

Q1a: Note since

$$(1-x)(1+x+\cdots+x^{q-1}) = (1-x^q)$$

Any root of the cyclotomic polynomial is also root of $1-x^q$. We see that $\Phi_q(0) \equiv 1 \pmod{p}$. Therefore by FLT the roots of $\Phi_q(x)$ must satisfy $x^{p-1} = 1$. We now check cases when $p \equiv 1 \pmod{q}$, $p = q$ or if neither are true. First consider the case where $p \equiv 1 \pmod{q}$, then there is some k such that $kq = p-1$

$$\begin{aligned} x^{p-1} - 1 &= x^{kq-1} - 1 \\ &= (x^q)^k - 1 \\ &= (x^q - 1)(x^{kq-q} + x^{kq-2q} + \cdots + 1) \\ &= (x^q - 1)(x^{p-1-q} + \cdots + 1) \end{aligned}$$

Hence by Lagrange's theorem the first term must have at most q roots and the second term must have at most $p-1-q$ roots. By Fermat's little theorem, $x^{p-1} - 1$ has $p-1$ roots mod p , so therefore $x^q - 1$ has q roots and $x^{p-1-q} + \cdots + 1$ has $p-1-q$ roots. Now since $(x-1)\Phi_q(x)$ has p roots, and $\Phi_q(1) \equiv q \pmod{p}$ which is not 0, so we must have that $\Phi_q(x)$ has $p-1$ roots. If $p \not\equiv 1 \pmod{q}$, so $\gcd(q, p-1) = 1$. Thus by Bezout's identity, there exist integers u, v with $u(p-1) + v(q) = 1$. Therefore, if x is a root of $\Phi_q(x)$, then $x^1 = x^{u(p-1)+v(q)} = (x^{p-1})^u \cdot (x^q)^v$. Now if $p = q$ then $\Phi_q(1) = 0 \pmod{p}$ so it has 1 root. Otherwise, $\Phi_q(1) \neq 0$ so $\Phi_q(x)$ has no roots.

Q1b: By the Chinese remainder theorem, any solution to $x^{18} + 4x^{14} + 3x + 10 \equiv 0 \pmod{21}$ must also be a solution to $x^{18} + 4x^{14} + 3x + 10 \equiv 0 \pmod{3}$ and $x^{18} + 4x^{14} + 3x + 10 \equiv 0 \pmod{7}$. By corollary 4.4, $x^{3k} \equiv x \pmod{3}$ for all $k \in \mathbb{Z}$. Therefore we can reduce our polynomials to

$$x^{18} + 4x^{14} + 3x + 10 \equiv (x^{3 \cdot 3})^2 + x^2 + 1 \equiv (2x^2 - 1) \equiv 1 - x^2 \equiv (1-x)(1+x) \pmod{3}$$

which has a solution of $x \equiv 1 \pmod{3}$ and $x \equiv 2 \pmod{3}$. Now for the $\pmod{7}$ polynomial,

$$x^{18} + 4x^{14} + 3x + 10 \equiv (x^7)^2 \cdot x^4 + 4(x^7)^2 + 3x + 10 \equiv x^6 + 4x^2 + 3x + 3 \equiv 0 \pmod{7}$$

By checking $x \in \{0, 1, 2, 3, 4, 5, 6\}$, we see that $x \equiv 3 \pmod{7}$ and $x \equiv 5 \pmod{7}$ are both solutions. By Chinese remainder theorem, the solutions are $x \equiv 5, 10, 17, 19 \pmod{21}$.

Q1c: We wish to solve $x^{59} + 2x^{40} + 5x^{25} + x^{15} + 17 \equiv 0 \pmod{221}$. By the Chinese remainder theorem, any solution to this will also be a solution to $x^{59} + 2x^{40} + 5x^{25} + x^{15} + 17 \equiv 0 \pmod{13}$ and $x^{59} + 2x^{40} + 5x^{25} + x^{15} + 17 \equiv 0 \pmod{17}$. We will first proceed with the first equivalency. Using corollary 4.4, we have that

$$x^{59} + 2x^{40} + 5x^{25} + x^{15} + 17 \equiv (x^{13})^4 \cdot x^7 + 2(x^{13})^3 \cdot x + 5(x^{13})x^{12} + x^{13} \cdot x^2 + 17 \equiv x^{11} + 2x^4 + x^3 + 5x + 4 \equiv 0 \pmod{13}$$

Taking $x \equiv 1 \pmod{13}$ will satisfy this. For $\pmod{17}$, we have that

$$x^{59} + 2x^{40} + 5x^{25} + x^{15} + 17 \equiv x^{59} + 2x^{40} + 5x^{25} + x^{15} \equiv 0 \pmod{17}$$

We see taking $x \equiv 0 \pmod{17}$ will satisfy. Therefore by the Chinese remainder theorem, a solution to the polynomial $\pmod{221}$ is $x \equiv 170 \pmod{221}$.

Q1d: To find a solution to $55x^{19} + 3x^{14} + x^2 + 55 \equiv 0 \pmod{66}$. By the Chinese remainder theorem, any solution to this must be a simultaneous solution to $55x^{19} + 3x^{14} + x^2 + 55 \equiv 0 \pmod{2}$, $55x^{19} + 3x^{14} + x^2 + 55 \equiv 0 \pmod{3}$, $55x^{19} + 3x^{14} + x^2 + 55 \equiv 0 \pmod{11}$. We will first look for solutions in the $\pmod{2}$ case. We see that

$$55x^{19} + 3x^{14} + x^2 + 55 \equiv x^{19} + x^{14} + x^2 + 1 \equiv 0 \pmod{2}$$

The only solution is $x \equiv 1 \pmod{2}$ is a solution. Now we look at the $\pmod{3}$ case.

$$55x^{19} + 3x^{14} + x^2 + 55 \equiv x^{19} + x^2 + 1 \equiv x^2 + x + 1 \equiv 0 \pmod{3}$$

We see that the only solution is $x \equiv 1 \pmod{3}$. Finally, we check mod (11).

$$55x^{19} + 3x^{14} + x^2 + 55 \equiv 3x^{11}x^3 + x^2 \equiv 3x^4 + x^2 \equiv x^2(3x^2 + 1) \equiv 0 \pmod{11}$$

By checking each $x \in \mathbb{Z}/11\mathbb{Z}$ we see that $3x^2 + 1 \not\equiv 0$ for all x . Thus we conclude that the only solution mod 11 is $x \equiv 0 \pmod{11}$. Therefore, by the chinese remainder theorem, the solution will be $x \equiv 55 \pmod{66}$.