Complete Solutions to Exercises 6.2

1. The gcd of each of the given integers and 5 is 1 so they are relatively prime which implies that in each case the order of the given integer modulo 5 exists.

(a) Clearly $1^1 \equiv 1 \pmod 5$ so the order of $1 \pmod 5$ is 1.

(b) We need to find the order of $2 \pmod 5$. By Corollary (6.5):

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

We have the order of $2 \pmod 5$ is a factor of $\phi(5) = 4$. Evaluating the indices 1, 2 and 4 of base 2 gives

$$2^1 \equiv 2,\ \ 2^2 \equiv 4 \equiv -1,\ 2^4 \equiv 1 \pmod 5.$$

Hence the order of $2 \pmod 5$ is 4. We didn't need to evaluate $2^4 \pmod 5$ because by Euler's Theorem we have $2^{\phi(5)} \equiv 2^4 \equiv 1 \pmod 5$.

(c) We are asked to find the order of $3 \pmod 5$. Using the positive divisors of 4 as indices of base 3 we have

$$3^1 \equiv 3,\ \ 3^2 \equiv 9,\ 3^4 \equiv 1 \pmod 5.$$

The order of $3 \pmod 5$ is 4.

(d) To find the order of $4 \pmod 5$ we note that

$$4 \equiv -1 \pmod 5 \quad \text{implies} \quad 4^2 \equiv (-1)^2 \equiv 1 \pmod 5.$$

The order of $4 \pmod 5$ is 2.

2. (a) The $\gcd(2,\ \ 11) = 1$ so the order of $2 \pmod{11}$ exists. Since 11 is prime so $\phi(11) = 10$ and the order must be a positive divisor of 10. The positive divisors of 10 are 1, 2, 5 and 10. We only need to evaluate the indices 2 and 5 because $2^1 \equiv 2 \pmod{11}$ and 10 index is going to give 1 modulo 11 by Euler's Theorem.

$$2^2 \equiv 4,\ 2^5 \equiv 32 \not\equiv 1 \pmod{11}.$$

Hence the order of $2 \pmod{11}$ is 10.

(b) Similarly we find the order of $3 \pmod{11}$:

$$3^2 \equiv 9,\ 3^5 \equiv 243 \equiv 1 \pmod{11}.$$

Therefore, the order of $3\pmod{11}$ is 5.

(c) This time we are asked to find the order of $5\pmod{11}$. Preceding as in the last two parts we have

$$5^2 \equiv 25 \equiv 3,\ 5^5 \equiv 5^4 \times 5 \equiv 3^2 \times 5 \equiv 45 \equiv 1\pmod{11}.$$

The order of $3\pmod{11}$ is 5.

(d) Again repeating the same argument we have

$$7^2 \equiv 49 \equiv 5,\ 7^5 \equiv 7^4 \times 7 \equiv 5^2 \times 7 \equiv 3 \times 7 \equiv 21 \equiv 10 \not\equiv 1\pmod{11}.$$

The order of $7\pmod{11}$ is 10.

3. We are asked to find the order of $1, 2, 3, 4, 5, 6, 7, 8, 9, 10\pmod{2520}$.

Clearly the order of $1\pmod{2520}$ is 1 because $1^1 \equiv 1\pmod{2520}$.

The remaining orders do not exist because

$$\gcd(2,\ 2520) = 2,\ \gcd(3,\ 2520) = 3,\ \gcd(4,\ 2520) = 4, \cdots, \gcd(10,\ 2520) = 10$$

None of the integers are relatively prime with 2520 so these integers have no order.

4. We need to find

$$3^1,\ 3^2,\ 3^3,\ \cdots, 3^{\phi(17)}\pmod{17}.$$

Since 17 is prime we have $\phi(17) = 16$. Evaluating each of these gives

$$3^1 \equiv 3,\ 3^2 \equiv 9,\ 3^3 \equiv 27 \equiv 10,\ 3^4 \equiv \left(3^2\right)^2 \equiv 81 \equiv 13,\ 3^5 \equiv 13 \times 3 \equiv 39 \equiv 5\pmod{17}$$

$$3^6 \equiv 5 \times 3 \equiv 15,\ 3^7 \equiv (-2) \times 3 \equiv 11,\ 3^8 \equiv \left(3^4\right)^2 \equiv (-4)^2 \equiv 16,\ 3^9 \equiv 3^8 \times 3 \equiv 14\pmod{17}$$

$$3^{10} \equiv 5^2 \equiv 8,\ 3^{11} \equiv 8 \times 3 \equiv 7,\ 3^{12} \equiv 7 \times 3 \equiv 4,\ 3^{13} \equiv 4 \times 3 \equiv 5,\ 3^{14} \equiv 5 \times 3 \equiv 15\pmod{17}$$

$$3^{15} \equiv 3^{14} \times 3 \equiv 15 \times 3 \equiv 11,\ 3^{16} \equiv \left(3^8\right)^2 \equiv (-1)^2 \equiv 1\pmod{17}$$

Notice that $3^x\pmod{17}$ generates the reduced residues system modulo 17:

$$\{1, 2, 3, 4, 5, \cdots, 15, 16\} \text{ in some order.}$$

5. (i) We need to find $7^1,\ 7^2,\ 7^3,\ \cdots, 7^{\phi(11)}\pmod{11}$ where $\phi(11) = 10$. By Euler's Theorem we have $7^{10} \equiv 1\pmod{11}$. Evaluating the remaining indices:

$$7^1 \equiv 7,\ \ 7^2 \equiv 5,\ \ 7^3 \equiv 5\times 7 \equiv 2, 7^4 \equiv 2\times 7 \equiv 3,\ \ 7^5 \equiv 3\times 7 \equiv 10,\ \ 7^6 \equiv \left(7^3\right)^2 \equiv 4 \left(\text{mod } 11\right)$$

$$7^7 \equiv 4\times 7 \equiv 6,\ \ 7^8 \equiv \left(7^4\right)^2 \equiv 3^2 \equiv 9,\ \ 7^9 \equiv 9\times 7 \equiv 63 \equiv 8 \left(\text{mod } 11\right)$$

From our results we can see that $7^x \left(\text{mod } 11\right)$ gives the reduced residues system modulo 11:

$$\left\{1, 2, 3, 4, 5, 7, 8, 9, 10\right\} \left(\text{mod } 11\right)$$

Completing the given table by using these results yields:

Integer a	1	2	3	4	5	6	7	8	9	10
s where $7^s \equiv a \left(\text{mod } 11\right)$	10	3	4	6	2	7	1	9	8	5

(ii) Evaluating the order of each of these integers modulo 11 by using the Order Formula (6.8):

$$\text{Order of } \ a^s = \frac{k}{\gcd\left(s,\ \ k\right)} \ \text{ where } k \text{ is the order of } a.$$

With $a = 7$ and the order of $7 \left(\text{mod } 11\right)$ is 10 so we let $k = 10$. In each case we need to evaluate

$$\text{Order of } \ 7^s = \frac{10}{\gcd\left(s,\ \ 10\right)}.$$

From the table of part (i) we have the following derivations:

The order of $7^{10} \equiv 1 \left(\text{mod } 11\right)$ is

$$\frac{10}{\gcd\left(10,\ \ 10\right)} = \frac{10}{10} = 1 \qquad \left[\text{Using (6.8) with } s = 10\right]$$

The order of $7^3 \equiv 2 \left(\text{mod } 11\right)$ is

$$\frac{10}{\gcd\left(3,\ \ 10\right)} = \frac{10}{1} = 10 \qquad \left[\text{Using (6.8) with } s = 3 \ \text{ and } \ k = 10\right]$$

The order of $7^4 \equiv 3 \ \left(\text{mod } 11\right)$ is

$$\frac{10}{\gcd\left(4,\ \ 10\right)} = \frac{10}{2} = 5 \qquad \left[\text{Using (6.8) with } s = 4 \ \text{ and } \ k = 10\right]$$

The order of $7^6 \equiv 4 \ \left(\text{mod } 11\right)$ is

$$\frac{10}{\gcd\left(6,\ \ 10\right)} = \frac{10}{2} = 5 \qquad \left[\text{Using (6.8) with } s = 6 \ \text{ and } \ k = 10\right]$$

The order of $7^2 \equiv 5 \pmod{11}$ is

$$\frac{10}{\gcd(2,\ 10)} = \frac{10}{2} = 5 \qquad [\text{Using (6.8) with } s = 2 \text{ and } k = 10]$$

The order of $7^7 \equiv 6 \pmod{11}$ is

$$\frac{10}{\gcd(7,\ 10)} = \frac{10}{1} = 10 \qquad [\text{Using (6.8) with } s = 7 \text{ and } k = 10]$$

The order of $7^1 \equiv 7 \pmod{11}$ is

$$\frac{10}{\gcd(1,\ 10)} = \frac{10}{1} = 10 \qquad [\text{Using (6.8) with } s = 1 \text{ and } k = 10]$$

The order of $7^9 \equiv 8 \pmod{11}$ is

$$\frac{10}{\gcd(9,\ 10)} = \frac{10}{1} = 10 \qquad [\text{Using (6.8) with } s = 9 \text{ and } k = 10]$$

The order of $7^8 \equiv 9 \pmod{11}$ is

$$\frac{10}{\gcd(8,\ 10)} = \frac{10}{2} = 5 \qquad [\text{Using (6.8) with } s = 8 \text{ and } k = 10]$$

The order of $7^5 \equiv 10 \pmod{11}$ is

$$\frac{10}{\gcd(5,\ 10)} = \frac{10}{5} = 2 \qquad [\text{Using (6.8) with } s = 5 \text{ and } k = 10]$$

Collecting all these results in a table gives

Integer a	1	2	3	4	5	6	7	8	9	10
Order of $a \pmod{11}$	1	10	5	5	5	10	10	10	5	2

Note that order of $a \pmod{11}$ must be a factor of 10.

6. We employ the same method as we did in Example 13.

$$1^1 \equiv 1 (\text{mod } 13).$$

Again, we'll express each integer a in terms of 2^a and use Order Formula (6.8) each time. In example 12, we were given that the order of 2 modulo 13 is 12, this is our k which we use in Order Formula (6.8):

$$2^2 \equiv 4 \ (\text{mod } 13)$$

The order of $a = 4$ is

$$\frac{12}{\gcd(2,12)} = \frac{12}{2} = 6$$

$$2^3 \equiv 8 \pmod{13}$$

The order of $a = 8$ is

$$\frac{12}{\gcd(3,12)} = \frac{12}{3} = 4$$

$$2^4 \equiv 16 \equiv 3 \pmod{13}$$

The order of $a = 3$ is

$$\frac{12}{\gcd(4,12)} = \frac{12}{4} = 3$$

$$2^5 \equiv 32 \equiv 6 \pmod{13}$$

The order of $a = 6$ is

$$\frac{12}{\gcd(5,12)} = \frac{12}{1} = 12$$

$$2^6 \equiv 64 \equiv 12 \pmod{13}$$

The order of $a = 12$ is

$$\frac{12}{\gcd(6,12)} = \frac{12}{6} = 2$$

$$2^7 \equiv 128 \equiv 11 \pmod{13}$$

The order of $a = 11$ is

$$\frac{12}{\gcd(7,12)} = \frac{12}{1} = 12$$

$$2^8 \equiv 256 \equiv 9 \pmod{13}$$

The order of $a = 9$ is

$$\frac{12}{\gcd(8,12)} = \frac{12}{4} = 3$$

$$2^9 \equiv 512 \equiv 5 \pmod{13}$$

The order of $a = 5$ is

$$\frac{12}{\gcd(9,12)} = \frac{12}{3} = 4$$

$$2^{10} \equiv 1024 \equiv 10 \pmod{13}$$

The order of $a = 10$ is

$$\frac{12}{\gcd(10,12)} = \frac{12}{2} = 6$$

$$2^{11} \equiv 2048 \equiv 7 \pmod{13}$$

The order of $a = 7$ is

$$\frac{12}{\gcd(11,12)} = \frac{12}{1} = 12$$

Filling in our table gives:

Integer a	1	2	3	4	5	6	7	8	9	10	11	12
Order k	1	12	3	6	4	12	12	4	3	6	12	2

Note that the order of $a \pmod{13}$ must be a factor of 12.

7. We are asked to find the orders of the complete residue system modulo 12. Recall that the *only* integers modulo 12 which have an order are the ones which are relatively prime to 12 or the ones which have a multiplicative inverse modulo 12. Therefore only 1, 5, 7 and 11 modulo 12 have an order.
   Since $1^1 \equiv 1 \pmod{12}$ so $1 \pmod{12}$ has order 1.
   The order of $11 \pmod{12}$ is easy because

$$11 \equiv -1 \quad \Rightarrow \quad 11^2 \equiv (-1)^2 \equiv 1 \pmod{12}.$$

   The order of $11 \pmod{12}$ is 2.
   The order of $5 \pmod{12}$ will be a positive divisor of $\phi(12)$ and from above we have $\phi(12) = 4$ because only 1, 5, 7 and 11 have an inverse modulo 12.
   Therefore, we evaluate the indices 1, 2 and 4 only.

$$5^1 \equiv 5, \;\; 5^2 \equiv 25 \equiv 1 \pmod{12}.$$

   The order of $5 \pmod{12}$ is 2.
   Lastly, we need to find the order of $7 \pmod{12}$:

$$7^1 \equiv 7, \;\; 7^2 \equiv 49 \equiv 1 \pmod{12}.$$

   Hence the order of $7 \pmod{12}$ is 2.
   The order for the remaining integers modulo 12 does *not* exist.

8. The number of integers which have order modulo n are the ones which are relatively prime to n. *How do we count the number of integers between 1 and n that are relatively prime to n?*
   By $\phi(n)$.

(a) We have $\phi\left(20\right)=\phi\left(2^2\times 5\right)=\phi\left(2^2\right)\times\phi\left(5\right)=\left(4-2\right)\times 4=8$. There are 8 integers modulo 20 which have an order.

(b) Similarly, we have

$$\phi\left(200\right)=\phi\left(2^3\times 5^2\right)=\phi\left(2^3\right)\times\phi\left(5^2\right)=\left(8-4\right)\times\left(25-20\right)=80\,.$$

There are 80 integers modulo 200 which have an order.

(c) We also have

$$\phi\left(2000\right)=2000\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)=800\,.$$

The number of integers which have an order modulo 2000 is 800.

(d) Arguing along the same lines:

$$\phi\left(20\ 000\right)=20\ 000\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)=8000\,.$$

There are 8000 integers modulo 20 000 where the order exists.

9. (a) We are asked to show that the order of $1\left(\text{mod } n\right)$ is 1.

Proof.

Since $1^1\equiv 1\left(\text{mod } n\right)$ so by the definition of order we have order of $1\left(\text{mod } n\right)$ is 1.

■

(b) We need to show that the order of $\left(n-1\right)\left(\text{mod } n\right)$ is 2.

Proof.

The $\gcd\left(n-1,\quad n\right)=1$. *Why?*

Suppose $\gcd\left(n-1,\quad n\right)=g>1$ then $g\,\middle|\,\left(n-1\right)$ and $g\,\middle|\,n$. This implies

$$g\,\middle|\,\left[n-\left(n-1\right)\right]\quad\Rightarrow\quad g\,\middle|\,1\,.$$

This result $g\,\middle|\,1$ is impossible because $g>1$. Therefore $\gcd\left(n-1,\quad n\right)=1$ and the order of $\left(n-1\right)\left(\text{mod } n\right)$ exists.

Note that $n-1\equiv -1\left(\text{mod } n\right)$. Squaring both sides gives

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

Therefore, the order of $\left(n-1\right)\left(\text{mod } n\right)$ is 2.

■

10. (a) We are required to prove that $a^{\frac{k}{2}} \equiv (p-1)\pmod{p}$ given $\gcd(a, \quad p) = 1$.

Proof.

We are given that $\gcd(a, \quad p) = 1$ so the order of $a\pmod{p}$ exists. We are also given that k is the order of $a\pmod{p}$ so

$$a^k \equiv 1\pmod{p}.$$

We are given that k is even so we can write this congruence as

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

Let $x = a^{\frac{k}{2}}$ then we have $x^2 \equiv 1\pmod{p}$. By Proposition (3.14) (b):

$$a^2 \equiv b^2 \pmod{p} \Leftrightarrow a \equiv \pm b \pmod{p}$$

Applying this to the above $x^2 \equiv 1 \equiv 1^2 \pmod{p}$ implies

$$x \equiv \pm 1\pmod{p}.$$

Therefore $x = a^{\frac{k}{2}} \equiv \pm 1\pmod{p}$. However $a^{\frac{k}{2}} \not\equiv 1\pmod{p}$. *Why not?*

Because we are given that k is the order of $a\pmod{p}$ and $\frac{k}{2} < k$ so

$$a^{\frac{k}{2}} \equiv -1 \equiv (p-1)\pmod{p}.$$

This completes our proof. ■

(b) *How do we disprove* $a^{\frac{k}{2}} \equiv \pm 1\pmod{n}$ *given* $\gcd(a, \quad n) = 1$ *?*

By producing a counter example.

Let $a = 2, \quad n = 15$ then $\gcd(2, \quad 15) = 1$ so the order of $2\pmod{15}$ exists and it is 4 because $2^4 \equiv 16 \equiv 1\pmod{15}$. However

$$2^{\frac{4}{2}} \equiv 2^2 \equiv 4 \not\equiv \pm 1\pmod{15}.$$

11. We need to disprove the following statement:

$$\text{If } a^{\frac{\phi(n)}{2}} \not\equiv 1\pmod{n} \text{ then the order of } a\pmod{n} \text{ is } \phi(n).$$

This means we need to produce a counter example.

Evaluating $10^{\frac{\phi(11)}{2}} \equiv 10^{\frac{10}{2}} \equiv 10^5 \equiv 10 \not\equiv 1 \pmod{11}$ but the order of 10 modulo 11 is $2 \neq \phi(11) = 10$ (see the result of the bottom table of question 5).

12. We need to prove:

If $a^k \not\equiv 1 \pmod{n}$ where $1 \le k \le \dfrac{\phi(n)}{2}$ then the order of $a \pmod{n}$ is $\phi(n)$.

Proof.

The order of $a \pmod{n}$ exists because we are given that a and n are relatively prime. Let r be the order of $a \pmod{n}$. Required to prove that $r = \phi(n)$.

By Corollary (6.5):

> Let a modulo n have order k. Then $k \mid \phi(n)$.

We have $r \mid \phi(n)$ which implies that $0 < r < \phi(n)$ or $r = \phi(n)$.

Since we are given $a^k \not\equiv 1 \pmod{n}$ where $1 \le k \le \dfrac{\phi(n)}{2}$ so by definition of order, $r > \dfrac{\phi(n)}{2}$. By question 19 of Exercise 1(a):

> $$m \mid n \;\Rightarrow\; m \le \frac{n}{2} \text{ where } m < n$$

Since $r > \dfrac{\phi(n)}{2}$ and $r \mid \phi(n)$ so $r = \phi(n)$.

■

13. Note that $32 = 2^5$ so we first find the order of $2 \pmod{89}$. Since 2 and 89 are relatively prime so by Euler's Theorem we have (recall 89 is prime)

$$2^{\phi(89)} \equiv 2^{88} \equiv 1 \pmod{89}.$$

We use Corollary (6.5):

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

Therefore, the order of $2 \pmod{89}$ is a positive divisor of 88. The prime factorization of 88 is $88 = 2^3 \times 11$ and so the positive divisors of 88 are

$$\{1, 2, 4, 8, 11, 22, 44, 88\}.$$

Clearly the indices 1, 2 and 4 of base 2 do *not* give $1 \pmod{89}$. Trying the next integer, 8, in the list as an index of 2:

$$2^8 \equiv 256 \equiv 78 \pmod{89}.$$

Similarly evaluating the next three integers in the list as indices of 2;

$$2^{11} \equiv 2^8 \times 2^3 \equiv 78 \times 8 \equiv 624 \equiv 1 \pmod{89}.$$

Hence we don't need to find any more of the indices as we have resulted in 1 modulo 89 with $2^{11} \equiv 1 \pmod{89}$. The order of $2 \pmod{89}$ is 11.

However we were asked to find the order of $32 = 2^5 \pmod{89}$. *How?*

Use the Order Formula (6.8):

> Let $a \pmod{n}$ have order k. Then $a^s \pmod{n}$ has order $\dfrac{k}{\gcd(s,\ k)}$.

Using this order formula we have

$$2^5 \pmod{89} \text{ has order } \frac{11}{\gcd(5,\ 11)} = \frac{11}{1} = 11.$$

The order of $32 \pmod{89}$ has order 11.

14. (a) We are asked to find the order of $81 \pmod{105}$. First note that 27 and 105 are *both* multiples of 3 so the $\gcd(81,\ 105) = 3 \neq 1$. By the definition of order, the order of $81 \pmod{105}$ does *not* exist.

(b) First we check that 81 and 106 are relatively prime;

$$\gcd(81,\ 106) = 1.$$

This gcd of 1 implies that the order of $81 \pmod{106}$ does exist.

Also notice that $81 = 3^4$. First we find the order of $3 \pmod{106}$ and then by the order formula we deduce the order of $81 \pmod{106}$.

By Euler's Theorem with

$$\phi(106) = \phi(2 \times 53) = \phi(2) \times \phi(53) = 1 \times 52 = 52.$$

We have $3^{52} \equiv 1 \pmod{106}$.

The order of $3 \pmod{106}$ is a positive divisor of 52. The positive divisors of 52 are $\{1, 2, 4, 13, 26, 52\}$. Clearly the indices 1, 2 and 4 of base 3 do *not* give 1 modulo 106. We only need to evaluate the indices 13 and 26 because from above we already have the index 52 of base 3. Thus

$$3^{13} \equiv (3^4)^3 \times 3 \equiv 81^3 \times 3 \equiv (-25)^3 \times 3 \equiv (-15\,625) \times 3 \equiv (-63) \times 3 \equiv -23 \equiv 83 \pmod{106}$$

$$3^{26} \equiv \left(3^{13}\right)^2 \equiv 83^2 \equiv 6889 \equiv 105 \left(\text{mod } 106\right)$$

Hence the order of $3\left(\text{mod } 106\right)$ is 52. Now using the Order Formula (6.8):

> Let $a\left(\text{mod } n\right)$ have order k. Then $a^s\left(\text{mod } n\right)$ has order $\dfrac{k}{\gcd\left(s,\ k\right)}$.

with $a = 3$ we have the order of

$$81 \equiv 3^4 \left(\text{mod } 106\right) \text{ is } \frac{52}{\gcd\left(4,\ 52\right)} = \frac{52}{4} = 13\,.$$

The order of $81\left(\text{mod } 106\right)$ is 13.

15. This question is phrased slightly differently to the ones in the previous exercises. We are asked to find the least positive integer x such that $4^x - 1$ is divisible by 83. This implies we need to find order of $4\left(\text{mod } 83\right)$ because this will give us $4^x \equiv 1\left(\text{mod } 83\right)$. Now 83 is prime so 4 and 83 are relatively prime and $4 = 2^2$. First we find the order of $2\left(\text{mod } 83\right)$ and then use the order formula. Since 83 is prime so $\phi\left(83\right) = 82$ and we have

$$2^{82} \equiv 1\left(\text{mod } 83\right).$$

The order of $2\left(\text{mod } 83\right)$ is a positive divisor of 82. The set of positive divisors of 82 are $\{1, 2, 41, 82\}$. We only need to test the index 41 because the indices 1 and 2 are clearly *not* going to give us $1\left(\text{mod } 83\right)$.

$$2^{41} \equiv y\left(\text{mod } 83\right).$$

Evaluating smaller powers of 2:

$$2^6 \equiv 64 \equiv -19\left(\text{mod } 83\right)$$

$$2^8 \equiv 2^6 \times 2^2 \equiv \left(-19\right) \times 4 \equiv -76 \equiv 7\left(\text{mod } 83\right)$$

$$\begin{aligned} 2^{41} \equiv \left(2^8\right)^5 \times 2 \equiv 7^5 \times 2 \equiv 49^2 \times 7 \times 2 \\ \equiv 2401 \times 14 \equiv 77 \times 14 \equiv \left(-6\right) \times 14 \equiv -84 \equiv -1\left(\text{mod } 83\right) \end{aligned}$$

Hence the order of $2\left(\text{mod } 83\right)$ is 82. By the Order Formula (6.8):

> Let $a\left(\text{mod } n\right)$ have order k. Then $a^s\left(\text{mod } n\right)$ has order $\dfrac{k}{\gcd\left(s,\ k\right)}$.

We deduce the order of $2^2 \equiv 4 \pmod{83}$ is $\dfrac{82}{\gcd(2,\ 82)} = \dfrac{82}{2} = 41$. Hence the smallest positive index x such that $83 \mid (4^x - 1)$ is 41.

16. We have to find the order of $2 \pmod{1001}$. The modulo 1001 factorizes into

$$1001 = 7 \times 11 \times 13 .$$

By Euler's Theorem we have

$$\phi(1001) = \phi(7) \times \phi(11) \times \phi(13) = 6 \times 10 \times 12 = 720 \qquad (*)$$

Let k be the order of $2 \pmod{1001}$ then by Corollary (6.5):

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

We have $k \mid 720$. Let us select some of the divisors of 720 from (*):

$$2^6 \equiv 64 \not\equiv 1 \pmod{1001}$$

$$2^{10} \equiv 1024 \equiv 23 \not\equiv 1 \pmod{1001}$$

$$2^{12} \equiv 23 \times 4 \equiv 92 \not\equiv 1 \pmod{1001}$$

Now let us consider product of two divisors:

$$6 \times 10 \quad \text{but } 2^{60} \equiv \underbrace{\left(2^{10}\right)^6}_{\text{From above}} \equiv 23^6 \equiv x \pmod{1001} \qquad (\dagger)$$

We need to evaluate $23^6 \equiv x \pmod{1001}$:

$$23^2 \equiv 529 \pmod{1001}$$

$$23^3 \equiv 529 \times 23 \equiv 12167 \equiv 155 \pmod{1001}$$

$$23^6 \equiv \left(23^3\right)^2 \equiv 155^2 \equiv 24025 \equiv 1 \pmod{1001}$$

Substituting this into (†) gives

$$2^{60} \equiv 23^6 \equiv 1 \pmod{1001}.$$

This implies the order could be 60. *Is there any smaller divisor of 720 which we have missed?*

There are divisors of 6, 10 and 12 which of course are also divisors of 720 but none of them will give $2^d \equiv 1 \pmod{1001}$. *Why not?*

If they did then 2^6, 2^{10} or 2^{12} would also be congruent to $1 \pmod{1001}$. There are other divisors of 720 below 60 which are a combination of divisors of 6, 10 or 12:

$$\{8,9,15,16,18,40,45,48\}.$$

Taking the first element 8 we have

$$2^8 \equiv 256 \not\equiv 1 \pmod{1001}.$$

Using this result we can deduce that

$$2^9 \equiv 512 \not\equiv 1 \pmod{1001} \text{ and } 2^{16} \equiv 256^2 \not\equiv 1 \pmod{1001}.$$

Similarly, we can compute the others by using the above results:

$$2^{15} \equiv 2^{12} \times 2^3 \equiv 92 \times 8 \not\equiv 1 \pmod{1001}$$

$$2^{18} \equiv \left(2^9\right)^2 \equiv 512^2 \not\equiv 1 \pmod{1001}$$

$$2^{40} \equiv \left(2^{10}\right)^4 \equiv 23^4 \equiv 23^3 \times 23 \equiv 155 \times 23 \equiv 3565 \equiv 562 \not\equiv 1 \pmod{1001}$$

$$2^{45} \equiv \left(2^{10}\right)^4 \times 2^5 \equiv 562 \times 32 \equiv 17984 \equiv 967 \not\equiv 1 \pmod{1001}$$

$$2^{48} \equiv 2^{45} \times 2^3 \equiv 967 \times 8 \equiv 7736 \equiv 729 \not\equiv 1 \pmod{1001}$$

Hence the order of $2 \pmod{1001}$ is 60.