Complete Solutions to Exercises 6.3

1. We need to find whether 3 and 5 are primitive roots of 7. *How?*
   Since 7 is prime so $\phi(7) = 6$ and the only positive divisors of 6 are 1, 2, 3 and 6. In each case we need to evaluate these indices to the bases 3 and 5.
   (a) We have
   $$3^2 \equiv 9 \equiv 3 \not\equiv 1 \pmod 7$$
   $$3^3 \equiv 27 \equiv 6 \not\equiv 1 \pmod 7$$
   $$3^6 \equiv 1 \pmod 7$$
   Therefore 3 is a primitive root of 7.
   (b) Checking if 5 is a primitive root of 7:
   $$5^2 \equiv 25 \equiv 4 \not\equiv 1 \pmod 7$$
   $$5^3 \equiv 4 \times 5 \equiv 20 \equiv 6 \not\equiv 1 \pmod 7$$
   By Euler's Theorem we have $5^6 \equiv 1 \pmod 7$. Hence 5 is a primitive root of 7.

2. We are required to find whether 3, 5 and 7 are primitive roots of 11. As 11 is prime so $\phi(11) = 10$ and the only positive divisors of 10 are 1, 2, 5 and 10.
   (a) Checking whether 3 is a primitive root of 11:
   $$3^2 \equiv 9 \not\equiv 1 \pmod{11}$$
   $$3^5 \equiv 243 \equiv 1 \pmod{11}$$
   Therefore 3 is *not* a primitive root of 11.
   (b) Using similar evaluations for base 5 we have
   $$5^2 \equiv 25 \equiv 3 \not\equiv 1 \pmod{11}$$
   $$5^5 \equiv 3125 \equiv 1 \pmod{11}$$
   5 is *not* a primitive root of 11.
   (c) Repeating the above calculations for 7 we have
   $$7^2 \equiv 49 \equiv 5 \not\equiv 1 \pmod{11}$$
   $$7^5 \equiv 16807 \equiv 10 \not\equiv 1 \pmod{11}$$
   By Euler's Theorem we have $7^{10} \equiv 1 \pmod{11}$. Hence 7 is a primitive root of 11.

3. We need to show that 2 is a primitive root of 9. *How?*
   First, we find $\phi\left(9\right)$:
   $$\phi\left(9\right)=\phi\left(3^2\right)=9\left(1-\frac{1}{3}\right)=6\,.$$
   The divisors of 6 are 1, 2, 3 and 6. Evaluating these indices with base 2:
   $$2^1\equiv 2\not\equiv 1,\;\; 2^2\equiv 4\not\equiv 1,\;\; 2^3\equiv 8\not\equiv 1\left(\text{mod } 9\right).$$
   Hence the order of 2 is $6=\phi\left(9\right)$ so 2 is a primitive root modulo 9.

4. We are required to show that 5 is a primitive root of 49. We first evaluate $\phi\left(49\right)$:
   $$\phi\left(49\right)=\phi\left(7^2\right)=7^2\left(1-\frac{1}{7}\right)=42\,.$$
   The only divisors of 42 are 1, 2, 3, 6, 7 14, 21 and 42. Finding these indices with base 5:
   $$5^2\equiv 25\not\equiv 1\left(\text{mod } 49\right)$$
   $$5^3\equiv 125\equiv 27\not\equiv 1\left(\text{mod } 49\right)$$
   $$5^6\equiv 15625\equiv 43\not\equiv 1\left(\text{mod } 49\right)$$
   $$5^7\equiv 78125\equiv 19\not\equiv 1\left(\text{mod } 49\right)$$
   $$5^{14}\equiv 19^2\equiv 361\equiv 18\not\equiv 1\left(\text{mod } 49\right)$$
   $$5^{21}\equiv\left(5^7\right)^3\equiv 19^3\equiv 6859\equiv 48\not\equiv 1\left(\text{mod } 49\right)$$
   Hence the order of 5 modulo 49 is $42=\phi\left(49\right)$. Therefore 5 is a primitive root modulo 49.

5. This time we need to show that 7 is *not* a primitive root of 19. Since 19 is prime we have
   $$\phi\left(19\right)=19-1=18\,.$$
   The divisors of 18 are 1, 2, 3, 6, 9 and 18. Evaluating these indices to the base 7:
   $$7^2\equiv 49\equiv 11\not\equiv 1\left(\text{mod } 19\right)$$
   $$7^3\equiv 7^2\times 7\equiv 11\times 7\equiv 77\equiv 1\left(\text{mod } 19\right)$$
   Hence the order of 7 modulo 19 is 3 and $\phi\left(19\right)=18\neq 3$ so 7 is *not* a primitive root of 19.

6. We first need to find a primitive root of 11. We should first try 2 because it is the smallest positive integer after 1. Clearly 1 *cannot* be a primitive root of 11 because $1^1 \equiv 1 \pmod{11}$.

Since 11 is prime we have $\phi(11) = 10$ and the only divisors of 10 are 1, 2, 5 and 10.

$$2^2 \equiv 4 \pmod{11}$$
$$2^5 \equiv 32 \equiv 10 \pmod{11}$$

The order of 2 modulo 11 is 10 so it is a primitive root of 11. We use 2 as a base to find the order of the residues modulo 11. We have

$$2^1 \equiv 2 \pmod{11}$$
$$2^2 \equiv 4 \pmod{11}$$
$$2^3 \equiv 8 \pmod{11}$$
$$2^4 \equiv 16 \equiv 5 \pmod{11}$$
$$2^5 \equiv 32 \equiv 10 \pmod{11}$$
$$2^6 \equiv 10 \times 2 \equiv 20 \equiv 9 \pmod{11}$$
$$2^7 \equiv 9 \times 2 \equiv 18 \equiv 7 \pmod{11}$$
$$2^8 \equiv 7 \times 2 \equiv 14 \equiv 3 \pmod{11}$$
$$2^9 \equiv 3 \times 2 \equiv 6 \pmod{11}$$
$$2^{10} \equiv 6 \times 2 \equiv 12 \equiv 1 \pmod{11}$$

Creating a table of indices:

a	1	2	3	4	5	6	7	8	9	10
$\text{ind}_2(a)$	10	1	8	2	4	9	7	3	6	5

(a) We are required to solve the congruence $2x^4 \equiv 7 \pmod{11}$. We convert this $2x^4 \equiv 7 \pmod{11}$ to linear form by taking indices of both sides;

$$\text{ind}_2(2x^4) = \text{ind}_2(7).$$

Using the rules of indices of Proposition (6.16):

(a) $\text{ind}_r(ab) \equiv \text{ind}_r(a) + \text{ind}_r(b) \pmod{\phi(n)}$

(b) $\text{ind}_r(a^k) \equiv k\,\text{ind}_r(a) \pmod{\phi(n)}$

(c) $\text{ind}_r(1) \equiv 0 \pmod{\phi(n)}$ and $\text{ind}_r(r) \equiv 1 \pmod{\phi(n)}$.

On $\text{ind}_2(2x^4) = \text{ind}_2(7)$ with $\phi(11) = 10$ gives

$$\text{ind}_2(2) + \text{ind}_2(x^4) = \text{ind}_2(7) \pmod{10}$$

$$\text{ind}_2(2) + 4\,\text{ind}_2(x) = \text{ind}_2(7) \pmod{10} \qquad (*)$$

From the above table we have $\text{ind}_2(2) = 1$ and $\text{ind}_2(7) = 7$. Substituting these into (*) gives

$$1 + 4\,\text{ind}_2(x) \equiv 7 \pmod{10}$$
$$4\,\text{ind}_2(x) \equiv 6 \pmod{10}$$

The $\gcd(4,\ 10) = 2$ and $2 \mid 6$ therefore there are 2 solutions. From the last line we have

$$4\,\text{ind}_2(x) \equiv 6 \pmod{10} \Rightarrow 2\,\text{ind}_2(x) \equiv 3 \pmod{5}$$
$$\Rightarrow \text{ind}_2(x) \equiv 4 \pmod{5}$$

From $\text{ind}_2(x) \equiv 4 \pmod{5}$ we have $\text{ind}_2(x) = 4 + 5k$ where k is an integer. Since we have 2 solutions so substituting $k = 0,\ 1$ gives

$$\text{ind}_2(x) \equiv 4,\ 9 \pmod{10}$$

Using the above table in reverse direction yields

$$x \equiv 5,\ 6 \pmod{11}$$

(b) This time we need to solve the quadratic $3x^2 \equiv 5 \pmod{11}$. Again we use the above table and the rules of indices given in Proposition (6.16) to convert the given quadratic into linear form. We have

$$\text{ind}_2(3x^2) \equiv \text{ind}_2(5) \pmod{10}$$
$$\text{ind}_2(3) + \text{ind}_2(x^2) \equiv \text{ind}_2(5) \pmod{10}$$
$$\text{ind}_2(3) + 2\,\text{ind}_2(x) \equiv \text{ind}_2(5) \pmod{10}$$

By the above table we have $\text{ind}_2(3) = 8$ and $\text{ind}_2(5) = 4$. Putting these into the above derivation yields

$$8 + 2\,\text{ind}_2(x) \equiv 4 \pmod{10} \Rightarrow 2\,\text{ind}_2(x) \equiv -4 \equiv 6 \pmod{10}.$$

We need to solve this equation $2\,\text{ind}_2(x) \equiv 6 \pmod{10}$. The $\gcd(2,\ 10) = 2$ and $2 \mid 6$ so we have 2 solutions. Dividing $2\,\text{ind}_2(x) \equiv 6 \pmod{10}$ by the gcd gives

$$\text{ind}_2(x) \equiv 3 \pmod{5}.$$

Hence $\text{ind}_2(x) = 3 + 5k$. Substituting $k = 0,\ 1$ gives

$$\text{ind}_2(x) \equiv 3,\ 8 \pmod{10}.$$

Using the above table in reverse order yields

$$x \equiv 8,\ 3 \pmod{11}.$$

Our solutions are $x \equiv 3,\ 8 \pmod{11}$.

(c) We are required to solve the congruence $5x^5 \equiv 6 \pmod{11}$. We have

$$\text{ind}_2(5x^5) \equiv \text{ind}_2(6) \pmod{10}.$$

Using the rules of indices we have

$$\begin{aligned} \text{ind}_2(5) + \text{ind}_2(x^5) &\equiv \text{ind}_2(6) \pmod{10} \\ \text{ind}_2(5) + 5\,\text{ind}_2(x) &\equiv \text{ind}_2(6) \pmod{10} \\ 5\,\text{ind}_2(x) &\equiv \text{ind}_2(6) - \text{ind}_2(5) \pmod{10} \qquad (\dagger) \end{aligned}$$

By using the table which we established at the start of this question we have

$$\text{ind}_2(6) = 9 \text{ and } \text{ind}_2(5) = 4.$$

Putting these values into (†) gives

$$5\,\text{ind}_2(x) \equiv 9 - 4 \equiv 5 \pmod{10}.$$

The $\gcd(5,\ 10) = 5$ and $5 \mid 5$ so we have 5 incongruent solutions to this congruence. Dividing by 5 yields $\text{ind}_2(x) \equiv 1 \pmod{2}$.

This $\text{ind}_2(x) \equiv 1 \pmod{2}$ implies $\text{ind}_2(x) = 1 + 2k$ where k is an integer.

Substituting $k = 0,\ 1,\ 2,\ 3,\ 4$ gives

$$\text{ind}_2(x) \equiv 1,\ 3,\ 5,\ 7,\ 9 \pmod{10}.$$

Using the table again in reverse direction we have

$$\begin{aligned} x &\equiv 2,\ 8,\ 10,\ 7,\ 6 \\ &\equiv 2,\ 6,\ 7,\ 8,\ 10 \pmod{11} \end{aligned}$$

7. Since 19 is prime so $\phi(19) = 18$.

(a) We need to solve $6x^5 \equiv 7 \pmod{19}$. Converting this to linear form by taking ind_2 of both sides gives

$$\text{ind}_2(6x^5) \equiv \text{ind}_2(7) \pmod{18}.$$

Using the rules of indices gives

$$\text{ind}_2(6) + 5\,\text{ind}_2(x) \equiv \text{ind}_2(7) \pmod{18} \qquad (*)$$

Evaluating powers of 2;

$$2^5 \equiv 32 \equiv 13 \pmod{19},\ 2^6 \equiv 13 \times 2 \equiv 26 \equiv 7 \pmod{19}$$

Therefore $\text{ind}_2\left(7\right) = 6$. Working out other powers of 2 gives

$$2^7 \equiv 7 \times 2 \equiv 14 \left(\text{mod } 19\right) \text{ and } 2^{14} \equiv 14 \times 14 \equiv 196 \equiv 6 \left(\text{mod } 19\right).$$

So we have $\text{ind}_2\left(6\right) = 14$. Putting these $\text{ind}_2\left(6\right) = 14$ and $\text{ind}_2\left(7\right) = 6$ into (*) gives

$$\begin{aligned} 14 + 5\,\text{ind}_2\left(x\right) &\equiv 6 \ \left(\text{mod } 18\right) \\ 5\,\text{ind}_2\left(x\right) &\equiv 6 - 14 \equiv -8 \equiv 10 \ \left(\text{mod } 18\right) \end{aligned}$$

The $\gcd\left(5,\ 18\right) = 1$ and of course $1 \mid 10$ so we have a unique solution. Hence

$$5\,\text{ind}_2\left(x\right) \equiv 10 \quad \text{implies} \quad \text{ind}_2\left(x\right) \equiv 2 \ \left(\text{mod } 18\right)$$

From $\text{ind}_2\left(x\right) \equiv 2 \ \left(\text{mod } 18\right)$ we have $x \equiv 2^2 \equiv 4 \left(\text{mod } 19\right)$.

(b) We need to solve $4x^9 \equiv 4 \left(\text{mod } 19\right)$. Using the rules of indices we have

$$\begin{aligned} \text{ind}_2\left(4x^9\right) &\equiv \text{ind}_2\left(4\right) \left(\text{mod } 18\right) \\ \text{ind}_2\left(4\right) + \text{ind}_2\left(x^9\right) &\equiv \text{ind}_2\left(4\right) \ \left(\text{mod } 18\right) \\ \text{ind}_2\left(4\right) + 9\,\text{ind}_2\left(x\right) &\equiv \text{ind}_2\left(4\right) \ \left(\text{mod } 18\right) \quad \left[\text{Linear Form}\right] \end{aligned}$$

Clearly $\text{ind}_2\left(4\right) = 2$ because $2^2 \equiv 4 \left(\text{mod } 19\right)$. Substituting this into the above derivation gives

$$2 + 9\,\text{ind}_2\left(x\right) \equiv 2 \quad \Rightarrow \ 9\,\text{ind}_2\left(x\right) \equiv 0 \ \left(\text{mod } 18\right).$$

The $\gcd\left(9,\ 18\right) = 9$ and $9 \mid 0$ so the given equation has 9 incongruent solutions.

Dividing $9\,\text{ind}_2\left(x\right) \equiv 0 \left(\text{mod } 18\right)$ through by 9 gives

$$\text{ind}_2\left(x\right) \equiv 0 \left(\text{mod } 2\right).$$

Hence $\text{ind}_2\left(x\right) = 2k$ where k is an integer. Substituting $k = 1, 2, \cdots, 8, 9$ yields

$$\text{ind}_2\left(x\right) \equiv 2,\ 4,\ 6,\ 8,\ 10,\ 12,\ 14,\ 16,\ 18 \ \left(\text{mod } 18\right).$$

Therefore

$$\begin{aligned} x &\equiv 2^2,\ 2^4,\ 2^6,\ 2^8,\ 2^{10},\ 2^{12},\ 2^{14},\ 2^{16},\ 2^{18} \\ &\equiv 4,\ 16,\ \underbrace{7}_{\text{by part (a)}},\ 9,\ 17,\ 15,\ 11,\ 6,\ 5,\ 1 \left(\text{mod } 19\right) \quad \left[\begin{array}{l}\text{Multiplying the} \\ \text{previous term by } 2^2 = 4\end{array}\right] \end{aligned}$$

Putting the residues into ascending order

$$x \equiv 1,\ 4,\ 5,\ 6,\ 7,\ 9,\ 11,\ 16,\ 17 \ \left(\text{mod } 19\right).$$

(c) We are required to solve $x^6 \equiv 7 \left(\text{mod } 19\right)$. Taking ind_2 of both sides gives

$$\begin{aligned}\operatorname{ind}_2\left(x^6\right) &\equiv \operatorname{ind}_2(7) \pmod{18}\\ 6\operatorname{ind}_2(x) &\equiv \operatorname{ind}_2(7) \underbrace{\equiv}_{\text{by part (a)}} 6 \pmod{18}\end{aligned}$$

We must find a solution of $6\operatorname{ind}_2(x) \equiv 6 \pmod{18}$. The $\gcd(6,\ 18) = 6$ and $6 \mid 6$ so we have 6 incongruent solutions. Dividing through by 6 gives

$$\operatorname{ind}_2(x) \equiv 1 \pmod{3}.$$

Hence $\operatorname{ind}_2(x) = 1 + 3k$ where k is an integer. Since we have 6 solutions so substituting $k = 0,\ 1,\ 2,\ 3,\ 4,\ 5$ gives

$$\operatorname{ind}_2(x) \equiv 1,\ 4,\ 7,\ 10,\ 13,\ 16 \pmod{18}.$$

Therefore

$$\begin{aligned}x &\equiv 2^1,\ 2^4,\ 2^7,\ 2^{10},\ 2^{13},\ 2^{16}\\ &\equiv 2,\ 16,\ 14,\ 17,\ 2^{13},\ 5 \pmod{19} \quad [\text{By parts (a) and (b)}]\end{aligned}$$

We still need to find $x \equiv 2^{13} \pmod{19}$. Well

$$2^{13} \equiv 2^7 \times 2^6 \equiv 14 \times 7 \equiv 98 \equiv 3 \pmod{19}$$

Placing these residues into ascending order gives

$$x \equiv 2,\ 3,\ 5,\ 14,\ 16,\ 17 \pmod{19}$$

8. First we show that 3 is a primitive root of 17. We have $\phi(17) = 16$.

The divisors of 16 are 1, 2, 4, 8 and 16. Finding the indices of these with base 3:

$$\begin{aligned}3^2 &\equiv 9 \not\equiv 1 \pmod{17}\\ 3^4 &\equiv 9^2 \equiv 81 \equiv 13 \not\equiv 1 \pmod{17}\\ 3^8 &\equiv \left(3^4\right)^2 \equiv 13^2 \equiv 169 \equiv 16 \not\equiv 1 \pmod{17}\end{aligned}$$

Hence 3 is a primitive root of 17 because the order of 3 modulo 17 is $\phi(17) = 16$.

Evaluating the indices of 3:

$$\begin{aligned}3 &\equiv 3 \pmod{17}\\ 3^2 &\equiv 9 \pmod{17}\\ 3^3 &\equiv 9 \times 3 \equiv 27 \equiv 10 \pmod{17}\\ 3^4 &\equiv 13 \pmod{17}\\ 3^5 &\equiv 13 \times 3 \equiv 39 \equiv 5 \pmod{17}\\ 3^6 &\equiv 5 \times 3 \equiv 15 \pmod{17}\\ 3^7 &\equiv (-2) \times 3 \equiv -6 \equiv 11 \pmod{17}\end{aligned}$$

$$3^8 \equiv 16 \pmod{17}$$
$$3^9 \equiv (-1)\times 3 \equiv -3 \equiv 14 \pmod{17}$$
$$3^{10} \equiv (-3)\times 3 \equiv -9 \equiv 8 \pmod{17}$$
$$3^{11} \equiv 8\times 3 \equiv 24 \equiv 7 \pmod{17}$$
$$3^{12} \equiv 7\times 3 \equiv 21 \equiv 4 \pmod{17}$$
$$3^{13} \equiv 4\times 3 \equiv 12 \pmod{17}$$
$$3^{14} \equiv 12\times 3 \equiv 36 \equiv 2 \pmod{17}$$
$$3^{15} \equiv 2\times 3 \equiv 6 \pmod{17}$$
$$3^{16} \equiv 1 \pmod{17}$$

Using this information to complete the table:

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\text{ind}_3(a)$	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

We use this table to solve the given equations.

(a) We are given the equation $x^4 \equiv 4 \pmod{17}$. Taking ind_3 of both sides gives

$$\text{ind}_3(x^4) \equiv \text{ind}_3(4) \pmod{16}$$

Using the established rules of indices given in Proposition (6.16):

(a) $\text{ind}_r(ab) \equiv \text{ind}_r(a) + \text{ind}_r(b) \pmod{\phi(n)}$

(b) $\text{ind}_r(a^k) \equiv k\,\text{ind}_r(a) \pmod{\phi(n)}$

(c) $\text{ind}_r(1) \equiv 0 \pmod{\phi(n)}$ and $\text{ind}_r(r) \equiv 1 \pmod{\phi(n)}$.

We have

$$4\,\text{ind}_3(x) \equiv \text{ind}_3(4) \pmod{16}. \qquad \text{[Linear Form]}$$

By the above table we have $\text{ind}_3(4) = 12$. Substituting this into the above yields

$$4\,\text{ind}_3(x) \equiv 12 \pmod{16}.$$

The $\gcd(4,\ 16) = 4$ and $4 \mid 12$ so we have 4 solutions. Dividing this

$$4\,\text{ind}_3(x) \equiv 12 \pmod{16}$$

by 4 gives

$$\text{ind}_3(x) \equiv 3 \pmod{4}.$$

This $\text{ind}_3(x) \equiv 3 \pmod{4}$ implies that $\text{ind}_3(x) = 3 + 4k$. As we have 4 solutions so substitute $k = 0,\ 1,\ 2,\ 3$ into $\text{ind}_3(x) = 3 + 4k$:

$$\text{ind}_3\left(x\right) \equiv 3,\ 7,\ 11,\ 15\ \left(\text{mod } 16\right).$$

Finding these numbers in the bottom row and reading the corresponding numbers in the top row we have

$$x \equiv 10,\ 11,\ 7,\ 6\ \left(\text{mod } 17\right).$$

Putting these in ascending order of residues we have $x \equiv 6,\ 7,\ 10,\ 11\ \left(\text{mod } 17\right)$.

(b) We need to solve $12x^8 \equiv 5\left(\text{mod } 17\right)$. Using ind_3 we have

$$\text{ind}_3\left(12x^8\right) \equiv \text{ind}\left(5\right)\left(\text{mod } 16\right)$$
$$\text{ind}_3\left(12\right) + 8\ \text{ind}_3\left(x\right) \equiv \text{ind}_3\left(5\right)\left(\text{mod } 16\right) \qquad \left[\text{Linear Form}\right]$$

By the above table we have $\text{ind}_3\left(12\right) = 13$ and $\text{ind}_3\left(5\right) = 5$. Putting this into the above derivation yields

$$13 + 8\ \text{ind}_3\left(x\right) \equiv 5 \quad \Rightarrow \quad 8\ \text{ind}_3\left(x\right) \equiv 5 - 13 \equiv -8 \equiv 8\left(\text{mod } 16\right).$$

The $\gcd\left(8,\ 16\right) = 8$ and $8 \mid 8$ so we have 8 incongruent solutions. Therefore

$$8\ \text{ind}_3\left(x\right) \equiv 8\left(\text{mod } 16\right) \ \Rightarrow\ \text{ind}_3\left(x\right) \equiv 1\left(\text{mod } 2\right).$$

Our 8 solutions are $\text{ind}_3\left(x\right) = 1 + 2k$ for $k = 0,\ 1,\ \cdots,\ 7$:

$$\text{ind}_3\left(x\right) \equiv 1,\ 3,\ 5,\ 7,\ 9,\ 11,\ 13,\ 15\ \left(\text{mod } 16\right).$$

Locating these in the bottom row of the table and reading off corresponding entries in the top row gives

$$x \equiv 3,\ 10,\ 5,\ 11,\ 14,\ 7,\ 12,\ 6\ \left(\text{mod } 17\right)$$

Putting these in order gives

$$x \equiv 3,\ 5,\ 6,\ 7,\ 10,\ 11,\ 12,\ 14\left(\text{mod } 17\right)$$

(c) This time we have a very similar equation to part (b) with only the residue on the right - hand side is 6 rather than 5. We can use the answer to part (b) to solve this $12x^8 \equiv 6\left(\text{mod } 17\right)$ equation.

$$\text{ind}_3\left(12x^8\right) \equiv \text{ind}_3\left(6\right)\left(\text{mod } 16\right)$$
$$\text{ind}_3\left(12\right) + 8\ \text{ind}_3\left(x\right) \equiv \text{ind}_3\left(6\right)\left(\text{mod } 16\right)$$

We have $\text{ind}_3\left(12\right) = 13$ and $\text{ind}_3\left(6\right) = 15$ so

$$13 + 8\ \text{ind}_3\left(x\right) \equiv 15 \ \Rightarrow\ 8\ \text{ind}_3\left(x\right) \equiv 15 - 13 \equiv 2\left(\text{mod } 16\right).$$

This time we have to solve $8\ \text{ind}_3\left(x\right) \equiv 2\left(\text{mod } 16\right)$. *How?*

First, we check that the $\gcd\left(8,\ \ 16\right)=8$ divides the right-hand side. However, $8 \not| 2$ so the given equation has *no* solution.

(d) We are required to solve $5^x \equiv 3 \left(\mathrm{mod}\ 17\right)$. Using ind_3 on this congruence

$$\mathrm{ind}_3\left(5^x\right) \equiv \mathrm{ind}_3\left(3\right) \left(\mathrm{mod}\ 16\right)$$
$$x\ \mathrm{ind}_3\left(5\right) \equiv \mathrm{ind}_3\left(3\right) \left(\mathrm{mod}\ 16\right)$$

By using the above table we have $\mathrm{ind}_3\left(5\right)=5$ and $\mathrm{ind}_3\left(3\right)=1$. Substituting this gives

$$5x \equiv 1 \left(\mathrm{mod}\ 16\right).$$

The $\gcd\left(5,\ \ 16\right)=1$ and $1 \mid 1$ so we have a unique solution. Hence our solution is

$$x \equiv 13 \left(\mathrm{mod}\ 16\right).$$

9. We need to find x the least non-negative residue such that $7^{100}6^{100} \equiv x \left(\mathrm{mod}\ 17\right)$.

Taking ind_3 of this we get

$$\mathrm{ind}_3\left(7^{100}6^{100}\right) \equiv \mathrm{ind}_3\left(x\right) \left(\mathrm{mod}\ 16\right).$$

Using the rules of indices established in Proposition (6.16) we have

$$\mathrm{ind}_3\left(7^{100}\right) + \mathrm{ind}_3\left(6^{100}\right) \equiv \mathrm{ind}_3\left(x\right) \left(\mathrm{mod}\ 16\right)$$
$$100\ \mathrm{ind}_3\left(7\right) + 100\ \mathrm{ind}_3\left(6\right) \equiv \mathrm{ind}_3\left(x\right) \left(\mathrm{mod}\ 16\right)$$
$$100\left[\mathrm{ind}_3\left(7\right) + \mathrm{ind}_3\left(6\right)\right] \equiv \mathrm{ind}_3\left(x\right) \left(\mathrm{mod}\ 16\right)$$
$$\underbrace{4}_{\text{because } 100\equiv 4 \left(\mathrm{mod}\ 16\right)} \left[\mathrm{ind}_3\left(7\right) + \mathrm{ind}_3\left(6\right)\right] \equiv \mathrm{ind}_3\left(x\right) \left(\mathrm{mod}\ 16\right) \qquad (\dagger)$$

By the table of the previous question, which is duplicated here:

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\mathrm{ind}_3\left(a\right)$	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

We have $\mathrm{ind}_3\left(7\right)=11$ and $\mathrm{ind}_3\left(6\right)=15$. Putting these into $(\dagger)$ gives

$$4\left[11+15\right] \equiv 4\left[26\right] \equiv 4\left[10\right] \equiv 40 \equiv 8 \equiv \mathrm{ind}_3\left(x\right) \left(\mathrm{mod}\ 16\right).$$

We have $\mathrm{ind}_3\left(x\right) \equiv 8 \left(\mathrm{mod}\ 16\right)$. By using the above table in reverse direction

$$x \equiv 16 \left(\mathrm{mod}\ 17\right).$$

The least non-negative residue is 16 modulo 17, that is $7^{100}6^{100} \equiv 16 \left(\mathrm{mod}\ 17\right)$.

10. (a) We have to solve $7^x \equiv 3 \pmod{13}$. Using the given table:

a	1	2	3	4	5	6	7	8	9	10	11	12
$\text{ind}_2(a)$	12	1	4	2	9	5	11	3	8	10	7	6

Taking ind_2 of both sides of $7^x \equiv 3 \pmod{13}$ we have

$$\begin{aligned} \text{ind}_2(7^x) &\equiv \text{ind}_2(3) \pmod{12} \\ x\,\text{ind}_2(7) &\equiv \text{ind}_2(3) \pmod{12} \\ 11x \equiv 4 \pmod{12} &\Rightarrow x \equiv 8 \pmod{12} \end{aligned}$$

Our solution is $x \equiv 8 \pmod{13}$.

(b) We need to find the remainder of $5^{100}7^{50}9^{99}$ after dividing by 13. This means solving the equation $5^{100}7^{50}9^{99} \equiv x \pmod{13}$ where x is the least non-negative residue.

Applying ind_2 of both sides of $5^{100}7^{50}9^{99} \equiv x \pmod{13}$ and using the rules of indices

$$\begin{aligned} \text{ind}_2(5^{100}7^{50}9^{99}) &\equiv \text{ind}_2(x) \pmod{12} \\ \text{ind}_2(5^{100}) + \text{ind}_2(7^{50}) + \text{ind}_2(9^{99}) &\equiv \text{ind}_2(x) \pmod{12} \\ 100\,\text{ind}_2(5) + 50\,\text{ind}_2(7) + 99\,\text{ind}_2(9) &\equiv \text{ind}_2(x) \pmod{12} \\ \underbrace{4}_{\text{Because } 100\equiv 4 \pmod{12}}\text{ind}_2(5) + \underbrace{2}_{50\equiv 2 \pmod{12}}\text{ind}_2(7) + \underbrace{3}_{99\equiv 3 \pmod{12}}\text{ind}_2(9) &\equiv \text{ind}_2(x) \pmod{12} \qquad (*) \end{aligned}$$

By the given table we have

$$\text{ind}_2(5) = 9,\ \text{ind}_2(7) = 11 \ \text{ and} \ \ \text{ind}_2(9) = 8\,.$$

Substituting these into (*) gives

$$\begin{aligned} (4\times 9) + (2\times 11) + (3\times 8) &\equiv \text{ind}_2(x) \pmod{12} \\ 82 \equiv 10 &\equiv \text{ind}_2(x) \pmod{12} \end{aligned}$$

From the given table we have $\text{ind}_2(x) = 10 \pmod{12}$ gives

$$x \equiv 10 \pmod{13}.$$

Dividing $5^{100}7^{50}9^{99}$ by 13 gives remainder 10.

(c) First, we establish under what conditions the given congruence has solutions. We need to find a such that $x^a \equiv 9 \pmod{13}$ has solutions. Taking ind_2 of this:

$$\begin{aligned} \text{ind}_2(x^a) &\equiv \text{ind}_2(9) \pmod{12} \\ a\,\text{ind}_2(x) &\equiv \text{ind}_2(9) \pmod{12} \quad [\text{Linear Form}] \end{aligned}$$

By the given table $\text{ind}_2(9) = 8$. Putting this into the above derivation

$$a \operatorname{ind}_2(x) \equiv 8 \pmod{12}.$$

Let $g = \gcd(a, 12)$. Hence this congruence can only have solutions if $g \mid 8$. The only divisors of 8 are 1, 2, 4 and 8. Therefore we can only have solutions provided

$$g = 1, \quad g = 2, \quad g = 4, \quad g = 8.$$

The integers a which are relatively prime to 12, that is $g = 1$ are

1, 5, 7 and 11.

The integers a such that $\gcd(a, 12) = 2$ are

2 and 10.

The integers a such that $\gcd(a, 12) = 4$ are

4, 8

We cannot have $\gcd(a, 12) = 8$ because $8 \not| 12$.

Summarizing these results, we have solutions if a is 1, 2, 4, 5, 7, 8, 10 and 11.

The remaining natural numbers below 12 are 3, 6, 9 and 12.

Hence if $a = 3, \ 6, \ 9, \ 12$ we have *no* solutions.

11. We need to find a such that $ax^6 \equiv 8 \pmod{17}$. We have already established a table for the primitive root 3 of 17 in question 8:

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\operatorname{ind}_3(a)$	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

Using ind_3 to convert into linear form on the given equation yields

$$\operatorname{ind}_3(a) + 6 \operatorname{ind}_3(x) \equiv \operatorname{ind}_3(8) \pmod{16}$$
$$\operatorname{ind}_3(a) + 6 \operatorname{ind}_3(x) \equiv 10 \pmod{16}$$
$$6 \operatorname{ind}_3(x) \equiv 10 - \operatorname{ind}_3(a) \pmod{16} \qquad (\dagger)$$

The $\gcd(6, 16) = 2$ so the equation $(\dagger)$ will only have a solution if

$$2 \mid [10 - \operatorname{ind}_3(a)] \quad \text{or} \quad 10 - \operatorname{ind}_3(a) = 2k.$$

By examining the bottom row of the table we know this $10 - \operatorname{ind}_3(a) = 2k$ is satisfied if $\operatorname{ind}_3(a)$ is even:

$$\operatorname{ind}_3(a) = 16, \ 14, \ 12, \ 10, \ 2, \ 4, \ 6, \ 8$$

Using the table in the reverse direction therefore

$$a \equiv 1, \ 2, \ 4, \ 8, \ 9, \ 13, \ 15, \ 16 \pmod{17}.$$

The integer a must satisfy $1 \le a \le 16$ so

$$a = 1,\ 2,\ 4,\ 8,\ 9,\ 13,\ 15,\ 16\,.$$

12. For this question we use Proposition (6.17):

> Let n have a primitive root and $\gcd\left(a,\ n\right) = 1$. The congruence
>
> $$x^m \equiv a \pmod{n}$$
>
> has a solution $\Leftrightarrow$
>
> $$a^{\phi(n)/g} \equiv 1 \pmod{n} \text{ where } g = \gcd\left(m,\ \phi\left(n\right)\right).$$

(a) We are given the cubic equation $x^3 \equiv 89 \pmod{197}$. Both 89 and 197 are prime so $\gcd\left(89,\ 197\right) = 1$. We also need to evaluate $\phi\left(197\right)$ which is equal to 196. Let

$$g = \gcd\left(3,\ 196\right) = 1\,.$$

For the given equation to have a solution we have to check that

$$89^{196/1} \equiv 89^{196} \equiv 1 \pmod{197}.$$

By Euler's Theorem (5.14):

> $$a^{\phi(n)} \equiv 1 \pmod{n}$$

The above result $89^{196} \equiv 1 \pmod{197}$ is true so the given congruence

$$x^3 \equiv 89 \pmod{197}$$

is solvable.

(b) We have the same numbers as part (a) except the index this time is 2 (quadratic rather than cubic). We have $g = \gcd\left(2,\ 196\right) = 2$.

We must check whether

$$89^{196/2} \equiv 89^{98} \equiv 1 \pmod{197}.$$

Let $x = 89^{98}$ then

$$x^2 \equiv 1 \pmod{197} \ \Rightarrow\ x \equiv 1 \pmod{197} \ \text{ or } \ x \equiv -1 \pmod{197}.$$

We only need to check *some* of the divisors of 98 which are 1, 2, 7, 14, 49, 98 :

$$89^2 \equiv 7921 \equiv 41 \pmod{197}$$

$$89^7 \equiv \left(89^2\right)^3 89 \equiv 41^3 \times 89$$

$$\equiv 68921 \times 89 \equiv 168 \times 89 \equiv 14952 \equiv 177 \equiv -20 \pmod{197}$$

$$89^{14} \equiv \left(89^7\right)^2 \equiv \left(-20\right)^2 \equiv 400 \equiv 6 \left(\text{mod } 197\right)$$

$$89^{98} \equiv \left(89^{14}\right)^7 \equiv 6^7 \equiv 279936 \equiv 196 \equiv -1 \left(\text{mod } 197\right)$$

Hence $89^{98} \not\equiv 1 \left(\text{mod } \ 197\right)$ therefore the given equation $x^2 \equiv 89 \left(\text{mod } 197\right)$ is *not* solvable.

(c) This time we need to check whether $x^2 \equiv 197 \left(\text{mod } 89\right)$ is solvable. First note that $197 \equiv 19 \left(\text{mod } 89\right)$ which means we look at the equivalent equation

$$x^2 \equiv 19 \left(\text{mod } 89\right).$$

We have $\phi\left(89\right) = 88$ and the $\gcd\left(2, \ \ 88\right) = 2$. By the above Proposition (6.17) the equation $x^2 \equiv 19 \left(\text{mod } 89\right)$ has a solution if and only if

$$19^{88/2} \ \equiv 19^{44} \equiv 1 \left(\text{mod } \ 89\right).$$

Examining the powers of some of the divisors of 44:

$$19^2 \equiv 361 \equiv 5 \left(\text{mod } 89\right).$$

$$\begin{aligned} 19^{11} &\equiv \left(19^2\right)^5 \times 19 \\ &\equiv 5^5 \times 19 \equiv 3125 \times 19 \equiv 10 \times 19 \equiv 190 \equiv 12 \left(\text{mod } 89\right) \end{aligned}$$

$$19^{44} \equiv \left(19^{11}\right)^4 \equiv 12^4 \equiv 20736 \equiv 88 \equiv -1 \left(\text{mod } 89\right)$$

Hence the equation $x^2 \equiv 197 \left(\text{mod } 89\right)$ has *no* solutions.

(d) We need to check if $x^2 \equiv 218 \left(\text{mod } 111\right)$ is solvable. First note that

$$218 \equiv -4 \left(\text{mod } 111\right).$$

We see if we can solve the easier equivalent equation $x^2 \equiv -4 \left(\text{mod } 111\right)$. *How?*

By using Proposition (6.17):

Let n have a primitive root and $\gcd\left(a, \ \ n\right) = 1$. The congruence

$$x^m \equiv a \ \ \left(\text{mod } \ n\right)$$

has a solution $\Leftrightarrow$

$$a^{\phi(n)/g} \ \equiv 1 \left(\text{mod } \ n\right) \text{ where } g = \gcd\left(m, \ \ \phi\left(n\right)\right).$$

We need to find $\phi\left(111\right)$. The prime decomposition of 111 is $111 = 3 \times 37$.

The Euler totient function $\phi\left(111\right)$ is given by

$$\phi\left(111\right) = \phi\left(3\right) \times \phi\left(37\right) = 2 \times 36 = 72.$$

Let $g = \gcd\left(2, \quad 72\right) = 2$. We need to check whether

$$\left(-4\right)^{72/2} \equiv \left(-2\right)^{72} \equiv 2^{72} \equiv 1 \left(\mathrm{mod}\ 111\right).$$

We use Euler's Theorem (5.14):

$$a^{\phi(n)} \equiv 1 \ \left(\mathrm{mod}\ n\right)$$

Since $\phi\left(111\right) = 72$ so $2^{72} \equiv 1 \left(\mathrm{mod}\ 111\right)$. Therefore, the given quadratic equation

$$x^2 \equiv 218 \left(\mathrm{mod}\ 111\right)$$

is solvable.

13. Again, we use Proposition (6.17):

Let n have a primitive root and $\gcd\left(a, \ n\right) = 1$. The congruence

$$x^m \equiv a \ \left(\mathrm{mod} \ \ n\right)$$

has a solution $\Leftrightarrow$

$$a^{\phi(n)/g} \ \equiv 1 \left(\mathrm{mod} \ \ n\right) \text{ where } g = \gcd\left(m, \ \phi\left(n\right)\right).$$

(a) We have to find the number of solutions of $x^3 \equiv 2 \left(\mathrm{mod}\ 29\right)$. We know that 29 is prime so $\phi\left(29\right) = 28$. The $\gcd\left(3, \quad 28\right) = 1$ so we have solutions provided

$$2^{28/1} \ \equiv 2^{28} \equiv 1 \left(\mathrm{mod} \ \ 29\right).$$

By Euler's Theorem (5.14):

$$a^{\phi(n)} \equiv 1 \ \left(\mathrm{mod}\ n\right)$$

We have $2^{28} \equiv 1 \left(\mathrm{mod} \ \ 29\right)$ so $x^3 \equiv 2 \left(\mathrm{mod}\ 29\right)$ has solution(s). As $\gcd\left(3, \quad 28\right) = 1$ therefore we have a unique solution.

(b) We have to find the number of solutions of $x^{16} \equiv 25 \left(\mathrm{mod}\ 29\right)$. The

$$\gcd\left(16, \quad 28\right) = 4.$$

The given equation will have solutions provided

$$25^{28/4} \ \equiv 25^7 \equiv 1 \left(\mathrm{mod} \ \ 29\right).$$

We need to find powers of 25. To reduce the arithmetic we note that

$$25 \equiv -4 \left(\mathrm{mod} \ \ 29\right).$$

It is simpler to evaluate $\left(-4\right)^7 \equiv ? \left(\mathrm{mod} \ \ 29\right)$:

$$\left(-4\right)^3 \equiv -64 \equiv -6 \left(\text{mod } 29\right)$$

$$\begin{aligned}\left(-4\right)^7 &\equiv \left(-4\right)^6 \times \left(-4\right) \\ &\equiv \left[\left(-4\right)^3\right]^2 \times \left(-4\right) \\ &\equiv \left(-6\right)^2 \times \left(-4\right) \\ &\equiv 36 \times \left(-4\right) \equiv 7 \times \left(-4\right) \equiv -28 \equiv 1 \left(\text{mod } 29\right)\end{aligned}$$

Since $\left(-4\right)^7 \equiv 1 \left(\text{mod } 29\right)$ so the given equation has solutions. Because $\gcd\left(16, \ 28\right) = 4$ so we have 4 incongruent solutions to $x^{16} \equiv 25 \left(\text{mod } 29\right)$.

14. (i) We are asked to show that 3 is a primitive root of modulo 223. First $\gcd\left(3, \ 223\right) = 1$ so 3 could be a primitive root. We are given that 223 is prime so $\phi\left(223\right) = 222$ and divisors of 222 are $\{1, 2, 3, 6, 37, 74, 111, 222\}$. We need to evaluate each of these indices $\{1, 2, 3, 6, 37, 74, 111, 222\}$ with base 3 and show that the last index, 222, is the only one which gives $1\left(\text{mod } 223\right)$. We know this index does by Euler's Theorem. Clearly the first three indices don't. Computing the remaining indices to the base 3 gives

$$3^6 \equiv 729 \equiv 60 \not\equiv 1\left(\text{mod } 223\right)$$

$$\begin{aligned}3^{37} &\equiv \left(3^6\right)^6 \times 3 \equiv 60^6 \times 3 \equiv \left(60^2\right)^3 \times 3 \\ &\equiv \left(3600\right)^3 \times 3 \equiv 32^3 \times 3 \equiv 32\,768 \times 3 \\ &\equiv 210 \times 3 \equiv 630 \equiv 184 \equiv -39 \not\equiv 1\left(\text{mod } 223\right) \quad (\dagger)\end{aligned}$$

$$3^{74} \equiv \left(3^{37}\right)^2 \equiv \left(-39\right)^2 \equiv 1521 \equiv 183 \equiv -40 \not\equiv 1\left(\text{mod } 223\right) \qquad (*)$$

$$3^{111} \equiv 3^{74} \times 3^{37} \equiv \left(-40\right) \times \left(-39\right) \equiv 1560 \equiv 222 \equiv -1\left(\text{mod } 223\right) \qquad (**)$$

Hence 3 is a primitive root of modulo 223.

(ii) We are asked to solve $x^2 \equiv 183\left(\text{mod } 223\right)$. Taking indices of both sides to the base 3 gives $2 \text{ ind}_3\left(x\right) \equiv \text{ind}_3\left(183\right)\left(\text{mod } 222\right)$. From (*) we have

$$\text{ind}_3\left(183\right) = 74 .$$

Substituting this $\text{ind}_3\left(183\right) = 74$ into $2 \text{ ind}_3\left(x\right) \equiv \text{ind}_3\left(183\right)\left(\text{mod } 222\right)$ gives

$$2 \text{ ind}_3\left(x\right) \equiv 74\left(\text{mod } 222\right).$$

The $\gcd\left(2, \ 222\right) = 2$ and $2 \mid 74$ so there are two incongruent solutions to the given quadratic. We can divide both sides of the above congruence by 2:

$$\text{ind}_3\left(x\right) \equiv 37 \left(\text{mod } 111\right) \;\Rightarrow\; \text{ind}_3\left(x\right) \equiv 37,\; 37+111=37,\; 148 \left(\text{mod } 222\right)$$

The x values are given by

$$x \equiv 3^{37},\; 3^{148} \left(\text{mod } 223\right)$$

We computed the first of these in part (i) (†):

$$x \equiv 3^{37} \equiv 184 \left(\text{mod } 223\right)$$

By Proposition (3.14) (b) we have

$$a^2 \equiv b^2 \left(\text{mod } p\right) \;\Leftrightarrow\; a \equiv \pm b \left(\text{mod } p\right)$$

This says that if $x \equiv 184 \left(\text{mod } 223\right)$ is a solution then so is

$$x \equiv -184 \equiv 39 \left(\text{mod } 223\right).$$

Our solutions are $x \equiv 39,\; 184 \left(\text{mod } 223\right)$ to the quadratic $x^2 \equiv 183 \left(\text{mod } 223\right)$.

We also need to solve the Diophantine equation $x^2 = 183 + 223y$. The given congruence $x^2 \equiv 183 \left(\text{mod } 223\right)$ means that x^2 is 183 more than a multiple of 223; that is $x^2 = 183 + 223y$. Using the solution $x = 39$ gives

$$39^2 = 183 + 223y \;\Rightarrow\; y = \frac{39^2 - 183}{223} = 6$$

Hence $x = 39,\; y = 6$ is a solution. Another solution can be obtained by substituting $x = 184$ which gives

$$184^2 = 183 + 223y \;\Rightarrow\; y = \frac{184^2 - 183}{223} = 151$$

Therefore $x = 184,\; y = 151$ is also a solution.

(iii) This time we have to solve the cubic $x^3 \equiv -1 \left(\text{mod } 223\right)$. The procedure is identical to part (ii). Taking indices gives

$$3\,\text{ind}_3\left(x\right) \equiv \text{ind}_3\left(-1\right) \left(\text{mod } 222\right) \quad \left[\text{Linear Form}\right]$$

From (**) of part (i) we have

$$\text{ind}_3\left(-1\right) = 111.$$

Substituting this into the above congruence yields

$$3\,\text{ind}_3\left(x\right) \equiv 111 \left(\text{mod } 222\right)$$

The $\gcd\left(3,\; 222\right) = 3$ and $3 \mid 111$ therefore the cubic congruence has three incongruent solutions. Simplifying $3\,\text{ind}_3\left(x\right) \equiv 111 \left(\text{mod } 222\right)$ gives

$$\text{ind}_3\left(x\right) \equiv 37 \left(\text{mod } 74\right)$$

By the definition of congruence we have $ind_3\left(x\right) = 37 + 74k$ where k is an integer. Substituting $k = 0, 1, 2$ into this yield

$$\text{ind}_3\left(x\right) \equiv 37,\, 37 + 74,\, 37 + 2\left(74\right) \equiv 37, 111, 185 \left(\text{mod } 222\right).$$

Our three solutions are given by

$$x \equiv 3^{37}, 3^{111},\, 3^{185} \left(\text{mod } 223\right)$$

The first two have been evaluated in part (i) by (†) and (**):

$$x \equiv 3^{37}, 3^{111} \equiv 184,\, 222 \left(\text{mod } 223\right)$$

Just need to compute the last index 185 to the base 3:

$$x \equiv 3^{185} \equiv 3^{111} \times 3^{74} \equiv \left(-1\right) \times \left(-40\right) \equiv 40 \left(\text{mod } 223\right)$$

Our solutions to $x^3 \equiv -1 \left(\text{mod } 223\right)$ are $x \equiv 40, 184, 222 \left(\text{mod } 223\right)$.

To solve the Diophantine equation, we have $x^3 \equiv -1 \left(\text{mod } 223\right)$ which implies that x^3 is one less than a multiple of 223 so

$$x^3 = 223y - 1$$

Transposing this we have $y = \dfrac{x^3 + 1}{223}$. Substituting $x = 40, 184, 222$ into this gives

$$y = \frac{40^3 + 1}{223} = 287$$

$$y = \frac{184^3 + 1}{223} = 27\ 935$$

$$y = \frac{222^3 + 1}{223} = 49\ 063$$

Our solutions are $\left\{x = 40,\ y = 287\right\}$, $\left\{x = 184,\ \ y = 27\ 935\right\}$ and $\left\{x = 222,\ \ y = 49\ 063\right\}$.

15. (a) We are asked to show that $1 \le \text{ind}_r\left(a\right) \le \phi\left(n\right)$.

Proof.

We are given that r is a primitive root of n. Therefore, the order of r is $\phi\left(n\right)$. The integer a is relatively prime to n so

$$r^{\text{ind}_r\left(a\right)} \equiv a \left(\text{mod } n\right).$$

The integer a is a member of the reduced residue system modulo n therefore the index of r which generators a must be $\le \phi\left(n\right)$. Hence $1 \le \text{ind}_r\left(a\right) \le \phi\left(n\right)$ which is our required result.

■

(b) We need to show that Proposition (6.16) part (c):

Proof.

Need to prove $\text{ind}_r\left(1\right) \equiv 0 \pmod{\phi\left(n\right)}$ and $\text{ind}_r\left(r\right) \equiv 1 \pmod{\phi\left(n\right)}$:

By (6.13):

$$r^{\text{ind}_r(a)} \equiv a \pmod{n}$$

We have

$$r^{\text{ind}_r(1)} \equiv 1 \pmod{n}.$$

Also $r^0 \equiv 1 \pmod{n}$. Equating these we have

$$r^{\text{ind}_r(1)} \equiv r^0 \pmod{n}.$$

Applying Proposition (6.6) to this gives

$$\text{ind}_r\left(1\right) \equiv 0 \pmod{\phi\left(n\right)}.$$

For $\text{ind}_r\left(r\right) \equiv 1 \pmod{\phi\left(n\right)}$ is Proposition (6.14).

■

16. The given equation $7x^6 \equiv 6 \pmod{13}$ is the same as the one in Example 19 but we are asked to use the primitive root 7 modulo 13:

$$\begin{aligned}
7^1 &\equiv 7 \pmod{13} \\
7^2 &\equiv 49 \equiv 10 \pmod{13} \\
7^3 &\equiv 10 \times 7 \equiv 70 \equiv 5 \pmod{13} \\
7^4 &\equiv 5 \times 7 \equiv 35 \equiv 9 \pmod{13} \\
7^5 &\equiv 9 \times 7 \equiv 63 \equiv 11 \pmod{13} \\
7^6 &\equiv 11 \times 7 \equiv 77 \equiv 12 \pmod{13} \\
7^7 &\equiv (-1) \times 7 \equiv -7 \equiv 6 \pmod{13} \\
7^8 &\equiv 6 \times 7 \equiv 42 \equiv 3 \pmod{13} \\
7^9 &\equiv 3 \times 7 \equiv 21 \equiv 8 \pmod{13} \\
7^{10} &\equiv 8 \times 7 \equiv 56 \equiv 4 \pmod{13} \\
7^{11} &\equiv 4 \times 7 \equiv 28 \equiv 2 \pmod{13} \\
7^{12} &\equiv 1 \pmod{13}
\end{aligned}$$

The table for primitive root 7 is:

a	1	2	3	4	5	6	7	8	9	10	11	12
$\text{ind}_7(a)$	12	11	8	10	3	7	1	9	4	2	5	6

For $7x^6 \equiv 6 \pmod{13}$ we have

$$\text{ind}_7(7) + 6\,\text{ind}_7(x) \equiv \text{ind}_7(6) \pmod{12}.$$

Using this table to find $\text{ind}_7(7)$ and $\text{ind}_7(6)$ gives

$$1 + 6\,\text{ind}_7(x) \equiv 7 \pmod{12}$$
$$6\,\text{ind}_7(x) \equiv 6 \pmod{12}$$

Again the $\gcd(6, 12) = 6$ and $6 \mid 6$ which means we have 6 incongruent solutions.

Simplifying the above equation $6\,\text{ind}_7(x) \equiv 6 \pmod{12}$ yields

$$\text{ind}_7(x) \equiv 1 \pmod{2}.$$

Recall that $\text{ind}_7(x) \equiv 1 \pmod{2}$ implies

$$\text{ind}_7(x) = 1 + 2k \text{ where } k \text{ is an integer.}$$

Substituting $k = 0,\ 1,\ 2,\ 3,\ 4,\ 5$ gives $\text{ind}_7(x) \equiv 1, 3, 5, 7, 9, 11 \pmod{12}$. Using the table in reverse direction by finding these residues in the bottom row of the table and reading off corresponding entries in the top row:

$$x \equiv 7, 5, 11, 6, 8, 2 \pmod{13}$$

Writing these in ascending order gives $x \equiv 2, 5, 6, 7, 8, 11 \pmod{13}$. Of course, these are the same solutions as we found in Example 19 but we used the primitive root 2 modulo 13 in that example.

You may have noticed that using a larger primitive root 7 rather than 2 involved evaluating powers of 7 rather than powers of 2. It is simpler to use a lower base as long as it is a primitive root of n.

We also need to find solutions to the non – linear Diophantine equation

$$7x^6 = 6 + 13y$$

Substituting the above x values 2, 5, 6, 7, 8 and 11 into this gives

$$7 \times 2^6 = 448 = 6 + 13y \ \Rightarrow\ y = \frac{448 - 6}{13} = 34$$

$$7 \times 5^6 = 109\,375 = 6 + 13y \ \Rightarrow\ y = \frac{109\,375 - 6}{13} = 8413$$

$$7\times 6^6 = 326\ 592 = 6+13y \ \Rightarrow\ y = \frac{326\ 592-6}{13} = 25\ 122$$

$$7\times 7^6 = 823\ 543 = 6+13y \ \Rightarrow\ y = \frac{5\ 764\ 801-6}{13} = 63\ 349$$

$$7\times 8^6 = 1\ 835\ 008 = 6+13y \ \Rightarrow\ y = \frac{1\ 835\ 008-6}{13} = 141\ 154$$

$$7\times 11^6 = 12\ 400\ 927 = 6+13y \ \Rightarrow\ y = \frac{12\ 400\ 927-6}{13} = 953\ 917$$

Our solutions are $\{x=2,\ y=34\}$, $\{x=5,\ y=8413\}$, $\{x=6,\ y=25\ 122\}$, $\{x=7,\ y=63\ 349\}$, $\{x=8,\ y=141\ 154\}$ and $\{x=11,\ y=953\ 917\}$.

17. We are given that 2 is a primitive root of modulo 37. Solving $x^{14}\equiv 27\pmod{37}$ by using index base 2 we have

$$\begin{aligned} \operatorname{ind}_2\left(x^{14}\right) &\equiv \operatorname{ind}_2(27)\pmod{36} \\ 14\times\operatorname{ind}_2(x) &\equiv \operatorname{ind}_2(27)\pmod{36} \qquad (\dagger) \end{aligned}$$

We must find the index m in $2^m\equiv 27\pmod{37}$. Evaluating powers of 2:

$$\begin{aligned} 2^5 &\equiv 32 \equiv -5\pmod{37} \\ 2^6 &\equiv 2^5\times 2 \equiv -5\times 2 \equiv -10 \equiv 27\pmod{37} \end{aligned}$$

Therefore $\operatorname{ind}_2(27)=6$ and substituting this into the above $(\dagger)$ yields

$$14\ \operatorname{ind}_2(x)\equiv 6\pmod{36}$$

The $\gcd(14,\ 36)=2$ and $2\mid 6$ so we have 2 incongruent solutions. Simplifying this congruence we have

$$7\ \operatorname{ind}_2(x)\equiv 3\pmod{18}.$$

By inspection $7\times 3=21$ so $\operatorname{ind}_2(x)\equiv 3,\ 3+18\equiv 3,21\pmod{36}$. Therefore

$$x\equiv 2^3,\ 2^{21}\equiv 8,\ 2^{21}\pmod{37}$$

Evaluating $2^{21}\pmod{37}$ gives

$$2^{21}\equiv\left(2^5\right)^4\times 2\equiv\left(-5\right)^4\times 2\equiv 25^2\times 2\equiv\left(-12\right)^2\times 2\equiv 144\times 2\equiv 288\equiv 29\pmod{37}$$

Hence our solutions are $x\equiv 8,\ 29\pmod{37}$.

18. We are required to prove that $\operatorname{ind}_r(p-1)=\dfrac{p-1}{2}$ where r is a primitive root of p.

Proof.

We are given that r is a primitive root of a prime p therefore

$$r^{p-1} \equiv 1 \pmod{p}.$$

We can write $r^{p-1} = r^{\frac{p-1}{2}} r^{\frac{p-1}{2}}$:

$$r^{p-1} \equiv r^{\frac{p-1}{2}} r^{\frac{p-1}{2}} \equiv \left(r^{\frac{p-1}{2}} \right)^2 \equiv 1 \pmod{p}.$$

By Lemma (4.3):

$$x^2 \equiv 1 \pmod{p} \quad \Leftrightarrow \quad x \equiv \pm 1 \pmod{p}$$

Applying this Lemma to the above equation $\left(r^{\frac{p-1}{2}} \right)^2 \equiv 1 \pmod{p}$ yields

$$r^{\frac{p-1}{2}} \equiv 1 \pmod{p} \quad \text{or} \quad r^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

We cannot have $r^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. *Why not?*

Because r is a primitive root of p so the smallest index to give 1 modulo p is $p-1$.

Therefore we must have

$$r^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Also note that $-1 \equiv p-1 \pmod{p}$ so rewriting this $r^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ as

$$r^{\frac{p-1}{2}} \equiv p-1 \pmod{p}.$$

Hence by definition of index we have $\text{ind}_r (p-1) = \dfrac{p-1}{2}$.

This completes our proof.

■

19. We are required to prove that $x^m \equiv a \pmod{p}$ has a solution $\Leftrightarrow$

$$a^{\frac{p-1}{g}} \equiv 1 \pmod{p} \text{ where } g = \gcd(m, \quad p-1).$$

How do we prove this result?

We use Proposition (6.17):

Let n have a primitive root and $\gcd(a, \quad n) = 1$. The congruence

$$x^m \equiv a \pmod{n}$$

has a solution $\Leftrightarrow$

$$a^{\phi(n)/g} \equiv 1 \pmod{n} \text{ where } g = \gcd\left(m, \phi(n)\right).$$

Proof.

Using this proposition with $n = p$ gives us our result because

$$\phi(p) = p - 1.$$

So $x^m \equiv a \pmod{p}$ has a solution $\Leftrightarrow$ $a^{\phi(p)/g} \equiv a^{\frac{p-1}{g}} \equiv 1 \pmod{p}$ where $g = \gcd\left(m, \quad p-1\right)$. This is our required result.

■

20. We are asked to prove that:

Let $\gcd(r, n) = 1$ and $r_1, r_2, r_3, \cdots, r_{\phi(n)}$ be integers relatively prime to n. If r is a primitive root of n, then

$$r, r^2, r^3, \cdots, r^{\phi(n)}$$

are congruent modulo n to $r_1, r_2, r_3, \cdots, r_{\phi(n)}$ in some order.

Proof.

The given $\left\{r_1, r_2, r_3, \cdots, r_{\phi(n)}\right\}$ is a reduced residue system modulo n. We need to show that the set $\left\{r, r^2, r^3, \cdots, r^{\phi(n)}\right\}$ is also a reduced residue system. *How?*

Show two things;

1) $\left\{r, r^2, r^3, \cdots, r^{\phi(n)}\right\}$ is incongruent.

2) $\gcd\left(r^j, \quad n\right) = 1$ for $j = 1, 2, 3, \cdots, \phi(n)$.

<u>Step 1</u>

We need to show that any two residues of the form r^j where $j = 1, 2, \cdots, \phi(n)$ are incongruent modulo n.

Suppose any two residues of this form are congruent modulo n:

$$r^j \equiv r^m \pmod{n}.$$

By applying Proposition (6.6):

Let the integer a modulo n have order k. Then

$$a^j \equiv a^m \pmod{n} \quad \Leftrightarrow \quad j \equiv m \pmod{k}.$$

We have $j \equiv m \pmod{\phi(n)}$ because r is a primitive root so its order is $\phi(n)$. We have $j = m$ because $j, m = 1, 2, 3, \cdots, \phi(n)$. This means that the set

$$\left\{r,\ r^2,\ r^3,\ \cdots,\ r^{\phi(n)}\right\} \text{ is incongruent modulo } n.$$

Step 2

Since $\gcd\left(r,\ \ n\right)=1$ so $\gcd\left(r^j,\ \ n\right)=1$ for $j=1,\ 2,\ 3,\ \cdots,\ \phi\left(n\right)$.

Hence the set $\left\{r,\ r^2,\ r^3,\ \cdots,\ r^{\phi(n)}\right\}$ satisfies both conditions for a reduced residue system.

Therefore, the elements in this set $\left\{r,\ r^2,\ r^3,\ \cdots,\ r^{\phi(n)}\right\}\left(\text{mod } n\right)$ are congruent $\left\{r_1,\ r_2,\ r_3,\ \cdots,\ r_{\phi(n)}\right\}\left(\text{mod } n\right)$ in some order.

This completes our proof.

■

21. We are asked to prove the following:

> Let n have a primitive root and a and n be relatively prime. The congruence
> $$x^m \equiv a\ \left(\text{mod}\ \ n\right)$$
> has a solution $\Leftrightarrow\ a^{\phi(n)/g}\ \equiv 1\left(\text{mod}\ \ n\right)$ where $g=\gcd\left(m,\ \ \phi\left(n\right)\right)$. Additionally, there are exactly g *incongruent* solutions.

Proof.

Let r be a primitive root of modulo n. Consider the given non – linear congruence $x^m \equiv a\ \left(\text{mod}\ \ n\right)$. Taking indices to the base r of this congruence

$$\text{ind}_r\left(x^m\right) \equiv \text{ind}_r\left(a\right)\ \left(\text{mod } \phi\left(n\right)\right).$$

Using the rules, we have

$$m\ \text{ind}_r\left(x\right) \equiv \text{ind}_r\left(a\right)\ \left(\text{mod } \phi\left(n\right)\right) \qquad (*)$$

This (*) is now a linear congruence so applying Proposition (3.15):

> The congruence $ax \equiv b\ \left(\text{mod } n\right)$ has a solution $\Leftrightarrow\ g \mid b$ where $g=\gcd\left(a,\ \ n\right)$.

We have $m\ \text{ind}_r\left(x\right) \equiv \text{ind}_r\left(a\right)\left(\text{mod } \phi\left(n\right)\right)$ has a solution $\Leftrightarrow\ g \mid ind_r\left(a\right)$ where $g=\gcd\left(m,\ \ \phi\left(n\right)\right)$. By Proposition (3.16):

> $ax \equiv b\ \left(\text{mod } n\right)$ has g incongruent solutions provided $g \mid b$ where $g=\gcd\left(a,\ \ n\right)$

We have g incongruent solutions of (*). Let $ind_r\left(a\right)=m$ then by the definition of index we have

$$r^m \equiv a\left(\text{mod } n\right)$$

Taking this congruence $r^m \equiv a \pmod{n}$ to the power $\dfrac{\phi(n)}{g}$ gives

$$\left(r^m\right)^{\frac{\phi(n)}{g}} \equiv a^{\frac{\phi(n)}{g}} \pmod{n}$$

Since we are given that $g = \gcd\left(m, \ \phi(n)\right)$ so there is an integer k such that

$$gk = m$$

Substituting this into the left – hand side of the above $\left(r^m\right)^{\frac{\phi(n)}{g}} \equiv a^{\frac{\phi(n)}{g}} \pmod{n}$:

$$\left(r^m\right)^{\frac{\phi(n)}{g}} \equiv \left(r^{gk}\right)^{\frac{\phi(n)}{g}} \underbrace{\equiv}_{\substack{\text{By the rules} \\ \text{of indices}}} r^{gk\times\frac{\phi(n)}{g}} \equiv r^{k\times\phi(n)} \equiv \left(r^{\phi(n)}\right)^k \equiv 1^k \equiv 1 \equiv a^{\frac{\phi(n)}{g}} \pmod{n}$$

Hence, we have our result $a^{\frac{\phi(n)}{g}} \equiv 1 \pmod{n}$. This completes our proof.

■

22. (a) We are asked to show that

$$x^2 \equiv -1 \pmod{p} \text{ has solutions} \quad \Leftrightarrow \quad p \equiv 1 \pmod{4}.$$

How do we prove this result?

We use Proposition (6.17):

> Let n have a primitive root and a and n be relatively prime. The congruence
>
> $$x^m \equiv a \pmod{n}$$
>
> has a solution $\Leftrightarrow$ $a^{\phi(n)/g} \equiv 1 \pmod{n}$ where $g = \gcd\left(m, \ \phi(n)\right)$.

Proof.

We are given that p is an odd prime. Let $g = \gcd\left(2, \ \phi(p)\right)$ then

$g = \gcd\left(2, \ \phi(p)\right) = \gcd\left(2, \ p-1\right) = 2$. By Proposition (6.17) we have

$$x^2 \equiv -1 \pmod{p} \text{ has solutions } \Leftrightarrow \left(-1\right)^{\frac{\phi(p)}{g}} \equiv \left(-1\right)^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

From the last part we have

$$\left(-1\right)^{\frac{p-1}{2}} \equiv 1 \pmod{p} \quad \Leftrightarrow \quad \frac{p-1}{2} = 2k \quad \Leftrightarrow \quad p-1 = 4k \quad \Leftrightarrow \quad p \equiv 1 \pmod{4}.$$

We have our result $x^2 \equiv -1 \pmod{p}$ has solutions $\Leftrightarrow$ $p \equiv 1 \pmod{4}$.

■

(b) Similar to part (a) but we need to consider two gcds.

We need to show that $x^4 \equiv -1 \pmod{p}$ has solutions $\Leftrightarrow$ $p \equiv 1 \pmod{8}$.

Proof.

We are given that p is an odd prime. Let $g = \gcd\Big(4, \quad \phi\big(p\big)\Big)$ then $g = \gcd\Big(4, \quad p-1\Big)$. By Proposition (6.17) we have

$$x^4 \equiv -1\Big(\text{mod } p\Big) \text{ has solutions } \Leftrightarrow \ \Big(-1\Big)^{(p-1)/g} \equiv 1\Big(\text{mod } \ p\Big).$$

We are given that p is odd so $p-1$ is even therefore

$$g = \gcd\Big(4, \quad p-1\Big) = 2 \ \text{ or } \ 4$$

Suppose $g = \gcd\Big(4, \quad p-1\Big) = 2$ then $p-1 = 2k$ where k is odd (if k was even then $g = 4$). Substituting this $p-1 = 2k$ into the above $\Big(-1\Big)^{(p-1)/g} \equiv 1\Big(\text{mod } \ p\Big)$ yields

$$\Big(-1\Big)^{(p-1)/g} \equiv \Big(-1\Big)^{2k/2} \equiv \Big(-1\Big)^{k} \underbrace{\equiv}_{\text{because } k \text{ is odd}} -1\Big(\text{mod } \ p\Big)$$

Therefore $g = 4$ and we have

$$x^4 \equiv -1\Big(\text{mod } p\Big) \text{ has solutions } \Leftrightarrow \ \Big(-1\Big)^{(p-1)/4} \equiv 1\Big(\text{mod } \ p\Big)$$

From the last part we have

$$\Big(-1\Big)^{(p-1)/4} \equiv 1\Big(\text{mod } \ p\Big) \quad \Leftrightarrow \quad \frac{p-1}{4} = 2k \quad \Leftrightarrow \quad p-1 = 8k \quad \Leftrightarrow \quad p \equiv 1\Big(\text{mod } 8\Big)$$

We have our result $x^4 \equiv -1\Big(\text{mod } p\Big)$ has solutions $\Leftrightarrow \quad p \equiv 1\Big(\text{mod } 8\Big)$.

■