Geoffrey Thomas
18.781 problem set 4

2.6 2. The single solution of $x^5 + x^4 + 1 \equiv 0 \pmod 3$ is $x \equiv 1 \pmod 3$. Note that $f'(1) = 9 \equiv 0 \pmod 3$, but $1^5 + 1^4 + 1 \not\equiv 0 \pmod 9$, so the root cannot be lifted and there are no solutions.

2.6 3. The single solution of $x^3 + x + 57 \equiv 0 \pmod 5$ is $x \equiv 4 \pmod 5$. We lift this root to $4 - 125 \cdot 4 \equiv 4 \pmod{5^2}$, which then lifts to $4 - 125 \cdot 4 \equiv 4 \pmod{5^3}$.

2.6 7. The single solution of $x^3 + x^2 - 5 \equiv 0 \pmod 7$ is $x \equiv 2 \pmod 7$. We lift this root to $2 - 7 \cdot 4 \equiv 23 \pmod{7^2}$, which then lifts to $23 - 12691 \cdot 4 \equiv 23 \pmod{7^3}$.

2.6 9.

2.6 10. Hensel's lemma tells us that if there is a solution x_0 to $x^2 \equiv a \pmod{p^j}$, then as long as $2x_0 \not\equiv 0 \pmod p$, then there is a solution to $x^2 \equiv a \pmod{p^{j+1}}$. Our constraint is true, because if $2x_0 \equiv 0 \pmod p$, then $0 \equiv 4x_0^2 \equiv a \pmod p$, but we know that $0 \not\equiv a \pmod p$. Therefore, by mathematial induction, as long as $x^2 \equiv a \pmod{p^j}$ has a solution for $j = 1$, it has a solution for all positive integers j.

2.7 3. As $(x^{13} + 12x)x \equiv 0 \pmod{13}$, the congruence is true if $x \equiv 0$ or $x^{13} + 12x \equiv 0 \pmod{13}$. By Fermat's Little Theorem, the latter is equivalent to $x + 12x \equiv 0 \pmod{13}$, which is identical.

2.7 8.

2.7 10. The unreduced numerator is σ_{p-2} from the discussion at the end of the section, so by Wolstenholme's congruence, p^2 divides it. The reduced numerator a is the same as the unreduced one

2.7 11.

2.8 2. By guessing numbers until they work, 5.

2.8 9. $3^4 \equiv -4 \pmod{17}$, so $3^8 \equiv (-4)^2 \equiv -1 \pmod{17}$. Therefore $3^16 \equiv (-1)^2 \equiv 1 \pmod{17}$, so the order of 3 divides 16. But the order of 3 does not divide 8, so the order must be exactly 16.

2.8 12.

2.8 13.

2.8 16.

2.8 24. Under these conditions, the order of a modulo n is $n - 1$, so $\phi(n) \geq n - 1$, so n must be prime.