Complete Solutions to Exercise 5.2

1. Evaluating $ar_j \equiv x_j \pmod 8$ with $a = 3$ and $r_1 = 1,\ r_2 = 3,\ r_3 = 5,\ r_4 = 7$:

$$3(1) \equiv 3 \pmod 8$$
$$3(3) \equiv 9 \equiv 1 \pmod 8$$
$$3(5) \equiv 15 \equiv 7 \pmod 8$$
$$3(7) \equiv 21 \equiv 5 \pmod 8$$

Note that $ar_j \equiv r_k \pmod n$ with $ar_1 = r_2,\ ar_2 = r_1,\ ar_3 = r_4$ and $ar_4 = r_3$.

2. Two different reduced residue system modulo 8:

$$\{1, 3, 5\ 7\} \text{ and } \{-1, 11, 13, 17\}$$

3. We need to find the last digit of 7^{2014}. This means we need to work with modulo 10 because we want to find the last digit. We need to determine x in $7^{2014} \equiv x \pmod{10}$ where x is the least non-negative residue modulo n.

We use Euler's Theorem (5.14):

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

With $n = 10$. We have $\phi(10) = 4$ so applying this theorem with $n = 10,\ a = 7$ gives

$$7^{\phi(10)} \equiv 7^4 \equiv 1 \pmod{10} \qquad (*)$$

Writing the index 2014 as a multiple of 4 and remainder we have

$$2014 = (503 \times 4) + 2.$$

Rewriting the index 2014 of 7 in $7^{2014} \equiv x \pmod{10}$ gives

$$\begin{aligned} 7^{2014} &\equiv 7^{(503\times 4)+2} \\ &\equiv \underbrace{\left(7^4\right)}_{\equiv 1}^{503} 7^2 \equiv 7^2 \equiv 49 \equiv 9 \pmod{10} \end{aligned}$$

The last digit of 7^{2014} is 9.

4. We need to find the last two digits of 13^{1000}. Since we are interested in the last two digits so we work with modulo 100. We are required to find

$$13^{1000} \equiv x \pmod{100}.$$

where x is the least non-negative residue modulo 100.

In order to use Euler's Theorem (5.14):

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

with $n = 100$ we must find $\phi(100)$. The prime decomposition of 100 is $100 = 2^2 \times 5^2$.

We use formula (5.9) to find $\phi(100)$:

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

Hence

$$\phi(100) = 100\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 40.$$

Applying Euler's Theorem with $\phi(100) = 40$, $n = 100$ and $a = 13$ gives

$$13^{40} \equiv 1 \pmod{100} \qquad (\dagger)$$

Writing the index 1000 as a multiple of 40 plus any remainder:

$$1000 = 40 \times 25.$$

Therefore

$$\begin{aligned} 13^{1000} &\equiv 13^{40\times 25} \\ &\equiv \left(13^{40}\right)^{25} \equiv 1^{25} \equiv 1 \equiv 01 \pmod{100} \qquad [\text{By } (\dagger)] \end{aligned}$$

Hence the last two digits of 13^{1000} are 01.

5. We are required to find the least non-negative residue x in

$$11^{1767} \equiv x \pmod{301}.$$

In order to use Euler's Theorem we need to first find $\phi(301)$.

The prime factorization of 301 is

$$301 = 7 \times 43$$

Using formula (5.9) to find $\phi(301)$:

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

with $n = 301$, $p_1 = 7$ and $p_2 = 43$ gives

$$\phi(301) = 301\left(1 - \frac{1}{7}\right)\left(1 - \frac{1}{43}\right) = 252.$$

Now we are in a position to use Euler's Theorem (5.14):

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

With $a = 11,\ n = 301$:

$$11^{\phi(301)} \equiv 11^{252} \equiv 1 \pmod{301} \qquad (\ddagger)$$

Recall we need to find the least non-negative residue x in $11^{1767} \equiv x \pmod{301}$.

Writing the index 1767 as a multiple of 252 and any remainder:

$$1767 = (7 \times 252) + 3\,.$$

We have

$$\begin{aligned} 11^{1767} &\equiv 11^{(7\times 252)+3} \\ &\equiv \underbrace{\left(11^{52}\right)^{7}}_{\equiv 1} 11^{3} \equiv 11^{3} \equiv 1331 \equiv 127 \pmod{301} \end{aligned}$$

Hence $11^{1767} \equiv 127 \pmod{301}$.

6. To find the last three digits of $27^{1\,000\,000}$ we need to work with modulo 1000. We need to find the least non-negative residue x in the following

$$27^{1\,000\,000} \equiv x \pmod{1000}.$$

We use Euler's Theorem but to use this we need to find $\phi(1000)$. Using the result of question 7 Exercises 5.1:

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

we have

$$\phi(1000) = \phi\left(10^{3}\right) = 10^{2} \times \phi(10) = 100 \times 4 = 400\,.$$

Using Euler's Theorem:

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

With $\phi(1000) = 400$, $a = 27$ and $n = 1000$ gives

$$27^{400} \equiv 1 \pmod{1000} \qquad (**)$$

Writing the index 1 000 000 as a multiple of 400 and any remainder;

$$1\,000\,000 = 2500 \times 400\,.$$

Therefore

$$27^{1\,000\,000} \equiv 27^{2500\times 400} \equiv \left(27^{400}\right)^{2500} \equiv 1 \pmod{1000} \quad [\text{By } (**)]$$

The last three digits of $27^{1\,000\,000}$ are 001.

7. In each case we use Euler's Theorem to find the multiplicative inverse.

(a) We are required to solve $7x \equiv 33 \pmod{50}$. One way to solve this is to find the inverse of 7 modulo 50 for which we can use Euler's Theorem:

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

Recall we can only use this theorem if the $\gcd(a, \quad n) = 1$.

Since $\gcd(7, \quad 50) = 1$ so we can use this result.

First we need to find $\phi(50)$. The prime factorization of 50 is

$$50 = 2 \times 5^2$$

By applying (5.9):

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

to find $\phi(50)$ gives

$$\phi(50) = 50\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 20.$$

Using Euler's Theorem with $a = 7, \ n = 50$ we have

$$7^{\phi(50)} \equiv 7^{20} \equiv 1 \pmod{50}.$$

We can rewrite the index 20 as 19+1:

$$7^{20} \equiv 7\left(7^{19}\right) \equiv 1 \pmod{50}.$$

Hence $7^{19} \pmod{50}$ is the inverse of $7 \pmod{50}$. We need to find $7^{19} \pmod{50}$. Evaluating a simpler power of 7;

$$7^2 \equiv 49 \equiv -1 \pmod{50} \qquad (\dagger)$$

Using this $7^2 \equiv -1 \pmod{50}$ to evaluate $7^{19} \pmod{50}$:

$$7^{19} \equiv 7^{(2\times 9)+1} \equiv \left(7^2\right)^9 7 \equiv \underbrace{(-1)^9}_{\text{By } (\dagger)} 7 \equiv -7 \equiv 43 \pmod{50}.$$

Therefore $43 \pmod{50}$ is the inverse of $7 \pmod{50}$. Multiplying both sides of the given equation $7x \equiv 33 \pmod{50}$ by 43 gives

$$\underbrace{43 \times 7}_{\equiv 1} x \equiv 43 \times 33 \equiv 19 \pmod{50}.$$

Our solution to $7x \equiv 33 \pmod{50}$ is $x \equiv 19 \pmod{50}$.

(b) We need to solve the linear congruence $13x \equiv 51 \pmod{100}$. Since $\gcd(13,\ 100) = 1$ so we can use Euler's Theorem. In order to use this we need to find $\phi(100)$ which we have evaluated many times:

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

Substituting $a = 13,\ n = 100$ and $\phi(100) = 40$ into

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

gives

$$13^{40} \equiv 1 \pmod{100}.$$

What is the inverse of $13 \pmod{100}$ *?*

$13^{39} \pmod{100}$ because

$$13^{40} \equiv 13^{39} \times 13 \equiv 1 \pmod{100}.$$

We need to find the least non-negative residue of $13^{39} \pmod{100}$. Evaluating some simple powers of 13:

$$13^2 \equiv 169 \equiv 68,\ 13^3 \equiv 2197 \equiv 97 \equiv -3 \pmod{100} \qquad (*)$$

We use the last result $13^3 \equiv -3 \pmod{100}$ because -3 is a small number to find powers of. Remember we have to evaluate $13^{39} \pmod{100}$ so writing this index 39 as a multiple of 3:

$$13^{39} \equiv 13^{3\times 13} \equiv \left(13^3\right)^{13} \underbrace{\equiv}_{\text{By (*)}} (-3)^{13} \equiv -1594323 \equiv -23 \pmod{100}.$$

The inverse of $13 \pmod{100}$ is $-23 \pmod{100}$. Multiplying both sides of the given equation $13x \equiv 51 \pmod{100}$ by -23 gives

$$\underbrace{-23 \times 13}_{\equiv 1} x \equiv -23 \times 51 \equiv -1173 \equiv -73 \equiv 27 \pmod{100}.$$

Therefore, the solution is $x \equiv 27 \pmod{100}$.

(c) The given equation is $13x \equiv 52 \pmod{100}$. Similarly we have the answer $x \equiv 4 \pmod{100}$.

(We can solve each of these congruences by solving the equivalent Diophantine equations.)

8. *How do we solve* $15x \equiv b_j \pmod{32}$ *?*

We need to find the inverse of $15 \pmod{32}$. We can use Euler's Theorem to find this inverse. To apply Euler's Theorem, we need to find $\phi(32)$:

$$\phi(32) = 32\left(1 - \frac{1}{2}\right) = 16.$$

By Euler's Theorem with $a = 15,\ n = 32$ and $\phi(32) = 16$ we have

$$15^{\phi(32)} \equiv 15^{16} \equiv 1 \pmod{32}.$$

Therefore, the inverse of $15 \pmod{32}$ is $15^{15} \pmod{32}$ because

$$15^{16} \equiv 15\left(15^{15}\right) \equiv 1 \pmod{32}.$$

We need to find $15^{15} \pmod{32}$. Finding some simple powers of 15:

$$15^2 \equiv 225 \equiv 1 \pmod{32} \qquad (*)$$

Therefore

$$15^{15} \equiv 15^{(2\times 7)+1} \equiv \left(15^2\right)^7 \times 15 \underbrace{\equiv}_{\text{By (*)}} 1^7 \times 15 \equiv 15 \pmod{32}.$$

Multiplying both sides of the $15x \equiv b_j \pmod{32}$ by 15 gives

$$\underbrace{15 \times 15}_{\equiv 1} x \equiv 15 \times b_j \pmod{32}.$$

Therefore

$$x_j \equiv 15 \times b_j \pmod{32} \qquad (**)$$

Substituting $b_j = 5,\ 7,\ 9,\ 11$ and 13 into (**) yields

$$x_1 \equiv 15 \times 5 \equiv 11 \pmod{32}$$

$$x_2 \equiv 15 \times 7 \equiv 105 \equiv 9 \pmod{32}$$

$$x_3 \equiv 15 \times 9 \equiv 135 \equiv 7 \pmod{32}$$

$$x_4 \equiv 15 \times 11 \equiv 165 \equiv 5 \pmod{32}$$

$$x_5 \equiv 15 \times 13 \equiv 195 \equiv 3 \pmod{32}$$

Note that the advantage of finding the inverse of $15 \pmod{32}$ is that you can solve $15x_j \equiv b_j \pmod{32}$ for different values of b_j in one go.

9. *How do we prove that* $n \mid 99\cdots99$ *where there are* $\phi(n)$ *number of 9's in* $99\cdots99$ *?*

Since we are given that $\gcd(n,\ 10) = 1$ so we can use Euler's Theorem.

Proof.

Using Euler's Theorem with $a = 10$ gives

$$10^{\phi(n)} \equiv 1 \pmod{n} \quad \text{which implies } 10^{\phi(n)} - 1 \equiv 0 \pmod{n}.$$

As $10^{\phi(n)} - 1 \equiv 0 \pmod{n}$ therefore $n \mid \left(10^{\phi(n)} - 1\right)$. *What does* $10^{\phi(n)}$ *represent?*

1 followed by $\phi(n)$ zeros. We have

$$10^{\phi(n)} - 1 = 1\underbrace{00\cdots00}_{\substack{\text{There are } \phi(n) \\ \text{zeros.}}} - 1 = \underbrace{99\cdots99}_{\substack{\text{There are } \phi(n) \\ \text{nines.}}}.$$

So $n \mid \left(10^{\phi(n)} - 1\right)$ implies $n \mid 99\cdots99$ where there are $\phi(n)$ 9's.

■

10. We need to show that $a^{p^n - p^{n-1}} \equiv 1 \pmod{p^n}$ provided $p \nmid a$.

Proof.

We are given that $p \nmid a$ so $\gcd(p,\ a) = 1$. *Why?*

Because by question 3 of Exercise 2.1 we have

> Let p *be* prime and it does *not* divide a then $\gcd(p,\ a) = 1$.

We also have

$$\gcd(p^n,\ a) = 1.$$

Why?

Because $\gcd(p,\ a) = 1$ and the only divisors of p^n are 1 and $p,\ p^2,\ \cdots,\ p^n$.

The integer a does *not* have prime p in its prime factorization.

As we have $\gcd(p^n,\ a) = 1$ therefore we can apply Euler's Theorem (5.14):

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

With $m = p^n$. By Proposition (5.4) of the last section:

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

We have $\phi(p^n) = p^n - p^{n-1}$. Substituting this into Euler's Theorem we have

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

We have our required result.

■

11. The given statement $a^{\phi(\phi(n))} \equiv 1 \pmod{n}$ is false. Consider the following:

Let $n = 5$ and $a = 3$ then $\gcd(3,\ 5) = 1$ and

$$3^{\phi(5)} \equiv 3^4 \equiv 1 \pmod{5}.$$

However

$$3^{\phi(\phi(5))} \equiv 3^{\phi(4)} \equiv 3^2 \equiv 9 \equiv 4 \pmod{5}.$$

12. (a) *Proof.*

Since we are given that $\gcd(a,\ n) = 1$ so $a^{-1} \pmod{n}$ exists. By Euler's Theorem we have

$$a^{\phi(n)} \equiv 1 \pmod{n}$$
$$a\left(a^{\phi(n)-1}\right) \equiv 1 \pmod{n} \qquad [\text{By rules of indices}]$$

By the definition of inverse of a modulo n we have

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

This completes our proof.

■

(b) *Proof.*

Substitute $x \equiv ba^{\phi(n)-1} \pmod{n}$ into the given equation:

$$ax \equiv aba^{\phi(n)-1} \equiv a^{\phi(n)-1+1}b \equiv a^{\phi(n)}b \pmod{n}.$$

By Euler's Theorem we have

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

Putting this into the right-hand term in the above yields

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

Since $x \equiv ba^{\phi(n)-1} \pmod{n}$ satisfies $ax \equiv b \pmod{n}$ so it is the solution. This is our required result.

■

13. (i) Using the multiplicative property of ϕ and $\phi(p) = p - 1$ we have

$$\phi(n) = \phi(p \times q) = \phi(3 \times 23) = \phi(3) \times \phi(23) = 2 \times 22 = 44.$$

(ii) The factorization of $44 = 2^2 \times 11$. Therefore

$$\gcd\left(3,\ \ 44\right) = \gcd\left(3,\ \ 2^2 \times 11\right) = 1.$$

We need to find $3^{-1}\left(\mathrm{mod}\ \phi\left(n\right)\right)$. This means we have to determine

$$3^{-1}\left(\mathrm{mod}\ 44\right).$$

Since $\gcd\left(3,\ \ 44\right) = 1$ so by Euler's theorem we have

$$3^{\phi(44)} \equiv 1\left(\mathrm{mod}\ 44\right).$$

Now $\phi\left(44\right) = \phi\left(4\right) \times \phi\left(11\right) = 2 \times 10 = 20$. Substituting this into the above yields

$$3^{20} \equiv 1\left(\mathrm{mod}\ 44\right) \ \Rightarrow\ 3\left(3^{19}\right) \equiv 1\left(\mathrm{mod}\ 44\right).$$

Hence the inverse of 3 modulo 44 is given by

$$3^{-1} \equiv 3^{19}\left(\mathrm{mod}\, 44\right) \qquad (*)$$

Evaluating powers of 3 gives

$$3^3 \equiv 27,\ \ 3^4 \equiv 81 \equiv -7\left(\mathrm{mod}\ 44\right).$$

Using the last power to evaluate (*) gives

$$3^{19} \equiv \left(3^4\right)^4 \times 3^3 \equiv \left(-7\right)^4 \times 27 \equiv 49^2 \times 27 \equiv 5^2 \times 27 \equiv 675 \equiv 15\left(\mathrm{mod}\ 44\right)$$

Putting this into (*) yields $3^{-1} \equiv 3^{19} \equiv 15\left(\mathrm{mod}\, 44\right)$.

14. We need to prove $m^{\phi(n)} + n^{\phi(m)} \equiv 1\left(\mathrm{mod}\ mn\right)$ given that $\gcd\left(m,\ \ n\right) = 1$.

Proof.

Since we are given that $\gcd\left(m,\ \ n\right) = 1$ so by Euler's Theorem we have

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

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

We have two simultaneous congruences so we can use the Chinese Remainder Theorem:

(3.23)	$x = a_1N_1x_1 + a_2N_2x_2 + a_3N_3x_3 + \cdots + a_rN_rx_r$

Given $x \equiv a_1\left(\mathrm{mod}\ n_1\right),\ \ x \equiv a_2\left(\mathrm{mod}\ n_2\right)$ the solution of this is

$$x \equiv a_1N_1x_1 + a_2N_2x_2\left(\mathrm{mod}\ \ n_1n_2\right) \quad (*)$$

We use this result with $x = 1$, $a_1 = m^{\phi(n)}$, $a_2 = n^{\phi(m)}$, $n_1 = n$ and $n_2 = m$. Substituting these into (*) gives

$$m^{\phi(n)}N_1x_1 + n^{\phi(m)}N_2x_2 \equiv 1 \pmod{mn} \qquad (**)$$

Remember $N_1 = \dfrac{n \times m}{n} = m$ and similarly $N_2 = n$. The x_j's are the multiplicative inverse of N_j:

$$N_1x_1 = mx_1 \equiv 1 \pmod{n} \text{ implies } mx_1 = kn + 1$$

$$N_2x_2 = nx_2 \equiv 1 \pmod{m} \text{ implies } nx_2 = lm + 1$$

Substituting these, $N_1x_1 = kn + 1$ and $N_2x_2 = lm + 1$ into (**) gives

$$m^{\phi(n)}N_1x_1 + n^{\phi(m)}N_2x_2 \equiv m^{\phi(n)}\left(kn+1\right) + n^{\phi(m)}\left(lm+1\right) \equiv 1 \pmod{mn}$$

Expanding out gives

$$\begin{aligned} m^{\phi(n)}\left(kn+1\right) + n^{\phi(m)}\left(lm+1\right) &\equiv m^{\phi(n)}kn + m^{\phi(n)} + n^{\phi(m)}lm + n^{\phi(m)} \\ &\equiv k\underbrace{\left(m^{\phi(n)}n\right)}_{\equiv 0 \pmod{mn}} + l\underbrace{\left(n^{\phi(m)}m\right)}_{\equiv 0 \pmod{mn}} + m^{\phi(n)} + n^{\phi(m)} \\ &\equiv m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn} \end{aligned}$$

Hence we have our required result

$$m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}$$

■

15. We need to prove $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

Proof.

Since p and q are distinct primes so $\gcd(p, q) = 1$. Using the result of the previous question;

$$m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}.$$

with $m = p$ and $n = q$ we have:

$$p^{\phi(q)} + q^{\phi(p)} \equiv 1 \pmod{pq} \qquad (\dagger)$$

As p and q are prime so using Proposition (5.2):

If r is prime then $\phi(r) = r - 1$.

to find $\phi(p)$ and $\phi(q)$ gives

$$\phi(p) = p - 1 \text{ and } \phi(q) = q - 1.$$

Substituting this into (†) yields

$$p^{\phi(q)} + q^{\phi(p)} \equiv p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}.$$

This completes our proof.

■

16. Since $\gcd\left(a,\ \ 16\right)=1$ so we can use Euler's Theorem:

$$a^{\phi(m)} \equiv 1 \ \left(\text{mod } m\right)$$

With $m=16$:

$$a^{\phi(16)} \equiv 1 \ \left(\text{mod } 16\right) \qquad (*)$$

What is $\phi\left(16\right)$ *equal to?*

We worked this out in section A;

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

Substituting this into (*) gives

$$a^{\phi(16)} \equiv a^8 \equiv 1 \ \left(\text{mod } 16\right).$$

We need to find the inverse of a^3 modulo 16. Rewriting the index 8 as $5+3$ we have

$$a^8 \equiv a^{3+5} \equiv a^3\left(a^5\right) \equiv 1 \ \left(\text{mod } 16\right).$$

Hence the inverse of a^3 modulo 16 is $a^5 \ \left(\text{mod } 16\right)$.

17. We use proof by contradiction.

Proof.

Let $r_j \in \left\{r_1,\ r_2,\ r_3,\ \cdots,\ r_{\phi(n)}\right\}$ then r_j has an inverse because it is in the reduced residue system. Suppose $r_j^{-1} \equiv r_k \left(\text{mod } n\right)$ where r_k is *not* in the reduced residue system. By the definition of the reduced residue system we have $\gcd\left(r_k,\ \ n\right)=g>1$. We have

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

By Proposition (3.16) of chapter 3:

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

We can only have $r_k\left(r_j^{-1}\right) \equiv 1\left(\text{mod } n\right)$ provided $g \mid 1$ which is impossible because from above we have $g>1$.

■

18. We are required to prove that

$r_1 \times r_2 \times r_3 \times \cdots \times r_{\phi(n)} \equiv 1 \pmod{n}$ or $-1 \pmod{n}$ where $\{r_1, r_2, r_3, \cdots, r_{\phi(n)}\}$ is a reduced residue system modulo n.

Proof.

We are given that $\{r_1, r_2, r_3, \cdots, r_{\phi(n)}\}$ is a reduced residue system modulo n, so each of these numbers are relatively prime to n. *Why?*

Because by the Definition (5.11) of the reduced residue system we have

$$\gcd(r_i, n) = 1 \text{ for all } i = 1, 2, 3, \cdots, \phi(n).$$

Each r_i must have an inverse modulo n because it is relatively prime to n.

The inverse of r_i must belong to the reduced residue system by $\gcd(r_i, n) = 1$. Hence the inverse of r_i modulo n must be an element in

$$\{r_1, r_2, r_3, \cdots, r_{\phi(n)}\}.$$

Let $x = r_1 \times r_2 \times r_3 \times \cdots \times r_{\phi(n)}$. Note that in this list of reduced residues we have both r_i and $n - r_i$. *Why?*

We consider two cases: 1) r_i has a self inverse 2) r_i does *not* have self inverse.

If r_i has a self inverse then multiply this by $n - r_i$ and we have

$$r_i(n - r_i) \equiv r_i(-r_i) \equiv -r_i^2 \equiv -1 \pmod{n}.$$

If r_i does not have self inverse then there is another reduced residue r_j where $i \neq j$ which is its inverse. This means you can pair up r_i with its inverse r_j to get

$$r_i \times r_j \equiv 1 \pmod{n}.$$

Therefore the product of all the reduced residues

$$r_1 \times r_2 \times r_3 \times \cdots \times r_{\phi(n)} \equiv (-1)^k \pmod{n}.$$

where k is the number of self inverses divided by 2.

This completes our proof.

■

(ii) Wilson's Theorem (4.4) is the following:

If p is prime, then $(p-1)! \equiv -1 \pmod{p}$.

Proof.

We use the result of part (i). Since p is prime so our reduced residues system is given by $\{1,\ 2,\ 3,\ \cdots,\ p-1\}$. By part (i) we have

$$1\times 2\times 3\times\ \cdots\times(p-1)\equiv(-1)^k\ (\text{mod}\ p).$$

where k is the number of self inverses divided by 2. Modulo p has two residues which have self-inverses and these are 1 and $p-1$. *Why?*

By Lemma (4.3):

$$x^2\equiv 1\ (\text{mod}\,p)\quad\Leftrightarrow\quad x\equiv\pm 1\,(\text{mod}\,p)$$

Therefore $k=1$ which gives

$$(p-1)!\equiv 1\times 2\times 3\times\ \cdots\times(p-1)\equiv(-1)^1\equiv -1\ (\text{mod}\ p).$$

This completes our proof.

■

19. We need to find the last three digits of $2019^{2019^{2019}}$. For the last three digits we need to work with modulo 1000. We need to find the least positive residue x which satisfies $2019^{2019^{2019}}\equiv x\,(\text{mod}\ 1000)$. Since the $\gcd(2019,\ \ 1000)=1$ so we can apply Euler's Theorem. First we note that $\phi(1000)=400$. Therefore

$$2019^{400}\equiv 1\,(\text{mod}\ 1000)\qquad\qquad (*)$$

We need to write the index 2019^{2019} as a multiple of 400 and any remainder. Again we can use Euler's Theorem to find this. However we have

$$2019\equiv 19\,(\text{mod}\ 400).$$

Therefore we have to find

$$2019^{2019}\equiv 19^{2019}\equiv y\,(\text{mod}\ 400)\qquad\qquad (\ddagger)$$

and $\phi(400)=160$ so

$$19^{160}\equiv 1\,(\text{mod}\ 400)\qquad\qquad (**)$$

Applying the division algorithm to index 2019 and 160 gives

$$2019=(12\times 160)+99.$$

Using this calculation in $19^{2019}\equiv y\,(\text{mod}\ 400)$ gives

$$19^{2019}\equiv 19^{(12\times 160)+99}\equiv\left(19^{160}\right)^{12}\times 19^{99}\equiv\underbrace{1}_{\text{By (**)}}\times 19^{99}\equiv 19^{99}\equiv y\,(\text{mod}\ 400).$$

Modulo 400 is too large to work with. We factorize 400:

$$400 = 16 \times 25 .$$

To find the above $19^{99} \equiv y \left(\text{mod } 400\right)$ we use moduli 16 and 25:

$$19^{99} \equiv y_1 \left(\text{mod } 16\right), \quad 19^{99} \equiv y_2 \left(\text{mod } 25\right).$$

Evaluating the first of these $19^{99} \equiv y_1 \left(\text{mod } 16\right)$:

$$y_1 \equiv 19^{99} \equiv 3^{99} \equiv 3^{(4\times 24)+3} \equiv \left(3^4\right)^{24} \times 3^3 \underbrace{\equiv}_{\text{By } 3^4 \equiv 1 \left(\text{mod } 16\right)} 3^3 \equiv 27 \equiv 11 \left(\text{mod } 16\right).$$

Now evaluating the other residue $19^{99} \equiv y_2 \left(\text{mod } 25\right)$. Since $\gcd\left(19, \ 25\right) = 1$ so we can apply Euler's Theorem to this by first evaluating $\phi\left(25\right) = 5^2 - 5 = 20$. Writing the index 99 as a multiple of 20 and any remainder gives

$$99 = \left(5 \times 20\right) - 1 .$$

By Euler's theorem we have

$$\begin{aligned} y_2 \equiv 19^{99} \equiv 19^{(20\times 5)-1} &\equiv \left(19^{20}\right)^5 \times 19^{-1} \\ &\equiv 1^5 \times 19^{-1} \\ &\equiv 19^{-1} \equiv \left(-6\right)^{-1} \equiv 4 \left(\text{mod } 25\right) \quad \left[\text{Because } -6 \times 4 = -24 \equiv 1 \left(\text{mod } 25\right)\right] \end{aligned}$$

Summarizing these results $19^{99} \equiv 11 \left(\text{mod } 16\right)$ and $19^{99} \equiv 4 \left(\text{mod } 25\right)$. Applying the Chinese Remainder Theorem to these two results gives

$$\begin{aligned} 19^{99} &\equiv \left(a_1 \times N_1 \times x_1\right) + \left(a_2 \times N_2 \times x_2\right) \\ &\equiv \left(4 \times 16 \times x_1\right) + \left(11 \times 25 \times x_2\right) \left(\text{mod } 25 \times 16\right) \qquad (\dagger) \end{aligned}$$

Solving

$$\begin{aligned} 16x_1 \equiv 1 \left(\text{mod } 25\right) \ &\Rightarrow \ x_1 \equiv 11 \left(\text{mod } 25\right) \\ 25x_2 \equiv 1 \left(\text{mod } 11\right) \ &\Rightarrow \ x_2 \equiv 9 \left(\text{mod } 16\right) \end{aligned}$$

Substituting these into $(\dagger)$ yields

$$19^{99} \equiv \left(4 \times 16 \times 11\right) + \left(11 \times 25 \times 9\right) \equiv 379 \left(\text{mod } 400\right).$$

Putting this into (‡) gives

$$y \equiv 2019^{2019} \equiv 19^{2019} \equiv 19^{99} \equiv 379 \left(\text{mod } 400\right).$$

Therefore, we have

$$x \equiv 2019^{2019^{2019}} \equiv 2019^{379+400k} \equiv 2019^{379} \equiv 19^{379} \left(\text{mod } 1000\right)$$

It is still pretty difficult to evaluate $x \equiv 2019^{2019^{2019}} \equiv 19^{379} \left(\text{mod } 1000\right)$ because of the large index. However this is much easier than dealing with the index 2019^{2019} which has 6674 digits.

Again modulo 1000 is too large to work with so we again use the Chinese Remainder Theorem by factorizing 1000 first; $1000 = 8 \times 125$. Both these moduli, 8 and 125, are much easier to work with. We need to evaluate

$$19^{379} \equiv n_1 \left(\text{mod } 8\right), \;\; 19^{379} \equiv n_2 \left(\text{mod } 125\right).$$

Applying Euler's Theorem with $\phi\left(8\right) = 4$ so $19^4 \equiv 3^4 \equiv 1\left(\text{mod } 8\right)$. Hence

$$n_1 \equiv 19^{379} \equiv 3^{4k} \times 3^3 \equiv 3^3 \equiv 27 \equiv 3\left(\text{mod } 8\right) \text{ where } k \text{ is an integer.}$$

Now evaluating n_2 we have $\phi\left(125\right) = 125 - 25 = 100$ so $19^{100} \equiv 1\left(\text{mod } 125\right)$. Therefore

$$n_2 \equiv 19^{379} \equiv 19^{79} \left(\text{mod } 125\right).$$

We still have a reasonable large index and modulo but let us preserve with this. By using a calculator we find that $19^6 \equiv 6\left(\text{mod } 125\right)$. Using this in the above calculation gives

$$\begin{aligned} n_2 \equiv 19^{79} &\equiv 19^{\left(6\times 13\right)+1} \\ &\equiv \left(19^6\right)^{13} \times 19 \equiv 6^{13} \times 19 \equiv 6^{12}\left(6 \times 19\right) \equiv 31^2\left(114\right) \equiv 54\left(\text{mod } 125\right) \end{aligned}$$

Summarizing these two calculations we have

$$19^{379} \equiv 3\left(\text{mod } 8\right) \text{ and } 19^{379} \equiv 54\left(\text{mod } 125\right).$$

Now using the Chinese Remainder Theorem we have

$$\begin{aligned} 19^{379} &\equiv \left(a_1 \times N_1 \times x_1\right) + \left(a_2 \times N_2 \times x_2\right) \\ &\equiv \left(3 \times 125 \times x_1\right) + \left(54 \times 8 \times x_2\right) \left(\text{mod } 125 \times 8\right) \qquad (\dagger\dagger) \end{aligned}$$

To find x_1 and x_2 we need to solve the following:

$$125x_1 \equiv 1\left(\text{mod } 8\right) \;\Rightarrow\; x_1 \equiv 5 \left(\text{mod } 8\right)$$

$$8x_2 \equiv 1\left(\text{mod } 125\right) \;\Rightarrow\; x_2 \equiv 47\left(\text{mod } 125\right)$$

Substituting these into (††) gives

$$19^{379} \equiv \left(3 \times 125 \times 5\right) + \left(54 \times 8 \times 47\right) \equiv 179 \left(\text{mod } 1000\right).$$

Hence, we have $x \equiv 2019^{2019^{2019}} \equiv 19^{379} \equiv 179\left(\text{mod } 1000\right)$. The last three digits of $2019^{2019^{2019}}$ is 179.