(k, n) = 1$. Hence, the primitive 5th roots of unity are all 5th roots of unity apart from $x = 1$. Hence,

   $$C_5(x) = \frac{x^5 - 1}{x - 1} = x^4 + x^3 + x^2 + x + 1.$$

   For $n = 6$, $k = 1$ or 5 gives $\gcd(k, n) = 1$. Hence,

   $$\begin{aligned} C_6(x) &= \left(x - \exp\left(\frac{1}{6} \cdot 2\pi i\right)\right)\left(x - \exp\left(\frac{5}{6} \cdot 2\pi i\right)\right) \\ &= \left(x - \exp\left(\frac{1}{3} \cdot \pi i\right)\right)\left(x - \exp\left(-\frac{1}{3} \cdot \pi i\right)\right) \\ &= x^2 - 2 \cdot \cos\left(\frac{1}{3} \cdot \pi\right) x + 1 \\ &= x^2 - x + 1. \end{aligned}$$

2. Notice that

   $$\begin{aligned} x^4 + 1 &= (x^2 + i)(x^2 - i) \\ &= \left[x^2 - \exp\left(\frac{3}{4} \cdot 2\pi i\right)\right]\left[x^2 - \exp\left(\frac{1}{4} \cdot 2\pi i\right)\right] \\ &= \left[x - \exp\left(\frac{3}{8} \cdot 2\pi i\right)\right]\left[x - \exp\left(\frac{7}{8} \cdot 2\pi i\right)\right]\left[x - \exp\left(\frac{1}{8} \cdot 2\pi i\right)\right]\left[x - \exp\left(\frac{5}{8} \cdot 2\pi i\right)\right], \end{aligned}$$

   and the roots to $C_n(x)$ are

   $$\exp\left(\frac{1}{8} \cdot 2\pi i\right), \exp\left(\frac{3}{8} \cdot 2\pi i\right), \exp\left(\frac{5}{8} \cdot 2\pi i\right), \exp\left(\frac{7}{8} \cdot 2\pi i\right).$$

   Since the number on the denominator is 8 (and all fractions are reduced), we can conclude that if n exists, then $n = 8$.

   On the other hand, for $n = 8$, only $k = 1, 3, 5$ and 7 give $\gcd(k, n) = 1$. This means that $n = 8$ satisfies that the primitive 8-th roots of unity being

   $$\exp\left(\frac{1}{8} \cdot 2\pi i\right), \exp\left(\frac{3}{8} \cdot 2\pi i\right), \exp\left(\frac{5}{8} \cdot 2\pi i\right), \exp\left(\frac{7}{8} \cdot 2\pi i\right).$$

   Hence, $n = 8$ satisfies $C_n(x) = x^4 + 1$, and hence $n = 8$.

3. Since p is prime, for $k = 1, 2, 3, \ldots, p-1$, we must have $\gcd(k, p) = 1$ (and for $k = 0$, $\gcd(k, p) = p \neq 1$). This means that all the pth roots of unity apart from $x = 1$ will be primitive pth roots of unity, and hence
$$C_p(x) = \frac{x^p - 1}{x - 1} = 1 + x + x^2 + \cdots + x^{p-1}.$$

4. A root of C_q must take the form of
$$\exp\left(\frac{Q}{q} \cdot 2\pi i\right)$$
where $0 \leq Q < q, \gcd(Q, q) = 1$.

   A root of C_r must take the form of
$$\exp\left(\frac{R}{r} \cdot 2\pi i\right)$$
where $0 \leq R < r, \gcd(R, r) = 1$, and a root of C_s must take the form of
$$\exp\left(\frac{S}{s} \cdot 2\pi i\right)$$
where $0 \leq S < s, \gcd(S, s) = 1$.

   Since a root to C_s must be a root to the right-hand side of the equation, and hence must be a root to the left-hand side of the equation, we have
$$\exp\left(\frac{Q}{q} \cdot 2\pi i\right) = \exp\left(\frac{S}{s} \cdot 2\pi i\right).$$

   Since $0 \leq \frac{Q}{q}, \frac{S}{s} < 1$, we must have
$$\frac{Q}{q} = \frac{S}{s},$$
and since they are both reduced fractions, we must have $q = s$.

   Similarly, we also have $q = r$.

   This means
$$C_q(x) = C_q(x)^2,$$
and hence
$$C_q(x)(C_q(x) - 1) = 0.$$

   Since C_q is a polynomial, this means either $C_q(x) = 0$ or $C_q(x) = 1$, both of which are not possible given q is a positive integer. For the first case, this is impossible since this polynomial has infinitely many roots, but there are only finitely many qth roots of unity, and hence only finitely many primitive qth roots of unity.

   For the second case, this means that there is no primitive qth roots of unity. But for $k = 1$, $\gcd(k, q) = 1$, and hence there must be a primitive qth root of unity
$$\exp\left(\frac{1}{q} \cdot 2\pi i\right),$$
and this must be impossible.

   Hence, there are no positive integers q, r and s such that
$$C_q(x) = C_r(x) \cdot C_s(x).$$