Complete Solutions to Exercises 6.1

1. In each case we are given modulo a prime so we use Corollary (6.5):

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

Remember this result means we have to find the divisors of $\phi(n)$.

(a) We need to find the order of 2 modulo 7. First, we determine $\phi(7)$. *What is* $\phi(7)$ *equal to?*

Since 7 is prime so using $\phi(p) = p-1$ we have $\phi(7) = 7-1 = 6$. The order k is a divisor of 6 which are 1, 2, 3 and 6. Let us evaluate 2 to each of these indices:

$$2^1 \equiv 2 \pmod 7,\ 2^2 \equiv 4 \pmod 7,\ 2^3 \equiv 8 \equiv 1 \pmod 7$$

We don't need to find $2^6 \equiv ? \pmod 7$ because the order is the *smallest index* x such that $2^x \equiv 1 \pmod 7$. Hence order of 2 modulo 7 is 3.

(b) Similarly we first evaluate $\phi(11)$:

$$\phi(11) = 11-1 = 10.$$

The divisors of 10 are 1, 2, 5 and 10. Working out these indices with base 2:

$$2^1 \equiv 2 \pmod{11},\ 2^2 \equiv 4 \pmod{11},\ 2^5 \equiv 32 \equiv 10 \pmod{11} \text{ and } 2^{10} \equiv 1 \pmod{11}$$

The order of 2 modulo 11 is 10.

(c) We are required to find the order of 2 modulo 17. First, we evaluate $\phi(17)$,

$$\phi(17) = 16.$$

The divisors of 16 are 1, 2, 4, 8 and 16. Evaluating 2 to each of these indices modulo 17 gives

$$2^1 \equiv 2 \pmod{17},\ 2^2 \equiv 4 \pmod{17},\ 2^4 \equiv 16 \pmod{17},\ 2^8 \equiv 256 \equiv 1 \pmod{17}$$

Hence the order of 2 modulo 17 is 8.

(d) We need to find the order of 2 modulo 23. Since 23 is prime so

$$\phi(23) = 22.$$

The divisors of 22 are 1, 2, 11 and 22. We have

$$2^1 \equiv 2 \pmod{23},\ 2^2 \equiv 4 \pmod{23},\ 2^{11} \equiv 2048 \equiv 1 \pmod{23}.$$

The first index to give 1 modulo 23 is 11 so the order of 2 modulo 23 is 11.

2. We use the above Corollary (6.5) to find the order of a modulo n.

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

(a) We need to evaluate the order of 3 modulo 10. Since 3 and 10 are relatively prime so the order of $3\pmod{10}$ exits. As in question 1 we have to find $\phi(10)$. We have $\phi(10)=4$ and the only divisors of 4 are 1, 2 and 4. Therefore working out 3 to each of these indices modulo 10 we have

$$3^1 \equiv 3 \pmod{10},\ \ 3^2 \equiv 9 \pmod{10},\ \ 3^4 \equiv 1 \pmod{10}.$$

Remember we don't need to work out $3^4 \equiv 1 \pmod{10}$ because by Euler's Theorem

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

We know that $3^{\phi(10)} \equiv 3^4 \equiv 1 \pmod{10}$. The order of 3 modulo 10 is 4.

(b) We need to find the order of 7 modulo 12. Repeating the above argument,

$$\phi(12)=4\,.$$

The only divisors of 4 are 1, 2 and 4:

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

Therefore, the order of 7 modulo 12 is 2.

(c) We are required to find the order of 9 modulo 16. First we find $\phi(16)$. *How?* Write the prime factorization of 16:

$$16 = 2^4$$

Using Proposition (5.4) of the last chapter:

$$\phi(p^k) = p^k - p^{k-1}$$

We have

$$\phi(16) = \phi(2^4) = 2^4 - 2^3 = 8\,.$$

The only divisors of 8 are 1, 2, 4 and 8. Evaluating these indices with base 9:

$$9^1 \equiv 9 \pmod{16},\ \ 9^2 \equiv 81 \equiv 1 \pmod{16}$$

The order of 9 modulo 16 is 2 because this is the first index to give 1 modulo 16.

(d) *How do we find the order of 11 modulo 25?*

Very similar to the previous method. First, we determine $\phi(25)$. *How?*

We have $\phi(5^2) = 5^2 - 5 = 20$. The divisors of 20 are 1, 2, 4, 5, 10 and 20:

$$11^1 \equiv 11 \pmod{25},\ \ 11^2 \equiv 121 \equiv 21 \equiv -4 \pmod{25},\ \ 11^4 \equiv (11^2)^2 \equiv (-4)^2 \equiv 16 \pmod{25},$$
$$11^5 \equiv (11^4)\times 11 \equiv 16 \times 11 \equiv 176 \equiv 1 \pmod{25}$$

Therefore the order of 11 modulo 25 is 5.

(e) Since 3 and 13 are relatively prime so the order of $3 \pmod{13}$ exists.

Again 13 is prime, so $\phi(13) = 12$. We only need to check the indices which are divisors of 12 and these are 1, 2, 3, 4, 6 and 12.

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

The order of 3 modulo 13 is 3. We don't need to test the remaining indices 4, 6 and 12 because we are only interested in the first index to give 1 modulo 13.

3. We are given that the order of 5 modulo 13 is 4 so we have

$$5^4 \equiv 1 \pmod{13} \qquad (*)$$

How do we evaluate x in the following $5^{101} \equiv x \pmod{13}$ *?*

We write the index 101 as a multiple of 4 plus any remainder;

$$101 = (25 \times 4) + 1.$$

Using the rules of indices we have

$$5^{101} \equiv 5^{(25\times 4)+1} \equiv \underbrace{\left(5^4\right)}_{\equiv 1 \text{ by } (*)}^{25} \times 5 \equiv 5 \pmod{13}.$$

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

4. First we are asked to find the order of 3 modulo 100. *How?*

We need to work out $\phi(100)$ which we found in the last chapter:

$$\phi(100) = 40.$$

What are the divisors of 40?

1, 2, 4, 5, 8, 10, 20 and 40. Now we have to find 3 to each of these indices and see which one gives 1 modulo 100:

$$3^1 \equiv 3, \quad 3^2 \equiv 9, \quad 3^4 \equiv 81, \quad 3^5 \equiv 243 \equiv 43, \quad 3^8 \equiv 6561 \equiv 61, \quad 3^{10} \equiv 59049 \equiv 49,$$

$$3^{20} \equiv \left(3^{10}\right)^2 \equiv (49)^2 \equiv 2401 \equiv 1 \pmod{100}$$

The order of 3 modulo 100 is 20. This means we have

$$3^{20} \equiv 1 \pmod{100} \qquad (\dagger)$$

We also need to find the least positive residue of $3^{1001} \pmod{100}$. *How?*

By using (†). We need to express the index 1001 as a multiple of 20 plus any remainder;

$$1001 = (50 \times 20) + 1.$$

Using this and (†) we have

$$3^{1001} \equiv 3^{(50\times 20)+1} \equiv \left(3^{20}\right)^{50} \times 3 \equiv \underbrace{(1)}_{\text{by } (\dagger)}^{50} \times 3 \equiv 3 \pmod{100}$$

The last two digits of 3^{1001} are 03.

5. We need to find the order of 7 modulo 60. First we have to find $\phi(60)$. *How?*
Find the prime decomposition of 60:

$$60 = 4 \times 15 = 2^2 \times 3 \times 5 .$$

Using Proposition (5.9):

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

With $n = 60$, $p_1 = 2$, $p_2 = 3$, $p_3 = 5$ we have

$$\phi(60) = 60\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 16 .$$

Next we find the divisors of 16 which are 1, 2, 4, 8 and 16. Evaluating 7 to each of these indices 1, 2, 4, 8 and 16 gives

$$7^1 \equiv 7 , \quad 7^2 \equiv 49 , \quad 7^4 \equiv 2401 \equiv 1 \pmod{60}$$

Therefore the order of 7 modulo 60 is 4 which we will use;

$$7^4 \equiv 1 \pmod{60} \qquad (*)$$

We also need to find the inverse of 7 modulo 60. *How?*
We use (*):

$$7^4 \equiv 7 \times 7^3 \pmod{60}$$

The inverse of 7 modulo 60 is 7^3 modulo 60. We want to write this as the least non-negative residue modulo 60:

$$7^3 \equiv 343 \equiv 43 \pmod{60}$$

The inverse of 7 is 43 modulo 60.

We are also asked to solve $7x \equiv 59 \pmod{60}$. Since the inverse of 7 is $43 \pmod{60}$ so we multiply this equation $7x \equiv 59 \pmod{60}$ by 43:

$$\underbrace{43 \times 7}_{\equiv 1} x \equiv 43 \times 59 \equiv 43 \times (-1) \equiv -43 \equiv 17 \pmod{60}.$$

Hence the solution of $7x \equiv 59 \pmod{60}$ is $x \equiv 17 \pmod{60}$.

6. First we are asked to find the order of 5 modulo 21. The simplest way to find this is to determine $\phi(21)$ and then examine the divisors of $\phi(21)$.

The prime factorization of $21 = 7 \times 3$. Using Proposition (5.9):

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

with $n = 21$, $p_1 = 7$, $p_2 = 3$ we have

$$\phi(21) = 21\left(1 - \frac{1}{7}\right)\left(1 - \frac{1}{3}\right) = 12.$$

The only divisors of 12 are 1, 2, 3, 4, 6 and 12. Working out 5 to some of these indices modulo 21 gives

$$5^1 \equiv 5,\ 5^2 \equiv 25 \equiv 4,\ 5^4 \equiv \left(5^2\right)^2 \equiv 4^2 \equiv 16,\ 5^6 \equiv \left(5^2\right)^3 \equiv 4^3 \equiv 64 \equiv 1 \pmod{21}.$$

Hence the order of 5 modulo 21 is 6 which means that

$$5^6 \equiv 1 \pmod{21} \qquad (\dagger\dagger)$$

We are also asked to solve $5x \equiv 16 \pmod{21}$. By using (††) we can find the inverse of 5 modulo 21 because

$$5^6 \equiv 5\left(5^5\right) \equiv 1 \pmod{21}$$

The inverse of 5 modulo 21 is 5^5 modulo 21. Therefore

$$5^{-1} \equiv 5^5 \equiv 5^4 \times 5 \underbrace{\equiv}_{\text{From above calculation}} 16 \times 5 \equiv 80 \equiv 17 \pmod{21}.$$

Hence $5^{-1} \equiv 17 \pmod{21}$. Multiplying both sides of the given equation $5x \equiv 16 \pmod{21}$ by 17 gives

$$\underbrace{17 \times 5}_{\equiv 1} x \equiv 17 \times 16 \equiv (-4) \times (-5) \equiv 20 \pmod{21}.$$

Therefore, our solution is $x \equiv 20 \pmod{21}$.

7. (a) We are asked to find the least non-negative residue x such that

$$3^{1000} \equiv x \pmod{17}.$$

To simplify our evaluation of this we first find the order of 3 modulo 17. Note that 17 is prime so $\phi(17) = 16$ and the divisors of 16 are 1, 2, 4, 8 and 16. We have

$$3^1 \equiv 3,\ 3^2 \equiv 9,\ 3^4 \equiv 81 \equiv 13 \equiv -4,\ 3^8 \equiv \left(3^4\right)^2 \equiv (-4)^2 \equiv -1 \pmod{17} \quad (\dagger)$$

As none of these are congruent to 1 modulo 17 so the order of 3 modulo 17 must be $\phi\left(17\right)=16$. We have

$$3^{16}\equiv 1\left(\mathrm{mod}\ 17\right) \qquad (*)$$

Writing the given index 1000 as a multiple of 16 and any remainder:

$$1000=\left(62\times 16\right)+8$$

Using this result to evaluate $3^{1000}\equiv x\left(\mathrm{mod}\ 17\right)$ gives

$$3^{1000}\equiv 3^{(62\times 16)+8}\equiv\left(3^{16}\right)^{62}\times 3^{8}\equiv\underbrace{\left(1\right)}_{\text{by }(*)}^{62}\times 3^{8}\equiv 3^{8}\underbrace{\equiv}_{\text{by }(\dagger)}16\left(\mathrm{mod}\ 17\right)$$

We have $3^{1000}\equiv 16\left(\mathrm{mod}\ 17\right)$.

(b) This time we have to find $3^{970}\equiv x\left(\mathrm{mod}\ 98\right)$. First we find the order of 3 modulo 98. The prime decomposition of 98 is given by

$$98=2\times 7^{2}.$$

Using Proposition (5.9):

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

With $n=98,\ p_1=2,\ p_2=7$ we have

$$\phi\left(98\right)=98\left(1-\frac{1}{2}\right)\left(1-\frac{1}{7}\right)=42.$$

What are the divisors of 42?

1, 2, 3, 6, 7 and 42. Evaluating

$3^{1}\equiv 3,\ 3^{2}\equiv 9,\ 3^{3}\equiv 27,\ 3^{6}\equiv 27^{2}\equiv 729\equiv 43,\ 3^{7}\equiv\left(3^{2}\right)^{3}3\equiv\left(9\right)^{3}3\equiv 2187\equiv 31\ \left(\mathrm{mod}\ 98\right)$

Therefore, the order of 3 modulo is $\phi\left(98\right)=42$:

$$3^{42}\equiv 1\left(\mathrm{mod}\ 98\right) \qquad (*)$$

Using this to evaluate $3^{970}\equiv x\left(\mathrm{mod}\ 98\right)$. We need to write the index 970 as a multiple of 42 and any remainder:

$$970=\left(23\times 42\right)+4.$$

We have

$$3^{970}\equiv 3^{(23\times 42)+4}\equiv\left(3^{42}\right)^{23}\times 3^{4}\underbrace{\equiv}_{\text{by }(*)}1\times 3^{4}\equiv 81\left(\mathrm{mod}\ 98\right).$$

Therefore $3^{970}\equiv 81\left(\mathrm{mod}\ 98\right)$.

8. From the introduction we know we have to find the least positive residue x such that

$$3^{311} \equiv x \left(\text{mod } 1000\right).$$

Recall we had $\phi\left(1000\right) = 400$ and the prime decomposition of $400 = 2^4 \times 5^2$. The divisors of 400 are 1, 2, 4, 5, 8, 10, 16, 20, 25, 40, 50, 80, 100, 200, $\cdots$. We only need to test these indices of 3:

$$3^1 \equiv 3, 3^2 \equiv 9, 3^4 \equiv 81, 3^5 \equiv 243, 3^8 \equiv 561, 3^{10} \equiv 49, \cdots, 3^{100} \equiv 1 \left(\text{mod } 1000\right).$$

Hence the order $3\left(\text{mod } 1000\right)$ is 100. Writing the index of 311 as multiple of 100 and any remainder gives $311 = \left(3 \times 100\right) + 11$. Therefore

$$3^{311} \equiv 3^{\left(3\times 100\right)+11} \equiv \left(3^{100}\right)^3 \times 3^{11} \equiv 1 \times 3^{11} \equiv 3^{10} \times 3 \equiv 49 \times 3 \equiv 147 \left(\text{mod } 1000\right).$$

The last three digits of 3^{311} is 147.

9. We need to show that the inverse of a modulo n is $a^{k-1} \left(\text{mod } n\right)$ given it has order k.

Proof.

Since we are given that a modulo n has order k so

$$a^k \equiv 1 \left(\text{mod } n\right) \qquad (*)$$

The inverse of a modulo n is x such that

$$ax \equiv 1 \left(\text{mod } n\right)$$

Since k is a positive integer so by (*) we have $a^k \equiv a\left(a^{k-1}\right) \equiv 1 \left(\text{mod } n\right)$.

Therefore

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

We have $a^{-1} \equiv a^{k-1} \left(\text{mod } n\right)$. This completes our proof.

■

10. We are required to prove that if a modulo n has order mk then a^m has order k.

Proof.

We are given that a modulo n has order mk therefore

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

Using the rules of indices we have

$$a^{mk} \equiv \left(a^m\right)^k \equiv 1 \left(\text{mod } n\right)$$

We also need to show k is the smallest index such that $\left(a^m\right)^k \equiv 1 \left(\text{mod } n\right)$. *How?*

By contradiction.

Suppose $\left(a^m\right)^b \equiv 1 \left(\text{mod } n\right)$ where $0 < b < k$. Then

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

Since $b < k$ and $m > 0$ so $mb < mk$ which implies that the order of a modulo n cannot be mk because we have a smaller index mb which gives 1 modulo n. This is impossible. Hence our supposition $b < k$ must be wrong so the order of a^m is k as required.

■

11. Note that

$$a \equiv 0 \text{ or } 1 \left(\text{mod } 2\right).$$

We cannot have $a \equiv 0 \left(\text{mod } 2\right)$ because the order is defined when a is relatively prime to 2. We can only have $a \equiv 1 \left(\text{mod } 2\right)$ so the order can only be 1.

12. We need to prove that if the order of a modulo p is k then $k \mid \left(p-1\right)$.

Proof.

We are given that p is prime. By Corollary (6.5):

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

We have $k \mid \phi\left(p\right)$ where k is the order of a modulo p. By Proposition (5.2):

> If p is prime then $\phi\left(p\right) = p - 1$.

Substituting $\phi\left(p\right) = p - 1$ into $k \mid \phi\left(p\right)$ gives

$$k \mid \left(p-1\right).$$

This is our required result.

■

13. We are required to prove that if a as order $2k$ modulo prime p where p is an odd prime then $a^k \equiv -1 \left(\text{mod } p\right)$.

Proof.

We are given that a as order $2k$ modulo prime p therefore

$$a^{2k} \equiv 1 \pmod{p}.$$

Using the rules of indices we have

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

By Lemma (4.3):

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

Applying this Lemma on $\left(a^k\right)^2 \equiv 1 \pmod{p}$ gives

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

However $a^k \not\equiv 1 \pmod{p}$. *Why not?*

Because a as order $2k$ which means that $2k$ is the smallest index of a which is congruent to 1 modulo p. Hence $a^k \equiv -1 \pmod{p}$.

■

14. We need to show that the order of a modulo p^m divides $p^m - p^{m-1}$.

Proof.

We are given that p is an odd prime. Let k be the order of a modulo p^m.

By Corollary (6.5):

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

We have $k \mid \phi\left(p^m\right)$. Using Proposition (5.4) to find $\phi\left(p^m\right)$:

$$\phi\left(p^m\right) = p^m - p^{m-1}$$

Therefore $\phi\left(p^m\right) = p^m - p^{m-1}$ and $k \mid \left(p^m - p^{m-1}\right)$.

■

15. We are given that km is the order of a modulo n. We need to prove that $k \mid \phi(n)$.

Proof.

The order of a always divides $\phi(n)$ because of Corollary (6.5):

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

Hence $km \mid \phi(n)$ which implies that $k \mid \phi(n)$. This completes our proof.

■

16. We are required to prove that if a modulo n has order k then so does the inverse of a modulo n.

Proof.

Since the order of $a \pmod{n}$ exists so the integers a and n are relatively prime which implies that $a^{-1} \pmod{n}$ exists.

Let b modulo n be the inverse of a modulo n. This implies that

$$ab \equiv 1 \pmod{n}.$$

We are given that a modulo n has order k therefore

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

Consider $(ab)^k \equiv 1^k \equiv 1 \pmod{n}$. Using the rules of indices we have

$$(a \times b)^k \equiv a^k \times b^k \equiv 1 \times b^k \equiv b^k \equiv 1 \pmod{n}.$$

We have $b^k \equiv 1 \pmod{n}$ but we need to show that k is the order of b modulo n.

Suppose h is the order of b modulo n where $h < k$. This gives

$$b^h \equiv 1 \pmod{n} \qquad (*)$$

Since $a \times b \equiv 1 \pmod{n}$ so $(a \times b)^h \equiv 1 \pmod{n}$ and

$$(a \times b)^h \equiv a^h \times b^h \underbrace{\equiv}_{\text{by (*)}} a^h \times 1 \equiv a^h \equiv 1 \pmod{n}.$$

This implies that h is the order of a modulo n. In our supposition we have $h < k$ which is impossible because k is the order of a modulo n. Therefore, k is the order of b modulo n. Remember b is the inverse of a modulo n. This completes our proof.

■

17. We have to prove that

$$2^{r(s-1)} + 2^{r(s-2)} + 2^{r(s-3)} + \cdots + 2^r + 1 \equiv 0 \pmod{p}$$

Given that 2 modulo prime p has order rs.

Proof.

We are given that 2 modulo prime p has order rs therefore

$$2^{rs} \equiv 1 \pmod{p} \text{ implies } 2^{rs} - 1 \equiv 0 \pmod{p}.$$

By using the given hint we have

$$2^{rs} - 1 \equiv \left(2^r - 1\right)\left(2^{r(s-1)} + 2^{r(s-2)} + 2^{r(s-3)} + \cdots + 2^r + 1\right) \equiv 0 \pmod{p}$$

By Proposition (3.14) (a) of chapter 3:

> If $a \times b \equiv 0 \pmod{p}$ where p is prime then $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$.

We have

$$2^r - 1 \equiv 0 \pmod{p} \text{ or } 2^{r(s-1)} + 2^{r(s-2)} + 2^{r(s-3)} + \cdots + 2^r + 1 \equiv 0 \pmod{p}.$$

We are also given that $s > 0$ so $2^r \not\equiv 1 \pmod{p}$ or in other words $2^r - 1 \not\equiv 0 \pmod{p}$. Therefore

$$2^{r(s-1)} + 2^{r(s-2)} + 2^{r(s-3)} + \cdots + 2^r + 1 \equiv 0 \pmod{p}.$$

This is our required result.

■

18. The proof of this result is similar in nature to the proof of the previous question. We need to prove that if a has order k modulo prime p then

$$a^{k-1} + a^{k-2} + a^{k-3} + \cdots + 1 \equiv 0 \pmod{p}.$$

Proof.

We are given that a has order k modulo prime p therefore

$$a^k \equiv 1 \pmod{p} \text{ implies that } a^k - 1 \equiv 0 \pmod{p}.$$

Factorizing $a^k - 1$ gives

$$a^k - 1 = (a-1)(a^{k-1} + a^{k-2} + a^{k-3} + \cdots + a + 1).$$

Using this we have

$$a^k - 1 \equiv (a-1)(a^{k-1} + a^{k-2} + a^{k-3} + \cdots + a + 1) \equiv 0 \pmod{p}.$$

By Proposition (3.14) of chapter 3:

> If $a \times b \equiv 0 \pmod{p}$ where p is prime then $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$.

We have

$$a - 1 \equiv 0 \pmod{p} \text{ or } a^{k-1} + a^{k-2} + a^{k-3} + \cdots + a + 1 \equiv 0 \pmod{p}.$$

We are given that $a \not\equiv 1 \pmod{p}$ so we have

$$a^{k-1} + a^{k-2} + a^{k-3} + \cdots + 1 \equiv 0 \pmod{p}.$$

This completes our proof.

■

19. We need to prove that $\left(a+1\right)^4 \equiv -4\left(\text{mod}\, p\right)$ given that a modulo p has order 4.

Proof.

Since the order of a modulo p is 4 so

$$a^4 \equiv 1\left(\text{mod } p\right).$$

Using the binomial theorem to expand $\left(a+1\right)^4$ gives

$$\left(a+1\right)^4 \equiv a^4 + 4a^3 + 6a^2 + 4a + 1\left(\text{mod } p\right) \qquad (*)$$

Using the result of question 13:

If a as order $2k$ modulo prime p where p is odd then $a^k \equiv -1\left(\text{mod } p\right)$.

Since the order of a modulo p is 4 so

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

Multiplying this by a gives

$$a^3 \equiv -a\left(\text{mod } p\right).$$

Putting all these results $a^4 \equiv 1\left(\text{mod } p\right)$, $a^3 \equiv -a\left(\text{mod } p\right)$ and $a^2 \equiv -1\left(\text{mod } p\right)$ into (*) yields

$$\begin{aligned}\left(a+1\right)^4 &\equiv a^4 + 4a^3 + 6a^2 + 4a + 1\\ &\equiv 1 + 4\left(-a\right) + 6\left(-1\right) + 4a + 1\\ &\equiv 1 - 4a - 6 + 4a + 1\\ &\equiv -4\left(\text{mod } p\right)\end{aligned}$$

Hence, we have $\left(a+1\right)^4 \equiv -4\left(\text{mod}\, p\right)$.

■