DMS (13/04/22)

Sequence: 1 2 4 8 16 32 ----

Index	1	2	3	4	5
value	2	4	8	16	32
	2^1	2^2	2^3	2^4	2^5

Explicit Formula:

$$a_k = 2^k$$

$a_m, a_{m+1}, a_{m+2}, \ldots a_n$

Terms. Index/Subscript Final Term.

Finite Sequence: Final Term involved.

Infinite Sequence: Final Term is missing.

Finding terms from explicit formula:

- $a_k = \frac{k}{k+1}$ 1st 6 terms.

Sol: $\frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{5}{6}, \frac{6}{7}$

- $a_i = \frac{i-1}{i}$ for $i \geq 2$

Sol: $\frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{5}{6}, \frac{6}{7}$

Write explicit formula when initial terms are given:

- $1, \frac{-1}{4}, \frac{1}{9}, \frac{-1}{16}, \frac{1}{25}, \frac{-1}{36}, \ldots$

Index	1	2	3	4	5	6
Value	1	$-1/4$	$1/9$	$-1/16$	$1/25$	$-1/36$

$$a_k = \frac{(-1)^{k+1}}{k^2}$$

- $2, 6, 12, 20, 30, 42, 56.$

Index	1	2	3	4	5	6	7
Value	2	6	12	20	30	42	56
	1×2	2×3	3×4	4×5	$\cdots$		

$$a_k = k(k+1) \quad \text{for } k \geq 1.$$

- $\frac{1}{2}, \frac{2}{9}, \frac{3}{16}, \frac{4}{25}, \frac{5}{36}, \ldots$

$$a_k = \frac{k}{(k+1)^2} \quad \text{for } k \geq 1.$$

Special Type Sequences.

- **Arithmetic Sequence / Progression:**

A sequence in which each term is achieved by adding a constant term in previous one.

e.g: 1, 2, 3, 4, 5, 6, ---- (constant = 1)

e.g: 5, 9, 13, 17, 21, 25 → $a_n = 25$

$a = 5$ $\quad d = 9 - 5 = 4$

General Term:

$$a_n = a + (n-1)d.$$

- Find 20th Term of sequence:

$S = 3, 9, 15, 21, \ldots$

$a = 3, \quad d = 9 - 3 = 6$

$a_{20} = a + 19(d) = 3 + 19(6)$

$\boxed{a_{20} = 117}$

- Find term of S which is -77.

$4, 1, -2, \ldots$

$a = 4, \quad d = 1 - 4 = -3$

$a_n = a + (n-1)d.$

$-77 = 4 + (n-1)(-3)$

$-81 = (n-1)(-3)$

$27 = n - 1$

$\Rightarrow \boxed{n = 28}$

- Find the 36th term of AP whose 3rd term is 7 and 8th term is 17.

$a_3 = a + 2d = 7$

$a_8 = a + 7d = 17$

$-5d = -10 \Rightarrow \boxed{d = 2}$

$a + 2(2) = 7$

$\boxed{a = 3}$

$a_{36} = 3 + 35(2)$

$\boxed{a_{36} = 73}$

Geometric Sequence:

A sequence in which each term except 1st term is achieved by multiplying preceding term with a constant.

S: 1, 2, 4, 8, ------, 16.

0.1, 0.01, 0.001, ------

General Term Formula:

$a_n = ar^{n-1}$ for all index $n \geq 2$

① Find the 8th term of the sequence

4, 12, 36, 108, ----

$a = 4$, $r = \frac{12}{4}$, $\frac{a_n}{a_{n-1}} = 3$

$a_8 = ar^{8-1} = ar^{7-1} = (4)(3)^6 = 4(2187)$

$= 8748.$

② Which term of G.P is 1/8, if 1st term is 4 and $r = 1/2$

$a_n = ar^{n-1}$

$a_n = \frac{1}{8} = 4\left(\frac{1}{2}\right)^{n-1}$

$$\frac{1}{32} = \left(\frac{1}{2}\right)^{n-1}$$

$$\left(\frac{1}{2}\right)^5 = \left(\frac{1}{2}\right)^{n-1}$$

$$5 = n-1$$

$$\Rightarrow \boxed{n = 6}$$

① Write G.P with +ve terms when 2nd term is 9 and 4th term is 1.

$$a_4 = 1 \quad , a_2 = 9$$

$$1 = ar^{4-1} \Rightarrow 1 = ar^3$$

$$9 = ar^{2-1} \Rightarrow 9 = ar$$

$$\frac{ar^3}{ar} = \frac{1}{9} \Rightarrow r^2 = \frac{1}{9}$$

$$\boxed{r = \frac{1}{3}}$$

$$9 = ar \Rightarrow a = 9/r = 9 \times 3$$

$$\boxed{a = 27}$$

Series

↳ Sum of any sequence.

$$2+4+8+16+32$$

$$\boxed{\sum_{i=1}^{5} = 2^i} = 2^1 + 2^2 + 2^3 + 2^4 + 2^5$$

↓

Summation Notation / Sigma:

$$\sum_{i=1}^{4} (2i-1) = [2(1)-1] + [2(2)-1] + [2(3)-1] + [2(4)-1]$$

$$= 1 + 3 + 5 + 7.$$

- $$\sum_{i=0}^{5} \frac{(-1)^i}{i+1}$$

$$= \frac{(-1)^0}{0+1} = \frac{1}{1}$$

$$= 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \frac{1}{5} - \frac{1}{6}$$

Properties of Summation:

(1) $$\sum_{k=m}^{n} c \cdot a_k = c \sum_{k=m}^{n} a_k$$

(2) $$\sum_{i=1}^{n} c = n \cdot c$$

(3) $$\sum_{k=m}^{n} (a_k + b_k) = \sum_{k=m}^{n} a_k + \sum_{k=m}^{n} b_k.$$

Arithmetic Series:

The sum of terms of AP is Arithmetic series.

$$S_n = \frac{n}{2} [2a + (n-1)d].$$

$$S_n = a + (a+d) + (a+2d) + \cdots + [a+(n-1)d] \quad a_n$$

$$S_n = a + (a+d) + (a+2d) + \cdots + a$$

$$a + a_n \qquad a + a_n \qquad a + a_n \qquad a + a_n$$

$$2S_n = n(a + a_n)$$

$$S_n = \frac{n}{2}[a + a_n]$$

$$= \frac{n}{2}[a + a + (n-1)d]$$

$$S_n = \frac{n}{2}[2a + (n-1)d]$$

Series of Natural Numbers:

$S: 1 + 2 + 3 + 4 + \cdots$

- Find sum of 50 terms.

$a = 1, \quad d = 1, \quad n = 50.$

$$S_n = \frac{50}{2}[2(1) + (49)(1)]$$

$$= 25(51) = 1275.$$

- Find S_{10}.

3, 9, 15, 21

$a = 3, \quad d = 6, \quad n = 10$

$$S_{10} = 5[2(3) + (9)(6)] = 5[6 + 54]$$

$$= 300.$$

- $S_n = ?$

$1 + 4 + 7 + 10 + 13$

$a = 1 \quad , d = 3 \quad , n = 8$

$S_n = 4[2(1) + 7(3)] = 4[2 + 21]$

$= 4 \times 23 = 92.$

- **Geometric Series:**

$$a + ar + ar^2 + ar^3 + \cdots + ar^{n-1}$$

Sigma Notation:

$$\sum_{i=1}^{n} = ar^{i-1}$$

$$S_n = \frac{a(r^n - 1)}{r - 1}$$

$$S_n = \frac{a(1 - r^n)}{1 - r} \quad \text{when } r < 1$$

- $2 + 2^2 + 2^3 + \cdots$

$a = 2 \quad , r = 2 \quad , n = 10.$

$$S_{10} = \frac{2(2^{10} - 1)}{2 - 1} = \frac{2(1023)}{1}$$

$$S_{10} = 2046$$

- Find S_6

$$\frac{9}{4} + \frac{3}{2} + 1 + \frac{2}{3} + \cdots$$

$a = \frac{9}{4}$, $r = \frac{2}{3}$

$S_6 =$

Principle of Mathematical Induction:

$$1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2} \quad \text{for } n \geq 1.$$

1- Basis Step:

Prove for $n = 1$.

$$L.H.S = 1 = \frac{n(n+1)}{2} = \frac{1(1+1)}{2} = \frac{2}{2} = 1 = R.H.S$$

2- Inductive Step:

Let it be true for $n = k$ $\{k \geq 1.$

$$1 + 2 + 3 + \dots + k = \frac{k(k+1)}{2}.$$

Now we have to show it is true for $n = k+1$

$$1 + 2 + 3 + \dots + k + (k+1) = \frac{k(k+1)}{2} + k + 1$$

$$= \frac{k(k+1) + 2(k+1)}{2}$$

$$= \frac{(k+1)(k+2)}{2}$$

$$= \frac{(k+1)(k+1+1)}{2}$$

Hence, it is proved

L.H.S = R.H.S

So the statement is true.

DMS 20/4/22

Prove that $\sum_{i=0}^{n} r^i = \frac{r^{n+1}-1}{r-1}$

(I) Let P(n) be the property

Basis Step:

Let it be true for $n=0$.

$$r^0 = \frac{r^{0+1}-1}{r-1}$$

$$1 = 1$$

L.H.S = R.H.S

Inductive Step: let P(k) be true for some $n = k > 0$

$$\sum_{i=0}^{k} r^i = \frac{r^{k+1}-1}{r-1}$$

We have to prove that P(k+1) is true.

$$\sum_{i=0}^{k} r^i + r^{k+1} = \frac{r^{k+1}-1}{r-1} + r^{k+1}$$

$$\sum_{i=0}^{k+1} r^i = \frac{r^{k+1}-1+(r-1)(r^{k+1})}{r-1}$$

$$= \frac{r^{k+1}-1+r^{k+1}-r^{k+1}}{r-1}$$

$$\sum_{i=0}^{k+1} r^i = \frac{r^{k+1+1}-1}{r-1}$$

So, it is proved that P(k+1) is also true, which completes the proof.

- Prove that: (using Mathematical Induction)

$1+3+5+\cdots+(2n-1)=n^2$ for $n \geq 1$

Basis Step:

Let it be true for $n=1$

$1 = (1)^2 = 1$

L.H.S = R.H.S

Induction Step:

Let P(k) is true for $k \geq 1$.

$1+3+5+\cdots+(2k-1)=(k)^2$.

We have to Prove that P(k+1) is true.

$1+3+5+\cdots+(2k-1)+[2(k+1)-1]=k^2+[2(k+1)-1]$

$= k^2+2k+2-1$

$$1+3+5+\cdots+[2(k+1)-1] = k+2k+1$$
$$= (k+1)^2$$

- Prove that:

$$1+6+11+\cdots+5n-4 = \frac{n(5n-3)}{2} \quad \text{for } n \geq 1$$

1- Basis Step:

[for $n=1$] $\quad 1 = \frac{1[5(1)-3]}{2} = \frac{5-3}{2} = 1$

L.H.S = R.H.S

2- Inductive Step:

Let $P(k)$ is true for $k>1$.

$$1+6+11+\cdots+5k-4 = \frac{k(5k-3)}{2}$$

Now, Prove for $n=k+1$

$$1+6+11+\cdots+5k-4+5(k+1)-4 = \frac{k(5k-3)+5(k+1)-4}{2}$$

$$1+6+11+\cdots+5(k+1)-4 = \frac{k(5k-3)}{2}+5k+1$$

$$= \frac{5k^2-3k+10k+2}{2}$$

$$= \frac{5k^2+7k+2}{2}$$

$$= \frac{5k^2+5k+2k+2}{2}$$

$$= \frac{5k(k+1) + 2(k+1)}{2}$$

$$= \frac{(k+1)(5k+2)}{2}$$

$$1+6+11+\ldots\ldots+5(k+1)-4 = \frac{(k+1)[5(k+1)-3]}{2}.$$

2nd Method:

$$L.H.S = \frac{k(5k-3)}{2} + 5(k+1) - 4$$

$$R.H.S = \frac{(k+1)[5(k+1)-3]}{2}$$

Simplify & prove Both are equal.

Proving Properties using Mathematical Induction:

(1) For all integers $n \geq 0$ prove that $2^{2n}-1$ is divisible by 3.

Let $P(n)$ $2^{2n}-1$ is divisible by 3.

Basis Step:

$$0 = 2^{2(0)} - 1 = 2^0 - 1 = 1-1.$$

$$= 0$$

$$\Rightarrow \quad 3 \times 0 = 0$$

Agar 3 ko kisi value se multiply kro or ye ajae tou means, it is divisible by 3

Inductive Step:

Let $P(k) = 2^{2k} - 1$ is divisible by 3.

$\Rightarrow$ Let $\boxed{2^{2k} - 1 = 3r}$

{ Means 3 ko kisi r integer se multiply kro to $2^{2k} - 1$ (value) aja gi }

Now prove it for $n = k+1$

$\Rightarrow 2^{2(k+1)} - 1 = 2^{2k+2} - 1$.

$= 2^{2k} \cdot 4 - 1 \cdot = 2^{2k}(3+1) - 1$.

$= 3 \cdot 2^{2k} + 2^{2k} - 1$

$= 3 \cdot 2^{2k} + 3r$

$= 3(2^{2k} + r)$

Hence $P(k+1)$ is divisible by 3.

Recursive Sequences:

1- Well Ordering Principle:

~~Set with all non-negative integers, there will be smallest element.~~

Every non-empty set S of non-negative integers contains a least element.

$S = \{2, 4, 6, 8\}$

- **Fibonacci Series:** A series whose every element after first two elements is obtained by adding previous two elements.

0 1 1 2 3 5 8 13 ---

$F_n = F_{n-1} + F_{n-2}$

Recursive Sequences: (Recursion)

Term is expressed in terms of previous terms.

↳ 2 Things

1- Initial Condition 2-Recursive Relationship.

$F_0 = 0$, $F_1 = 1$.

↳ If any sequence is represented by explicit formula, it can also be represented by recursive formula.

- $C_k = C_{k-1} + k C_{k-2} + 1$ for $k \geq 2$

and $C_1 = 1$, $C_2 = 2$

- C_3 , C_4 , C_5 = ?

$C_3 = C_{3-1} + 3C_{3-2} + 1$

$= C_2 + 3C_1 + 1$

$= 2 + 3.1 + 1$

$\boxed{C_3 = 6}$

$C_4 = C_{4-1} + 4C_{4-2} + 1$

$= C_3 + C_2 + 1$

$= 6 + 4(2) + 1 = 6 + 8 + 1$

$\boxed{C_4 = 15}$

$$C_5 = C_{5-1} + 5C_{5-2} + 1$$
$$= C_4 + 5C_3 + 1$$
$$= 15 + 5(6) + 1$$
$$\boxed{C_5 = 46}$$

- $F_n = F_{n-1} + F_{n-2}$

  $F_0 = 1 \quad , F_1 = 1$

$F_3 = ?$

$$F_3 = F_{3-1} + F_{3-2}$$
$$= F_2 + F_1$$
$$= F_{2-1} + F_{2-2} + F_1$$
$$= F_1 + F_0 + F_1 = 1+1+1$$
$$\boxed{F_3 = 3}$$

(21/04/22)

- Find 1st four terms of following Recurrence Relation (RR)

- $a_k = 2a_{k-1} + k$ for all $k \geq 1$

  $a_1 = 1.$

  $a_2 = 2a_1 + 2 = 2(1) + 2 = 4$

  $a_3 = 2a_2 + 3 = 2(4) + 3 = 11$

  $a_4 = 2a_3 + 4 = 2(11) + 4 = 26.$

- $S_k = S_{k-1} + 2S_{k-2}$ for $k \geq 2$

  $S_0 = 1 \quad , S_1 = 1$

  $S_2 = S_1 + 2S_0 = 1 + 2 = 3.$

  $S_3 = S_2 + 2S_1 = 3 + 2 = 5.$

$$S_4 = S_3 + 2S_2 = 5 + 2(3) = 11.$$

- **Does an explicit formula satisfies RR.**

Let $a_n = 3n+1$ for $n \geq 0$ (RR)

Show that is satisfies RR.

$$a_k = a_{k-1} + 3 \quad \text{for } k \geq 1.$$

$$a_k = 3k+1 \qquad \left| \begin{array}{l} a_{k-1} = 3(k-1)+1 \\ a_{k-1} = 3k-2. \end{array} \right.$$

$$a_k = 3k-2+3.$$

$$= 3k+1. \quad = L.H.S.$$

Hence proved.

- **Let $b_n = 4^n$ for $n \geq 0$, show that it satisfies RR**

$$b_k = 4b_{k-1} \quad \text{for } k \geq 1.$$

$$b_k = 4^k, \quad b_{k-1} = 4^{k-1}$$

$$b_k = 4b_{k-1} = 4 \cdot 4^{k-1}$$

$$= 4^{k-1+1}$$

$$\boxed{b_k = 4^k}$$

Hence proved.

- Let $t_n = 2+n$

RR $\Rightarrow$ $t_k = 2t_{k-1} - t_{k-2}$ for $k \geq 1$

$t_k = 2+k$ | $t_{k-1} = 2+k-1 = k+1$ | $t_{k-2} = 2+k-2 = k$

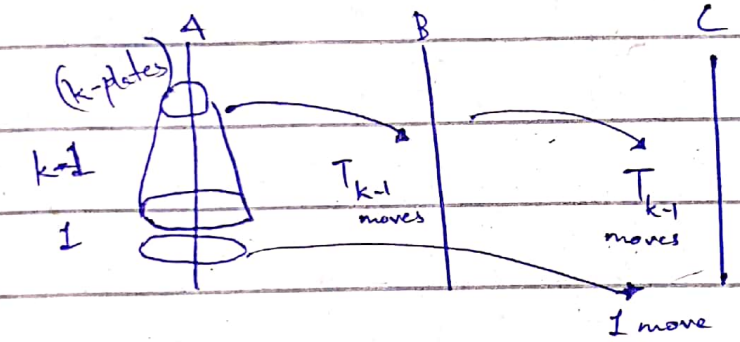
$t_k = 2k_{-1} - t_{k-2}$

$= 2(k+1) - k$.

$= 2k + 2 - k$

$t_k = k+2 = 2+k$

Hence proved.



Plates should be moved to C, given condition.

$T_k = T_{k-1} + 1 + T_{k-1}$

$= 2T_{k-1} + 1$.

$T_1 = 1, \quad T_2 = 3$ { These values were tested

$T_3 = 7$

Verify: $T_3 = 2T_{3-1} + 1$

$= 2T_2 + 1$.

$T_3 = 2(3) + 1 = 7$.

$T_6 = ?$

$T_4 = 2T_3 + 1 = 2(7) + 1 = 15$

$T_5 = 2(15) + 1 = 31$

$T_6 = 2(31) + 1 = 63$

DMS (27/04/22)

③ Solve Recurrance Eq find closed form/ explicit formula.

1- Iterative Method (Guess)

$a_0, a_1, a_2, \ldots\ldots$

$a_k = a_{k-1} + 2$

$a_0 = 1$

It is RR, Guess explicit formula:

$a_0 = 1$	$a_0 = 1 + 2 \times 0$
$a_1 = 1 + 2$	$a_1 = 1 + 2 \times 1$
$a_2 = (1+2) + 2$	$a_2 = 1 + 2 \times 2$
$a_3 = (1+2+2) + 2$	$a_3 = 1 + 2 \times 3$

Explicit Formula: $a_n = 1 + 2n$

- Let $a_k = r a_{k-1}$ for $k \geq 1$

$a_0 = a$

$a_1 = ra$

$a_2 = r^2 a$

$\boxed{a_n = r^n a}$

- $c_k = 3c_{k-1} + 1$ for $k \geq 2$

$c_1 = 1$

$c_2 = 3(1) + 1 = 4$

$c_3 = 3(4) + 1 = 13$

$c_4 = 3(13) + 1 = 40$

$c_5 = 3(40) + 1 = 121$.

OR (2nd Method)

$c_1 = 1$ (By RR)

$c_2 = 3(1) + 1$

$c_3 = 3(3+1) + 1 = 3^2 + 3 + 1$

$c_4 = 3(3^2 + 3 + 1) + 1 = 3^3 + 3^2 + 3 + 1$.

Explicit formula: $c_n = 3^{n-1} + 3^{n-2} + \cdots + 3 + 1$.

or $c_n = \sum_{n=0}^{n-1} 3^i$

Sum: $S_n = \frac{a(r^n - 1)}{r - 1}$

$S_n = \frac{1(3^n - 1)}{3 - 1} = \frac{3^n - 1}{2}$

- Statement: A worker is promised bonus if he can increase productivity by 2 units a day everyday for 30 days. If his productivity is 170 on day 0, what will be the productivity on day 30?

Recursive formula:

$$d_k = d_{k-1} + 2 \quad , d_0 = 170$$

$d_{30} = ?$

$d_1 = 172$

$d_2 = 174$

$d_3 = 176$ ..... (Time taking).

$$\boxed{d_k = 170 + 2k}$$

$d_{30} = 170 + 2(30)$

$= 230$

- **Statement:** A runner targets himself to improve on a track, 3 seconds a day. On day zero, he runs track in 3 mins, How fast will he run on day 14.

$d_k = d_{k-1} - 3$

$d_0 = 3$ min $= 180$ sec

$d_1 = 180 - 3 \quad = 177$

$d_2 = 180 - 3 - 3 \quad = 174$

or $180 - 2(3) \quad = 174$

$d_n = 180 - 3n$

$d_{14} = 180 - 3(14)$

$$\boxed{d_{14} = 138}$$

#Purani Kahani

@ Tower of hanoi

$T_1 = 1$

$T_2 = 3$

$T_3 = 7$

$T_k = 2T_{k-1} + 1$

$T_1 = 2(1) + 1$

$T_2 = 2(2+1) + 1 = 2^2 + 2 + 1$

$T_3 = 2(2^2 + 2 + 1) + 1 = 2^3 + 2^2 + 2 + 1$

Explicit formula: $T_n = 2^{n-1} + 2^{n-2} + \cdots + \frac{1}{2^0}$

Closed form or $T_n = \sum_{i=0}^{n-1} 2^i$

Sum: $S_n = \frac{a(r^n - 1)}{r - 1} = \frac{1(2^n - 1)}{1}$

$$\boxed{S_n = 2^n - 1}$$

$T_{64} = 2^{64} - 1$

$= 1.844 \times 10^{19}$ sec

$= 5.84 \times 10^{11}$ years.

$= 584$ billion years.

Modular Arithmetic (In terms of Remainder).

$19 \equiv 1 \text{ Mod } 2$

Congruent — Congruence — Modulus of Congruence.

$$\begin{array}{r|l} & 9 \\ 2 & 19 \\ & 18 \\ \hline & 1 \end{array}$$

// It means 2 divides 19 - 1.

$25 \equiv 4 \text{ Mod } 7$

$7 \mid 25 - 4 \Rightarrow 7 \mid 21$.

⇒ Applicable for all integers $\mathbb{Z}$, $-\infty$ to $+\infty$, no fraction.

$-5 \mid 2 \text{ Mod } 7$

7 divide $-5 - 2$ $\qquad$ $7 \overline{)-5}$

$7 \mid -7$ $\qquad$ $\frac{7}{2}$

- $5 \mid 33 - 3$

$33 \equiv 3 \text{ Mod } 5$.

↳ Two integers with same remainder are congruent to each other

⇒ Two integers 'a' & 'b' Mod 'n' are congruent to each other Mod 'n', if their remainder mod 'n' is same.

$18 \equiv 0 \text{ Mod } 2$.

$16 \equiv 0 \text{ Mod } 2$

$22 \equiv 0 \text{ Mod } 2$

$\Rightarrow \quad 18 \equiv 16 \text{ Mod } 2$

$z \quad \text{Mod } 2$

(even) 0 ↙ ↘ 1 (odd)

DMS (28/04/22)

1- Modulus Arithmetic

1- Congruences:

$-8 \equiv 2 \text{ Mod } 5$ $\quad 5 \mid -8-2$

$5 \mid -10.$

Modular Arithmetic is operated on $\mathbb{Z}$

→ set of integers

$\mathbb{Z}$ Mod 2 ⟹ Either 0 or 1.

e.g $29 \equiv 1 \text{ Mod } 2.$

$30 \equiv 0 \text{ Mod } 2.$

$31 \equiv 1 \text{ Mod } 2.$

$32 \equiv 0 \text{ Mod } 2.$

$\mathbb{Z}_2 = \{0, 1\}$

⇒ 0 Represents all 0 Mod 2. (Even Integers)

1 Represents all 1 Mod 2. (Odd Integers)

- $Z_3 = ?$

$30 \equiv 0 \text{ Mod } 3$

$31 \equiv 1 \text{ Mod } 3$

$32 \equiv 2 \text{ Mod } 3$

$33 \equiv 0 \text{ Mod } 3$

$34 \equiv 1 \text{ Mod } 3$

$\Rightarrow Z_3 = \{0, 1, 2\}$

$Z_4 = \{0, 1, 2, 3\}$

$Z_n = \{0, 1, 2, \ldots, n-1\}$ ← Group

- $4 \overline{)-13}$

16

3

- $-41 \text{ Mod } 4 = ?$

$4 \overline{)-41}$

44

3

- **Modular Addition:**

$3 \text{Mod } 5 + 4 \text{Mod } 5 \equiv 7 \text{Mod } 5 \equiv 2 \text{Mod } 5$

$3 \text{Mod } 5 + 2 \text{Mod } 5 + 5 \text{Mod } 5 \equiv 10 \text{ Mod } 5$

$\equiv 0 \text{ Mod } 5$

↳ Set Z_5 is closed under Addition (Closure Property).

⇒ Every set Z_n is closed under addition.

Modular Subtraction:

$3 \text{Mod} 5 - 4 \text{Mod} 5 \equiv -1 \text{Mod} 5 \equiv 4 \text{Mod} 5$

$2 \text{Mod} 5 - 4 \text{Mod} 5 \equiv -2 \text{Mod} 5 \equiv 3 \text{Mod} 5$

∴ Set Z_5 is closed under subtraction.

⇒ Every set Z_n is closed under subtraction.

Encryption:

$Z_{26} = \{0, 1, 2, \ldots, 25\}$

key = k = 17

(select any key for encryption).

formula ⇒ $y = x + k \text{Mod} 26$

1- Lets encrypt FAN

F	A	N
↓	↓	↓
5	0	13
x_1	x_2	x_3

$y_1 = x_1 + k \text{Mod} 26$

$= 5 + 17 \text{Mod} 26 \equiv 22 \text{Mod} 26$

$\equiv W$

$y_2 = x_2 + k \text{Mod} 26.$

$= 0 + 17 \text{Mod} 26 \equiv 17 \text{Mod} 26$

$\equiv R$

$y_3 = x_3 + k \text{ Mod } 26$

$= 13 + 17 \text{ Mod } 26 \equiv 30 \text{ Mod } 26$.

$\equiv 4 \text{ Mod } 26 = F$

FAN ⟶ WRE

Decryption:

WRE. $(k = 17)$.

$x = y - k \text{ Mod } 26$.

$W = 22$, $R = 17$, $E = 4$

$x_1 = 22 - 17 \text{ Mod } 26$

$\equiv 5 \text{ Mod } 26 \equiv F$

$x_2 = 17 - 17 \text{ Mod } 26$

$\equiv 0 \text{ Mod } 26 \equiv A$

$x_3 = 4 - 17 \text{ Mod } 26$

$\equiv -13 \text{ Mod } 26 \equiv 13 \text{ Mod } 26 \equiv N$

WRE ⟶ FAN

- **Encrypt** FAST ($\overline{5}\ \overline{0}\ \overline{18}\ 19$), $k = 20$

$y_1 = 5 + 20 \text{ Mod } 26$

$\equiv 25 \text{ Mod } 26 \equiv Z$

$y_2 = 0 + 20 \text{ Mod } 26$

$\equiv 20 \text{ Mod } 26 \equiv U$

$y_3 \equiv 18 + 20 \text{ Mod } 26$

$\equiv 38 \text{ Mod } 26$

$\equiv 12 \text{ Mod } 26 \equiv M$

$y_4 = 19 + 20 \text{ Mod } 26$

$\equiv 39 \text{ Mod } 26 \equiv 13 \text{ Mod } 26 \equiv N$

FAST → ZUMN

- Decrypt ZUMN

$x_1 = y_1 - k \text{ Mod } 26$

$= 25 - 20 \text{ Mod } 26 \equiv 5 \text{ Mod } 26 \equiv F$

$x_2 = 20 - 20 \text{ Mod } 26$

$\equiv 0 \text{ Mod } 26 \equiv A$

$x_3 = 12 - 20 \text{ Mod } 26$

$\equiv -8 \text{ Mod } 26 \equiv 18 \text{ Mod } 26$

$\equiv S$

$x_4 = 13 - 20 \text{ Mod } 26$

$\equiv -7 \text{ Mod } 26 \equiv 19 \text{ Mod } 26$

$\equiv T$

ZUMN → FAST