Complete Solutions to Exercise 3.1

1. (a) Here is a sample of 3 sets of modulo 5:

$$\{0,\ 1,\ 2,\ 3,\ 4\},\ \{0,\ -1,\ -2,\ -3,\ -4\} \text{ and } \{5,\ 6,\ 7,\ 8,\ 9\}.$$

(b) A sample of 3 sets modulo 10 is:

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\},\ \{-1, -2, -3, -4, -5, -6, -7, -8, -9, -10\} \text{ and}$$
$$\{10, 11, 12, 13, 14, 15, 16, 17, 18, 19\}$$

(c) Similarly, we have

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\},\ \{-1, -2, -3, -4, -5, -6, -7, -8, -9, -10, -11, -12, -13\}$$
$$\text{and } \{13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25\}.$$

2. (a) From this set $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ the stop 0 modulo 11 is missing.

(b) In this set $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$ we have two integers congruent to each other: $11 \equiv 0 \pmod{11}$. Remember for a complete system of residues any two numbers *cannot* be congruent to each other.

(c) From this set $\{0, 2, 4, 6, 8, 10, 12, 13, 14, 15, 16\}$ clearly the first 6 numbers are *not* congruent to each other so they form part of the system. Let us check 12 and 13 entries in this set:

$$12 \equiv 1 \pmod{11}$$
$$13 \equiv 2 \pmod{11}$$

We already have the integer 2 in the given set. Again two integers, 2 and 13, in the given set are congruent to each other so the set *cannot* form a complete system of residues modulo 11.

3. (a) The complete system of least non-negative residues modulo 6 is

$$\{0, 1, 2, 3, 4, 5\}$$

(b) Similarly, for modulo 12 the complete system of the least non-negative residues is

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$$

(c) For modulo 17 we have the set

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}$$

4. (a) We need to find the remainder after dividing 100 by 12 because we are given $100 \equiv x \pmod{12}$. We have $100 = (8 \times 12) + 4$ so

$$100 \equiv 4 \pmod{12}$$

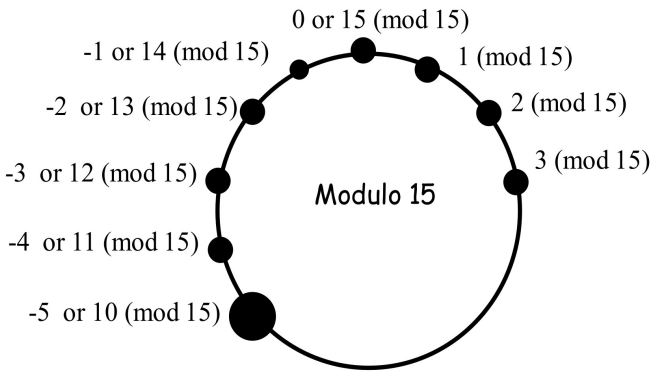
Hence $x = 4$.

(b) We have $666 = (60 \times 11) + 6$ so we have A remainder of 6:

$$666 \equiv 6 \pmod{11} \text{ which gives } x = 6.$$

(c) *What is -5 modulo 15 equal to?*

It is 10 modulo 15 because we count 5 stops from 15 in an anti-clockwise direction:



We have $-5 \equiv 10 \pmod{15}$ so $x = 10$.

(d) Clearly for $1000 \equiv x \pmod{1001}$ if we divide 1001 by 1000 we have the remainder of 1000 because $1000 = (0 \times 1001) + 1000$ so $x = 1000$.

(e) We are given $-25 \equiv x \pmod{7}$. As -21 is a multiple of 7 and $-25 = -21 - 4$ so we have

$$-25 \equiv -4 \equiv 3 \pmod{7}$$

Hence $x = 3$.

(f) *How do we find the least non-negative residue in the case $-100 \equiv x \pmod{24}$?*

$$-100 = (-4 \times 24) - 4$$

This remainder -4 is *not* the least non-negative residue (remainder). *What is -4 modulo 24 equal to?*

Well $24 - 4 = 20$ so we have

$$-100 \equiv -4 \equiv 20 \pmod{24}$$

Hence $x = 20$.

5. In each case we use Proposition (3.6):

If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then	
(i) $a + c \equiv b + d \pmod{n}$	(ii) $ac \equiv bd \pmod{n}$

(a) We are given $2789 + 2788 \equiv x \pmod{2787}$ but we don't need to add these numbers. We have

$$2789 \equiv 2 \pmod{2787} \text{ and } 2788 \equiv 1 \pmod{2787}.$$

Using part (i) of the above proposition gives

$$x \equiv 2789 + 2788 \equiv 2 + 1 \equiv 3 \pmod{2787}$$

(b) Using part (ii) of the above proposition gives

$$x \equiv 2789 \times 2788 \equiv 2 \times 1 \equiv 2 \pmod{2787}$$

(c) Similarly for $5201 + 5211 \equiv x \pmod{5200}$ we have

$$5201 \equiv 1 \pmod{5200} \text{ and } 5211 \equiv 11 \pmod{5200}$$

Again using (3.6) part (i) we have

$$x \equiv 5201 + 5211 \equiv 1 + 11 \equiv 12 \pmod{5200}$$

(d) Applying part (ii) for $5201 \times 5211 \equiv x \pmod{5200}$ yields

$$x \equiv 5201 \times 5211 \equiv 1 \times 11 = 11 \pmod{5200}$$

(e) We need to evaluate $5198 + 5188 \equiv x \pmod{5200}$. Note that 5198 is 2 less than 5200 and 5188 is 12 less than 5200 therefore we have

$$5198 \equiv -2 \pmod{5200} \text{ and } 5188 \equiv -12 \pmod{5200}$$

Applying Proposition (3.6) part (i) to these congruences we have

$$\begin{aligned} x &\equiv 5198 + 5188 \\ &\equiv -2 + (-12) \\ &\equiv -14 \equiv 5186 \pmod{5200} \end{aligned}$$

(f) We need to find the least non-negative residue x modulo 5200 of:

$$5198 \times 5180 \equiv x \pmod{5200}$$

We have $5180 \equiv -20 \pmod{5200}$. Using Proposition (3.6) part (ii) on

$$5198 \equiv -2 \Big(\mathrm{mod}\ 5200\Big) \text{ and } 5180 \equiv -20 \Big(\mathrm{mod}\ 5200\Big).$$

Gives

$$\begin{aligned} x &\equiv 5198 \times 5180 \\ &\equiv -2 \times \Big(-20\Big) \\ &\equiv 40 \Big(\mathrm{mod}\ 5200\Big) \end{aligned}$$

6. We just need to find the remainder of dividing 1729 by 5, 11 and 1001:

$$\begin{aligned} 1729 &\equiv 4 \Big(\mathrm{mod}\ 5\Big) \\ 1729 &\equiv 2 \Big(\mathrm{mod}\ 11\Big) \\ 1729 &\equiv 728 \Big(\mathrm{mod}\ 1001\Big) \end{aligned}$$

7. Since we are interested in the last two digits so we work with modulo 100. We find the least non-negative residue module 100 of each integer and then do the calculation.

   (a) Evaluating the least non-negative residues:

$$4\ 352\ 709 \equiv 9 \bmod \Big(100\Big) \text{ and } 4\ 678\ 829 \equiv 29 \Big(\mathrm{mod}\ 100\Big)$$

   Carrying out the multiplication

$$\begin{aligned} 4\ 352\ 709 \times 4\ 678\ 829 &\equiv 9 \times 29 \\ &\equiv 261 \equiv 61 \Big(\mathrm{mod}\ 100\Big) \end{aligned}$$

   Hence the last two digits are 61.

   (b) First, we find the least non-negative residue $4\,352\,783$ modulo 100:

$$4\ 352\ 783 \equiv 83 \equiv -17 \Big(\mathrm{mod}\ 100\Big)$$

   Also finding a power of -17 which makes the arithmetic easier:

$$\Big(-17\Big)^2 \equiv 289 \equiv 89 \equiv -11 \Big(\mathrm{mod}\ 100\Big) \qquad (*)$$

   Therefore

$$\begin{aligned} 4\ 352\ 783^5 &\equiv \Big(-17\Big)^5 \\ &\equiv \Big(-17\Big)^4 \times \Big(-17\Big) \\ &\equiv \Big[\Big(-17\Big)^2\Big]^2 \times \Big(-17\Big) \\ &\equiv \underbrace{\Big[-11\Big]^2}_{\text{By } (*)} \times \Big(-17\Big) \\ &\equiv 121 \times \Big(-17\Big) \\ &\equiv 21 \times \Big(-17\Big) \equiv -357 \equiv -57 \equiv 43 \Big(\mathrm{mod}\ 100\Big) \end{aligned}$$

The last two digits of $4\,352\,783^5$ are 43.

8. (a) The congruence $12 \equiv 232 \pmod 5$ is true because when we divide 232 and 12 by 5 we end up with the same remainder 2.

(b) This result $15 \not\equiv 5 \pmod{10}$ is false because 15 and 5 divided by 10 give the same remainder, so $15 \equiv 5 \pmod{10}$.

(c) This $12 \equiv -1 \pmod{11}$ is also false because dividing 12 by 11 gives remainder $+1$ *not* -1, that is $12 \equiv 1 \pmod{11}$.

(d) We are given $365 \not\equiv 1 \pmod 7$. Dividing 365 by 7 gives remainder 1 so

$$365 \equiv 1 \pmod 7$$

Hence our given result is false.

(e) The given congruence $-65 \equiv -29 \pmod{12}$ in this case is bit more complex than the above. It is *not* easy to spot whether this result is true or false. We have

$$-65 \equiv -5 \pmod{12} \text{ and } -29 \equiv -5 \pmod{12}.$$

Therefore $-65 \equiv -29 \pmod{12}$ so the result is true.

(f) We are given $-43 \not\equiv -46 \pmod 2$. Now -43 divided by 2 gives remainder -1 and -46 divided by 2 gives remainder 0. Therefore they are incongruent, so $-43 \not\equiv -46 \pmod 2$ is true.

9. *How can we find the last digit of any number?*

By using modulo 10 and finding the least non-negative residue modulo 10.

(a) We are given 3^{100}. First we try to find an index of 3 which makes our arithmetic much easier. Well $3^2 = 9$ so

$$3^2 \equiv 9 \equiv -1 \pmod{10}$$

Next we break the index 100 into a multiple of 2 and any remainder:

$$100 = 2 \times 50$$

Using this we have

$$\begin{aligned} 3^{100} &\equiv 3^{2\times 50} \\ &\equiv \left(3^2\right)^{50} \qquad \left[\text{Using rules of indices}\right] \\ &\equiv \left(-1\right)^{50} \equiv 1 \pmod{10} \end{aligned}$$

The last digit of 3^{100} is 1.

(b) *How do we find the last digit of* 9^{100} *?*

Since $3^2 = 9$ we can use the result of part (a):

$$\begin{aligned} 9^{100} &\equiv \left(3^2\right)^{100} \\ &\equiv \left(3^{100}\right)^2 \equiv 1^2 \equiv 1 \left(\text{mod } 10\right) \end{aligned}$$

The last digit of 9^{100} is 1.

(c) We are given 2^{100} and we look for an index of 2 which will make the arithmetic easier. Well $2^5 \equiv 32 \equiv 2\left(\text{mod } 10\right)$.

Next we break the index 100 into a multiple of 5:

$$5 \times 20 = 100$$

This is still going to be pretty tedious because we don't have ± 1 which always makes the arithmetic a lot easier because index of these numbers are easy to evaluate. However we cannot change the question so let us try to slog this out.

We make repeated use of the above result $2^5 \equiv 2\left(\text{mod } 10\right)$:

$$\begin{aligned} 2^{100} &\equiv 2^{5\times 20} \\ &\equiv \left(2^5\right)^{20} \\ &\equiv 2^{20} \\ &\equiv 2^{5\times 4} \equiv \left(2^5\right)^4 \equiv 2^4 \equiv 16 \equiv 6 \left(\text{mod } 10\right) \end{aligned}$$

The remainder is 6 so the last digit of 2^{100} is 6.

(d) *How do we find the last digit of* 4^{100} *?*

Since $4 = 2^2$, we use the result of part (c). We have

$$4^{100} \equiv \left(2^2\right)^{100} \underbrace{\equiv}_{\text{Using the rules of indices}} \left(2^{100}\right)^2 \underbrace{\equiv}_{\text{By part (c)}} 6^2 \equiv 36 \equiv 6 \left(\text{mod } 10\right)$$

The last digit of 4^{100} is 6.

10. *How can we find the last two digits of any number?*

By finding the least non-negative residue module 100. We are informed that the number 2014^{2014} has 6655 digits but we are not interested in finding all these digits but just the last two. *How do we find these?*

Let us first obtain the least non-negative residue of 2014 modulo 100:

$$2014 \equiv 14 \left(\text{mod } 100\right)$$

Now $14^2 = 196$ and $196 \equiv 96 \equiv -4 \pmod{100}$. We would rather deal with -4 than 14. We have

$$\begin{aligned} 2014^{2014} &\equiv 14^{2014} \\ &\equiv \left(14^2\right)^{1007} \\ &\equiv \left(-4\right)^{1007} \pmod{100} \end{aligned}$$

The index 1007 is too large to evaluate by calculator. We can write

$$-4^{1007} = -1^{1007}4^{1007} = -1\left(4^{1007}\right)$$

Therefore we have

$$\begin{aligned} 2014^{2014} &\equiv \left(-4\right)^{1007} \\ &\equiv -1\left(4^{1007}\right) \pmod{100} \qquad (*) \end{aligned}$$

Let us examine the last term on the right-hand side, 4^{1007}. We need to rewrite 1007 in terms of a simpler index. We have

$$4^{11} \equiv 4\,194\,304 \equiv 4 \pmod{100} \qquad (**)$$

We need to express the index 1007 as a multiple of 11 and any remainder:

$$1007 = \left(91 \times 11\right) + 6 \qquad (\dagger)$$

Using result (†) to find 4^{1007} we have

$$\begin{aligned} 4^{1007} &\equiv 4^{(11\times 91)+6} \\ &\equiv \left(4^{11}\right)^{91} \times 4^6 \qquad \left[\text{Using the rules of indices}\right] \\ &\underbrace{\equiv}_{\text{By (**)}} \left(4\right)^{91} \times 4^6 \\ &\equiv \left(4\right)^{(11\times 8)+3} \times 4^6 \\ &\equiv \left(4^{11}\right)^{8} \times 4^3 \times 4^6 \\ &\underbrace{\equiv}_{\text{By (**)}} \left(4\right)^{8} \times 4^3 \times 4^6 \\ &\equiv 4^{11} \times 4^6 \equiv 4 \times 4^6 \equiv 4^7 \equiv 16384 \equiv 84 \equiv -16 \pmod{100} \end{aligned}$$

Putting this result $4^{1007} \equiv -16 \pmod{100}$ into (*) gives

$$\begin{aligned} 2014^{2014} &\equiv -1\left(4^{1007}\right) \\ &\equiv -1 \times \left(-16\right) \equiv 16 \pmod{100} \end{aligned}$$

Hence the last two digits of 2014^{2014} are 16.

11. (a) *Proof.*

An even number is congruent to 0 modulo 2.

Let $a = 2m$ then

$$a^n \equiv \left(2m\right)^n \equiv 2^n m^n \equiv 0m^n \equiv 0 \left(\text{mod } 2\right)$$

We have $a^n \equiv 0 \left(\text{mod } 2\right)$ therefore a^n is even.

■

(b) *Proof.*

An odd number a is congruent to 1 modulo 2, that is

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

Therefore by Proposition (3.8):

> If $a \equiv b \left(\text{mod } n\right)$ then $a^k \equiv b^k \left(\text{mod } n\right)$ where k is a natural number.

We have

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

Since $a^n \equiv 1 \left(\text{mod } 2\right)$ so a^n is odd.

■

12. (a) We need to prove that a square number a^2 divided by 3 gives only remainders 0 or 1.

Proof.

Let a be any integer then we can write a in modulo 3 as

$$a \equiv 0, 1 \text{ or } 2 \left(\text{mod } 3\right)$$

Note that $a \equiv 2 \equiv -1 \left(\text{mod } 3\right)$. Squaring a gives

$$\begin{aligned} a^2 &\equiv 0^2, 1^2 \text{ or } \left(-1\right)^2 \\ &\equiv 0 \text{ or } 1 \left(\text{mod } 3\right) \end{aligned}$$

This completes our proof that a square number divided by 3 can only have remainders 0 or 1.

■

(b) Repeating a similar argument for modulo 4.

Proof.

Let a be any integer then we can write a in modulo 4 as

$$\begin{aligned} a &\equiv 0, 1, 2 \text{ or } 3 \left(\text{mod } 4\right) \\ &\equiv 0, 1, 2 \text{ or } -1 \left(\text{mod } 4\right) \end{aligned}$$

Squaring a gives

$$\begin{aligned} a^2 &\equiv 0^2, 1^2, 2^2 \text{ or } \left(-1\right)^2 \\ &\equiv 0, 1, 0 \text{ or } 1 \left(\text{mod } 4\right) \end{aligned}$$

This completes our proof.

13. We need to prove that $p \equiv 3 \left(\text{mod } 4\right)$ *cannot* be written as the sum of two squares.

Proof.

Let $p = a^2 + b^2$.

Using the result of question 12(b) and evaluating the least non-negative residue modulo 4 for each of these square numbers gives

$$\begin{aligned} a^2 &\equiv 0,\ 1 \left(\text{mod } 4\right) \\ b^2 &\equiv 0, 1 \left(\text{mod } 4\right) \end{aligned}$$

Adding them together yields

$$\begin{aligned} p = a^2 + b^2 &\equiv 0+0,\ \ 0+1, 1+0 \text{ or } 1+1 \\ &\equiv 0,\ \ 1, 1 \text{ or } 2 \\ &\equiv 0,\ \ 1,\ \ 2 \left(\text{mod } 4\right) \end{aligned}$$

Therefore $p \equiv 3 \left(\text{mod } 4\right)$ *cannot* be written as the sum of two squares.

■

14. We need to prove that $6^n \equiv 6 \left(\text{mod } 10\right)$. *How?*

Use mathematical induction which involves the following three steps:

Step 1: Check the result for a base case k_0.

Step 2: Assume the result is true for $k = m$.

Step 3: Prove the result for $k = m + 1$.

Proof.

Step 1: Clearly the result is true for the base case $n = 1$ because

$$6 \equiv 6 \left(\text{mod } 10\right)$$

Step 2: Assume the result is true for $k = m$:

$$6^m \equiv 6 \left(\text{mod } 10\right) \qquad (*)$$

Step 3: We are required to prove $6^{m+1} \equiv 6 \left(\text{mod } 10\right)$. Expanding the left - hand side

$$\begin{aligned} 6^{m+1} &\equiv 6^m \times 6 \\ &\equiv \underbrace{6}_{\text{By (*)}} \times 6 \equiv 36 \equiv 6 \pmod{10} \end{aligned}$$

By mathematical induction we have our result $6^n \equiv 6 \pmod{10}$.

■

The last digit of 6 to any natural number index will be 6.

15. We need to show that $2^m \not\equiv 0 \pmod{10}$.

Proof.

Evaluating the first few powers of 2 and finding the least non-negative residues modulo 10:

$$2 \equiv 2 \pmod{10},\ 2^2 \equiv 4 \pmod{10},\ 2^3 \equiv 8 \pmod{10},\ 2^4 \equiv 6 \pmod{10}$$

Let m be any natural number. Then by using the Division Algorithm (1.7) of Chapter 1:

> There exist unique integers q and r such that
> $$a = nq + r \quad \text{where } 0 \le r < n\,.$$

We can write the index m as a multiple of 4 and a remainder:

$$m = 4k + r \text{ where } 0 \le r < 4\,.$$

Substituting this $m = 4k + r$ into the index of 2 gives

$$\begin{aligned} 2^m &\equiv 2^{4k+r} \\ &\equiv \left(2^4\right)^k \times 2^r \\ &\equiv \left(6\right)^k \times 2^r \\ &\equiv \underbrace{6}_{\text{By question 14}} \times 2^r \pmod{10} \qquad (\dagger) \end{aligned}$$

Remember the remainder r satisfies $0 \le r < 4$ so can only have values of r equal to:

0, 1, 2 or 3

Substituting each of these values into $(\dagger)$ yields

$$\begin{aligned} 2^m &\equiv 6 \times 2^r \\ &\equiv 6 \times 2^0,\ 6 \times 2^1,\ 6 \times 2^2 \text{ or } 6 \times 2^3 \\ &\equiv 6,\ 12,\ 24 \text{ or } 48 \\ &\equiv 6,\ 2,\ 4 \text{ or } 8 \pmod{10} \\ &\equiv 2,\ 4,\ 6 \text{ or } 8 \pmod{10} \end{aligned}$$

Hence $2^m \not\equiv 0 \pmod{10}$.

■

The last digit of powers of 2 *cannot* be zero.

16. We need to prove that the last digit of a square can only be 0, 1, 4, 5, 6 and 9.

Proof.

Let n be any integer. By using the Division Algorithm we can write this as a multiple of 10 plus any remainder:

$$n = 10q + r \text{ where } 0 \leq r < 10\,.$$

Squaring this $n = 10q + r$ and using modulo 10 gives

$$\begin{aligned} n^2 &\equiv \left(10q + r\right)^2 \\ &\equiv \underbrace{100q^2 + 20qr}_{\equiv 0 \left(\mathrm{mod}\ 10\right)} + r^2 \\ &\equiv r^2 \ \left(\mathrm{mod}\ 10\right) \end{aligned}$$

Substituting the possible values of the remainder $r = 0,\ 1,\ 2,\ \cdots,\ 8,\ 9$ into the above:

$$\begin{aligned} n^2 &\equiv r^2 \\ &\equiv 0^2,\ 1^2,\ 2^2,\ 3^2,\ 4^2,\ 5^2,\ 6^2,\ 7^2,\ 8^2 \text{ and } 9^2 \\ &\equiv 0,\ 1,\ 4,\ 9,\ 16,\ 25,\ 36,\ 49,\ 64 \text{ and } 81 \\ &\equiv 0,\ 1,\ 4,\ 9,\ 6,\ 5,\ 6,\ 9,\ 4 \text{ and } 1 \left(\mathrm{mod}\ 10\right) \end{aligned}$$

Hence $n^2 \equiv 0,\ 1,\ 4,\ 5,\ 6,\ 9\ \left(\mathrm{mod}\ 10\right)$, therefore the last digit of a square number can only be 0, 1, 4, 5, 6 and 9.

■

17. We need to prove that the last digit of a cube can be any digit.

Proof.

The proof in this case is very similar to the proof of the previous question. The only difference is we examine

$$\begin{aligned} n^3 &\equiv r^3 \\ &\equiv 0^3,\ 1^3,\ 2^3,\ 3^3,\ 4^3,\ 5^3,\ 6^3,\ 7^3,\ 8^3 \text{ and } 9^3 \\ &\equiv 0,\ 1,\ 8,\ 7,\ 4,\ 5,\ 6,\ 3,\ 2 \text{ and } 9\ \left(\mathrm{mod}\ 10\right) \end{aligned}$$

Hence the last digit of a cube can be any integer from 0 to 9.

■

18. *How do we prove something is not true?*

By giving a counter example. You can come up with many counter examples but you only need one to disprove a statement.

(a) We need to show that $a^2 \equiv b^2 \pmod{n} \Rightarrow a \equiv b \pmod{n}$ is *not* true.

Consider the following:

$$2^2 \equiv 3^2 \equiv 4 \pmod{5} \not\Rightarrow 2 \equiv 3 \pmod{5}$$

(b) We need to find a counter example to

$$a \times b \equiv 0 \pmod{n} \Rightarrow a \equiv 0 \pmod{n} \text{ or } b \equiv 0 \pmod{n}$$

Consider

$$2 \times 3 \equiv 0 \pmod{6} \Rightarrow 2 \not\equiv 0 \pmod{6} \text{ or } 3 \not\equiv 0 \pmod{6}$$

(c) In this case the counter example is

$$2 \times 6 \equiv 2 \times 1 \pmod{10} \text{ but } 6 \not\equiv 1 \pmod{10}$$

19. (a) We are required to find the remainder when 11^{567} is divided by 61.

We first examine a lower power of 11:

$$11^2 \equiv 121 \equiv -1 \pmod{61} \quad (*)$$

Now we write the index 567 as a multiple of 2 plus remainder. *Why?*

So that we can use result (*):

$$567 = (283 \times 2) + 1$$

Applying the rules of indices and using this $567 = (283 \times 2) + 1$ to evaluate 11^{567}:

$$\begin{aligned} 11^{567} &\equiv 11^{(283\times 2)+1} \\ &\equiv \left(11^2\right)^{283} \times 11 \\ &\equiv \underbrace{(-1)^{283}}_{\text{By (*)}} \times 11 \\ &\equiv -11 \equiv 50 \pmod{61} \end{aligned}$$

The remainder is 50 after 11^{567} is divided by 61.

(b) Similarly we evaluate small powers of 11 to reduce our arithmetic.

$$11^2 \equiv 121 \equiv 35 \pmod{43}$$

Dealing with 35 will be time consuming. Let us try other powers of 11:

$$11^3 \equiv 1331 \equiv 41 \equiv -2 \pmod{43} \quad (**)$$

Easier to deal with -2 than 35. In order to use this result (**) we need to write the index 567 as a multiple of 3 plus any remainder:

$$567 = 189 \times 3$$

Therefore

$$11^{567} \equiv 11^{3\times 189} \equiv \left(11^3\right)^{189} \equiv \left(-2\right)^{189} \left(\text{mod } 43\right) \qquad (\dagger)$$

The index 189 is too large to deal with. Evaluating powers of 2:

$$2^2 \equiv 4 \left(\text{mod } 43\right),\ 2^3 \equiv 8 \left(\text{mod } 43\right),\ 2^4 \equiv 16 \left(\text{mod } 43\right),\ 2^5 \equiv 32 \left(\text{mod } 43\right),$$
$$2^6 \equiv 21 \left(\text{mod } 43\right),\ \boxed{2^7 \equiv 128 \equiv -1 \left(\text{mod } 43\right)}$$

We want to use $2^7 \equiv -1 \left(\text{mod } 43\right)$ because -1 to any index gives 1 or -1.

Using this in (†) yields

$$\begin{aligned} 11^{567} &\equiv \left(-2\right)^{189} \\ &\equiv \left(-1\right)^{189} \times 2^{189} \\ &\equiv \left(-1\right) \times \left(2^7\right)^{27} \\ &\equiv -1 \times \left(-1\right)^{27} \equiv -1 \times \left(-1\right) \equiv 1 \left(\text{mod } 43\right) \end{aligned}$$

The remainder of dividing 11^{567} by 43 is 1.

20. *What does this* $2^{2^5} + 1$ *mean?*

$$2^{2^5} + 1 = 2^{\left(2^5\right)} + 1 = 2^{32} + 1$$

For the time being forget about the plus 1. We will add this in at the end.

Evaluating some powers of 2 which are close to 641:

$$2^8 = 256,\ 2^9 = 512,\ \ 2^{10} = 1024$$

$2^9 = 512$ will give us the smallest number if we count in an anti-clockwise direction:

$$2^9 \equiv 512 \equiv -129 \left(\text{mod } 641\right)$$

Writing the index 32 as a multiple of 9 plus remainder we have

$$32 = \left(3 \times 9\right) + 5$$

We have

$$\begin{aligned} 2^{2^5} \equiv 2^{32} &\equiv 2^{\left(3\times 9\right)+5} \\ &\equiv \left(2^9\right)^3 \times 2^5 \\ &\equiv \left(-129\right)^3 \times 32 \\ &\equiv -2\ 146\ 689 \times 32 \\ &\equiv -621 \times 32 \\ &\equiv -20 \times 32 \equiv -640 \equiv -1 \left(\text{mod } 641\right) \end{aligned}$$

Therefore

$$2^{2^5} + 1 \equiv -1 + 1 \equiv 0 \left(\text{mod } 641\right)$$

Hence 641 divides $2^{2^5}+1$. [100 years after Fermat stipulated that $2^{2^n}+1$ were primes numbers, Euler found this factor, 641, of $2^{2^5}+1$. For a more detailed account of this see[1]].

21. *How do we find the last digit of* $1!+2!+3!+4!+\cdots+1000!$ *?*

You will recall that $n!=1\times2\times3\times\cdots\times\left(n-2\right)\times\left(n-1\right)\times n$. From 5! onwards we will have a multiple of 10 because each term will have a 5 and a 2 which are multiplied:

$$\begin{aligned}
5! &= 1\times\boxed{2}\times3\times4\times\boxed{5}\equiv0\left(\text{mod }10\right)\\
6! &= 1\times\boxed{2}\times3\times4\times\boxed{5}\times6\equiv0\left(\text{mod }10\right)\\
7! &= 1\times\boxed{2}\times3\times4\times\boxed{5}\times6\times7\equiv0\left(\text{mod }10\right)\\
&\vdots\qquad\qquad\vdots\qquad\qquad\vdots\\
1000! &= 1\times\boxed{2}\times3\times4\times\boxed{5}\times6\times\cdots\times999\times1000\equiv0\left(\text{mod }10\right)
\end{aligned}$$

Since all these terms are congruent to 0 modulo 10 we can ignore them in the given addition $1!+2!+3!+4!+\cdots+1000!$ We only need to add the first 4 terms:

$$1!+2!+3!+4!=1+2+6+24\equiv33\equiv3\left(\text{mod }10\right)$$

The last digit of $1!+2!+3!+4!+\cdots+1000!$ is 3.

22. Since we are interested in finding the last digit so we work with modulo 10.

(a) We are given 1961^{1961}. Finding the least non-negative residue modulo 10:

$$1961^{1961}\equiv1^{1961}\equiv1\left(\text{mod }10\right)$$

The last digit of 1961^{1961} is 1. (Seems obvious because the last digit is 1).

(b) We examine the number 1023^{1022}. First we find the least non-negative residue of the number 1023 modulo 10:

$$1023\equiv3\left(\text{mod }10\right)$$

Also

$$1023^2\equiv3^2\equiv9\equiv-1\left(\text{mod }10\right)$$

It makes the arithmetic a lot easier if we use 1023^2 because we have -1 and it is straightforward to find -1 to any integer index. We have

[1] Number Theory A Historical Approach by John Watkins pages 137-39.

$$1023^{1022} \equiv \left(1023^2\right)^{511}$$
$$\equiv \left(-1\right)^{511} \equiv \left(-1\right) \equiv 9 \left(\text{mod } 10\right)$$

The last digit of 1023^{1022} is 9.

(c) We are given 2019^{2019}. Note that

$$2019 \equiv -1 \left(\text{mod } 10\right)$$

Therefore $2019^{2019} \equiv \left(-1\right)^{2019} \equiv -1 \equiv 9 \left(\text{mod } 10\right)$. Hence the last digit of 2019^{2019} is 9.

23. We are asked to prove that at least one of k consecutive integers is divisible by k.

Proof.

If we only have one integer then clearly the result holds. Assume $k \geq 2$.

Let $n,\ n+1,\ n+2,\ \cdots,\ n+\left(k-1\right)$ be k consecutive integers. We work with modulo k and show that one of these is congruent to $0\left(\text{mod } k\right)$.

If $k \mid n$ then we are done. Let us consider the case where $k \nmid n$ then by the division algorithm there are integers q and r such that

$$n = kq + r \qquad 0 < r < k \qquad (*)$$

Writing this out in modular arithmetic

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

By (*) the largest value of r is $k-1$ and as these integers are consecutive therefore they go through

$$0 < r,\ r+1,\ r+2,\ \cdots,\ r+\left(k-1\right) \leq \left(k-1\right)+\left(k-1\right) = 2k-2 \left(\text{mod } k\right)$$

Since $k \geq 2$ these consecutive residues modulo k lie between 0 and $2k-2$:

$$1, 2, 3, \cdots, k-1, k, k+1, \cdots, 2k-2$$

Hence one of these, $r+j$ say, is congruent to k, that is

$$r + j \equiv k \equiv 0 \left(\text{mod } k\right)$$

Therefore one of the integers $n,\ n+1,\ n+2,\ \cdots,\ n+\left(k-1\right)$ is divisible by k.

This completes our proof.

■

24. (a) We are required to prove $m \mid n$ and $a \equiv b \left(\text{mod } n\right)$ then $a \equiv b \left(\text{mod } m\right)$.

Proof.

We are given that $a \equiv b \pmod{n}$ which implies that there is an integer k which satisfies:

$$a - b = kn \quad [a - b \text{ is multiple of } n]$$

We are also given $m \mid n$ so there is an integer x such that $mx = n$.

Substituting this into the above result gives

$$a - b = kn = kmx = m(kx)$$

Hence $a - b$ is a multiple of m therefore we have $a \equiv b \pmod{m}$.

■

(b) We are asked to prove if $ka \equiv kb \pmod{kn}$ then $a \equiv b \pmod{n}$.

Proof.

From the definition of congruence we have

$$ka \equiv kb \pmod{kn} \quad \Leftrightarrow \quad ka - kb = mkn$$

We are given that $k \neq 0$ so dividing $ka - kb = mkn$ by k gives

$$a - b = mn \quad \Leftrightarrow \quad a \equiv b \pmod{n}$$

This completes our proof.

■

(c) We are asked to prove if $a \equiv b \pmod{n}$ and $a \equiv b \pmod{m}$ then $a \equiv b \pmod{m \times n}$ provided $\gcd(m, n) = 1$.

Proof.

From $a \equiv b \pmod{n}$ and $a \equiv b \pmod{m}$ we have

$$n \mid (a - b) \text{ and } m \mid (a - b).$$

Using the result of question 12(i) Exercises 1.3:

> If $a \mid c$ and $b \mid c$, and $\gcd(a, b) = 1$ then $(a \times b) \mid c$.

Applying this to $n \mid (a - b)$ and $m \mid (a - b)$ gives

$$(n \times m) \mid (a - b)$$

Because $(n \times m) \mid (a - b)$ so we have our result $a \equiv b \pmod{m \times n}$.

■

(d) We have to prove if $a \equiv b \left(\text{mod } n_k\right)$ for $k = 1, 2, 3, \cdots, r$ where $\gcd\left(n_i, \quad n_j\right) = 1$ then $a \equiv b \left(\text{mod } n_1 \times n_2 \times \cdots \times n_r\right)$.

Proof.

We prove this by induction on r.

By part (c) the result holds for $r = 2$, that is $a \equiv b \left(\text{mod } n_1 \times n_2\right)$.

Assume the result is true for $r = m$;

$$a \equiv b \left(\text{mod } n_1 \times n_2 \times \cdots \times n_m\right) \qquad (*)$$

Required to prove the result for $r = m + 1$;

$$a \equiv b \left(\text{mod } n_1 \times n_2 \times \cdots \times n_m \times n_{m+1}\right)$$

We are given that $a \equiv b \left(\text{mod } n_{m+1}\right)$ and also $\gcd\left(n_i, \quad n_j\right) = 1$ where $i \neq j$ which implies

$$\gcd\left(n_{m+1}, \quad n_1\right) = \gcd\left(n_{m+1}, \quad n_2\right) = \cdots = \gcd\left(n_{m+1}, \quad n_m\right) = 1$$

By the result of question 15(ii) of Exercises 1.3:

$$\gcd\left(a, \quad n_1\right) = \gcd\left(a, \quad n_2\right) = \cdots = \gcd\left(a, \quad n_k\right) = 1 \;\Rightarrow\; \gcd\left(a, \quad n_1 \times n_2 \times \cdots \times n_k\right) = 1$$

Therefore, $\gcd\left(n_1 \times n_2 \times \cdots \times n_m, \quad n_{m+1}\right) = 1$. Hence by (*) and $a \equiv b \left(\text{mod } n_{m+1}\right)$ we obtain

$$a \equiv b \left(\text{mod } n_1 \times n_2 \times \cdots \times n_m \times n_{m+1}\right)$$

This completes our proof.

■

(e) We are required to prove that if $n = p_1^{k_1} \times p_2^{k_2} \times \cdots \times p_m^{k_m}$ and $a \equiv b \left(\text{mod } n\right)$ then $a \equiv b \left(\text{mod } p_j\right)$.

Proof.

We are given that $a \equiv b \left(\text{mod } n\right)$ which implies $n \mid \left(a - b\right)$.

We are also given $n = p_1^{k_1} \times p_2^{k_2} \times \cdots \times p_m^{k_m}$ so

$$p_j \mid n \text{ for } j = 1, \; 2, \; \cdots, \; m$$

Hence we have $p_j \mid n$ and $n \mid \left(a - b\right)$ so $p_j \mid \left(a - b\right)$ for $j = 1, \; 2, \; \cdots, \; m$. By the definition of congruence we have $a \equiv b \left(\text{mod } p_j\right)$ for $j = 1, \; 2, \; \cdots, \; m$.

■

25. We are asked to prove $a^3 - a \equiv 0 \left(\text{mod } 3\right)$.

Proof.

A complete residue system modulo 3 is the residues 0, 1 and 2. Substituting each of these 0, 1 and 2 into $a^3 - a$ gives

$$0^3 - 0 = 0 \equiv 0 \pmod 3$$
$$1^3 - 1 = 0 \equiv 0 \pmod 3$$
$$2^3 - 2 = 6 \equiv 0 \pmod 3$$

Since for every residue 0, 1 and 2 in the complete residue system we have $a^3 - a \equiv 0 \pmod 3$ so this completes our proof.

■

26. We are required to prove 3 divides $4^n - 1$. *How?*

Use mathematical induction with modulo 3.

The three steps of mathematical induction are:

Step 1: Check the result for a base case n_0.

Step 2: Assume the result is true for $n = k$.

Step 3: Prove the result for $n = k + 1$.

Proof.

Step 1:

Clearly the result is true for $n = 1$ because $4^1 - 1 = 3$ and

$$3 \equiv 0 \pmod 3$$

Step 2:

Assume the result is true for $n = k$:

$$4^k - 1 \equiv 0 \pmod 3 \qquad (*)$$

Step 3:

We need to prove that $4^{k+1} - 1 \equiv 0 \pmod 3$. Examining the left - hand side of this:

$$\begin{aligned} 4^{k+1} - 1 &\equiv 4\left(4^k\right) - 1 \\ &\equiv 3\left(4^k\right) + 4^k - 1 \qquad \left[\text{Writing } 4x = 3x + x \text{ where } x = 4^k\right] \\ &\equiv \underbrace{0}_{\substack{\text{Because } 3\left(4^k\right) \\ \text{is a multiple of 3}}} + \underbrace{0}_{\text{By (*)}} \equiv 0 \pmod 3 \end{aligned}$$

We have shown $4^{k+1} - 1 \equiv 0 \pmod 3$ therefore by mathematical induction we have 3 divides $4^n - 1$.

■

27. We need to show that a natural number N is divisible by 3 $\Leftrightarrow$ the sum of its digits is divisible by 3.

The proof is more or less identical to Example 8.

Proof.

$\left(\Leftarrow\right)$. Let the integer be $N = a_n a_{n-1} a_{n-2} \cdots a_2 a_1 a_0$. The sum S of the digits is given by

$$S = a_n + a_{n-1} + a_{n-2} + \cdots + a_2 + a_1 + a_0 \qquad (*)$$

We are given that 3 divides into S, that is $3 \mid S \Leftrightarrow$

$$S \equiv 0 \pmod 3 \qquad (\dagger)$$

How do we show that this results in 3 divides into the given integer N?

We first write out the integer N and then show that $N \equiv 0 \pmod 3$. *What does* $N = a_n a_{n-1} a_{n-2} \cdots a_2 a_1 a_0$ *mean?*

We can write this in expanded form as:

$$\begin{aligned} N &= a_n a_{n-1} a_{n-2} \cdots a_2 a_1 a_0 \\ &= \left(a_n \times 10^n\right) + \left(a_{n-1} \times 10^{n-1}\right) + \left(a_{n-2} \times 10^{n-2}\right) + \cdots + \left(a_2 \times 10^2\right) + \left(a_1 \times 10\right) + \left(a_0 \times 1\right) \end{aligned}$$

Since we are interested in divisibility by 3 so we use modulo 3. *What is 10 modulo 3 congruent to?*

$$10 \equiv 1 \pmod 3$$

By applying Proposition (3.8) $a \equiv b \pmod n$ implies $a^k \equiv b^k \pmod n$ we have

$$10^k \equiv 1^k \equiv 1 \pmod 3.$$

Using these in the congruence below:

$$\begin{aligned} N &\equiv a_n a_{n-1} a_{n-2} \cdots a_2 a_1 a_0 \\ &\equiv \left(a_n \times 10^n\right) + \left(a_{n-1} \times 10^{n-1}\right) + \cdots + \left(a_2 \times 10^2\right) + \left(a_1 \times 10\right) + \left(a_0 \times 1\right) \pmod 3 \\ &\equiv \left(a_n \times 1\right) + \left(a_{n-1} \times 1\right) + \cdots + \left(a_2 \times 1\right) + \left(a_1 \times 1\right) + \left(a_0 \times 1\right) \quad \left[\text{By above results}\right] \\ &\equiv a_n + a_{n-1} + a_{n-2} + \cdots + a_2 + a_1 + a_0 \\ &\underbrace{\equiv}_{\text{By (*)}} S \equiv 0 \pmod 3 \qquad \left[\text{By } (\dagger)\right] \end{aligned}$$

Hence $3 \mid N$.

$\left(\Rightarrow\right)$. Since in the above we have $N \equiv S \pmod 3$ so if $N \mid 3$ then $S \mid 3$.

■

28. (i) *How to show* $x^7 \equiv x\left(\mathrm{mod}\ 7\right)$ *?*

By substituting each of the integers which make up the complete residue system modulo 7.

Proof.

Evaluating $x^7\left(\mathrm{mod}\ 7\right)$ for each $x = 0, 1, 2, 3, 4, 5$ and 6 and then finding the least non-negative residue modulo 7:

$$0^7 \equiv 0\left(\mathrm{mod}\ 7\right)$$

$$1^7 \equiv 1\left(\mathrm{mod}\ 7\right)$$

$$2^7 \equiv 128 \equiv 2\left(\mathrm{mod}\ 7\right)$$

$$3^7 \equiv 2187 \equiv 3\left(\mathrm{mod}\ 7\right)$$

$$4^7 \equiv \left(-3\right)^7 \equiv -2187 \equiv -3 \equiv 4\left(\mathrm{mod}\ 7\right)$$

$$5^7 \equiv \left(-2\right)^7 \equiv -128 \equiv -2 \equiv 5\left(\mathrm{mod}\ 7\right)$$

$$6^7 \equiv \left(-1\right)^7 \equiv -1 \equiv 6\left(\mathrm{mod}\ 7\right)$$

Since for the complete residue system $\left\{0, 1, 2, 3, 4, 5, 6\right\}$ we have

$$x^7 \equiv x\left(\mathrm{mod}\ 7\right)$$

So $x^7 \equiv x\left(\mathrm{mod}\ 7\right)$.

■

(ii) We need to show $x^7 \equiv x\left(\mathrm{mod}\ 6\right)$.

Proof.

Similarly to part (i) we have for the complete residue system $\left\{0, 1, 2, 3, 4, 5\right\}$

$$0^7 \equiv 0\left(\mathrm{mod}\ 6\right)$$

$$1^7 \equiv 1\left(\mathrm{mod}\ 6\right)$$

$$2^7 \equiv 128 \equiv 2\left(\mathrm{mod}\ 6\right)$$

$$3^7 \equiv 2187 \equiv 3\left(\mathrm{mod}\ 6\right)$$

$$4^7 \equiv \left(-3\right)^7 \equiv -2187 \equiv 4\left(\mathrm{mod}\ 6\right)$$

$$5^7 \equiv \left(-1\right)^7 \equiv -1 \equiv 5\left(\mathrm{mod}\ 6\right)$$

Therefore $x^7 \equiv x\left(\mathrm{mod}\ 6\right)$.

■

(iii) We need to show $x^7 \equiv x\left(\text{mod } 42\right)$. *How?*

We use the results of part (i) and (ii).

Proof.

From parts (i) and (ii) we have

$$x^7 \equiv x\left(\text{mod } 7\right) \text{ and } x^7 \equiv x\left(\text{mod } 6\right)$$

Now using the result of question 24 part (c):

If $a \equiv b\left(\text{mod } n\right)$ and $a \equiv b\left(\text{mod } m\right)$ then $a \equiv b\left(\text{mod } m \times n\right)$ provided $\gcd\left(m,\ \ n\right) = 1$.

Checking that $\gcd\left(7,\ \ 6\right) = 1$ and so applying this to $x^7 \equiv x\left(\text{mod } 7\right)$ and $x^7 \equiv x\left(\text{mod } 6\right)$ gives

$$x^7 \equiv x\left(\text{mod } 6 \times 7\right) \equiv x\left(\text{mod } 42\right)$$

This completes our proof.

■

29. We are required to prove $2^{2n+1} \equiv 9n^2 - 3n + 2 \ \left(\text{mod } 54\right)$ by using induction.

Proof.

Check the base case $n = 1$:

$$2^{(2\times 1)+1} \equiv 8\left(\text{mod } 54\right)$$
$$9\left(1\right)^2 - \left(3 \times 1\right) + 2 \equiv 8\left(\text{mod } 54\right)$$

Therefore, the result is true for $n = 1$.

Assume the result holds for $n = k$:

$$2^{2k+1} \equiv 9k^2 - 3k + 2 \ \left(\text{mod } 54\right) \qquad (\dagger)$$

We need to prove the result for $n = k + 1$:

$$2^{2(k+1)+1} \equiv 9\left(k+1\right)^2 - 3\left(k+1\right) + 2 \ \left(\text{mod } 54\right) \qquad (*)$$

How do we prove this?

Expanding the right-hand side of (*) gives

$$\begin{aligned}9\left(k+1\right)^2-3\left(k+1\right)+2 &\equiv 9k^2+18k+9-3k-3+2\\ &\equiv 9k^2+15k+8\\ &\equiv 4\underbrace{\left(9k^2-3k+2\right)}_{=2^{2k+1}\ \text{by}\ (\dagger)}-27k^2+27k\\ &\equiv 4\left(2^{2k+1}\right)-27k^2+27k\\ &\equiv 4\left(2^{2k+1}\right)-27k\left(k-1\right)\pmod{54}\end{aligned}$$

Note that

$$k\left(k-1\right)=2m \qquad \left[\text{Because } k\left(k-1\right) \text{ is even}\right]$$

Substituting this $k\left(k-1\right)=2m$ into the above calculation gives

$$\begin{aligned}9\left(k+1\right)^2-3\left(k+1\right)+2 &\equiv 4\left(2^{2k+1}\right)-27k\left(k-1\right)\\ &\equiv 4\left(2^{2k+1}\right)-27\left(2m\right)\\ &\equiv 4\left(2^{2k+1}\right)-54m\\ &\equiv 4\left(2^{2k+1}\right)\pmod{54}\end{aligned}$$

Using the rules of indices on the final line gives

$$4\left(2^{2k+1}\right)\equiv 2^2\left(2^{2k+1}\right)\equiv 2^{2k+2+1}\equiv 2^{2\left(k+1\right)+1}\pmod{54}$$

We have proven the result for $n=k+1$:

$$9\left(k+1\right)^2-3\left(k+1\right)+2\equiv 2^{2\left(k+1\right)+1}\pmod{54}$$

By mathematical induction we conclude that $2^{2n+1}\equiv 9n^2-3n+2\pmod{54}$.

30. We need to find the last two digits of 9^{9^9}. This means we need to work with modulo 100. Evaluating the first few powers of 9:

$9^2\equiv 81\pmod{100}$, $9^3\equiv 729\equiv 29\pmod{100}$, $\cdots$, $9^{10}\equiv 3\,486\,784\,401\equiv 1\pmod{100}$

We want to use the last result

$$9^{10}\equiv 1\pmod{100} \qquad (*)$$

because 1 to any index gives 1. This makes our arithmetic a lot easier.

We want to write the highlight index in $9^{\boxed{9^9}}$ in multiples of 10 plus remainder.

$$9^9=387\,420\,489=\left(38\,742\,048\times 10\right)+9\,.$$

Writing 9^{9^9} by using this result we have

$$\begin{aligned}
9^{9^9} &\equiv 9^{387420489} \\
&\equiv 9^{\left(38742048\times 10\right)+9} \\
&\equiv \left(9^{10}\right)^{38742048}\times 9^9 \\
&\equiv \underbrace{\left(1\right)^{38742048}}_{\text{By (*)}}\times 9^9 \equiv 9^9 \equiv \underbrace{387\ 420\ 489}_{\text{From above calculation}} \equiv 89 \pmod{100}
\end{aligned}$$

Hence the last two digits of 9^{9^9} is 89.

31. To show that if $a \equiv b \pmod{n}$ then $P(a) \equiv P(b) \pmod{n}$ we use the following propositions:

> Proposition (3.6). If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then
> (i) $a + c \equiv b + d \pmod{n}$ (ii) $ac \equiv bd \pmod{n}$

> Proposition (3.8).
> If $a \equiv b \pmod{n}$ then $a^k \equiv b^k \pmod{n}$ where k is a natural number.

Proof.

Writing out $P(a)$ and $P(b)$ we have

$$\begin{aligned}
P(a) &= c_0 + c_1 a + c_2 a^2 + \cdots + c_{m-1} a^{m-1} + c_m a^m \\
P(b) &= c_0 + c_1 b + c_2 b^2 + \cdots + c_{m-1} b^{m-1} + c_m b^m
\end{aligned}$$

All the coefficients are congruent to each other

$$c_0 \equiv c_0 \pmod{n},\ c_1 \equiv c_1 \pmod{n},\ \cdots,\ c_m \equiv c_m \pmod{n}$$

We are given that $a \equiv b \pmod{n}$ so by the above Proposition (3.8) we have

$$a^2 \equiv b^2 \pmod{n},\ a^3 \equiv b^3 \pmod{n},\ \cdots,\ a^m \equiv b^m \pmod{n}$$

By Proposition (3.6) we have

$$c_0 + c_1 a + c_2 a^2 + \cdots + c_{m-1} a^{m-1} + c_m a^m \equiv c_0 + c_1 b + c_2 b^2 + \cdots + c_{m-1} b^{m-1} + c_m b^m \pmod{n}$$

Therefore $P(a) \equiv P(b) \pmod{n}$ which is our required result.

■

32. The given result is an easy test for divisibility by 11.

Proof.

Let the integer be $N = a_n a_{n-1} a_{n-2} \cdots a_2 a_1 a_0$ and T be given by:

$$T = a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^n a_n \qquad (*)$$

We can write N in expanded form as:

$$\begin{aligned} N &= a_n a_{n-1} a_{n-2} \cdots a_2 a_1 a_0 \\ &= \left(a_n \times 10^n\right) + \left(a_{n-1} \times 10^{n-1}\right) + \left(a_{n-2} \times 10^{n-2}\right) + \cdots + \left(a_2 \times 10^2\right) + \left(a_1 \times 10\right) + \left(a_0 \times 1\right) \end{aligned}$$

Since we are interested in divisibility by 11 so we use modulo 11. *What is 10 modulo 11 equal to?*

$$10 \equiv -1 \left(\text{mod } 11\right)$$

By applying Proposition (3.8) $a \equiv b \left(\text{mod } n\right)$ implies $a^k \equiv b^k \left(\text{mod } n\right)$ we have

$$10^k \equiv \left(-1\right)^k \left(\text{mod } 11\right)$$

Using these in the congruence below:

$$\begin{aligned} N &\equiv a_n a_{n-1} a_{n-2} \cdots a_2 a_1 a_0 \\ &\equiv \left(a_n \times 10^n\right) + \left(a_{n-1} \times 10^{n-1}\right) + \cdots + \left(a_2 \times 10^2\right) + \left(a_1 \times 10\right) + \left(a_0 \times 1\right) \ \left(\text{mod } 11\right) \\ &\equiv \left(a_n \times \left(-1\right)^n\right) + \left(a_{n-1} \times \left(-1\right)^{n-1}\right) + \cdots + \left(a_2 \times \left(-1\right)^2\right) + \left(a_1 \times \left(-1\right)\right) + \left(a_0 \times 1\right) \quad \left[\text{By above results}\right] \\ &\equiv \left(-1\right)^n a_n + \left(-1\right)^{n-1} a_{n-1} + \cdots + a_2 - a_1 + a_0 \\ &\equiv T \ \left(\text{mod } 11\right) \qquad \left[\text{By } \ (\dagger)\right] \end{aligned}$$

Both N and T are divisible by 11 or neither is.

■