Unit B

Suggested Answers and Guidelines

Suggested Answers and Guidelines for Unit B

Pre-lesson Worksheet 2

Ex1: Yes, Yes

Ex2: Yes, No

Ex3: No, Yes

Why does **Rule 1** work?

We can write $756 = 7 \times \underline{100} + 5 \times \underline{10} + 6$

Then,

$756 = 7 \times (\underline{99} + 1) + 5 \times (\underline{9} + 1) + 6$

$= 7 \times \underline{99} + \underline{7} + 5 \times \underline{9} + \underline{5} + 6$

$= 3 \times (\underline{7 \times 33 + 5 \times 3}) + 7 + 5 + 6$

So if $7 + 5 + 6$ is divisible by 3 , the whole expression will be divisible by 3 .

Rule 2 is similar to Rule 1

Rule 3 , observe that

$10 = 11 - 1$

$100 = 99 + 1 = 11\times9 +1$

$1000 = 1001 - 1 = 11\times91 - 1$

$10000 = 9999 + 1 = 11\times909 +1$

…

Rule for 4 : Only need to check the last two digits

e.g. $104928 = 1049\times 100 + 28 = 1049 \times 25 \times 4 + 28$. Therefore, we only need to check 28.

Unit B

Suggested Answers and Guidelines

Lesson Worksheet 2

Example: Consider the number 36

Prime Factorization : $36 = 2^2 \times 3^2$

$36 = 1 \times 36$, 2×18 , 3×12 , 4×9 , 6×6

Factors of 36 : 1 , 2 , 3 , 4 , 6 , 9 , 18 , 36 Number of Factors: 9

Following the example, fill in the table.

Number	Prime Factorization	Factors	No. of Factors
36	$36 = 2^2 \times 3^2$	1,2,3,4,6,9,18,36	9
56	$56 = 7^1 \times 2^3$	1,2,4,7,8,14,28,56	8
72	$72 = 2^3 \times 3^2$	1,2,3,4,6,8,9,12,18,24,36,72	12
510	$510 = 2 \times 3 \times 5 \times 17$	1,2,3,5,15,17,30,34,102,170,255,510	16
700	$700 = 2^2 \times 5^2 \times 7$	1,2,4,5,7,10,14,20,25,28,35,50, 70,100,140,175,350,700	18
3125	$3125 = 5^5$	1,5,25,125,625,3125	6

Question 1

Can you find out the relation between the Prime Factorization and the number of factors?

[Hint: Look at the Indices of the Prime Factorization.]

Number of Factors = Product of all (index + 1) in the prime factorization.

Question 2

Apply your conclusion in question 1 to find out the number of factors for the following numbers.

$250 = 2 \times 5^3$ → Number of factors = 8

$1156375 = 5^3 \times 11 \times 29^2$ → Number of factors = 24

$864 = 2^5 \times 3^3$ → Number of factors = 24

Question 3

Can you explain/prove your conclusion about the number of factors ?

Taking $72 = 2^3 \times 3^2$ as example,

We observe that each factor is formed by choosing (0/1/2/3) for the index on 2, and (0/1/2) for the index on 3

e.g. $9 = 3^2$, $12 = 2^2 \times 3$

Therefore, (0/1/2/3) → 4 choices, (0/1/2) → 3 choices . Number of Factors = $4 \times 3 = 12$

Unit B

Suggested Answers and Guidelines

Inquiry Activity 2 --- Fermat Little Theorem

Fermat's Little theorem is related to a pattern about remainder. In this worksheet, we are going to deduce the theorem.

Part I : Introducing a new symbol

If a and b have the same remainder when divided by a number k,

we write : ' $\boldsymbol{a \equiv b \ (mod\ k)}$ ' . We call it ' $\boldsymbol{a}$ **is congruent to** $\boldsymbol{b}$ ***modulo*** $\boldsymbol{k}$ '.

E.g. When 62 is divided by 7, the remainder is 6. When 27 is divided by 7, the remainder is also 6.

So, we write $62 \equiv 27 \ (mod\ 7)$

Practice: True or False

$43 \equiv 27 \ (mod\ 4)$	**True**	$74 \equiv 27 \ (mod\ 11)$	**False**
$66 \equiv 49 \ (mod\ 3)$	**False**	$63 \equiv 70 \ (mod\ 7)$	**True**

Practice: Fill in the blank with a suitable number

Fill in a number less than 7 on the line: $55 \equiv \mathbf{6} \ (mod\ 7)$

Fill in a number less than 10 on the line: $123 \equiv \mathbf{3} \ (mod\ 10)$

Fill in a number between 30 and 40 on the line: $65 \equiv \mathbf{33} \ (mod\ 8)$

Fill in a number between 30 and 40 on the line: $19 \equiv \mathbf{37} \ (mod\ 9)$

Part II : Basic Theorem

To look into the Fermat's Theorem, we will first look at some basic theorem about the remainder.

Theorem 1 If $a \equiv b \ (mod\ k)$ and $c \equiv d \ (mod\ k)$, then $ac \equiv bd \ (mod\ k)$

Examples: $17 \equiv 3 \ (mod\ 7)$ and $9 \equiv 2 \ (mod\ 7)$, therefore $17 \times 9 \equiv 3 \times 2 = 6 \ (mod\ 7)$

[Check: $17 \times 9 = 153$ | For $153 \div 7$, reminder = 6]

$23 \equiv 5 \ (mod\ 6)$ and $19 \equiv 1 \ (mod\ 6)$, therefore $23 \times 19 \equiv \mathbf{5} \times \mathbf{1} = \mathbf{5} \ (mod\ 6)$

[Check: $23 \times 19 = 437$ | For $437 \div 6$, reminder = **5**]

Since $11 \equiv 5 \ (mod\ 5)$, $19 \equiv \mathbf{1} \ (mod\ 6)$, $33 \equiv \mathbf{3} \ (mod\ 6)$,

therefore $11 \times 19 \times 33 \equiv$ $\underline{\mathbf{5 \times 1 \times 3 = 3}}$ $(mod\ 6)$

Proof of Theorem 1:

If $a \equiv b \ (mod\ k)$, we can write that $a - b = kM$, where M is an integer.

If $c \equiv d \ (mod\ k)$, we can write that $c - d = kN$, where N is an integer.

$ac - bd = ac - bc + bc - bd = c(a - b) + b(c - d) = ckM + bkN = k(cM + bN)$

The expression in the bracket $(cM + bN)$ is an integer, therefore $ac \equiv bd \ (mod\ k)$

Unit B

Suggested Answers and Guidlines

Theorem 2	Let h be a number coprime with k. (Coprime means that h and k have no common factor except 1) If $ha \equiv hb \pmod{k}$, then $a \equiv b \pmod{k}$.

Example: $44 \equiv 16 \pmod{7}$

44 and 16 has a common factor 4, which is coprime with 7.

When we divide 4 from both sides, the relation is still true.

$44 \equiv 16 \pmod{7}$ **divide 4 →** $11 \equiv 4 \pmod{7}$ is also true.

$65 \equiv 25 \pmod{8}$ **divide 5 →** $13 \equiv 5 \pmod{8}$ is also true.

$82 \equiv 10 \pmod{8}$ **divide 2 →** $41 \equiv 5 \pmod{8}$ which is a False relation.

Why can't we divide 2 from both sides here? **2 and 8 have a common factor 2 .**

Proof of Theorem 2:

Let h be a number coprime with k. (Coprime means that h and k have no common factor except 1)

If $ha \equiv hb \pmod{k}$, then $ha - hb = kM$, where M is an integer.

$\to h(a - b) = kM$, this implies h is a factor of kM

Since h and k have no common factor except 1, h is a factor of M.

Therefore, $a - b = k(M/h)$, where M/h is an integer.

$\therefore a \equiv b \pmod{k}$.

Question : Is the following true? Explain your answer.

If $a \equiv b \pmod{k}$ and $c \equiv d \pmod{k}$, then $a + c \equiv b + d \pmod{k}$

If $a \equiv b \pmod{k}$ and $c \equiv d \pmod{k}$, then $a - b = kM$ and $c - d = kN$.

$(a + c) - (b + d) = a - b + c - d = kM + kN = k(M + N)$

$M + N$ is an integer, $a + c \equiv b + d \pmod{k}$

Part III : Observation

Fermat's Little Theorem is about a prime number p and another number a such that a and p are coprime.

E.g.1 Let $p = 5$ and $a = 7$	
Multiple of a	Remainder when divided by p (Write a number less than 5)
$1a = 7$	$7 \equiv \boldsymbol{2} \pmod{5}$
$2a = 14$	$14 \equiv \boldsymbol{4} \pmod{5}$
$3a = 21$	$21 \equiv \boldsymbol{1} \pmod{5}$
$4a = 28$	$28 \equiv \boldsymbol{3} \pmod{5}$

E.g.2 Let $p = 5$ and $a = 13$	
Multiple of a	Remainder when divided by p (Write a number less than 5)
$1a = 13$	$13 \equiv \mathbf{3} \pmod{5}$
$2a = 26$	$26 \equiv \mathbf{1} \pmod{5}$
$3a = 39$	$39 \equiv \mathbf{4} \pmod{5}$
$4a = 52$	$52 \equiv \boldsymbol{2} \pmod{5}$

Observation:

When $p = 5$, the first 4 multiple of a gives the reminders: 1, 2 ,3 ,4 when divided by p.

Unit B

Suggested Answers and Guidlines

E.g.3 Let $p = 7$ and $a = 3$	
Multiple of a	Remainder when divided by p (Write a number less than 7)
$1a = 3$	$3 \equiv \boldsymbol{3}$ (mod 7)
$2a = 6$	$6 \equiv \boldsymbol{6}$ (mod 7)
$3a = 9$	$9 \equiv \boldsymbol{2}$ (mod 7)
$4a = 12$	$12 \equiv \boldsymbol{5}$ (mod 7)
$5a = 15$	$15 \equiv \boldsymbol{1}$ (mod 7)
$6a = 18$	$18 \equiv \boldsymbol{4}$ (mod 7)

E.g.4 Let $p = 7$ and $a = 11$	
Multiple of a	Remainder when divided by p (Write a number less than 7)
$1a = 11$	$11 \equiv \boldsymbol{4}$ (mod 7)
$2a = 22$	$22 \equiv \boldsymbol{1}$ (mod 7)
$3a = 33$	$33 \equiv \boldsymbol{5}$ (mod 7)
$4a = 44$	$44 \equiv \boldsymbol{2}$ (mod 7)
$5a = 55$	$55 \equiv \boldsymbol{6}$ (mod 7)
$6a = 66$	$66 \equiv \boldsymbol{3}$ (mod 7)

Observation:

When $p = 7$, the first 6 multiple of a gives the reminders: 1 ,2 ,3 ,4 ,5 ,6 when divided by p.

Part IV : Apply the theorem

The first $(p - 1)$ multiples of a : $\underline{a}$, $\underline{2a}$, $\underline{3a}$,... , $\underline{(p-1)\,a}$ gives the reminders 1 , 2 , 3 … , $p-1$

when they are divided by p.

By Theorem 1, we can multiply them together and give the relation:

$$(a)(2a)(3a)\ldots[(p-1)\,a] \equiv 1 \times 2 \times 3 \times \ldots \times (p-1) \quad (mod\ p)$$

$$1 \times 2 \times 3 \ldots \times (p-1) \times a^{p-1} \equiv 1 \times 2 \times 3 \times \ldots \times (p-1) \quad (mod\ p)$$

Since $1 \times 2 \times 3 \ldots \times (p-1)$ and p has no common factor .

By Theorem 2, $a^{p-1} \equiv 1 \ (mod\ p)$

Conclusion: Fermat's Little Theorem

If p is a prime number and a is coprime with p, then $a^{p-1} \equiv 1 \quad (mod\ p)$