SOLUTIONS TO PROBLEM SET 5

SECTION 9.1

Exercise 2. Recall that for \((a, m) = 1\) we have \(\text{ord}_m a\) divides \(\phi(m)\).

a) We have \(\phi(11) = 10\) thus \(\text{ord}_{11} 3 \in \{1, 2, 5, 10\}\). We check
\[
3^1 \equiv 3 \pmod{11}, \quad 3^2 \equiv 9 \pmod{11}, \quad 3^5 \equiv 9 \cdot 27 \equiv 9 \cdot 5 \equiv 45 \equiv 1 \pmod{11}
\]
Thus \(\text{ord}_{11} 3 = 5\).

b) We have \(\phi(17) = 16\) thus \(\text{ord}_{17} 2 \in \{1, 2, 4, 8, 16\}\). We compute
\[
2^2 \equiv 4 \pmod{17}, \quad 2^4 \equiv -1 \pmod{17}, \quad 2^8 \equiv (-1)^2 \equiv 1 \pmod{17}
\]
Thus \(\text{ord}_{17} 2 = 8\).

c) We have \(\phi(21) = 2 \cdot 6 = 12\) thus \(\text{ord}_{21} 10 \in \{1, 2, 3, 4, 6, 12\}\). We compute
\[
10^2 \equiv 16 \pmod{21}, \quad 10^3 \equiv 13 \pmod{21}, \quad 10^4 \equiv (-5)^2 \equiv 4 \pmod{21}
\]
and \(10^6 \equiv 4 \cdot 16 \equiv 1 \pmod{21}\). Thus \(\text{ord}_{21} 10 = 6\).

d) We have \(\phi(25) = 20\), thus \(\text{ord}_{25} 9 \in \{1, 2, 4, 5, 10\}\). We compute
\[
9^2 \equiv 81 \equiv 6 \pmod{25}, \quad 9^4 \equiv 36 \equiv 11 \pmod{25}, \quad 9^5 \equiv 99 \equiv -1 \pmod{25}.
\]
Thus \(\text{ord}_{25} 9 = 10\).

Exercise 6. Recall that a primitive root (PR) modulo \(m\) is an element \(r\) with maximal order, that is \(\text{ord}_m r = \phi(m)\).

a) Note that \(\phi(4) = 2\), so we are looking for an element \(r\) such that \(r^2 \equiv 1 \pmod{4}\), while \(r \not\equiv 1 \pmod{4}\). Taking \(r = 3\), we observe that indeed \(3 \not\equiv 1 \pmod{4}\) and \(\phi(4) = 2\), so \(r = 3\) is a PR modulo 4.

b) \(r = 2\) is a PR mod 5, as \(\phi(5) = 4\) and \(2^4 \equiv 16\) is the first power of 2 congruent to 1 mod 5.

c) \(r = 3\) is a PR mod 10, as \(\phi(10) = 4\), \(3^2 = 9 \not\equiv 1 \pmod{10}\) and the possible orders are \(\{1, 2, 4\}\).

d) Note that \(\phi(13) = 12\), hence \(\text{ord}_{13} a \in \{1, 2, 3, 4, 6, 12\}\) for all \(a \in \mathbb{Z}\) such that \((a, 13) = 1\). For example, we compute
\[
2^2 \equiv 4 \pmod{13}, \quad 2^3 \equiv 8 \pmod{13}, \quad 2^4 \equiv 3 \pmod{13}
\]
and \(2^6 \equiv 64 \equiv -1 \pmod{13}\). Thus \(\text{ord}_{13} 2 = 12\), hence \(r = 2\) is a PR mod 13.

e) Note that \(\phi(14) = 6\), hence \(\text{ord}_{14} a \in \{1, 2, 3, 6\}\) for all \(a \in \mathbb{Z}\) such that \((a, 14) = 1\). For example, we compute
\[
3^2 \equiv 9 \pmod{14}, \quad 3^3 \equiv 27 \equiv -1 \pmod{14}
\]
and so \(\text{ord}_{14} 3 = 6\), that is \(r = 3\) is a PR mod 14.
f) Note that $\phi(18) = 6$, hence $\text{ord}_{18} a \in \{1, 2, 3, 6\}$ for all $a \in \mathbb{Z}$ such that $(a, 18) = 1$. For example, we compute

$$5^2 \equiv 7 \pmod{18}, \quad 5^3 \equiv 35 \equiv -1 \pmod{18}$$

and so $\text{ord}_{18} 5 = 6$, that is $r = 5$ is a PR mod 18.

**Exercise 8.** We have $\phi(20) = \phi(4)\phi(5) = 8$, hence $\text{ord}_{20}(a) \in \{1, 2, 4, 8\}$ for all $a \in \mathbb{Z}$ such that $(a, 20) = 1$. To prove there are no primitive roots mod 20 we have to show that $\text{ord}_{20}(a) = 8$ never occurs.

It suffices to show that for all $a$ such that $0 \leq a \leq 19$ and $(a, 20) = 1$ we have $a^d \equiv 1 \pmod{20}$ for some $d \in \{1, 2, 4\}$. Indeed, all such values of $a$ are $\{1, 3, 7, 9, 11, 13, 17, 19\}$. Clearly, $1^1 \equiv 1 \pmod{20}$ and direct calculations show that

$$9^2 \equiv 11^2 \equiv 19^2 \equiv 1 \pmod{20} \quad \text{and} \quad 3^4 \equiv 7^4 \equiv 13^4 \equiv 17^4 \equiv 1 \pmod{20}.$$

**Exercise 12.** Let $a, b, n \in \mathbb{Z}$ satisfy $n > 0$, $(a, n) = (b, n) = 1$ and $(\text{ord}_n a, \text{ord}_n b) = 1$.

Write $y = \text{ord}_n a \cdot \text{ord}_n b$. We have

$$(ab)^y = a^y b^y = (a^{\text{ord}_n a})^{\text{ord}_n b} (b^{\text{ord}_n b})^{\text{ord}_n a} \equiv 1 \cdot 1 \equiv 1 \pmod{n},$$

hence $\text{ord}_n(a b) | y$. Therefore $\text{ord}_n(ab) \leq \text{ord}_n(a) \cdot \text{ord}_n(b)$.

To finish the proof, we will now show the opposite inequality $\text{ord}_n(ab) \geq \text{ord}_n(a) \cdot \text{ord}_n(b)$.

Note that $(b, n) = 1$ implies $b$ has an inverse $b^{-1}$ modulo $n$. Furthermore, for $k \geq 0$ we have $(b^k, n) = 1$ and the inverse of $b^k$ is $(b^{-1})^k$ which is usually denoted $b^{-k}$. Suppose $(ab)^x \equiv 1 \pmod{n}$, which is equivalent to $a^x \equiv b^{-x} \pmod{n}$, because $b^{-1}$ exists. We now compute

$$a^{-x} b = (a^x)^{\text{ord}_n b} \equiv (b^{-x})^{\text{ord}_n b} \equiv (b^{-x})^{\text{ord}_n b} \equiv (b^{x \text{ord}_n b})^{-1} \equiv ((b^{\text{ord}_n b})^x)^{-1} \equiv 1 \pmod{n},$$

hence $\text{ord}_n a | x \cdot \text{ord}_n b$. Since $(\text{ord}_n a, \text{ord}_n b) = 1$ we have $\text{ord}_n a | x$.

Note that the argument in the previous paragraph also holds if we swap $a$ and $b$, so we also have $\text{ord}_n b | x$.

We have just shown that $(ab)^x \equiv 1 \pmod{n}$ implies $\text{ord}_n(a) \cdot \text{ord}_n(b) | x$. In particular, taking $x = \text{ord}_n(ab)$ implies $\text{ord}_n(ab) \geq \text{ord}_n(a) \cdot \text{ord}_n(b)$, as desired.

We conclude $\text{ord}_n(ab) = \text{ord}_n(a) \cdot \text{ord}_n(b)$.

**Exercise 16.** By definition $\phi(m)$ is the number of integers $a$ in the interval $1 \leq a \leq m - 1$ satisfying $(a, m) = 1$. In particular, it follows that $1 \leq \phi(m) \leq m - 1$.

Let $a, m \in \mathbb{Z}$ satisfy $m > 0$ and $(a, m) = 1$. We know that $\text{ord}_m a | \phi(m)$.

Suppose $\text{ord}_m a = m - 1$; then $\phi(m) \geq m - 1$. We conclude $\phi(m) = m - 1$. This can only occur if $m$ is prime, finishing the proof. Indeed, suppose $m$ is composite hence it has some factor $n$ in the interval $1 < n < m - 1$. Clearly, $(n, m) = n \neq 1$ therefore $\phi(m)$ is at most $m - 2$. 


Exercise 5. We know that there are \( \phi(\phi(13)) = \phi(12) = 4 \) incongruent primitive roots \( \text{mod} \ 13 \). For each \( k \) in \( 1 \leq k \leq 12 \) we have \( (k, 13) = 1 \) and we compute \( k^i \pmod{13} \) for all \( i > 0 \) dividing \( \phi(13) = 12 \), that is \( i \in \{1, 2, 3, 4, 6, 12\} \).

From FLT we know that \( k^{12} \equiv 1 \pmod{13} \), so the primitive roots are the values of \( k \) such that \( k^i \not\equiv 1 \pmod{13} \) for all \( i \in \{1, 2, 3, 4, 6\} \). We stop when we find four such values of \( k \); these are \( \{2, 6, 7, 11\} \).

Alternative proof requiring less computations. Computing \( 2^i \pmod{13} \) for \( i \) a positive divisor of \( \phi(13) = 12 \), that is \( i \in \{1, 2, 3, 4, 6, 12\} \) (the possible orders of 2 modulo 13) we verify that \( 2^i \not\equiv 1 \pmod{13} \) for all \( i \in \{1, 2, 3, 4, 6\} \), hence 2 has order 12, so it is a primitive root \( \text{mod} \ 13 \). Thus \( \{2^i\}, \ 1 \leq i \leq 12 \) forms a reduced residue system. We also know that

\[
\text{ord}_{13} 2^i = \frac{\text{ord}_{13} 2}{(i, \text{ord}_{13} 2)}.
\]

Now, if \( \text{ord}_{13} 2^i = 12 \) then \( (i, \text{ord}_{13} 2) = (i, 12) = 1 \) which occurs exactly when \( i = 1, 5, 7, 11 \). Therefore, 2, \( 2^5 \), \( 2^7 \) and \( 2^{11} \) are four non-congruent primitive roots modulo 13.

If we want to obtain the smallest representatives for each of these primitive roots we have to reduce them modulo 13, obtaining

\[
2^1 \equiv 2, \quad 2^5 \equiv 6, \quad 2^7 \equiv 11, \quad 2^{11} \equiv 7 \pmod{13}
\]

to conclude that \( \{2, 6, 7, 11\} \) is a set of all incongruent primitive roots modulo 13 with smallest possible representatives, which was expected by our previous solution.

Exercise 8. Let \( r \) be a primitive root \( \text{mod} \ p \), that is \( \text{ord}_p \ r = \phi(p) = p - 1 \).

We first show that \( r^{\frac{p-1}{2}} \equiv -1 \pmod{p} \). Indeed, denote \( r^{\frac{p-1}{2}} \) by \( x \); then \( x^2 \equiv r^{p-1} \equiv 1 \pmod{p} \). Hence \( x \equiv 1 \) or \( -1 \pmod{p} \). But \( x = r^{\frac{p-1}{2}} \) cannot be \( 1 \pmod{p} \), because it would contradict \( \text{ord}_p \ r = p - 1 \). Hence \( x \equiv -1 \pmod{p} \) as claimed.

Now we want to show that \( -r \) is a primitive root, that is \( \text{ord}_p (-r) = p - 1 \).

We have that

\[
-r \equiv (-1)r \equiv r^{\frac{p-1}{2}+1} \pmod{p},
\]

where in the second congruence we used that \( r^{\frac{p-1}{2}} \equiv -1 \pmod{p} \). We will determine the order of \( r^{\frac{p-1}{2}+1} \pmod{p} \) by using the formula

\[
\text{ord}_p r^k = \frac{\text{ord}_p r}{(\text{ord}_p r, k)}.
\]

Taking \( k = \frac{p-1}{2} + 1 \) and since \( \text{ord}_p r = p - 1 \) we have to show that \( (p - 1, \frac{p-1}{2} + 1) = 1 \).

We note that up to this point we have not yet used the hypothesis \( p \equiv 1 \pmod{4} \).

From \( p \equiv 1 \pmod{4} \), we can write \( p \) as \( 4m + 1 \) for some integer \( m \geq 1 \). Then \( p - 1 = 4m \), and \( \frac{p-1}{2} + 1 = 2m + 1 \). Thus we want to prove that \( (4m, 2m + 1) = 1 \) for any integer \( m \geq 1 \).

Recall that for all \( a, b, q \in \mathbb{Z} \) with \( a \geq b > 0 \) we have \( (a, b) = (b, a - bq) \). This gives

\[
(4m, 2m + 1) = (2m + 1, 4m - 2(2m + 1)) = (2m + 1, -2) = (2m + 1, 2) = 1,
\]

Section 9.2
as desired. In summary, \( \text{ord}_p(-r) = \text{ord}_p(r^{2m+1}) = \frac{p-1}{\gcd(4m, 2m+1)} = \frac{p-1}{1} = p-1 \), that is \(-r\) is a primitive root.

**Exercise 10.**

a) 
\[ x^2 - x \text{ has 4 incongruent solutions mod 6, namely, 0, 1, 3, and 4. Indeed, modulo 6 we have } \]
\[ 0^2 - 0 \equiv 0, \quad 1^2 - 1 \equiv 0, \quad 2^2 - 2 \equiv 2 \not\equiv 0 \pmod{6}, \]
\[ 3^2 - 3 \equiv 3 - 3 \equiv 0, \quad 4^2 - 4 \equiv 4 - 4 \equiv 0, \quad \text{and} \quad 5^2 - 5 \equiv 2 \not\equiv 0 \pmod{6}. \]

b) 
Part (a) does not violate Lagrange’s theorem because the modulus in Lagrange’s theorem must be prime, but the modulus in part a) is composite.

**Exercise 16.** Let \( p \) be a prime of the form \( p = 2q + 1 \), where \( q \) is an odd prime.

Let \( a \in \mathbb{Z} \) satisfy \( 1 < a < p - 1 \); in particular, \( (a, p) = 1 \). Since \( p - a^2 \equiv -a^2 \pmod{p} \) we have \( \text{ord}_p(p - a^2) = \text{ord}_p(-a^2) \). We will show that \( \text{ord}_p(-a^2) = p - 1 \).

We know that \( \text{ord}_p(-a^2) \) divides \( \phi(p) = p - 1 = 2q \). Thus \( \text{ord}_p(-a^2) = 1, 2, q \), or \( 2q \). We have to rule out 1, 2 and \( q \). Equivalently, we need to show that

\[
\begin{align*}
(1) \quad (-a^2)^2 &\not\equiv 1 \pmod{p} \\
(2) \quad (-a^2)^q &\not\equiv 1 \pmod{p}
\end{align*}
\]

Proof of (1): Assume the contrary. Then, \( a^4 \equiv 1 \pmod{p} \). Thus \( \text{ord}_p a \) divides both 4 and \( p - 1 = 2q \). Hence, \( \text{ord}_p a \) divides \( \gcd(4, 2q) = 2 \). In particular, \( a^2 \equiv 1 \pmod{p} \), therefore \( a \equiv \pm 1 \pmod{p} \). This contradicts \( 1 < a < p - 1 \), completing the proof of (1).

Proof of (2): Assume the contrary, that is \( (-a^2)^q \equiv 1 \pmod{p} \). Therefore,
\[
1 \equiv (-a^2)^q \equiv (-1)^q a^{2q} \equiv (-1)^q \equiv -1 \pmod{p},
\]
where in the 3rd congruence we applied FLT and in the last one we used the fact that \( q \) is odd. Thus, \(-1 \equiv 1 \pmod{p} \), a contradiction since \( p > 2 \).

**Section 9.4**

**Exercise 2.** We first note that 5 is a primitive root of 23.

To solve this problem consult the table of indexes relative to 5 modulo 23. It is given as the answer to problem 1 of Section 9.4.

a) We want to solve \( 3x^5 \equiv 1 \pmod{23} \).

Taking the index of both sides of our equation, gives
\[
\text{ind}_5(3x^5) \equiv \text{ind}_5(1) \equiv 0 \pmod{\phi(23) = 22}
\]
which expands into
\[
\text{ind}_5(3) + 5 \text{ind}_5(x) \equiv 0 \pmod{22} \iff 5 \text{ind}_5(x) \equiv -16 \equiv 6 \pmod{22}.
\]
Since $5^{-1} \equiv 9 \pmod{22}$ we get $\text{ind}_5(x) \equiv 10 \pmod{22}$ which means that $x \equiv 9 \pmod{23}$.

b) We want to solve $3x^{14} \equiv 2 \pmod{23}$. The procedure is similar as before.

Take the index of both sides of our equation, giving $\text{ind}_5(3x^{14}) \equiv \text{ind}_5(2) \equiv 2 \pmod{22}$.
Now, we expand this into $\text{ind}_5(3) + 14\text{ind}_5(x) \equiv 2 \pmod{22}$. Hence, $14\text{ind}_5(x) \equiv -14 \equiv 8 \pmod{22}$. We then reduce this equation on all sides by 2, giving us $7\text{ind}_5(x) \equiv 4 \pmod{11}$.

Since $7^{-1} \equiv 8 \pmod{11}$ we obtain $\text{ind}_5(x) \equiv 10 \pmod{11}$. Therefore, $\text{ind}_5(x) \equiv 10, 21 \pmod{22}$. Using the table of indices, we find that this means that $x \equiv 9, 14 \pmod{23}$.

**Exercise 3.**

a) We want to solve $3^x \equiv 2 \pmod{23}$.

We know 5 is a primitive root mod 23. Note that $\phi(23) = 22$. We take the index of both sides giving

$$x \text{ind}_5(3) \equiv 2 \pmod{22} \iff 16x \equiv 2 \pmod{22}.$$ 
Thus $8x \equiv 1 \pmod{11}$ and since $8^{-1} \equiv 7 \pmod{11}$ we have $x \equiv 7 \pmod{11}$.

Thus, $x \equiv 7, 18 \pmod{22}$.

b) We want to solve $13^x \equiv 5 \pmod{23}$.

If there is such an $x$, taking the index of both sides we obtain $x \text{ind}_5(13) \equiv 1 \pmod{22}$, or rather, $14x \equiv 1 \pmod{22}$, which means that 14 is invertible mod 22. But since $(14, 22) = 2$ we know that 14 is not invertible mod 22; thus the initial equation cannot have solutions.

**Exercise 4.** Consider the equation $ax^4 \equiv 2 \pmod{13}$.

We check that 2 is a primitive root mod 13. Taking the index of both sides we have $\text{ind}_2(a) + 4\text{ind}_2(x) \equiv 1 \pmod{12}$, or rather, $4\text{ind}_2(x) \equiv 1 - \text{ind}_2(a) \pmod{12}$.

Write $y = \text{ind}_2(x)$. Thus, the above gives the linear congruence

$$4y \equiv 1 - \text{ind}_2(a) \pmod{12}$$
which, since $\gcd(4, 12) = 4$, will have a solution if and only if $4 | 1 - \text{ind}_2(a)$. This will be the case only when $\text{ind}_2(a) \equiv 1, 5, 9 \pmod{12}$, which correspond to $a \equiv 2, 6, 5 \pmod{13}$.

**Alternative proof:** If $13 | a$ then clearly there are no solutions. Suppose $13 \nmid a$. Thus $a^{-1}$ mod 13 exists and we multiply the congruence by it to obtain $x^4 \equiv 2a^{-1} \pmod{13}$. Write $d = (4, \phi(13)) = (4, 12) = 4$. Thus, we have seen in class that $x^4 \equiv 2a^{-1} \pmod{13}$ will have solutions if and only if $(2a^{-1})^{\phi(13)/d} \equiv 1 \pmod{13}$. This is equivalent to $a^3 \equiv 8 \pmod{13}$. Direct computations show this holds exactly when $a \equiv 2, 5, 6 \pmod{13}$, as expected.

**Exercise 5.** Consider the equation $8x^7 \equiv b \pmod{29}$.

We check that 2 is a primitive root mod 29.

If $b \equiv 0 \pmod{29}$ then the equation has the solution of $x \equiv 0 \pmod{29}$.

Suppose that $b \not\equiv 0 \pmod{29}$. Taking the index gives $\text{ind}_2(8) + 7\text{ind}_2(x) \equiv \text{ind}_2(b) \pmod{28}$, or rather, $7\text{ind}_2(x) \equiv \text{ind}_2(b) - 3 \pmod{28}$.

Write $y = \text{ind}_2(x)$. The previous gives the linear congruence

$$7y \equiv \text{ind}_2(b) - 3 \pmod{28},$$
which, since $\gcd(7, 28) = 7$, will have a solution if and only if $7 | \text{ind}_2(b) - 3$. This will be the case only when $\text{ind}_2(b) \equiv 1, 4, 7, 10, 13, 16, 19, 22 \pmod{28}$, which correspond to $b \equiv 8, 15, 22 \pmod{29}$.
which, since \( \gcd(7, 28) = 7 \), will have a solution if and only if \( 7 \mid \text{ind}_2(b) - 3 \). This is the case when \( \text{ind}_2(b) \equiv 3, 10, 17, 24 \pmod{28} \), which correspond to \( b \equiv 8, 9, 20, 21 \pmod{29} \).

We conclude that the complete list of values of \( b \) such that the initial equation has solutions is \( b \equiv 0, 8, 9, 20, 21 \pmod{29} \).

**Alternative proof for the case** \( b \not\equiv 0 \pmod{29} \): Multiply the congruence by \( 8^{-1} \pmod{29} \) obtaining \( x^7 \equiv 8^{-1}b \pmod{29} \). Write \( d = (7, \phi(29)) = (7, 28) = 7 \). Thus, we have seen in class that \( x^7 \equiv 8^{-1}b \pmod{29} \) will have solutions if and only if \( (8^{-1}b)^{\phi(29)/d} \equiv 1 \pmod{29} \). This is equivalent to \( b^4 \equiv 7 \pmod{29} \). Direct computations show this holds exactly when \( b \equiv 8, 9, 20, 21 \pmod{29} \).

**Exercise 18.** Let \( p \) be an odd prime and \( r \) a primitive root mod \( p \), that is \( \text{ord}_p r = \phi(p) = p - 1 \).

Note that \( p - 1 \equiv -1 \pmod{p} \). Thus we have to show that
\[
r^{p-1} \equiv -1 \pmod{p} \quad \text{and} \quad r^i \not\equiv -1 \pmod{p} \quad \text{for} \quad 1 \leq i < (p - 1)/2.
\]

Since \( p \) is odd, \( p - 1 \) is even and \( (r^{p-1})^2 = r^{p-1} \equiv 1 \pmod{p} \); thus \( r^k \equiv \pm 1 \pmod{p} \). If \( r^k \equiv 1 \pmod{p} \) then \( \text{ord}_p r < p - 1 \), a contradiction. We conclude \( r^k \equiv -1 \pmod{p} \).

Suppose that \( r^i \equiv -1 \pmod{p} \) for some \( i < (p - 1)/2 \); therefore \( (r^i)^2 = r^{2i} \equiv 1 \pmod{p} \) and \( 2i < 2(p - 1)/2 = p - 1 \), which again means \( \text{ord}_p r < p - 1 \), a contradiction.

**Exercise 9.** Let \( p \) be an odd prime. We have \( \phi(p) = p - 1 \) is even.

Write \( d = (4, p - 1) \). From class or Theorem 9.17 in Rosen, we know that \( x^4 \equiv -1 \pmod{p} \) has a solution if and only if \( (-1)^{\phi(p)/x} \equiv 1 \pmod{p} \). Since the order of \(-1 \pmod{p} \) is 2 we must have \( 2 \mid \frac{p - 1}{x} \). That is, there exists \( k \) such that \( 2k = \frac{p - 1}{(p - 1, 4)} \).

Since \( p - 1 \) is even we have \( (p - 1, 4) = 2 \) or 4. If \( (p - 1, 4) = 2 \) then \( \frac{p - 1}{(p - 1, 4)} \) must be odd, a contradiction. Therefore, \( (p - 1, 4) = 4 \), so \( 2k = \frac{p - 1}{4} \), or rather, \( 8k + 1 = p \), as required.

**Exercise 18.** An integer \( a \) is called a cubic residue mod \( p \) when there is an integer \( r \) such that \( r^3 \equiv a \pmod{p} \). In other words, the congruence equation \( x^3 \equiv a \pmod{p} \) has a solution. Let \( p > 3 \) be a prime and \( a \) an integer not divisible by 3. We want to know if the congruence \( x^3 \equiv a \pmod{p} \) has a solution, where \( a \) is fixed and we are solving for \( x \).

Let \( d = \gcd(3, p - 1) \). By Theorem 9.17 a solution exists if and only if \( a^{\frac{p-1}{3}} \equiv 1 \pmod{p} \).

1. Suppose \( p \equiv 2 \pmod{3} \). Then \( d = 1 \) and \( a^{\frac{p-1}{3}} \equiv a^{p-1} \equiv 1 \pmod{p} \) for every \( a \neq 0 \pmod{p} \).
2. Suppose \( p \equiv 1 \pmod{3} \). Then \( d = 3 \) and a solution exists if and only if \( a^{\frac{p-1}{3}} \equiv 1 \pmod{p} \).

Why is \( d = 1 \) in part (1) and \( d = 3 \) in part (2).EntityFramework

Since the only divisors of 3 are 1 and 3 it follows that \( d = 1 \) if \( 3 \mid p - 1 \) and \( d = 3 \) if \( 3 \mid p - 1 \). In part (1) we have \( p - 1 \equiv 1 \pmod{3} \) so \( p - 1 \) is not divisible by 3. In part (2) we have \( p - 1 \equiv 0 \pmod{3} \) so \( p - 1 \) is divisible by 3.