Math 44S H.W. #4 Solutions

15. How many solutions?

(a) \[ x^{12} \equiv 16 \pmod{17} \] \[ (12, 16) = 4 \]
Check: \[ 16^{16/4} \equiv (-1)^4 \equiv 1 \]
so eqn has 4 solutions.

(b) \[ x^{48} \equiv 9 \pmod{17} \] \[ (48, 16) = 16 \]
Check: \[ 9^{-16} = 9^{-1} \neq 1 \]
so eqn has 0 solutions.

(c) \[ x^{20} \equiv 13 \pmod{17} \] \[ (20, 16) = (5, 4, 14) = 4 \]
Check: \[ 13 \cdot (16/4) \equiv 13^4 \equiv (169)^2 \equiv (-1)^2 \equiv 1 \]
so eqn has 4 solutions.

(d) \[ x^9 \equiv 9 \pmod{17} \] \[ (11, 16) = 1 \]
Check: \[ 9^{-16} = 9^{-1} \equiv 1 \] by Fermat's Little Theorem.
so eqn has 1 solution.

16. \( p \) prime, \( p \equiv 3 \pmod{4} \) then \( x \equiv a \pmod{p} \) has a solution \( \iff \) \( x^2 \equiv a \pmod{p} \) does.

\( x^4 \equiv a \pmod{p} \) has a solution \( \iff \frac{p-1}{4} \equiv 0 \pmod{p} \)
\( x^2 \equiv a \pmod{p} \) has a solution \( \iff \frac{p-1}{2} \equiv 0 \pmod{p} \).

But \( p \equiv 3 \pmod{4} \) \( \implies \) \( p = 4n + 3 \) for some \( n \), so \( p-1 = 4n+2 = 2(2n+1) \)
So \( (p-1, 2) = 2 \) (ie. \( 2 \mid p-1 \)) and \( (p-1, 4) = 2 \), and otherwise \( (p-1, 4) = 1 \), i.e. \( 4 \mid p-1 = 2(2n+1) \), a contradiction.
So \((p-1,2) = (p-1,4)\), so \(a^{\frac{p+1}{3}} \equiv 1 \pmod{p} \iff a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.

This implies our conclusion.

17. If \(p\) prime and \(\text{ord}_p(a) = 3\), then \(a^2 + a + 1 \equiv 0 \pmod{p}\) and \(\text{ord}_p(a+1) = 6\).

\[\text{ord}_p(a) = 3 \implies a^3 \equiv 1 \pmod{p} \iff p | a^2 - 1 = (a-1)(a^2 + a + 1).\]

But \(p \nmid (a-1)\), since otherwise \(a^3 \equiv 1 \pmod{p}\) so \(\text{ord}_p(a) = 1\).

So since \(p\) is prime, \(p | a^2 + a + 1\), i.e. \(a^2 + a + 1 \equiv 0 \pmod{p}\). This implies that \(a+1 \equiv -a^2 \pmod{p}\).

So \((a+1)^6 \equiv (-a^2)^6 \equiv (-1)^6 a^{12} \equiv a^{12} \equiv 1 \pmod{p}\), since \(3 | 12\). So \(\text{ord}_p(a+1) \mid 6\), so \(\text{ord}_p(a) = 1, 2, 3\) or \(6\).

But \((a+1) \equiv 0 \pmod{p}\), so \(a\) would have no order, so \(a^3 \equiv 1 \pmod{p}\), so \(a\) would have order \(1\).

\[1 \equiv (a+1)^3 \equiv (-a^2)^3 \equiv a^9 \equiv a \pmod{p} \iff a \equiv 1 \pmod{p}, \text{ so } a \text{ would have order } 1;\]

\[1 \equiv (a+1)^3 \equiv (-a^2)^3 \equiv (a^3)^3 \equiv (a^3)^3 \equiv a^{12} \equiv 1 \pmod{p} \implies p \nmid a+1 \equiv 0 \pmod{p} \implies 2p \nmid 2 \implies p = 2, \text{ but then } a \equiv 0 \pmod{2} \text{ so again does not have order } 3. \text{ So } (a+1)^k \not\equiv 1 \pmod{p} \text{ for } 0 < k < 6, \text{ so } \text{ord}_p(a+1) = 6. \]

18. If \(a^2 \equiv 2\), then \((a^n-1, a^{n+1}) = 2\) if \(m\) is odd.

Set \(d = (a^n-1, a^{n+1})\), so \(d | a^n - 1, d | a^{n+1}\), i.e.

\[a^n \equiv 1 \pmod{d}, a^{n+1} \equiv 1 \pmod{d} \implies \text{ord}_d(a) | m, \text{ which is odd. Only odd numbers divide odd numbers, so } \text{ord}_d(a) \text{ is odd.}\]

\[a^n \equiv 1 \implies a^{2n} \equiv (a^n)^2 \equiv 1, \text{ so } \text{ord}_d(a) | 2n. \text{ But}\]
\[ \phi(p) \text{ is odd} \quad \text{and} \quad \phi(p) > p-1 \]

So \( \phi(\phi(p)) = p \) if and only if \( p \) is prime.

For the sake of the argument, let \( p = 2 \).

Since \( p \) is a prime number, \( \frac{p}{2} \) is even.

Let \( a \equiv \frac{p}{2} \equiv 0 \pmod{p} \) and \( p \equiv 1 \pmod{2} \).

Since \( p \) is odd, \( p-1 \equiv 2 \pmod{2} \).

Thus, \( p \) is a prime number, and

\[ \phi(p) = p-1. \]

For \( a = 2 \), we have \( \phi(a) = a-1 = 1 \).

But since \( a = 2 \), we have \( \phi(a) = 1 \).

And for \( a = p \), we have \( \phi(a) = a-1 \).

Thus, \( a = 2 \) is discarded.

So let \( a = \frac{p}{2} \).