Complete Solutions to Supplementary Problems 6

1. In each case we use corollary (6.5):

> Let the integer a modulo n have order k, then $k \mid \phi(n)$.

(a) Since 7 is prime so $\phi(7) = 6$. The divisors of 6 are 1, 2, 3 and 6.

We need to check each of these indices to 3 modulo 7. Clearly 1 is not going to be the order because $3^1 \equiv 3 \pmod 7$ and by Euler's theorem we have $3^6 \equiv 1 \pmod 7$. So checking the remaining two integers gives

$$3^2 \equiv 9 \equiv 2 \pmod 7 \text{ and } 3^3 \equiv 27 \equiv 6 \pmod 7.$$

Hence the order of 3 modulo 7 is 6.

(b) This time we are asked to work with modulo 13. The Euler phi function of 13 is 12 because 13 is prime. The divisors of 12 are 1, 2, 3, 4, 6 and 12. Again not bothering with the last and first of these integers as indices and checking the others gives

$$3^2 \equiv 9 \pmod{13}, \quad 3^3 \equiv 27 \equiv 1 \pmod{13}.$$

Hence the order of 3 modulo 13 is 3.

(c) We know that 23 is prime so $\phi(23) = 22$ and the divisors of 22 are 1, 2, 11 and 22:

$$3^2 \equiv 9 \pmod{23}, \quad 3^{11} \equiv 177147 \equiv 1 \pmod{23}.$$

The order of $3 \pmod{23}$ is 11.

(d) Similarly we have

$$\phi(29) = 28.$$

The divisors of 28 are 1, 2, 4, 7, 14 and 28.

$$3^2 \equiv 9 \pmod{29}, \quad 3^4 \equiv 23 \pmod{29}, \quad 3^7 \equiv 12 \pmod{29}, \; 3^{14} \equiv 28 \pmod{29}.$$

By Euler's theorem we have $3^{28} \equiv 1 \pmod{29}$. Hence the order of $3 \pmod{29}$ is 28.

Clearly by the above results, 3 is a primitive root of 7 and 29.

2. (i) The order of 5 modulo 31 is found by first evaluating Euler's phi function of 31:

$$\phi(31) = 30 \qquad [\text{Because 31 is prime}]$$

The divisors of 30 are 1, 2, 3, 5, 6, 10, 15 and 30. Checking these integers as indices of 5 modulo 31 gives:

$$5^2 \equiv 25 \pmod{31}, \quad 5^3 \equiv 125 \equiv 1 \pmod{31}.$$

Therefore, the order of $5 \pmod{31}$ is 3.

(ii) We are asked to find the least non-negative residue x modulo 31 in

$$5^{1000} \equiv x \pmod{31}.$$

By part (i) we have the order of $5 \pmod{31}$ is 3. We need to write the index 1000 as a multiple of 3 plus any remainder. By the division algorithm

$$1000 = 333(3) + 1.$$

Substituting this $1000 = 333(3) + 1$ into the above index gives

$$5^{1000} \equiv 5^{333(3)+1} \equiv \left(5^3\right)^{333} \times 5 \equiv 1^{333} \times 5 \equiv 5 \pmod{31}.$$

We have $5^{1000} \equiv 5 \pmod{31}$.

3. The Euler totient function $\phi(100) = 40$. The divisors of 40 are 1, 2, 4, 5, 8, 10, 20 and 40. The order of 7 modulo 100 will be one of these integers. We have

$$7^2 \equiv 49, \quad 7^3 \equiv 343 \equiv 43, \quad 7^4 \equiv 2401 \equiv 1 \pmod{100}.$$

Hence the order of $7 \pmod{100}$ is 4.

The last two digits of 7^{1003} is given by the least non-negative residue $x \pmod{100}$ which satisfies

$$7^{1003} \equiv x \pmod{100}.$$

Writing the index 1003 as a multiple of 4 plus remainder because 4 is the order of $7 \pmod{100}$:

$$1003 = (250 \times 4) + 3.$$

We have

$$7^{1003} \equiv 7^{(250\times4)+3} \equiv \left(7^4\right)^{250} \times 7^3 \equiv 1^{250} \times 7^3 \equiv 7^3 \equiv 43 \pmod{100}.$$

The last two digits of 7^{1003} are 43.

4. We need to find the order of $10 \pmod{37}$. Since 37 is prime so

$$\phi(37) = 36.$$

The divisors of 36 are 1, 2, 3, 4, 6, 9, 12, 18 and 36. One of these integers is the order of $10 \pmod{37}$:

$$10^2 \equiv 100 \equiv 26 \pmod{37}, \quad 10^3 \equiv 1000 \equiv 1 \pmod{37}.$$

Thus, the order of $10 \pmod{37}$ is 3.

The inverse of $10 \pmod{37}$ is $10^2 \equiv 26 \pmod{37}$ because

$$10\left(10^2\right) \equiv 1000 \equiv 1 \pmod{37}.$$

We also need to solve $10x \equiv 21 \pmod{37}$. Multiplying both sides of this congruence by 26 (as this is the inverse) gives

$$26 \times 10x \equiv 26 \times 21 \pmod{37}$$
$$x \equiv 546 \equiv 28 \pmod{37}$$

5. We are given the following table in the question:

a	1	2	3	4	5	6	7	8	9	10	11	12
$ind_2(a)$	12	1	4	2	9	5	11	3	8	10	7	6

We use the following 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 $\text{ind}_r(r) \equiv 1 \pmod{\phi(n)}$

(i) We are asked to solve $5x^7 \equiv 1 \pmod{13}$. Applying indices to both sides gives

$$\text{ind}_2\left(5x^7\right) \equiv \text{ind}_2(1) \pmod{12}$$
$$\text{ind}_2(5) + \left[7 \times \text{ind}_2(x)\right] \equiv \text{ind}_2(1) \pmod{12} \quad \text{[Linear Form]}$$

By the above table we have $\text{ind}_2(5) = 9$ and $\text{ind}_2(1) = 12$. Putting these values into the above derivation gives

$$9 + 7\,\text{ind}_2(x) \equiv 12 \pmod{12}$$
$$7\,\text{ind}_2(x) \equiv 3 \pmod{12}$$

The $\gcd(7, 12) = 1$ so we have a unique solution. By inspection the solution is

$$\text{ind}_2(x) \equiv 9 \pmod{12}$$

Using the above table in reverse order we have

$$x \equiv 5 \pmod{13}$$

Hence our solution is $x \equiv 5 \pmod{13}$.

(ii) Let $y \pmod{13}$ be the multiplicative inverse of $5 \pmod{13}$ then

$$5y \equiv 1 \pmod{13} \text{ which implies } y \equiv 5^7 \pmod{13} \text{ by part (i)}$$

Evaluating this gives

$$y \equiv 5^7 \equiv 8 \pmod{13}$$

The inverse of $5 \pmod{13}$ is $8 \pmod{13}$.

(iii) We are asked to solve $8x^7 \equiv 12 \pmod{13}$. We can be smart about solving this. Note that $-8 \equiv -5,\ 12 \equiv -1 \pmod{13}$ and substituting these gives us the equation

$$-5x^7 \equiv -1 \pmod{13} \underbrace{\Rightarrow}_{\text{Multiplying by } -1} 5x^7 \equiv 1 \pmod{13}$$

We solved this $5x^7 \equiv 1 \pmod{13}$ in part (i) and the solution is $x \equiv 5 \pmod{13}$.

(iv) We have more or less the same congruence as part (iii) but this time the index is 6. By applying indices, we have the linear form;

$$6 \operatorname{ind}_2(x) \equiv 3 \pmod{12}.$$

The $\gcd(6,\ 12) = 6$ but $6 \not| 3$ so the given equation has *no* solution.

(v) Similarly we have

$$8 \operatorname{ind}_2(x) \equiv 3 \pmod{12}.$$

The $\gcd(8,\ 12) = 4$ and $4 \not| 3$ therefore $8x^8 \equiv 12 \pmod{13}$ has *no* solution.

6. We fill in the given table by evaluating powers of 5 modulo 23:

$$5^1 \equiv 5,\ 5^2 \equiv 25 \equiv 2 \pmod{23},\ 5^3 \equiv 125 \equiv 10,\ 5^4 \equiv 10 \times 5 \equiv 50 \equiv 4,$$
$$5^5 \equiv 4 \times 5 \equiv 20,\ 5^6 \equiv 100 \equiv 8,\ 5^7 \equiv 8 \times 5 \equiv 40 \equiv 17,$$
$$5^8 \equiv 16,\ 5^9 \equiv 11,\ 5^{10} \equiv 9,\ 5^{11} \equiv 22,\ 5^{12} \equiv 18,\ 5^{13} \equiv 21,\ 5^{14} \equiv 13,$$
$$5^{15} \equiv 19,\ 5^{16} \equiv 3,\ 5^{17} \equiv 15,\ 5^{18} \equiv 6,\ 5^{19} \equiv 7,\ 5^{20} \equiv 12,\ 5^{21} \equiv 14$$
$$\text{and } 5^{22} \equiv 1 \pmod{23}$$

Hence 5 is a primitive root of 23.

Putting these into the table gives

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$ind_5(a)$	22	2	16	4	1	18	19	6	10	3	9	20	14	21	17	8

a	17	18	19	20	21	22
$ind_5(a)$	7	12	15	5	13	11

(a) We are asked to solve $x^{12} \equiv 4 \pmod{23}$. Using the rules of indices we have

$$\text{ind}_5\left(x^{12}\right) \equiv \text{ind}_5(4) \pmod{22}$$
$$12\ \text{ind}_5(x) \equiv \text{ind}_5(4) \underbrace{\equiv}_{\text{By the above table}} 4 \pmod{22}$$

The $\gcd(12,\ 22) = 2$ and $2 \mid 4$ so we have two incongruent solutions.

Applying Proposition (3.10) of chapter 3:

> If $ac \equiv bc \pmod{n}$ then $a \equiv b \left(\text{mod } \frac{n}{g}\right)$ where $g = \gcd(c,\ n)$.

To $12\ \text{ind}_5(x) \equiv 4 \pmod{22}$ with $g = 2$ gives

$$6\ \text{ind}_5(x) \equiv 2 \pmod{11} \text{ which implies } \text{ind}_5(x) \equiv 4 \pmod{11}.$$

So we have $\text{ind}_5(x) \equiv 4 \pmod{11}$ and our two solutions are given by

$$\text{ind}_5(x) \equiv 4,\ 11+4 \equiv 4,\ 15 \pmod{22}.$$

Reading these entries in the bottom row of the above table and finding the corresponding integers in the top row we have

$$x \equiv 4,\ 19 \pmod{23}. \quad [\pm 4 \pmod{23}]$$

(b) Now we are asked to solve $7x^{10} \equiv 2 \pmod{23}$. Again using indices we have

$$\text{ind}_5\left(7x^{10}\right) \equiv \text{ind}_5(2) \pmod{22}$$
$$\text{ind}_5(7) + 10\left[\text{ind}_5(x)\right] \equiv \text{ind}_5(2) \pmod{22}$$

Using the above table gives

$$19 + 10\ \text{ind}_5(x) \equiv 2 \pmod{22}$$
$$10\ \text{ind}_5(x) \equiv 2 - 19 \equiv -17 \equiv 5 \pmod{22}$$

What is the solution of $10\ \text{ind}_5(x) \equiv 5 \pmod{22}$ *?*

There are *no* solutions to this congruence because $\gcd(10,\ 22) = 2$ and $2 \not| 5$. Hence we have no solution.

(c) We are asked to solve $9x^{11} \equiv 14 \pmod{23}$. Taking indices gives

$$\text{ind}_5\left(9x^{11}\right) \equiv \text{ind}_5\left(14\right) \pmod{22}$$
$$\text{ind}_5\left(9\right) + \left[11 \times \text{ind}_5\left(x\right)\right] \equiv \text{ind}_5\left(14\right) \pmod{22}$$

By the above table we have

$$\text{ind}_5\left(9\right) + \left[11 \times \text{ind}_5\left(x\right)\right] \equiv \text{ind}_5\left(14\right) \pmod{22}$$
$$10 + \left[11 \times \text{ind}_5\left(x\right)\right] \equiv 21 \quad \Rightarrow \quad 11\ \text{ind}_5\left(x\right) \equiv 21 - 10 \equiv 11 \pmod{22}$$

The $\gcd\left(11,\ \ 22\right) = 11$ and $11 \mid 11$ so we have 11 *incongruent* solutions. By using Proposition (3.10) of chapter 3:

> If $ac \equiv bc \pmod{n}$ then $a \equiv b \pmod{\frac{n}{g}}$ where $g = \gcd\left(c,\ \ n\right)$.

On $11\ ind_5\left(x\right) \equiv 11 \pmod{22}$ gives

$$ind_5\left(x\right) \equiv 1 \pmod{2}.$$

Our solutions are of the form $2k + 1$ [odd integer] where k is 0, 1, 2, 3, … and 10 because we have 11 solutions:

$$ind_5\left(x\right) \equiv 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21 \pmod{22}.$$

Using the table in reverse order gives

$$ind_5\left(x\right) \equiv 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21$$
$$x \equiv 5, 10, 20, 17, 11, 22, 21, 19, 15, 7, 14$$
$$\equiv 5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22 \pmod{23} \quad \left[\begin{matrix}\text{Putting them in} \\ \text{ascending order}\end{matrix}\right]$$

(d) Now we are asked to solve $11^x \equiv 5 \pmod{23}$. Again using the rules of indices highlighted in the previous question yields

$$x\ ind_5\left(11\right) \equiv ind_5\left(5\right) \pmod{22}$$
$$9x \equiv 1 \pmod{22}$$

This equation has a unique solution because $\gcd\left(9,\ \ 22\right) = 1$ and $1 \mid 1$. By trial and error we have our unique solution $x \equiv 5 \pmod{22}$.

7. (a) We are asked to find the least non-negative residue $x \pmod{23}$ such that

$$6^{69}7^{70} \equiv x \pmod{23}.$$

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

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

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

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

On $6^{69}7^{70} \equiv x \pmod{23}$ gives

$$\begin{aligned} \text{ind}_5\left(6^{69}7^{70}\right) &\equiv \text{ind}_5\left(x\right) \pmod{22} \\ \text{ind}_5\left(6^{69}\right) + \text{ind}_5\left(7^{70}\right) &\equiv \text{ind}_5\left(x\right) \pmod{22} \\ 69\ \text{ind}_5\left(6\right) + 70\ \text{ind}_5\left(7\right) &\equiv \text{ind}_5\left(x\right) \pmod{22} \end{aligned}$$

Using the above table in solution to the previous question we have

$$\begin{aligned} 69\ \text{ind}_5\left(6\right) + 70\ \text{ind}_5\left(7\right) &\equiv \text{ind}_5\left(x\right) \\ \left(69 \times 18\right) + \left(70 \times 19\right) &\equiv \text{ind}_5\left(x\right) \\ \text{ind}_5\left(x\right) &\equiv 2572 \equiv 20 \pmod{22} \end{aligned}$$

Locating the residue 20 in the bottom row of the table and reading off the corresponding value in the top row we have

$$x \equiv 12 \pmod{23}.$$

Hence $6^{69}7^{70} \equiv 12 \pmod{23}$.

(b) This time we are asked to find $x \equiv 9^{666}11^{100}17^{1000} \pmod{23}$. Like part (a) we have

$$\begin{aligned} \text{ind}_5\left(x\right) &\equiv \text{ind}_5\left(9^{666}11^{100}17^{1000}\right) \\ &\equiv 666\ \text{ind}_5\left(9\right) + 100\ \text{ind}_5\left(11\right) + 1000\ \text{ind}_5\left(17\right) \qquad (*) \end{aligned}$$

Looking up at the table of the previous question to evaluate

$$\text{ind}_5\left(9\right),\ \text{ind}_5\left(11\right) \text{ and } \text{ind}_5\left(17\right)$$

We have $\text{ind}_5\left(9\right) = 10,\ \text{ind}_5\left(11\right) = 9$ and $\text{ind}_5\left(17\right) = 7$. Substituting these into (*) yields

$$\begin{aligned} \text{ind}_5\left(x\right) &\equiv 666\ \text{ind}_5\left(9\right) + 100\ \text{ind}_5\left(11\right) + 1000\ \text{ind}_5\left(17\right) \\ &\equiv \left(666 \times 10\right) + \left(100 \times 9\right) + \left(1000 \times 7\right) \\ &\equiv 14560 \equiv 18 \pmod{22} \end{aligned}$$

Again using the table in reverse order gives

$$x \equiv 6 \pmod{23}.$$

Hence $9^{666}11^{100}17^{1000} \equiv 6 \pmod{23}$.

8. This question is very similar to the previous question. We use the given table:

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\text{ind}_2(a)$	18	1	13	2	16	14	6	3	8	17	12	15	5	7	11	4	10	9

(a) We are given $x \equiv 5^{100}7^{100}8^{100}9^{100} \pmod{19}$. Using the 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 $\text{ind}_r(r) \equiv 1 \pmod{\phi(n)}$

On $x \equiv 5^{100}7^{100}8^{100}9^{100} \pmod{19}$ yields

$$\begin{aligned}\text{ind}_2(x) &\equiv \left[100 \times \text{ind}_2(5)\right] + \left[100 \times \text{ind}_2(7)\right] + \left[100 \times \text{ind}_2(8)\right] + \left[100 \times \text{ind}_2(9)\right] \\ &\underbrace{\equiv}_{\text{Factorizing}} 100\left[\text{ind}_2(5) + \text{ind}_2(7) + \text{ind}_2(8) + \text{ind}_2(9)\right] \pmod{18}\end{aligned}$$

Using the above table to evaluate these indices gives

$$\begin{aligned}\text{ind}_2(x) &\equiv 100\left[\text{ind}_2(5) + \text{ind}_2(7) + \text{ind}_2(8) + \text{ind}_2(9)\right] \\ &\equiv 100\left[16 + 6 + 3 + 8\right] \\ &\equiv 3300 \equiv 6 \pmod{18}\end{aligned}$$

Using the above table in reverse direction (we locate 6 in the bottom row of the table and see what integer it corresponds to in the top row):

$$x \equiv 7 \pmod{19}.$$

Therefore $5^{100}7^{100}8^{100}9^{100} \equiv 7 \pmod{19}$.

(b) This time we are asked to compute $x \equiv 11^{1\,000\,001}15^{1\,000\,003}18^{1\,000\,007} \pmod{19}$. By the same token we have

$$\begin{aligned}\text{ind}_2(x) &\equiv \text{ind}_2\left(11^{1\,000\,001}15^{1\,000\,003}18^{1\,000\,007}\right) \\ &\equiv 1\,000\,001\,\text{ind}_2(11) + 1\,000\,003\,\text{ind}_2(15) + 1\,000\,007\,\text{ind}_2(18) \\ &\equiv \left(1\,000\,001 \times 12\right) + \left(1\,000\,003 \times 11\right) + \left(1\,000\,007 \times 9\right) \\ &\equiv 32\,000\,108 \equiv 14 \pmod{18}\end{aligned}$$

Finding the integer 14 in the bottom row of the above table and reading off the corresponding value in the top row we have

$$x \equiv 6 \pmod{19}.$$

Hence $11^{1\,000\,001}15^{1\,000\,003}18^{1\,000\,007} \equiv 6 \pmod{19}$.

(c) We are asked to find $x \equiv 5^{100^{100}} \pmod{19}$ where $x \pmod{19}$ is the least non-negative residue. Taking indices gives

$$\begin{aligned}\operatorname{ind}_2(x) &\equiv \operatorname{ind}_2\left(5^{100^{100}}\right) \\ &\equiv 100^{100}\operatorname{ind}_2(5) \underbrace{\equiv}_{\text{Because } 100\equiv 10 \pmod{18}} 10^{100}\operatorname{ind}_2(5) \pmod{18}\end{aligned}$$

From the given table $\operatorname{ind}_2(5) = 16$. Substituting this into the above gives

$$\operatorname{ind}_2(x) \equiv 10^{100} \times 16 \pmod{18} \qquad (\ddagger)$$

Using the given hint $10^n \equiv 10 \pmod{18}$ we have

$$\operatorname{ind}_2(x) \equiv 10^{100} \times 16 \equiv 10 \times 16 \equiv 160 \equiv 16 \pmod{18}.$$

Using the above table in the reverse direction we have

$$x \equiv 5 \pmod{19}.$$

Hence the least non-negative residue of $5^{100^{100}}$ is $5 \pmod{19}$.

9. We are asked to show that $a^k \not\equiv 1 \pmod{p}$ where $1 \le k < p-1$ and a is a primitive root.

Proof.

We are given that a is a primitive root. Therefore by Proposition (6.10):

> If $\gcd(a, n) = 1$ and a has order $\phi(n)$ then the integer a is called the **primitive root** of the integer n.

Since p is prime so $\phi(p) = p-1$. Recall that the order is the *smallest* positive integer m such that $a^m \equiv 1 \pmod{n}$. Our given a is a primitive root so order is $\phi(p) = p-1$ which implies that $a^k \not\equiv 1 \pmod{p}$ for $1 \le k < p-1$.

This completes our proof.

■

10. The order of 10 modulo 18 does *not* exist because by definition (6.1) we need the $\gcd(a, n) = 1$ but we have $\gcd(10, 18) = 2$:

> Let $n > 1$ and $\gcd(a, n) = 1$. The *order* of a modulo n is the *smallest positive* integer k such that $a^k \equiv 1 \pmod{n}$.

See Example 3 of main text.

11. (a) We need to solve $x^3 \equiv 2 \pmod{37}$ by using the primitive root 2. Taking the index to the base 2 of both sides of this equation and using the rules of indices gives

$$\begin{aligned} \text{ind}_2\left(x^3\right) &\equiv \text{ind}_2\left(2\right) \pmod{36} \\ 3 \times \text{ind}_2\left(x\right) &\equiv 1 \pmod{36} \end{aligned}$$

The $\gcd\left(3,\ 36\right) = 3$ and $3 \not| 1$ so there are *no* solutions.

(b) This time we solve $x^{16} \equiv 10 \pmod{37}$. By taking the index to the base 2 of this we have

$$\begin{aligned} \text{ind}_2\left(x^{16}\right) &\equiv \text{ind}_2\left(10\right) \pmod{36} \\ 16 \times \text{ind}_2\left(x\right) &\equiv \text{ind}_2\left(10\right) \pmod{36} \qquad (\dagger) \end{aligned}$$

We need to find the index k such that $2^k \equiv 10 \pmod{37}$. Evaluating powers of 2 yields

$$\begin{aligned} 2^5 \equiv 32 \equiv -5,\ 2^6 \equiv -10,\ 2^7 \equiv -20,\ 2^8 \equiv -40 \equiv -3,\ 2^9 \equiv -6, \\ 2^{10} \equiv -12,\ 2^{11} \equiv -24,\ 2^{12} \equiv -11 \pmod{37} \end{aligned}$$

Now $\left(-11\right)^2 \equiv 121 \equiv 10 \pmod{37}$. Therefore $2^{24} \equiv \left(-11\right)^2 \equiv 10 \pmod{37}$ which implies that $k = 24$. Hence $\text{ind}_2\left(10\right) = 24$ so substituting this into $(\dagger)$ gives

$$16 \times \text{ind}_2\left(x\right) \equiv 24 \pmod{36}.$$

The $\gcd\left(16,\ 24\right) = 4$ and $4 \mid 36$ so we have 4 incongruent solutions. Dividing this congruence by 4

$$4 \times \text{ind}_2\left(x\right) \equiv 6 \pmod{9}.$$

By inspection we have $\text{ind}_2\left(x\right) = 6$ and the other 3 solutions are given by adding equal steps of 9 to each

$$\text{ind}_2\left(x\right) \equiv 6,\ 6+9,\ 6+18,\ 6+27 \equiv 6,\ 15,\ 24,\ 33 \pmod{36}.$$

The 4 incongruent solutions to the given equation are

$$\begin{aligned} x &\equiv 2^6,\ 2^{15},\ 2^{24},\ 2^{33} \\ &\equiv 27, \left(-5\right)^3,\ 10,\ \left(-24\right)^3 \quad \left[\text{By above calculations}\right] \\ &\equiv 27, 23,\ 10,\ 13^3 \equiv 27,\ 23,\ 10,\ 14 \pmod{37} \end{aligned}$$

Our 4 solutions in ascending order are $x \equiv 10,\ 14,\ 23,\ 27 \pmod{37}$.

12. We are given that the order of $a \pmod{n}$ and $b \pmod{n}$ is r. However we need to show that the order of $ab \pmod{n}$ is *not* necessarily equal to r.

(a) We consider modulo 9. Let us evaluate the order of $2 \pmod{9}$ and $5 \pmod{9}$. *How?*

By corollary (6.5):

> Let the integer a modulo n have order k, then $k \mid \phi(n)$.

The Euler phi function $\phi(9) = 6$. The only divisors of 6 are 1, 2, 3 and 6:

$$2^2 \equiv 4,\ 2^3 \equiv 8,\ 2^6 \equiv 64 \equiv 1 \pmod{9}.$$

The order of $2 \pmod{9}$ is 6. Similarly we have

$$5^2 \equiv 25 \equiv 7,\ 5^3 \equiv 125 \equiv 8,\ 5^6 \equiv 1 \pmod{9}.$$

The order of $5 \pmod{9}$ is 6 as well. However the order of

$$2 \times 5 \equiv 10 \equiv 1 \pmod{9} \text{ is clearly 1.}$$

Hence the order of $(2 \times 5) \pmod{9}$ is *not* equal to 6.

(b) The order of both $2 \pmod{19}$ and $3 \pmod{19}$ is 18.

Let us evaluate the order of $2 \times 3 \equiv 6 \pmod{19}$. By corollary (6.5):

> Let the integer a modulo n have order k, then $k \mid \phi(n)$.

The order of $6 \pmod{19}$ is a divisor of $\phi(19) = 18$. The only divisors of 18 are 1, 2, 9 and 18:

$$6^2 \equiv 36 \equiv 17,\ 6^9 \equiv 10077696 \equiv 1 \pmod{19}$$

Hence the order of $6 \pmod{19}$ is 9 *not* 18.

13. We are asked to prove the order of a modulo $(a^n - 1)$ is n.

Proof.

Clearly $\left(a^n-1\right) \mid \left(a^n-1\right)$ which implies that

$$a^n-1 \equiv 0 \left(\text{mod } \left(a^n-1\right)\right) \Rightarrow \quad a^n \equiv 1 \left(\text{mod } \left(a^n-1\right)\right).$$

We need to show n is the smallest positive integer such that the above holds.

Suppose $a^m \equiv 1 \left(\text{mod } \left(a^n-1\right)\right)$ where $m < n$. Then

$$a^m-1 \equiv 0 \left(\text{mod } \left(a^n-1\right)\right) \text{ which implies } \left(a^n-1\right) \mid \left(a^m-1\right).$$

By Theorem (1.2) (e):

> If $x \mid y$ and $y \neq 0$ then $|x| \leq |y|$

We have $\left|a^n-1\right| \leq \left|a^m-1\right|$. However this is impossible because $m < n$. Hence n is the smallest positive integer which implies that the order of a modulo $\left(a^n-1\right)$ is n. This completes our proof.

■

14. We are given that the order of a modulo n is k where $n = 2^m$ and we need to prove that $k \mid 2^{m-1}$.

Proof.

We use Corollary (6.5) to prove this result:

> Let the integer a modulo n have order k, then $k \mid \phi(n)$.

Let k be the order of n. We are given that $n = 2^m$ so by Proposition (5.9):

$$\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)$$

We have $\phi\left(2^m\right) = 2^m\left(1-\frac{1}{2}\right) = 2^m\left(\frac{1}{2}\right) = 2^{m-1}$. Therefore by the above Corollary we have $k \mid 2^{m-1}$ which is our required result.

■

15. We need to show that if a modulo n has order k then a^m also has order k $\Leftrightarrow \gcd(k, \quad m) = 1$.

Proof.

$(\Leftarrow)$. We are given that $\gcd(k, \quad m) = 1$. Therefore by applying Proposition (6.8):

> Let a modulo n have order k. Then the integer a^s has order
> $$\frac{k}{\gcd(s, \quad k)} \quad \text{where } s \text{ is a positive integer}$$

We have the order of a^m is $\dfrac{k}{\gcd(m, \quad k)} = \dfrac{k}{1} = k$.

$(\Rightarrow)$. Now we assume that a^m also has order k and need to show that

$$\gcd(k, \quad m) = 1.$$

Suppose the $\gcd(k, \quad m) = g > 1$. Then the order of a^m by the above Proposition (6.8) is

$$\frac{k}{\gcd(m, \quad k)} = \frac{k}{g} < k \qquad [\text{Because } \quad g > 1]$$

However, we are assuming that the order of a^m is k. We *cannot* have order of a^m is k and it is less than k. Hence our supposition $\gcd(k, \quad m) = g > 1$ must be wrong so $\gcd(k, \quad m) = 1$. This completes our proof.

■

16. We are given that r is a primitive root of the prime p and we need to show that the least non-negative residue of $r^m \pmod p$ is also a primitive root of p $\Leftrightarrow \gcd(m, \quad p-1) = 1$.

Proof.

Since we are given r is a primitive root of p so the order of $r \pmod p$ is

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

By the result of previous question we have the order of r^m is $p-1 \Leftrightarrow \gcd(m, \quad p-1) = 1$. Hence $r^m \pmod p$ has the same order $p-1$ because $\gcd(m, \quad p-1) = 1$. This completes our proof.

■

17. We are required to prove that if n has a primitive root then it has exactly $\phi\left(\phi\left(n\right)\right)$ incongruent primitive roots.

Proof.

Very similar to the proof of the previous question.

Let r be a primitive root of n. Then the elements of

$$S = \left\{r,\ r^2,\ r^3,\ \cdots,\ r^{\phi(n)}\right\}$$

belong to the reduced residue system modulo n.

Let $r^m \in S$ then r^m is a primitive root of p if it has order $\phi\left(n\right)$.

By Corollary (6.9) we have

$$r^m \text{ has order } \phi\left(n\right) \quad \Leftrightarrow \quad \gcd\left(m,\ \phi\left(n\right)\right) = 1$$

It is the number of integers m which are relatively prime to $\phi\left(n\right)$. This is given by the Euler phi function. Hence the number of primitive roots of n is $\phi\left(\phi\left(n\right)\right)$.

This completes our proof.

■

18. We are asked to prove that if a has order $n-1$ modulo n then n is prime.

Proof.

We are given that a has order $n-1$ modulo n which gives

$$a^{n-1} \equiv 1 \left(\text{mod } n\right).$$

This implies that the *smallest positive* index of a with this property is $n-1$. By the definition of the Euler totient function $\phi\left(n\right) \leq n-1$ for $n > 1$. *Why?*

Because the definition is

$$\phi\left(n\right) = Card\left\{m \;\middle|\; \gcd\left(m,\ \ n\right) = 1 \text{ and } 1 \leq m \leq n\right\}.$$

And this set can have at most $n-1$ elements. Hence a must be primitive root of n. *Why?*

Because we are given that the order of a modulo n is $n-1$.

Since a is primitive root so $\phi\left(n\right) = n-1$. By Proposition (5.2):

$$n \text{ is prime} \Leftrightarrow \phi\left(n\right) = n-1$$

Thus n is prime. This completes our proof.

■

19. We are asked to solve $x^6 \equiv 11 \pmod{19}$. Since 19 is prime so it has a primitive root. We need to find one. Let us test 2 for a primitive root. The factors of $\phi(19) = 19 - 1 = 18$ are 1, 2, 3, 6, 9 and 18. We have

$$2^5 \equiv 32 \equiv 13 \pmod{19}$$

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

$$2^9 \equiv 8 \times 7 \equiv 56 \equiv -1 \pmod{19}$$

Hence 2 is a primitive root of 19.

Taking index to the base 2 of the given equation $x^6 \equiv 11 \pmod{19}$ yields

$$\text{ind}_2(x^6) \equiv \text{ind}_2(11) \pmod{18}$$

$$6 \times \text{ind}_2(x) \equiv \text{ind}_2(11) \pmod{18} \qquad (*)$$

We need to find $\text{ind}_2(11)$. We know that $7^2 \equiv 49 \equiv 11 \pmod{19}$ so squaring $2^6 \equiv 7 \pmod{19}$ gives

$$2^{12} \equiv 7^2 \equiv 11 \pmod{19}.$$

Therefore $\text{ind}_2(11) = 12$ and substituting this into (*) gives

$$6 \times \text{ind}_2(x) \equiv 12 \pmod{18}.$$

The $\gcd(6, 18) = 6$ and $6 \mid 18$ so the given congruence equation has 6 incongruent solutions. Dividing through by 6 gives

$$\text{ind}_2(x) \equiv 2 \pmod{3} \iff \text{ind}_2(x) = 2 + 3k.$$

Hence, we have $\text{ind}_2(x) = 2 + 3k \equiv 2, 5, 8, 11, 14, 17 \pmod{18}$. Therefore

$$\begin{aligned} x &\equiv 2^2, 2^5, 2^8, 2^{11}, 2^{14}, 2^{17} \\ &\equiv 4, 13, 13 \times 8, -1 \times 4, -4 \times 8, -4 \times 7 \\ &\equiv 4, 13, 9, 15, 6, 10 \pmod{19} \end{aligned}$$

Our solutions in ascending order are $x \equiv 4, 6, 9, 10, 13, 15 \pmod{19}$.

We also need to solve the Diophantine equation $x^6 = 11 + 19y$. Substituting $x = 4,\ 6,\ 9,\ 10,\ 13,\ 15$ into $x^6 = 11 + 19y$ and transposing gives

$$4^6 = 4096 = 11 + 19y \ \Rightarrow\ y = \frac{4096 - 11}{19} = 215$$

$$6^6 = 46\,656 = 11 + 19y \ \Rightarrow\ y = \frac{46\,656 - 11}{19} = 2455$$

$$9^6 = 531\,441 = 11 + 19y \ \Rightarrow\ y = \frac{531\,441 - 11}{19} = 27\,970$$

$$10^6 = 1\,000\,000 = 11 + 19y \ \Rightarrow\ y = \frac{1\,000\,000 - 11}{19} = 52\,631$$

$$13^6 = 4\,826\,809 = 11 + 19y \ \Rightarrow\ y = \frac{4\,826\,809 - 11}{19} = 254\,042$$

$$15^6 = 11\,390\,625 = 11 + 19y \ \Rightarrow\ y = \frac{11\,390\,625 - 11}{19} = 599\,506$$

Our solutions are $\{x = 4, y = 215\}$, $\{x = 6, y = 2455\}$, $\{x = 9, y = 27\,970\}$, $\{x = 10, y = 52\,631\}$, $\{x = 13, y = 254\,042\}$ and $\{x = 15, y = 599\,506\}$.

20. The positive integer $n = 15$ has no primitive roots because the relatively prime integers with 15 are $\{1, 2, 4, 7, 8, 11, 13, 14\}$ which means that $\phi(15) = 8$ and the order of these is given in the table below:

Integer	1	2	4	7	8	11	13	14
Order	1	4	2	4	4	2	4	2

None of the relatively prime integers have order 8 so 15 has *no* primitive roots.

21. We need to show that mn does *not* necessarily have primitive roots given that both m and n have primitive roots.

How?

Produce a counter example.

Let $m = 3$ and $n = 5$ then both have primitive roots. *Why?*

Because 3 and 5 are prime and by Primitive Root Theorem (6.21):

Every prime has a primitive root.

However we have shown in the previous question that $m \times n = 3 \times 5 = 15$ does *not* have primitive roots.

22. (i) We are asked to prove $r^{2^{m-2}} \equiv 1 \pmod{2^m}$ for $m \geq 3$.

Proof.

We use mathematical induction.

Let $m = 3$ then we need to check that

$$r^{2^{3-2}} \equiv r^2 \equiv 1 \pmod{8}.$$

How do we know $r^2 \equiv 1 \pmod{8}$ *is true for all* r*?*

Well we are given that r is odd so let $r = 2j+1$. Then we have

$$\begin{aligned} r^2 = (2j+1)^2 &= 4j^2 + 4j + 1 \\ &= 4j(j+1) + 1 \end{aligned}$$

Now the product of two consecutive numbers $j(j+1)$ must be even, say $2l$.

Therefore we have

$$r^2 = 4j(j+1) + 1 = 4(2l) + 1 = 8l + 1.$$

Hence $r^2 \equiv 1 \pmod{8}$ which implies that the result is true for $m = 3$.

Assume the result is true for $m = k$, that is

$$r^{2^{k-2}} \equiv 1 \pmod{2^k} \qquad (\dagger)$$

Required to prove the result for $m = k+1$:

$$r^{2^{k-1}} \equiv 1 \pmod{2^{k+1}}$$

Examining the left hand side of this

$$r^{2^{k-1}} \equiv r^{2^{k-2+1}} \equiv r^{2^{k-2}2} \equiv \left(r^{2^{k-2}}\right)^2 \pmod{2^{k+1}} \qquad (*)$$

We have an expression for $r^{2^{k-2}}$ from (†). Using this and the definition of congruence

$$r^{2^{k-2}} = 1 + \alpha 2^k \text{ where } \alpha \text{ is an integer.}$$

Squaring this gives

$$\begin{aligned} \left(r^{2^{k-2}}\right)^2 = (\alpha 2^k + 1)^2 &= \alpha^2 (2^k)^2 + 2\alpha 2^k + 1 \\ &= 2^k \left[\alpha^2 2^k + 2\alpha\right] + 1 \\ &= 2^k 2 \left[\alpha^2 2^{k-1} + \alpha\right] + 1 \\ &= 2^{k+1} \left[\alpha^2 2^{k-1} + \alpha\right] + 1 \end{aligned}$$

Note that we have $\left(r^{2^{k-2}}\right)^2 = 2^{k+1}\underbrace{\left[\alpha^2 2^{k-1} + \alpha\right]}_{\text{integer}} + 1$. Hence

$$\left(r^{2^{k-2}}\right)^2 = 2^{k+1}\left[\text{integer}\right] + 1 \equiv 0 + 1 \equiv 1 \left(\text{mod } 2^{k+1}\right).$$

Substituting this into (*) yields

$$r^{2^{k-1}} \equiv \left(r^{2^{k-2}}\right)^2 \equiv 1 \left(\text{mod } 2^{k+1}\right)$$

which is our required result.

By mathematical induction we have $r^{2^{m-2}} \equiv 1 \left(\text{mod } 2^m\right)$ for $m \geq 3$.

■

(ii) In this part we are asked to prove that the integer 2^m for $m \geq 3$ has *no* primitive roots. *How do we prove this?*

By contradiction and then use the result of part (i).

Proof.

Suppose r is a primitive root of 2^m. Then clearly r is odd because we can only have an order provided $\gcd\left(r, \quad 2^m\right) = 1$.

The order of $r \left(\text{mod } 2^m\right)$ is given by the Euler phi function of 2^m which is

$$\phi\left(2^m\right) = 2^m\left(1 - \frac{1}{2}\right) = 2^{m-1}.$$

Therefore, we have that the order of $r \left(\text{mod } 2^m\right)$ is 2^{m-1} which implies that

$$r^{2^{m-1}} \equiv 1 \left(\text{mod } 2^m\right).$$

where 2^{m-1} is the smallest positive integer such that the result holds.

However, by part (i) we have $r^{2^{m-2}} \equiv 1 \left(\text{mod } 2^m\right)$ and the index $2^{m-2} < 2^{m-1}$.

This is a contradiction because we have found a lower index therefore our supposition of r being a primitive root of 2^m must be false.

Thus 2^m for $m \geq 3$ has *no* primitive roots.

■

23. We are asked to show if $m, \quad n > 2$ and $\gcd\left(m, \quad n\right) = 1$ then the integer mn has *no* primitive roots.

Proof.

Let r be a primitive root of mn. This implies the order of r is

$$\phi\left(mn\right) = \phi\left(m\right)\phi\left(n\right) \qquad \left[\text{Because } \gcd\left(m, \quad n\right) = 1\right]$$

By Euler's theorem we have

$$r^{\phi(m)} \equiv 1 \pmod{m} \quad \text{and} \quad r^{\phi(n)} \equiv 1 \pmod{n}$$

By Proposition (5.10):

> For $k > 2$, $\phi(k)$ is an even integer.

We have $\phi(n)$ is an even integer so $\dfrac{\phi(n)}{2}$ is an integer. Therefore

$$\left(r^{\phi(m)}\right)^{\frac{\phi(n)}{2}} \equiv r^{\phi(m)\frac{\phi(n)}{2}} \equiv r^{\frac{\phi(m)\phi(n)}{2}} \equiv 1 \pmod{m}.$$

Similarly, $\dfrac{\phi(m)}{2}$ is an integer so

$$\left(r^{\phi(n)}\right)^{\frac{\phi(m)}{2}} \equiv r^{\phi(n)\frac{\phi(m)}{2}} \equiv r^{\frac{\phi(n)\phi(m)}{2}} \equiv 1 \pmod{n}.$$

Using the result given in the hint on

$$r^{\frac{\phi(m)\phi(n)}{2}} \equiv 1 \pmod{m} \quad \text{and} \quad r^{\frac{\phi(n)\phi(m)}{2}} \equiv 1 \pmod{n}.$$

Yields

$$r^{\frac{\phi(m)\phi(n)}{2}} \equiv 1 \pmod{mn} \quad \left[\text{LCM of } (m,\ n) \text{ is } mn\right]$$

We have an index $\dfrac{\phi(m)\phi(n)}{2} < \phi(m)\phi(n)$ so r *cannot* be a primitive root of modulo mn.

Hence the integer mn has *no* primitive roots.

■

24. We need to prove that $r^{\frac{\phi(n)}{2}} \equiv 1 \pmod{n}$ given that n has *no* primitive roots.

Proof.

The integer n must be *composite* because by result of question 17:

> Every prime p has $\phi(p-1)$ incongruent primitive roots.

If $n = p^k$ for odd prime p and $k \geq 2$ then it has a primitive root. *Why?*

By Theorem (6.27):

> p^k for $k \geq 1$ has a primitive root

If $n = 2p^r$ then by Proposition (6.30):

There is a primitive root of $2\,p^k$ where $k \geq 1$.

The integer $n = 2p^r$ has primitive roots. Hence $n \neq p^k$ and $n \neq 2p^k$.

Let r be a member of the reduced residue system modulo n.

We consider two cases of n for which there are *no* primitive roots.

Case 1 For $n = 2^m$.

If $n = 2^m$ for $m \geq 3$ then by the result of question 22 (i):

$$r^{2^{m-2}} \equiv 1 \pmod{2^m}$$

We have $\phi\left(2^m\right) = 2^{m-1}$ therefore $\dfrac{\phi\left(2^m\right)}{2} = \dfrac{2^{m-1}}{2} = 2^{m-2}$. Putting this into the above yields

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

Hence for $n = 2^m$ we have our required result.

Case II For $n = mk$ where $\gcd\left(m,\ \ k\right) = 1$ and $m, k > 2$.

By the solution of the previous question we have:

$$r^{\frac{\phi(m)\phi(k)}{2}} \equiv 1 \pmod{mk}$$

Recall that $\phi\left(n\right) = \phi\left(mk\right) = \phi\left(m\right)\phi\left(k\right)$ because $\gcd\left(m,\ \ k\right) = 1$. Hence we have

$$r^{\frac{\phi(m)\phi(k)}{2}} \equiv r^{\frac{\phi(mk)}{2}} \equiv 1 \pmod{mk}$$

This is our required result for $n = mk$.

This completes our proof.

■