MTH213_Class Notes_Summer 21

Lina Salman

6/13/2021

Integers

Notations: $\mathbb{Z} \rightarrow$ set of all integers (whole numbers)

$\mathbb{Z}^+ \rightarrow$ set of all +ve integers

$\mathbb{Q} \rightarrow$ set of all rational numbers

$\exists \rightarrow$ exists

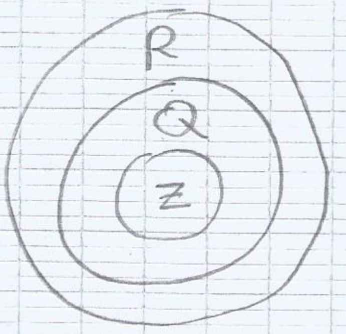
ex: $\frac{\sqrt{2}}{3} \rightarrow$ not rational (irrational)

$\exists! \rightarrow$ exists unique

$\frac{3}{5}, \frac{7}{9}, \frac{-12}{13} \rightarrow$ rational numbers

$\mathbb{R} \rightarrow$ set of all real numbers

Rational Numbers $= \frac{n}{m}$, $n, m \in \mathbb{Z}$ & $m \neq 0$



- * Every integer is rational
- * R separates into rational & irrational

Belong-to-Notation:

$3 \in \mathbb{Z}, \ \frac{1}{2} \in \mathbb{Q}, \ \sqrt{2} \in \mathbb{R}$

$\underbrace{\frac{3}{2} \notin}_{\text{does not belong}} \mathbb{Z}, \ \frac{\sqrt{3}}{5} \notin \mathbb{Q}$

Set-Notations:

A is a set

$A^* = A - \{0\}$

$\mathbb{Z}^* = \mathbb{Z} - \{0\}$

$N^* = \mathbb{Z}^+$ (whole numbers → +ve Integers)

$N = \{0, 1, 2, 3, \cdots\}$

$N^* = \{1, 2, 3, 4, \cdots\} \rightarrow$ Natural numbers

Prime Number Definition:

- $a \in \mathbb{Z}^*$ is prime iff $a \neq 1, -1$ and a is divisible by ±itself and $1, -1$ only

ex: 1 → not prime by definition

ex: 2 → prime

ex: −5 → prime

- Every prime is odd except for 2 & −2 → (the only even prime numbers)

Fact: choose a number $k > 0$

ex: $k = 10^{30}$ there exists an integer x s.t. none of the k consecutive numbers are prime

so $x, x+1, x+2, x+3, \ldots, x+k \rightarrow$ none are prime!

Modulus:

ex: $7 \pmod 5 = 2 \rightarrow$ remainder

$n \pmod m =$ remainder of $n \div m$ where $n \in \mathbb{Z}$, $m \in \mathbb{Z}^+$

ex: $12 \pmod 9 = 3$ ex: $-12 \pmod 3 = 0$

ex: $10 \pmod 5 = 0$ $\underbrace{\text{ex: } -12 \pmod 5 = 3}$

Fundamental Theorem of Number Theory:

$n \in \mathbb{Z}$, $m \in \mathbb{Z}^+$ $\exists!$

$q \in \mathbb{Z}$ & $r \in \mathbb{Z}^+$ s.t. $n = qm + r$, where $0 \leq r < m$

(quotient) (remainder)

ex: $-12 = n$, $5 = m$

$\exists! q$ & $\exists! r$, $0 \leq r < 5$

so $-12 = \underset{q}{\boxed{-3}} \times 5 + \underset{r}{\boxed{3}}$

$\exists!$ q & r means 1 and only 1 integer (q) & 1 and only 1 +ve integer (r), $0 \leq r < 5$ can make this true $-12 = q \times 5 + r$

ex: $-17 \pmod{16} = ?$

$\hookrightarrow \exists! q$ & $\exists! r$ where $0 \leq r < 16$

so $-17 = \boxed{2} \times 16 + \boxed{15}$

so $-17 \pmod{16} = 15$

ex: $-16 \pmod{15} = ?$

$\exists! q$, $\exists! r$, $0 \leq r < 15$

$-16 = \underset{q}{\boxed{-2}} \times 15 + \underset{r}{\boxed{14}}$

so $-16 \pmod{15} = 14$

ex: $-32 \pmod{11} = ?$

$-32 = \boxed{-3} \times 11 + \boxed{1}$

$-32 \pmod{11} = 1$

ex: $20 \pmod 7 = 6$

ex: $-20 \pmod 7 = 1$

Fact: Assume n is negative and $m \in \mathbb{Z}^+$

then $n \pmod m = m - [-n \pmod m]$

↳ ex: $-30 \pmod{11} = ?$

Fundamental Theorem:

↳ $30 \pmod{11} = 8 \overset{\text{or}}{\Longleftrightarrow}$ same as $-30 = \boxed{-3} \times 11 + \boxed{3}$

so $-30 \pmod{11} = 11 - 8 = 3$

then $-30 \pmod{11} = 3$

ex: $-50 \pmod 7 = \boxed{6} \leftarrow$

$50 \pmod 7 = 1$

$7 - 1 = 6$

$\overset{\text{or}}{\Longleftrightarrow} -50 = \underbrace{\boxed{-8}}_{q} \times 7 + \underbrace{\boxed{6}}_{r}$

Practice Questions:

True or False:

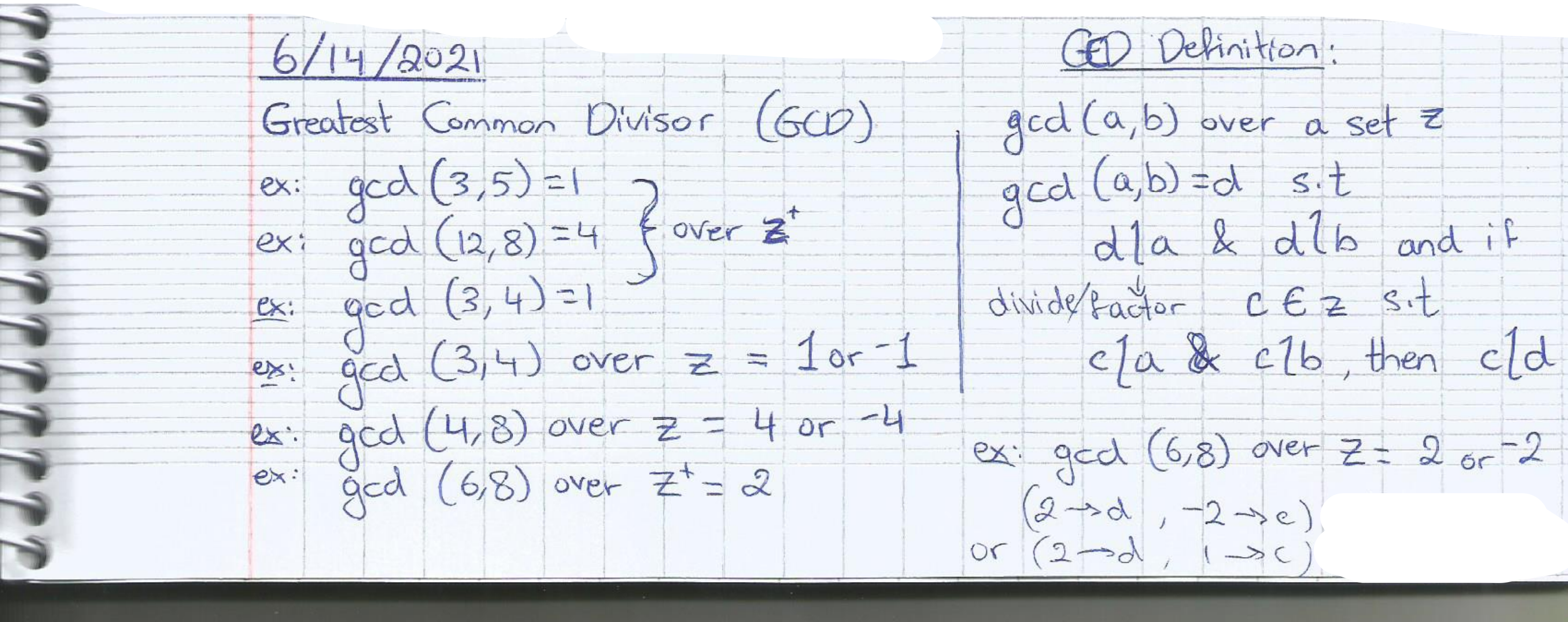
1) $\frac{2}{3} \in \mathbb{R} \rightarrow T$ 3) $\sqrt[3]{8} \in \mathbb{Z} \rightarrow T$

2) $\sqrt{3} \in \mathbb{Q} \rightarrow F$ 4) $\sqrt{13} \in \mathbb{Q} \rightarrow F$

5) $-40 \pmod 3 = 2$

$-40 = \underbrace{\boxed{-14}}_{q} \times 3 + \underbrace{\boxed{2}}_{r} \overset{\text{or}}{\Longleftrightarrow} 40 \pmod 3 = 1$

$3 - 1 = \boxed{2}$



6/14/2021

Greatest Common Divisor (GCD)

ex: gcd $(3,5) = 1$
ex: gcd $(12,8) = 4$ $\Big\}$ over $\mathbb{Z}^+$
ex: gcd $(3,4) = 1$
ex: gcd $(3,4)$ over $\mathbb{Z}$ = 1 or -1
ex: gcd $(4,8)$ over $\mathbb{Z}$ = 4 or -4
ex: gcd $(6,8)$ over $\mathbb{Z}^+ = 2$

GCD Definition:

gcd (a,b) over a set $\mathbb{Z}$
gcd $(a,b) = d$ s.t
$d \mid a$ & $d \mid b$ and if
divide/factor $c \in \mathbb{Z}$ s.t
$c \mid a$ & $c \mid b$, then $c \mid d$

ex: gcd $(6,8)$ over $\mathbb{Z} = 2$ or -2
$(2 \rightarrow d, -2 \rightarrow e)$
or $(2 \rightarrow d, 1 \rightarrow c)$

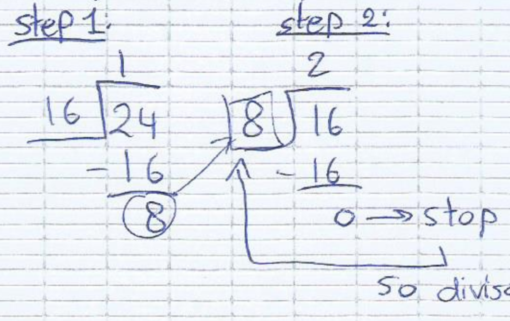
Important: * Every common factor (c) of 2 numbers is a factor of the greatest common factor!! (d)

- gcd (-3, 4) over $\mathbb{Z}^+$ → Incorrect Question
- gcd (-3, 4) over $\mathbb{Z}$ → Correct (= -1, 1)

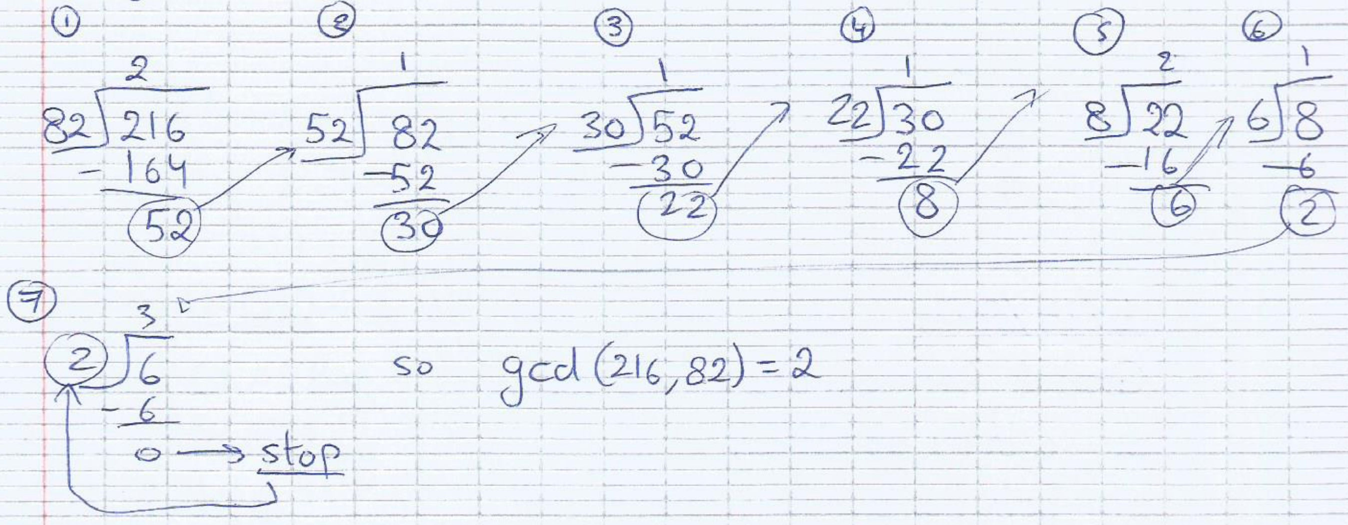
* gcd over $\mathbb{Q}$ or $\mathbb{R}$ allows almost any answer & divisor
* if no 'planet' is given assume it is over $\mathbb{Z}^+$

How to find gcd: → Use Division Algorithm:

ex: gcd (24, 16) = 8



ex: gcd (216, 82)



so gcd (216, 82) = 2

ex: gcd(324, 48) → Use division algorithm to find ↲.

```
      6            1          3
 48 ) 324     36 ) 48    →[12] ) 36
    - 288        - 36          - 36
     (36)  ↗      (12) ↗        0 → stop
```

so gcd (324, 48) = 12

Q: Find the smallest positive integer n s.t. n (mod 3) = 2, n (mod 4) = 1, n (mod 5) = 3. Describe all +ve integers.

↳ ① n (mod 3) = 2
② n (mod 4) = 1 or $n \cong 2 \pmod{3}$
③ n (mod 5) = 3 $n \cong 1 \pmod{4}$
$n \cong 3 \pmod{5}$

* To solve use the Chinese Remainder Theorem

Notation:

ex: Find $7^{-1} \pmod{9}$

↳ Inverse of 7 under multiplication modulo 9

↳ $7 \times \underbrace{\square}_{7^{-1}} \pmod{9} = 1$ where the $\boxed{0 \leq \text{integer} < 9}$ because possible remainder of mod 9 is 0 … 8

so $7^{-1} \pmod{9} = 4$ ✓ ⟷ $7 \times 4 \pmod{9} = 1$ ✓
28 mod 9 = 1 ✓

$Z_n = \{0, 1, \dots, n-1\}$
Integer module n

So $7^{-1} \pmod{9}$
means Find the multiplicative inverse of 7 over Z_9
or Find an integer in Z_9, say c, s.t.
$7 \times c \pmod{9} = 1$

ex: $3^{-1} \pmod{7}$

$3 \times \underbrace{\square}_{3^{-1}} \pmod{7} = 1$

so $3^{-1} \pmod{7} = 5$

ex: Find 5^{-1} over Z_{11}

$5 \times \boxed{c} \pmod{11} = 1$
in Z_{11} → $c \in \{0, \dots, 10\}$

5^{-1} over Z_{11} is 9 ✓
or $5^{-1} \pmod{11} = 9$ ✓

ex: Find 4^{-1} over $\mathbb{Z}_{12}$

4^{-1} over $\mathbb{Z}_{12}$ does not exist.

Fact: a^{-1} over $\mathbb{Z}_n$ exists iff $\gcd(a,n)=1$

ex: Can we find 3^{-1} over $\mathbb{Z}_6$?

No, $\gcd(3,6) \neq 1$

ex: Find 2^{-1} over $\mathbb{Z}_9$

& $\gcd(2,9)=1$

so $2 \times \underbrace{\boxed{c}}_{2^{-1}} \pmod{9} = 1$

$2^{-1} \pmod{9} = 5$ ✓ or 2^{-1} over $\mathbb{Z}_9$ is 5 ✓

Chinese Remainder Theorem:

$$x \cong a_1 \pmod{m_1}$$
$$x \cong a_2 \pmod{m_2}$$
$$\vdots$$
$$x \cong a_k \pmod{m_k}$$

Assume $\gcd(\text{every two distinct } m_i\text{'s}) = 1$
Then the ~~abc~~ system has a solution.
(we should be able to find x)

Q. Find smallest +ve integer n s.t.

$n \cong 2 \pmod{3}$ $\quad a_1=2,\ a_2=3,\ a_3=1$ $\quad \gcd(5,3)=1$ ✓
$n \cong 3 \pmod{5}$ $\quad m_1=3,\ m_2=5,\ m_3=4$ $\quad \gcd(4,3)=1$ ✓
$n \cong 1 \pmod{4}$ $\quad \gcd(5,4)=1$ ✓

} so we can find x

Algorithm:

① Find $m = m_1 \times m_2 \times m_3$ so $m = 3 \times 5 \times 4 = \boxed{60}$

② Define $n_1 = \frac{m}{m_1}$, $n_2 = \frac{m}{m_2}$, $n_3 = \frac{m}{m_3}$ so $n_1 = \frac{60}{3} = \boxed{20}$

$n_2 = \frac{60}{5} = \boxed{12}$

$n_3 = \frac{60}{4} = \boxed{15}$

③ $n_1^{-1} \pmod{m_1}$ so $20^{-1} \pmod{3} = 2$

$n_2^{-1} \pmod{m_2}$ $\quad 12^{-1} \pmod{5} = 3$

$n_3^{-1} \pmod{m_3}$ $\quad 15^{-1} \pmod{4} = 3$

④ n ~~(smallest)~~ $= \sum_{i=1}^{3} a_i n_i n_i^{-1}$ so $n = 2 \times 20 \times 2 + 3 \times 12 \times 3 + 1 \times 15 \times 3$

$n = 233$ (not the smallest)

⑤ smallest $= n \pmod{m}$ so $233 \pmod{60} = \boxed{53}$

6/15/2021

Q. Find the smallest +ve integer s.t

$x \cong 2 \pmod 9 \longrightarrow x \pmod 9 = 2$

$x \cong 7 \pmod 8 \longrightarrow x \pmod 8 = 7$

Describe all +ve integers that satisfy the above condition

S1. $\left.\begin{matrix} a_1 = 2, & a_2 = 7 \\ m_1 = 9, & m_2 = 8 \end{matrix}\right\}$ gcd(9,8) = 1 → we can use Chinese Remainder Theorem!

① $m = m_1 \times m_2 = 9 \times 8 = \boxed{72}$

② $n_i = \frac{m}{m_i}$ $n_1 = \frac{72}{9} = \boxed{8}$ $n_2 = \frac{72}{8} = \boxed{9}$

* Fact: Smallest +ve integer x, $0 < x < m$

③ $n_i^{-1} \pmod{m_i}$ $8^{-1} \pmod 9 = \boxed{8}$ $9^{-1} \pmod 8 = \boxed{1}$

n_i^{-1} over $\mathbb{Z}_{m_i}$ ↳ $8 \times \square \pmod 9 = 1$ ↳ $9 \times \square \pmod 8 = 1$

④ $n = \sum_{i=1}^{a} a_i n_i n_i^{-1} = \sum_{i=1}^{2} a_i n_i n_i^{-1} = (2 \times 8 \times 8) + (7 \times 9 \times 1) = 128 + 63 = \boxed{191}$

⑤ smallest $x = n \pmod m = x = 191 \pmod{72} = \boxed{47}$

S2. Describe all +ve integers that satisfy the given conditions:

- All integers are of the form $47 + mk$, where $k \in$ ~~Z~~ $\mathbb{N}$ $\mathbb{N} = \{0, 1, 2 \ldots\}$

So: $\boxed{47 + 72k, \; k \in \mathbb{N}}$

at $k=0$
$x = 47$

at $k=1$
$x = 47 + 72 = 119$

at $k=2$
$x = 47 + 72(2) = 191$

⋮

Note: If you need all -ve integers then:

$47 + 72k$, $k \in \mathbb{Z}^-$ where $k=-1$ is the largest negative x

$\mathbb{Z}^- = \{\dots,-3,-2,-1\}$

- If you need all possible integers then: $k \in \mathbb{Z}$.

Practice Questions:

1] Find $-27 \pmod 8$

$-27 = \underbrace{\boxed{-4}}_{q} \times 8 + \underbrace{\boxed{5}}_{r}$ ✓

or

$27 \pmod 8 = 3 \rightarrow 8-3 = \boxed{5}$ ✓

2] Find $123 \pmod{21}$

$$\begin{array}{r} 5 \\ 21\overline{)123} \\ -105 \\ \hline 18 \end{array} = \boxed{18}$$ ✓

3] Find $-203 \pmod{13}$

$-203 = \underbrace{\boxed{-16}}_{q} \times 13 + \underbrace{\boxed{5}}_{r}$ ✓

or

$203 \pmod{13} = 8 \rightarrow 13-8 = \boxed{5}$ ✓

4] Find $-32 = \underbrace{\boxed{-5}}_{q} \times 7 + \underbrace{\boxed{3}}_{r}$, $0 \leq r < 7$ ✓

↳ same as $-32 \pmod 7$

or $32 \pmod 7 = 4 \rightarrow 7-4 = \boxed{3}$ ✓

5] Find $\gcd(326, 104)$ (Use division algorithm)

$$\begin{array}{r} 3 \\ 104\overline{)326} \\ -312 \\ \hline 14 \end{array} \quad \begin{array}{r} 7 \\ 14\overline{)104} \\ -98 \\ \hline 6 \end{array} \quad \begin{array}{r} 2 \\ 6\overline{)14} \\ -12 \\ \hline 2 \end{array} \quad \begin{array}{r} 3 \\ \textcircled{2}\overline{)6} \\ -6 \\ \hline 0 \end{array}$$

0 → stop

so $\gcd(326, 104) = \boxed{2}$ ✓

6] Find $\gcd(308, 126)$ (Use D.A)

$$\begin{array}{r} 2 \\ 126\overline{)308} \\ -252 \\ \hline 56 \end{array} \quad \begin{array}{r} 2 \\ 56\overline{)126} \\ -112 \\ \hline 14 \end{array} \quad \begin{array}{r} 4 \\ \textcircled{14}\overline{)56} \\ -56 \\ \hline 0 \end{array}$$

stop

so $\gcd(308, 126) = \boxed{14}$ ✓

7] Find the smallest +ve integer and the largest negative integer s.t.

$x \equiv 3 \pmod{4}$

$x \equiv 2 \pmod{7}$

$x \cong 6 \pmod{9}$

$\left.\begin{array}{l} \gcd(4,7)=1 \\ \gcd(4,9)=1 \\ \gcd(7,9)=1 \end{array}\right\}$ gcd (every 2 distinct m_i's) =
So system has a solution

(Use C.R.T.)

$a_1 = 3,\ a_2 = 2,\ a_3 = 6$

$m_1 = 4,\ m_2 = 7,\ m_3 = 9$

① $m = 4 \times 7 \times 9 = 252$

② $n_1 = \frac{252}{4} = 63$, $n_2 = \frac{252}{7} = 36$, $n_3 = \frac{252}{9} = 28$

③ $63^{-1} \pmod{4} = 3$ $\quad 36^{-1} \pmod{7} = 1$ $\quad 28^{-1} \pmod{9} = 1$

④ $n = (3 \times 63 \times 3) + (2 \times 36 \times 1) + (6 \times 28 \times 1) = 807$

⑤ $x = 807 \pmod{252} = \boxed{51}$ ✓

⑥ $51 + 252K,\ K \in Z$

⑦ largest negative integer:
$k = -1$: $51 - 252 = \boxed{-201}$ ✓

8] Give me 3 +ve integers s.t.

$x \equiv 1 \pmod{11}$

$x \cong 6 \pmod{13}$

$\gcd(11,13) = 1 \rightarrow$ gcd (every 2 m_i's) $= 1$
there is a solution

$a_1 = 1,\ a_2 = 6$

$m_1 = 11,\ m_2 = 13$

① $m = 11 \times 13 = 143$

② $n_1 = \frac{143}{11} = 13$ $\quad n_2 = \frac{143}{13} = 11$

③ $13^{-1} \pmod{11} = 6$ $\quad 11^{-1} \pmod{13} = 6$

④ $n = (1 \times 13 \times 6) + (6 \times 11 \times 6) = \boxed{474}$ ✓

⑤ $x = 474 \pmod{143} = \boxed{45}$ ✓

⑥ $45 + 143K,\ K \in N$

⑦ $K = 1$
$x = 45 + 143 = \boxed{188}$ ✓

3 +ve integers: 45, 188, 474

or

$K = 2$
$x = 45 + 143(2) = \boxed{331}$ ✓

9] Find 8(mod 11)

$8<11$, $q=0$ so $\boxed{r=8}$

10] Find smallest +ve integer s.t.

$x \equiv 3 \pmod{20}$

$x \equiv 3 \pmod{11}$

since both answers = 3

then $x=3$ is the smallest +ve integer,

It satisfies: $3 \pmod{20} = 3$ since $3<20$ & $3<11$

$3 \pmod{11} = 3$

Q. Solve $3x \equiv 6 \pmod 7$, $0 \leq x < 7$

or Solve $3x=6$ over $\mathbb{Z}_7$

or Find $0 \leq x < 7$ s.t. $3x \pmod 7 = 6$

S. so $3 \times \square \pmod 7 = 6$

$\boxed{x=2}$ because $3 \times 2 \pmod 7 = 6$

$6 \pmod 7 = 6$ ✓

Fact: $a \in \mathbb{Z}^+$, $m \in \mathbb{Z}^+$, $ax=b$ over $\mathbb{Z}_m$ where $b \in \mathbb{N}$
has a solution iff $\gcd(a,m) \mid b$
# of all distinct solutions is $\gcd(a,m)$

Q. Solve $4x=6$ over $\mathbb{Z}_{10}$

Meaning: Find all possible values of x inside $\mathbb{Z}_{10}$, $0 \leq x \leq 9$
s.t. $4x \pmod{10} = 6$

S. so $a=4$, $m=10$, $\gcd(a,m) = \gcd(4,10) = 2$

$b=6$. Is $2 \mid 6$? yes. → We have 2 solutions.

$4x \equiv 6 \pmod{10}$

$4 \times \square \pmod{10} = 6$ so $\boxed{x=4,9}$

Q. Solve $3x=7$ over $\mathbb{Z}_{12}$

Meaning: Find $0 \leq x \leq 11$ s.t. $3x \pmod{12} = 7$

S. $a=3$, $m=12$, $\gcd(3,12)=3$

$b=7$ Is $3 \mid 7$? No. $3 \nmid 7$ (3 is not a factor of 7)

So no solution

Q. Solve $3x=2$ over $\mathbb{Z}_5$

S. $a=3$, $m=5$, $\gcd(3,5)=1$

$b=2$ Is $1 \mid 2$? Yes. So we have 1 solution inside $\mathbb{Z}_5$

So $3x \pmod 5 = 2$ where $0 \leq x \leq 4$

$3 \times \square \pmod 5 = 2$

$\downarrow$

$\boxed{x=4}$

Note: $b<m$ for the answer to be correct.

ex: $3x=10$ over $\mathbb{Z}_6$ is incorrect!

ex: $3x=4$ over $\mathbb{Z}_6$ is correct.

Practice Questions

Q_1 Solve $6x=5$ over $\mathbb{Z}_7$

so Find $6x \pmod 7 = 5$ $\gcd(6,7)=1$, $1 \mid 5$ ✓ 1 solution

$6 \times \square \pmod 7 = 5$ where $0 \leq x \leq 6$

$\downarrow$

$\boxed{x=2}$

Q_2 Solve $8x=6$ over $\mathbb{Z}_{10}$

so Find $8x \pmod{10} = 6$ $\gcd(8,10)=2$, $2 \mid 6$ ✓ 2 solutions

$8 \times \square \pmod{10} = 6$

$\downarrow$

$\boxed{x=2}$ ✓

$\boxed{x=7}$ ✓

Q_3 Solve $5x = 8$ over $\mathbb{Z}_{15}$

So Find $5x \pmod{15} = 8$ $\gcd(5,15) = 5$

So this has no solution $5 \nmid 8$

Q_3 Solve $5x = 8$ over $\mathbb{Z}_{15}$

So Find $5x \pmod{15} = 8$ $\quad$ $\gcd(5,15) = 5$

So this has no solution $\quad$ $5 \nmid 8$

6/16/2021

Q. Solve $4x = 8$ over $\mathbb{Z}_{12}$

meaning Find ~~#~~ $0 \leq x \leq 11$ s.t. $4x \pmod{12} = 8$

S. $\gcd(4,12) = 4$ $\quad$ $4 | 8$? Yes so there are 4 solutions

$4 \times \square \pmod{12} = 8$

$\downarrow$

~~x~~ $\boxed{x = 2}$

Math ① Let $n = \frac{m}{d} = \frac{12}{4} = 3$ $\quad$ while $a \rightarrow$ smallest solution

where d is the gcd $\quad$ all other solutions: $a, a+n, a+2n,$

(4 solutions) $a + 3n.$

② 2 is the smallest.

$a = 2$

③ so $\boxed{x_1 = \boxed{2}}$ $\quad$ $\boxed{x_2 = 2 + 3 = \boxed{5}}$

$\boxed{x_3 = 2 + (3)(2) = \boxed{8}}$ $\quad$ $\boxed{x_4 = 2 + (3)(3) = \boxed{11}}$

Q. Solve $5x = 10$ over $\mathbb{Z}_{30}$

S. $\gcd(5,30) = 5$ $\quad$ $5 | 10$? Yes $\rightarrow$ 5 solutions

$5x \pmod{30} = 10$ $\quad$ $0 \leq x \leq 29$

$5 \times \square \pmod{30} = 10$

$\downarrow$

$\boxed{x = 2} \rightarrow$ smallest

$n = \frac{m}{d} = \frac{30}{5} = 6$

$x_1 = \boxed{2}$ $\quad$ $x_2 = 2 + 6 = \boxed{8}$ $\quad$ $x_3 = 2 + 6(2) = \boxed{14}$

$x_4 = 2 + 6(3) = \boxed{20}$ $\quad$ $x_5 = 2 + 6(4) = \boxed{26}$

Practice Questions:

Q_1. Solve $6x=9$ over Z_{27}

S. $\gcd(6,27)=3$, $3|9$?, yes so there are 3 solutions

$6\times\square \pmod{27}=9$ $\quad 0\leq x\leq 26$

$\downarrow$

$\boxed{x=6}$

$n=\frac{m}{d}=\frac{27}{3}=9$

$\boxed{x_1=6}$ $\quad \boxed{x_2=6+9}$ $\quad x_3=6+9(2)$

$\boxed{x_2=15}$ $\quad \boxed{x_3=24}$

Q_2: Solve $12x=16$ over Z_{28}

S. $\gcd(12,28)=4$, $4|16$? yes, so there are 4 solutions

$12\times\square \pmod{28}=16$ $\quad 0\leq x\leq 27$

$\downarrow$

$\boxed{x=6}$

$n=\frac{m}{d}=\frac{28}{4}=7$

$\boxed{x_1=6}$ $\quad x_2=6+7$ $\quad x_3=6+7(2)$ $\quad x_4=6+7(3)$

$\boxed{x_2=13}$ $\quad \boxed{x_3=20}$ $\quad \boxed{x_4=27}$

Q_3 Solve $18x=27$ over Z_{81}

$\gcd(18,81)=9$, $9|27$? Yes, so there are 9 solutions

$18\times\square \pmod{81}=27$ $\quad 0\leq 0\leq 80$

$\downarrow$

$\boxed{x=6}$

$n=\frac{m}{d}=\frac{81}{9}=9$

$\boxed{x_1=6}$ $\quad x_2=6+9$ $\quad x_3=6+9(2)$ $\quad x_4=6+9(3)$ $\quad x_5=6+9(4)$

$\boxed{x_2=15}$ $\quad \boxed{x_3=24}$ $\quad \boxed{x_4=33}$ $\quad \boxed{x_5=42}$

$x_6=6+9(5)$ $\quad x_7=6+9(6)$ $\quad x_8=6+9(7)$ $\quad x_9=6+9(8)$

$\boxed{x_6=51}$ $\quad \boxed{x_7=60}$ $\quad \boxed{x_8=69}$ $\quad \boxed{x_9=78}$

Proofs:

Definition: - An integer m is called an even integer iff $m=2k$ for some $k \in \mathbb{Z}$

- An integer m is called odd iff $m=2K+1$ for some $K \in \mathbb{Z}$

Result: Prove that ① even + even = even

② odd + even = odd

③ odd + odd = even

④ even x odd = even

⑤ odd x odd = odd

Proof: (*) → Let n be an even integer and m be an odd integer

& Let w be an even integer and y be an odd integer

① We need to show that $n+w =$ even

We show $n+w = 2h$ ✓ for some $h \in \mathbb{Z}$

Since n is even, $n = 2K_1$ for some $K_1 \in \mathbb{Z}$

since w is even, $w = 2K_2$ for some $K_2 \in \mathbb{Z}$

So $n+w = 2K_1 + 2K_2 = 2\underbrace{(K_1+K_2)}_{h \in \mathbb{Z}}$ ✓

② Since n is even, $n = 2K_1$ for some $K_1 \in \mathbb{Z}$

Since m is odd, $m = 2K_2+1$ for some $K_2 \in \mathbb{Z}$

Show $n+m = 2h+1$ ✓ for some $h \in \mathbb{Z}$

So $n+m = 2K_1 + 2K_2 + 1 = 2\underbrace{(K_1+K_2)}_{h \in \mathbb{Z}} + 1$ ✓

④ since n is even, $n = 2K_1$ for some $K_1 \in \mathbb{Z}$

since m is odd, $m = 2K_2+1$ for some $K_2 \in \mathbb{Z}$

show $n \times m = 2h$ ✓ for some $h \in \mathbb{Z}$

So $n \times m = 2K_1 \times (2K_2+1) = 4K_1K_2 + 2K_1 = 2\underbrace{(2K_1K_2 + K_1)}_{h \in \mathbb{Z}}$ ✓

③ Since m, y are odd, $m = 2k_1 + 1$ for some $k_1 \in \mathbb{Z}$ & $y = 2k_2 + 1$, $k_2 \in \mathbb{Z}$

show $m + y = 2h$, $h \in \mathbb{Z}$

so $m + y = 2k_1 + 1 + 2k_2 + 1 = 2k_1 + 2k_2 + 2 = 2(\underbrace{k_1 + k_2 + 1}_{h \in \mathbb{Z}})$

⑤ since m, y are odd, $m = 2k_1 + 1$, $y = 2k_2 + 1$, $k_1, k_2 \in \mathbb{Z}$

show $mxy = 2h + 1$ ✓, $h \in \mathbb{Z}$

so $mxy = (2k_1 + 1)(2k_2 + 1) = 4k_1k_2 + 2k_1 + 2k_2 + 1 = 2(\underbrace{2k_1k_2 + k_1 + k_2}_{h \in \mathbb{Z} ✓}) + 1$

6/17/2021

Proofs → Direct (such as above)

Proofs → Contradiction

Direct Proof ex:

Let $n, a \in \mathbb{Z}$, show $an^2 + an$ is an even integer

Proof: ① Assume n is even. Hence $n = 2k$, $k \in \mathbb{Z}$

we show $an^2 + an = 2h$ for $h \in \mathbb{Z}$

$$a(2k)^2 + a(2k)$$

$$4ak^2 + 2ak$$

$$2(\underbrace{2ak^2 + ak}_{\text{integer } (h \in \mathbb{Z})})$$

Hence $an^2 + an = 2h$ is even for n is even

② Assume n is odd. Hence $n = 2k + 1$, $k \in \mathbb{Z}$

we show $an^2 + an = 2h$, $h \in \mathbb{Z}$

$$\begin{aligned} an^2 + an &= a(2k+1)^2 + a(2k+1) \\ &= a(4k^2 + 4k + 1) + 2ak + a \\ &= 4ak^2 + 4ak + a + 2ak + a \\ &= 4ak^2 + 6ak + 2a \\ &= 2(\underbrace{2ak^2 + 3ak + a}_{\text{integer} \rightarrow (h \in \mathbb{Z})}) \end{aligned}$$

Hence $an^2 + an = 2h$ is even for n is odd

③ Since m, y are odd, $m = 2k_1 + 1$ for some $k_1 \in \mathbb{Z}$ & $y = 2k_2 + 1$, $k_2 \in \mathbb{Z}$

show $m + y = 2h$, $h \in \mathbb{Z}$

so $m + y = 2k_1 + 1 + 2k_2 + 1 = 2k_1 + 2k_2 + 2 = 2\underbrace{(k_1 + k_2 + 1)}_{h \in \mathbb{Z}}$

⑤ since m, y are odd, $m = 2k_1 + 1$, $y = 2k_2 + 1$, $k_1, k_2 \in \mathbb{Z}$

show $mxy = 2h + 1$ ✓, $h \in \mathbb{Z}$

so $mxy = (2k_1 + 1)(2k_2 + 1) = 4k_1k_2 + 2k_1 + 2k_2 + 1 = 2\underbrace{(2k_1k_2 + k_1 + k_2)}_{h \in \mathbb{Z}\ ✓} + 1$

6/17/2021

Proofs → Direct (such as above)

Proofs → Contradiction

Direct Proof ex:

Let $n, a \in \mathbb{Z}$, show $an^2 + an$ is an even integer

Proof: ① Assume n is even. Hence $n = 2k$, $k \in \mathbb{Z}$

we show $an^2 + an = 2h$ for $h \in \mathbb{Z}$

$a(2k)^2 + a(2k)$

$4ak^2 + 2ak$

$2\underbrace{(2ak^2 + ak)}_{\text{integer } (h \in \mathbb{Z})}$

Hence $an^2 + an = 2h$ is even for n is even

② Assume n is odd. Hence $n = 2k + 1$, $k \in \mathbb{Z}$

we show $an^2 + an = 2h$, $h \in \mathbb{Z}$

$$\begin{aligned} an^2 + an &= a(2k+1)^2 + a(2k+1) \\ &= a(4k^2 + 4k + 1) + 2ak + a \\ &= 4ak^2 + 4ak + a + 2ak + a \\ &= 4ak^2 + 6ak + 2a \\ &= 2\underbrace{(2ak^2 + 3ak + a)}_{\text{integer} \rightarrow (h \in \mathbb{Z})} \end{aligned}$$

Hence $an^2 + an = 2h$ is even for n is odd

- Prove $\sqrt{5}$ is irrational

$\mathbb{R} \rightarrow$ set of all real #s $\nearrow$ rational $\left(\frac{int}{int}\right)$
$\searrow$ irrational (cannot be written as $\frac{int}{int}$)

Assume x is rational

where $x = \frac{a}{b}$ s.t. $\begin{cases} a, b \in \mathbb{Z} \\ b \neq 0 \\ \gcd(a,b) = 1 \\ \text{reduced form} \end{cases}$

show $\sqrt{5}$ is irrational

Use the 4-method to prove { Prove by Contraction:

- Deny: Hence $\sqrt{5}$ is rational
- $\sqrt{5} = \frac{a}{b}$ for $\begin{cases} a, b \in \mathbb{Z} \\ b \neq 0 \\ \gcd(a,b) = 1 \end{cases}$

$$(\sqrt{5})^2 = \left(\frac{a}{b}\right)^2$$

$$5 = \frac{a^2}{b^2} \rightarrow 5b^2 = a^2$$

→ By staring, since $\gcd(a,b) = 1$, a,b cannot be both even (then otherwise $\gcd = 2$)

- So a is odd while b is even (vice versa)

or a is odd while b is odd

- Assume a is odd while b is even, then:

$$5 = \frac{a^2}{b^2} \rightarrow 5b^2 = a^2$$

$$\underbrace{\text{even} \times \text{even}}_{\text{even}} \qquad \underbrace{\text{~~odd~~} \times \text{even}}_{\text{even}}$$

both can't be even (gcd rule)

- Hence $5 = \frac{a^2}{b^2}$ where ~~$5b^2 = a^2$~~ ~~even~~ ~~even~~

a,b are both odd AND $\gcd(a,b) = 1$

- So $a = 2n+1$, $b = 2m+1$, $n, m \in \mathbb{Z}$

$$5b^2 = a^2$$
$$5(2m+1)^2 = (2n+1)^2$$
$$5[4m^2 + 4m + 1] = 4n^2 + 4n + 1$$
$$5 \times 4m^2 + 5 \times 4m + 5 = 4n^2 + 4n + 1$$
$$5 \times 4m^2 + 5 \times 4m + 4 = 4n^2 + 4n$$

→ divide by 4

$$5m^2 + 5m + 1 = n^2 + n$$

we know $am^2 + am$ always even

so $$\underbrace{\underbrace{5m^2 + 5m}_{\text{even}} + 1}_{\text{odd}} = \underbrace{n^2 + n}_{\text{even}}$$

odd ≠ even contradiction

Hence our assumption $\sqrt{5}$ is rational is wrong. Thus $\sqrt{5}$ is irrational

- Use the 4-method to prove $\sqrt{2}$ is irrational:
(By contradiction)

① Deny: Hence $\sqrt{2}$ is rational

② s.t $\sqrt{2} = \frac{a}{b}$, $\begin{cases} a, b \in \mathbb{Z} \\ b \neq 0 \\ \gcd(a, b) = 1 \end{cases}$

③ $2 = \frac{a^2}{b^2} \longrightarrow 2b^2 = a^2$

④ ~~Assume~~ a is even, b is odd since $\gcd(a,b) = 1$

since a is even, $a = 2n$, $n \in \mathbb{Z}$

and since b is odd, $b = 2m + 1$, $m \in \mathbb{Z}$

so $2b^2 = a^2$

$2(2m+1)^2 = (2n)^2$

$2(4m^2 + 4m + 1) = 4n^2$

$2 \times 4 m^2 + 2 \times 4 m + 2 = 4n^2$

divide by 4

$\underbrace{2m^2 + 2m}_{\text{integer}} + \underbrace{\frac{1}{2}}_{\text{(rational)}} = \underbrace{n^2}_{\text{integer}}$

integer + $\frac{1}{2}$ = integer $\longrightarrow$ Impossible, contradiction
Hence $\sqrt{2}$ is irrational

- Prove rational x irrational = irrational

- x is rational (and not 0), y is irrational. We show xy is irrational

- we know rational ÷ rational = rational $\left(\frac{a}{b} * \frac{d}{c} \Leftrightarrow \frac{a}{b} \div \frac{c}{d} \right)$

- Deny: Hence xy is rational

say $xy = w$, $w \in \mathbb{Z}$

implies $\underbrace{y}_{\text{irrational}} = \underbrace{\frac{w}{x}}_{\text{rational} \div \text{rational} = \text{rational}}$

Impossible, contradiction

6/20/2021

Using the Fundamental Theorem:

- $\gcd(30,16) = d$ where $d \mid r$

Note: the remainders are always divisible by the gcd: $2 \mid 14$ ✓ $2 \mid 2$ ✓

$$30 = \underset{q}{\boxed{1}} \times 16 + \underset{r}{\boxed{14}} \qquad 0 \leq r \leq 15$$

and $$16 = \boxed{1} \times 14 + \underset{r}{\boxed{2}} \qquad 0 \leq r \leq 13$$

$$14 = \boxed{7} \times \underset{\text{stop}}{2} + \boxed{0} \qquad 0 \leq r \leq 1$$

- solve $3x = 6$ over planet $\mathbb{Z}_9$

means $3x \pmod 9 = 6$ where $0 \leq x \leq 8$

Q. Solve $3x \pmod 9 = 6$ over planet $\mathbb{Z}$

S: ① over $\mathbb{Z}_9$: $3 \times \square \pmod 9 = 6$ $\gcd(3,9) = 3$, $3 \mid 6 \rightarrow 3$ solutions

$\boxed{x = 2}$ $n = \frac{m}{d} = \frac{9}{3} = \boxed{3}$

$x = \{2, 5, 8\}$

② over $\mathbb{Z}$: $(z + nk)$, $k \in \mathbb{Z}$

$\rightarrow \boxed{2 + 3k,\ k \in \mathbb{Z}}$

③ or $\boxed{2 + 9k,\ 5 + 9k,\ 8 + 9k} \rightarrow (x + mk)$

- $\mathbb{Z}_2 \rightarrow \{0, 1\} \rightarrow$ binary
- $\mathbb{Z}_{16} \rightarrow \{0, 1, \cdots 15\} \rightarrow$ hexadecimal
- $\mathbb{Z}_8 \rightarrow \{0, 1 \cdots 7\} \rightarrow$ Octa

Convert to Decimal:

Base: digits base $n = \mathbb{Z}_n = \{0, \cdots, n-1\}$

ex: digits base $7 = \mathbb{Z}_7 = \{0, \cdots 6\}$

ex: digits base $10 = \mathbb{Z}_9 = \{0, \ldots, 9\} \rightarrow$ Decimal

Notation:

ex: $(124)_5 \rightarrow$ base 5

$(567)_9 \rightarrow$ 567 base 9

Convert $(124)_5$ to base 10 (Decimal):

ex: $(\overset{2}{1}\overset{1}{2}\overset{0}{4})_5 = 1\times5^2 + 2\times5^1 + 4\times5^0 = 25+10+4 = \boxed{39}$

note → smallest base: 2

Convert $(2341)_8$ to base 10:

ex: $(\overset{3}{2}\overset{2}{3}\overset{1}{4}\overset{0}{1})_8 = (2\times8^3) + (3\times8^2) + (4\times8^1) + (1\times8^0) = \boxed{1249}$

ex: Convert $(A8E1)_{16}$ to base 10: $\left(\mathbb{Z}_{16} = \{0 \ldots 9, \underset{\overset{\downarrow}{10}}{A}, \underset{\overset{\downarrow}{11}}{B}, \underset{\overset{\downarrow}{12}}{C}, \underset{\overset{\downarrow}{13}}{D}, \underset{\overset{\downarrow}{14}}{E}, \underset{\overset{\downarrow}{15}}{F}\}\right)$

$(A8E1)_{16} = (A\times16^3) + (8\times16^2) + (14\times16) + 1 = \boxed{43233}$

ex: Convert 39 (base 10) to base 5:

$$\begin{array}{lll} \text{①} & \text{②} & \text{③} \\ \begin{array}{r} 7 \\ 5\overline{)39} \\ -35 \\ \hline \text{④} \end{array} & \begin{array}{r} 1 \\ 5\overline{)7} \\ -5 \\ \hline \text{②} \end{array} & \begin{array}{r} 0 \rightarrow \text{stop} \\ 5\overline{)1} \quad\quad \\ -0 \quad\quad \\ \hline \text{①} \quad\quad \end{array} \end{array}$$

read backwards

so $39 = (124)_5$

ex: Convert 45 to base 8:

$$\begin{array}{ll} \begin{array}{r} 5 \\ 8\overline{)45} \\ -40 \\ \hline \text{⑤} \end{array} & \begin{array}{r} 0 \rightarrow \text{stop} \\ 8\overline{)5} \quad\quad \\ -0 \quad\quad \\ \hline \text{⑤} \quad\quad \end{array} \end{array}$$

so $45 = (55)_8$

Adding:

ex:
$$\begin{array}{r} \textcircled{1} \\ 2\,7 \\ +\ 9\,8 \\ \hline 12\,\textcircled{5} \end{array}$$

$(7+8=15)$

$(15 = \underset{q}{\boxed{1}} \times 10 + \underset{r}{\boxed{5}})$

- write down remainder
- carry on with quotient

ex: add
$$\begin{array}{r} \textcircled{1}\textcircled{1} \\ (1\,3\,6)_8 \\ +\ (5\,4\,5)_8 \\ \hline (\textcircled{7}\textcircled{0}\textcircled{3})_8 \end{array}$$

$$\begin{cases} 6+5=11 \\ 11 = \underset{q}{\boxed{1}} \times 8 + \underset{r}{\boxed{3}} \end{cases}$$

$$\begin{cases} 1+3+4=8 \\ 8 = \boxed{1} \times 8 + \boxed{0} \end{cases}$$

$$\begin{cases} 1+1+5=7 \\ 7 = \boxed{0} \times 8 + \boxed{7} \end{cases}$$

ex:
$$\begin{array}{r} 1\,1 \\ (1\,4\,5)_6 \\ +\ (5\,4\,3)_6 \\ \hline (1\,1\,3\,2)_6 \end{array}$$

(last step) = $1+1+5=7$

$7 \bmod 6$

$q=1 \quad r=1$ (write both down last step)

ex:
$$\begin{array}{r} 1\,1 \\ 1\,1 \\ (1\,2\,3)_5 \\ \times\ (3\,2)_5 \\ \hline (0\,3\,0\,1)_5 \\ +\ (4\,2\,4\,0)_5 \\ \hline (1\,0\,0\,4\,1)_5 \end{array}$$

ex:
$$\begin{array}{r} 3\;22\phantom{)_{16}} \\ (3\,\cancel{4}\,\cancel{6})_{16} \\ -\ (1\,2\,B)_{16} \\ \hline (2\,1\,B)_{16} \end{array}$$

ex:
$$\begin{array}{r} 2\,5 \\ (1\,\cancel{3}\,\cancel{1})_4 \\ -\ (0\,1\,2)_4 \\ \hline (1\,1\,3)_4 \end{array}$$

borrow the base

Practice Questions:

Q1:
$$\begin{array}{rr} & (\overset{\overset{\textcircled{1}}{\textcircled{1}}}{2}\;\overset{\overset{\textcircled{3}}{\cancel{\textcircled{2}}}}{3}\;7)_8 \\ \times & (4\;3)_8 \\ \hline & \textcircled{1}7\;3\;5 \\ + & 1\;1\;7\;4\;0 \\ \hline & (1\;2\;6\;7\;5)_8 \end{array}$$

Q2:
$$\begin{array}{rr} & (A\;\overset{\textcircled{5}}{\cancel{6}}\;\overset{\textcircled{18}}{\cancel{2}})_{16} \\ - & (6\;3\;F)_{16} \\ \hline & (4\;2\;3)_{16} \end{array}$$

Q3:
$$\begin{array}{rr} & (2\;\overset{\overset{\textcircled{4}}{\textcircled{2}}}{0}\;5)_6 \\ \times & (5\;3)_6 \\ \hline & 1\;0\;2\;3 \\ + & 1\;4\;4\;1\;0 \\ \hline & (1\;5\;4\;3\;3)_6 \end{array}$$

Q4:
$$\begin{array}{rr} & (\overset{\textcircled{1}}{A}\;B\;2\;3)_{16} \\ + & (1\;F\;A\;B)_{16} \\ \hline & (C\;A\;C\;E)_{16} \end{array}$$

Q5:
$$\begin{array}{rr} & (\overset{\textcircled{1}}{3}\;7\;\overset{\textcircled{1}}{1}\;\overset{\textcircled{1}}{2})_8 \\ + & (5\;1\;7\;6)_8 \\ \hline & (1\;1\;1\;1\;0)_8 \end{array}$$

* Quantifiers:

Notations:

$\exists$, exists (at least one ...) $\nexists$, does not exist

$\exists!$, exists unique (only one ...)

$\forall$, for all

$\in$, belong $\notin$, does not belong

$\subset$, subset $\not\subset$, is not a subset ex: $\exists!\ x \in N$ s.t. $x^2 - 4 = 0$, T,F?

True $(x=2)$

ex: $\exists!\ x \in Z$ s.t. $x^2 - 4 = 0$, T,F?

False $(x = \{2, -2\}$

ex: $\exists\ x \in Z$ s.t. $x^2 - 4 = 0$, T,F?

True (at least 1 solution: $x = \{2, 2\}$)

ex: $\forall\ x \in \mathbb{R}$ $0x = 0$

True (for all x times zero = zero)

ex: $\forall\ x \in Q$ $\exists\ y \in Q$ s.t. $xy = 1$

False $(x=0)$

ex: $\forall\ x \in Q^*$ $\exists y \in Q$ s.t $xy = 1$

True (every rational has a reciprocal except 0)

6/21/20:

* $\exists\ x \in N^*$ s.t $x^2 - x = 0$ → True

* $\exists!\ x \in N^*$ s.t $x^2 - x = 0$ → True $(x=1)$

Important{ * $\exists\ y \in Q^*$ s.t $\forall\ x \in Q^*$ we have $yx = 1$ → False! (exists a y where $yx = 1$ for every x)

* $\forall x \in Q^*$, $\exists\ y \in Q^*$ s.t $xy = 1$ → True

or $\forall x \in Q^*$, $\exists y \in Q$ s.t $xy = 1$ → also True

→ means: exists a $y \in Q^*$ and same y multiplied with every x in $Q^* = 1$

→ the y depends on x

ex: $\exists!\ x \in N$ s.t. $x^2 - 4 = 0$, T,F?

True ($x=2$)

ex: $\exists!\ x \in Z$ s.t. $x^2 - 4 = 0$, T,F?

False ($x = \{2, -2\}$

ex: $\exists\ x \in Z$ s.t. $x^2 - 4 = 0$, T,F?

True (at least 1 solution: $x = \{2, 2\}$)

ex: $\forall\ x \in \mathbb{R}$ $0x = 0$

True (for all x times zero = zero)

ex: $\forall\ x \in Q$ $\exists\ y \in Q$ s.t. $xy = 1$

False ($x=0$)

ex: $\forall\ x \in Q^*$ $\exists y \in Q$ s.t $xy = 1$

True (every rational has a reciprocal except 0)

6/21/20:

* $\exists\ x \in N^*$ s.t $x^2 - x = 0$ → True

* $\exists!\ x \in N^*$ s.t $x^2 - x = 0$ → True ($x=1$)

Important * $\exists\ y \in Q^*$ s.t $\forall\ x \in Q^*$ ~~we~~ have $yx = 1$ → False! (exists a y where $yx = 1$ for every x)

* $\forall x \in Q^*$, $\exists\ y \in Q^*$ s.t $xy = 1$ → True

or ~~∀*~~ $x \in Q^*$, $\exists y \in Q$ s.t $xy = 1$ → also True

→ means: exists a $y \in Q^*$ and same y multiplied with every x in $Q^* = 1$

→ the y depends on x

- $\exists\ y \in \mathbb{R}$ s.t $\forall\ x \in \mathbb{R}$ $x+y=x$ → true ($y=0$)
- $\exists!\ y \in \mathbb{R}$ s.t $\forall\ x \in \mathbb{R}$ $x+y=x$ → True

- $\exists\ y \in \mathbb{Z}_{10}$ s.t $2y \pmod{10} = 6$ → True ($y=\{3,8\}$)
- $\exists!\ y \in \mathbb{Z}_{10}$ s.t $2y \pmod{10} = 6$ → False (2 solutions exist)

Logical Statements: If $\underset{S1}{\underline{\qquad}}$, then $\underline{S_2}$

ex: $\underbrace{\text{If}}_{\text{ignore}}$ $\underbrace{1+1=3}_{\text{read } S_1}$, $\underbrace{\text{then}}_{\text{ignore}}$ $\underbrace{\sqrt{2} \text{ is rational}}_{\text{read } S_2}$

↓

$\underbrace{T/F?}_{F}$ so S_2 does not matter if T or F

Rules:
- If (F), then (S_2) (not does matter) → $\boxed{\text{True}}$ (for whole statement)
- If S_1, then S_2 where (T), (T) so the whole statement is $\boxed{\text{true}}$
- If S_1, then S_2 where (T), (F) so the whole statement is $\boxed{\text{false}}$.

ex: If $\underbrace{\sqrt{2} \text{ is irrational}}_{\text{True}}$, then $\underbrace{3+2=8}_{\text{False}}$ → (False) so

ex: S_1 iff S_2: T only if both S_1, S_2 (True) or both S_1, S_2 (False)

ex: $\underbrace{1+1=3}_{F}$ iff $\underbrace{n^2+1=0 \text{ has a real solution}}_{F}$: → true so ex: → $\underbrace{\text{The temp. in Dubai now is } 42°C}_{\textcircled{T}}$ iff $\underbrace{\text{it is snowing in Sharjah}}_{\textcircled{F}}$:

so ⟶ $\boxed{\text{False}}$

ex: $\underbrace{\sqrt{2} \text{ is irrational}}_{\textcircled{T}}$ iff $\underbrace{\sqrt{17} \text{ is irrational}}_{\textcircled{T}}$ ⟶ $\boxed{\text{True}}$
so

AND/OR:

- $\underset{\substack{\downarrow \\ \text{AND}}}{S_1 \wedge S_2}$: T iff both $\textcircled{S_1}$, $\textcircled{S_2}$ are $\boxed{\text{true}}$.

- $\underset{\substack{\downarrow \\ \text{OR}}}{S_1 \vee S_2}$: T iff at least 1 of them is $\boxed{\text{true}}$.

ex: Notation: $a \wedge b$, $a \cdot b$ → both mean a and b
$a \vee b$, $a + b$ → both mean a or b

Truth Table:
Show that:

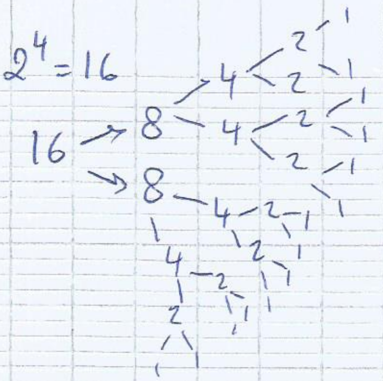
$$\overline{(a+b)} + c \equiv (c+\bar{a})(c+\bar{b})$$

# variables = 3
so 2^3 different strings (combinations of 0s, 1s)
= 8 → 4 1s
↘ 4 0s

a	b	c
1	0	1
1	0	0
1	1	0
1	1	1
0	1	0
0	1	1
0	0	1
0	0	0

For 4 variables:

$2^4=16$

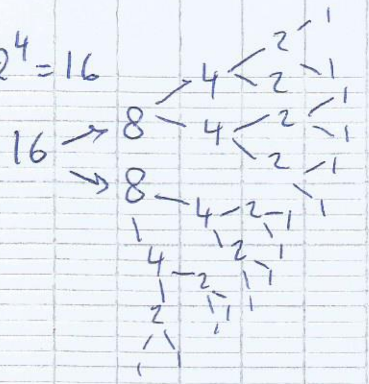


a	b	c	d
1	0	1	0
1	0	1	1
1	0	0	1
1	0	0	0
1	1	0	1
1	1	0	0
1	1	1	0
1	1	1	1
0	1	0	1
0	1	0	0
0	1	1	0
0	1	1	1
0	0	1	0
0	0	1	1
0	0	0	1
0	0	0	0

For 4 variables:

a	b	c	d
1	0	1	0
1	0	1	1
1	0	0	1
1	0	0	0
1	1	0	1
1	1	0	0
1	1	1	0
1	1	1	1
0	1	0	1
0	1	0	0
0	1	1	0
0	1	1	1
0	0	1	0
0	0	1	1
0	0	0	1
0	0	0	0

$2^4 = 16$



x	y	$x+y = (x \vee y)$	$x \oplus y$
1	1	1	0
1	0	1	1
0	1	1	1
0	0	0	0

$x \oplus y$ is T (=1) iff the corresponding 2 digits are diff.

$$\left.\begin{array}{l} S_1 = 101011 \\ S_2 = 111001 \end{array}\right\} S_1 \oplus S_2 = 010010$$

6/22/2021

Logical AND, OR, Exclusive OR.

Notation:

$\wedge$ (and) $\cdot$

V (OR) +

(Exclusive OR), $\oplus$

1 -> on, True

0 -> off, False

Truth Table:

x	y	$xy = (x \wedge y)$
1	1	1
1	0	0
0	1	0
0	0	0

Q1: Use truth table to convince me that $\overline{(x+y)} = \bar{x} \cdot \bar{y}$ or $\overline{(x \vee y)} = \bar{x} \wedge \bar{y}$

x	y	$\bar{x}$	$\bar{y}$	$\overline{(x+y)}$	$\bar{x} \cdot \bar{y}$
1	1	0	0	0	0
1	0	0	1	0	0
0	1	1	0	0	0
0	0	1	1	1	1

thus $\overline{(x+y)} = \bar{x} \cdot \bar{y}$ is true

Q_2: Use the Truth Table to show $A \cdot (B+C) = A \cdot B + A \cdot C$

A	B	C	B+C	A.B	A.C	A.(B+C)	A.B + A.C
1	1	1	1	1	1	1	1
1	1	0	1	1	0	1	1
1	0	1	1	0	1	1	1
1	0	0	0	0	0	0	0
0	1	1	1	0	0	0	0
0	1	0	1	0	0	0	0
0	0	1	1	0	0	0	0
0	0	0	0	0	0	0	0

thus $A.(B+C) = A \cdot B + A \cdot C$ is true

~~Q_3~~ $n = 50$ $\phi(n) = \text{phi}(n)$

Q_1 How many positive integers between $1 \rightarrow 50$ s.t: $\gcd(\text{integer}, 50) = 1$?

Q_2: $n = 10$, same question above↑.

for $n = 10$, $1, 3, 7, 9$

- $\phi(n)$ is the answer to such questions.

* Def: a, b are relatively prime iff $\gcd(a,b) = 1$.

Q. Let n be a positive integer. How many numbers between 1 and n that are relatively prime to n. ($\gcd(\text{number}, n) = 1$)?

S. → $\phi(n)$

How to Find $\phi(n)$:

ex: $n = 100$, find $\phi(100)$:

step 1: Write n as product of primes

thus $n = 2 \times 50 = 2 \times 2 \times 25 = 2 \times 2 \times 5 \times 5 = \underbrace{2^2 \times 5^2}$ → prime factorization of 100.

step 2: $\phi(100) = (2-1)2^1 \times (5-1)5^1$

$= 2 \times 20 = \boxed{40}$ → there are 40 numbers b/w 1→100 that are relatively prime with 100 ex: $n=10$

$10 = 2^1 \times 5^1$

$\phi(10) = (2-1)\,2^0 \times (5-1)\,5^0$

$= 1 \times 4 = \boxed{4}$

<u>Know:</u> $n = q_1^{\alpha_1} \times q_2^{\alpha_2} \dots \times q_k^{\alpha_k}$ s.t

the q_i's are distinct prime

<u>Then:</u> $\phi(n) = (q_1 - 1)\,q_1^{(\alpha_1 - 1)} \times (q_2 - 1)\,q_2^{(\alpha_2 - 1)} \dots \times (q_k - 1)\,q_k^{(\alpha_k - 1)}$

<u>ex:</u> $n = 245$, Find $\phi(245)$:

$245 = 5 \times 49 = 5 \times 7 \times 7 = 5^1 \times 7^2$

$\phi(245) = (5-1)\,5^0 \times (7-1)\,7^1$

$= 4 \times 42 = \boxed{168}$

Q. ~~ex~~: Let $n \geq 2$ be a positive integer, and $d \mid n$. How many numbers between 1 and n s.t. $\gcd(\text{number}, n) = d$?

S. $\phi\left(\frac{n}{d}\right)$ <u>Note:</u> $\left[\phi\left(\frac{n}{d}\right) \neq \phi(n) \div \phi(d)\right]$

<u>ex:</u> $n = 68$, $\underline{d = 2}$, $d \mid 68$? yes:

Q. Find how many numbers between 1 and 68 satisfy $\gcd(\text{number}, 68) = 2$?

S. ~~First~~: Find $\frac{n}{d} = \frac{68}{2} = 34$

Answer is $\phi(34)$:

$34 = 2 \times 17 = 2^1 \times 17^1$

$\phi(34) = (2-1)\,2^0 \times (17-1)\,17^0$

$= 1 \times 16 = \boxed{16}$

Note:

If $\phi(q)$ where q is prime, then $\phi(q) = (q-1) \times q^0 = \boxed{q-1}$

<u>ex:</u> $\phi(11) = (11-1)\,11^0 = \boxed{10}$

Fermat Theorem:

- q is prime, $a \in \mathbb{Z}^+$, s.t $q \nmid a$, then $a^{q-1} \pmod{q} = 1$

ex: $q = 5$, $a = 8$

$5 \nmid 8$

so $8^{5-1} \pmod 5$

$= 8^4 \pmod 5 = 4096 \pmod 5 = 1$ ✓ true

Euler generalized Fermat's result:

Euler: Let $a, n \in \mathbb{Z}^+$ s.t $\gcd(a,n) = 1$. Then $a^{\Phi(n)} \pmod n = 1$

or $n^{\Phi(a)} \pmod a = 1$

ex: $n = 100$, $a = 33$

$\gcd(33, 100) = 1$

$33^{\Phi(100)} \pmod{100} = 1$

$\hookrightarrow 33^{40} \pmod{100} = 1$

ex: $n = 77$, $a = 30$

$\gcd(77, 30) = 1$

$30^{\Phi(77)} \pmod{77} = 1 = 77^{\Phi(30)} \pmod{30}$

$\hookrightarrow 30^{60} \pmod{77} = 1$

Practice Q1: Show $x + (y \cdot z) = (x+y) \cdot (x+z)$, Use truth table:

x	y	z	y.z	x+y	x+z	(x+y).(x+z)	x + (y.z)
1	1	1	1	1	1	1	1
1	1	0	0	1	1	1	1
1	0	1	0	1	1	1	1
1	0	0	0	1	1	1	1
0	1	1	1	1	1	1	1
0	1	0	0	1	0	0	0
0	0	1	0	0	1	0	0
0	0	0	0	0	0	0	0

thus statement is true.

Q_2: $S_1 = 1011110$

$S_2 = 1010010$

Find $S_1 \oplus S_2$:

$= 0001100$

Q_3: Find $\Phi(310)$:

$310 = 2 \times 155 = 2^1 \times 5^1 \times 31^1$

$\Phi(310) = (2-1)2^0 \times (5-1)5^0 \times (31-1)31^0$

$= 1 \times 4 \times 30 = \boxed{120}$

Q_4: Find $\Phi(96)$:

$96 = 2 \times 48 = 2 \times 2 \times 24 =$

$2 \times 2 \times 2 \times 12 = 2 \times 2 \times 2 \times 2 \times 2 \times 3$

$= 2^5 \times 3^1$

$\Phi(96) = (2-1)2^4 \times (3-1)3^0 = \boxed{32}$

Q_5: $\Phi(422)$:

$422 = 2^1 \times 211^1$

$\Phi(422) = (2-1)2^0 \times (211-1)2^0$

$= 1 \times 210 = \boxed{210}$

Q_7: $3^{43} \pmod{100}$: $\gcd(3,100) = 1$ ✓

(Hint: $3^{a+b} \pmod n = [3^a \pmod n \times 3^b \pmod n$

all mod n.

$3^{43} \pmod{100} = [3^{40} \pmod{100} \times 3^3 \pmod{100}] \pmod{100}$

where $40 = \Phi(100)$:

So $[\underbrace{3^{40} \pmod{100}}_{1} \times \underbrace{27 \pmod{100}}_{27}] \pmod{100}$

$(1 \times 27) \pmod{100}$

$= \boxed{27}$

Q_8: $5^{602} \pmod 7$: $\rightarrow \gcd(5,7) = 1$ ✓

$= \Big[\underbrace{[5^6 \pmod 7]}^{100} \times [5^2 \pmod 7] \Big] \underbrace{\pmod 7}$

makes sure everything is < 7

$= [1^{100} \times 25 \pmod 7] \pmod 7$

$= (1 \times 4) \pmod 7$

$= \boxed{4}$

Q_6: $n = 217$, $d = 7$, How many numbers < 217 satisfy gcd(number, 217) = 7?

$\frac{n}{d} = \frac{217}{7} = 31$

$\Phi(31) = (31-1)31^0$

$= \boxed{30}$

6/23/2021

For:

$\gcd(a,n)=1$

Find:

$a^m \pmod n$

1) $\Phi(n)$

2) $m = q \times \Phi(n) + r$ where $0 \leq r < \Phi(n)$

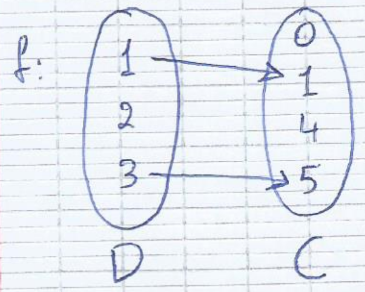
3) so $a^m \pmod n = a^r \pmod n$

Functions:

Definition: $\underset{\substack{\downarrow \\ \text{function}}}{f} : \underset{\substack{\downarrow \\ \text{domain} \\ \Downarrow \\ \text{input}}}{D} \longrightarrow \underset{\substack{\searrow \\ \text{co-domain} \\ \Downarrow \\ \text{output}}}{C}$

$\Downarrow$

$\forall\, x \in D,$ ~~f(x)~~ $\underbrace{\exists!}_{\text{one and only one } y \in C.}\ y \in C$ s.t. $f(x) = y.$

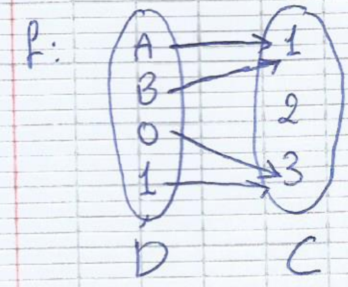


$f(1)=1$ $f(2)=$ undefined

$f(3)=5$

Not a function!

(not every x has a y)



$f(A)=1$

$f(B)=1$

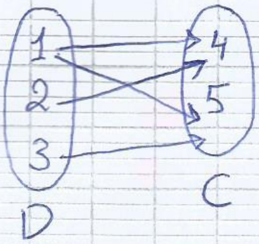
$f(0)=3$

$f(1)=3$

This is a function!

(every x has 1 unique y).

f:



$f(1) = 4$ or 5

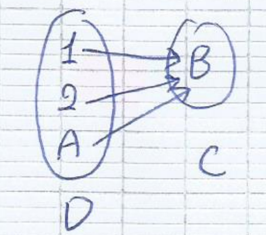
$f(2) = 4$

$f(3) = 5$

NOT a function! (It is a Relation)

(1 has more than 1 y)

f:



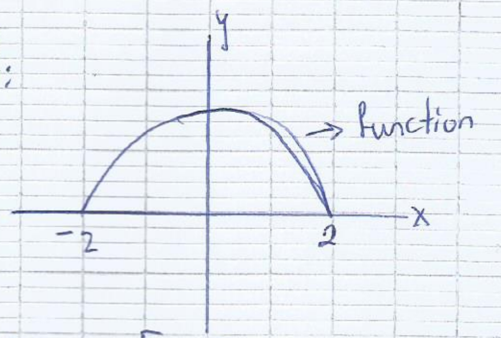
$f(1) = B$

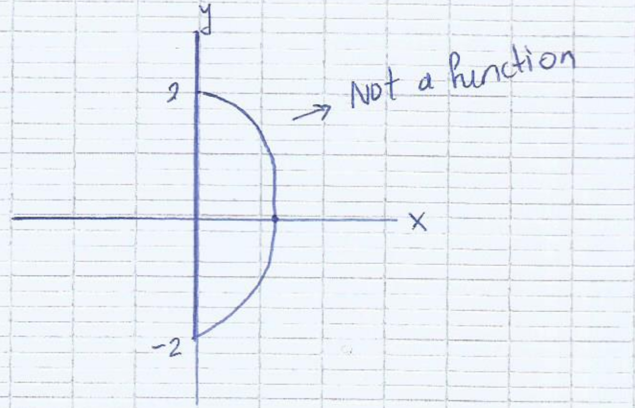
$f(2) = B$

$f(A) = B$

Function! (called a constant function)

f:



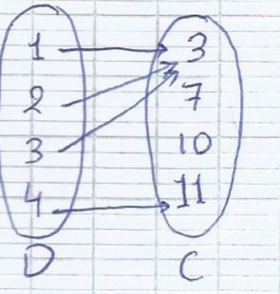


Domain: $[-2, 2]$

~~x in terms of y~~

Range:

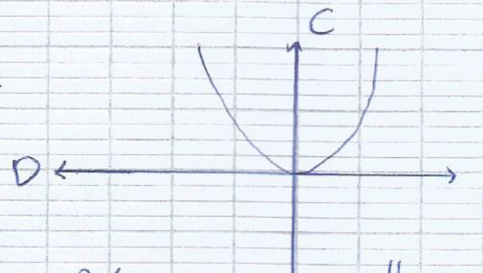
f:



$\text{Range}(f) = \{3, 11\} \neq C$

* Range (f) "lives" inside C

ex: $f(x) = x^2$



D: $\mathbb{R}$

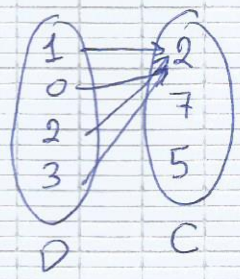
R: $[0, \infty)$ → $0 \leq y < \infty$ → all possible outputs

* $y=x^3$

$f: \underbrace{x\text{-axis}}_{D} \longrightarrow \underbrace{y\text{-axis}}_{C}$

Range(f) = y-axis = C

* f:



Range = {2}

so R ≠ C

because C = {2, 7, 5}

__Definition:__ A function is onto (Surjective) iff R=C.

__ex:__ $y=x^3=f(x) \longrightarrow$ onto since $R=C$

__ex:__ $f: \underbrace{\mathbb{R}}_{x\text{-axis}} \longrightarrow \underbrace{y\text{-axis}}_{\mathbb{R}}$

$f(x)=x^2 \longrightarrow$ f is <u>not onto</u>

ex: $f: \underbrace{\mathbb{R}}_{x\text{-axis}} \longrightarrow \underbrace{[0,\infty)}_{+ve\ y\text{-axis}}$

$f(x)=x^2 \longrightarrow$ f <u>is onto</u> $(C=[0,\infty)=x^2)$

__ex:__ $f: \mathbb{R} \longrightarrow [3,\infty]$

$\underbrace{f(x)=x^2}_{\text{Not a function!}}$

Not every x has a y:

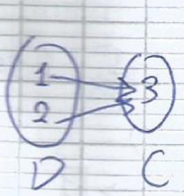
ex: $f(0)=0,\ f(1)=1,\ f(-1)=1$

__Definition:__ A function is 1-1 (one to one) if $\forall y$ in Range(f)

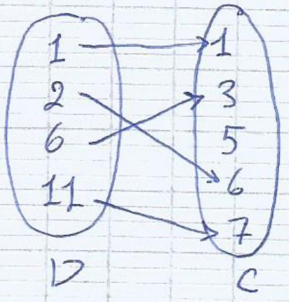
* $\underbrace{\exists \text{ one and only one}}_{\exists!}$ x in domain s.t. $f(x)=y$.

Meaning: the output of any 2 diff. elements in domain is 2 diff. elements in the co-domain

ex:

f:  → Not 1-1.

ex

f: 

It is a function

Range = $\{1, 3, 6, 7\}$
$\neq C$

So f is not onto

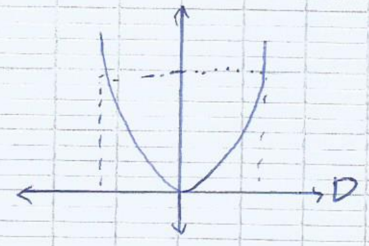
f is 1-1 (every y in range has 1 x in domain)

$f: \underbrace{\mathbb{R}}_{x\text{-axis}} \to \underbrace{[0, \infty)}_{+ve\ y\text{-axis}}$

$f(x) = x^2$ → this is a function

f is onto,

f is not 1-1. ex: $y = 4$ → $x = 2$, → $x = -2$



- vertical-line test
  ↳ proves if it's a function
- horizontal-line test
  ↳ proves if it's 1-1

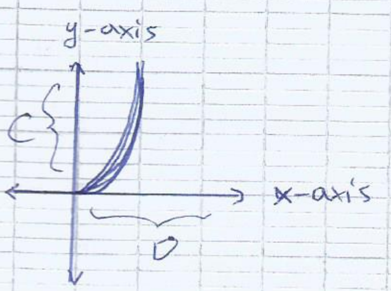
Practice Q:

Q1: $f: [0, \infty) \to [0, \infty)$

$f(x) = x^2$

Is f 1-1? Yes

Is f onto? Yes



Definition: If a function f is 1-1 and onto, we say f is a bijective function → (invertible)

Result: A function f is invertible (f^{-1} exists) iff it is bijective.

6/24/2021

- A function f has an inverse iff f is 1-1 and onto. (bijective)

Assume f is invertible

Thus f^{-1} (inverse of f) exists ⟹ $(f \circ f^{-1})(x) = x$

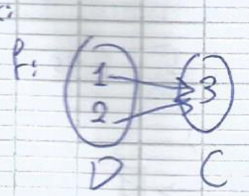
↓ composition

↳ $f(f^{-1}(x)) = x$

↳ does not mean $\frac{1}{f}$.

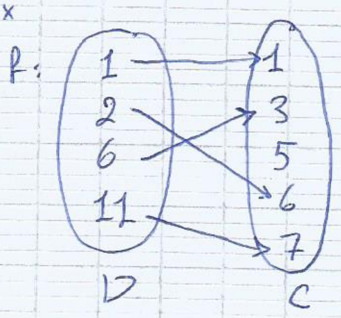
Meaning: the output of any 2 diff. elements in domain is 2 diff. elements in the co-domain

ex:



→ Not 1-1.

ex



It is a function

Range = $\{1, 3, 6, 7\}$

$\neq C$

So f is not onto

f is 1-1 (every y in range has 1 x in domain)

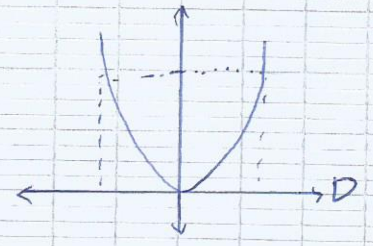
$f: \underbrace{\mathbb{R}}_{x\text{-axis}} \rightarrow \underbrace{[0, \infty)}_{+ve\ y\text{-axis}}$

$f(x) = x^2$ → this is a function

f is onto,

f is not 1-1. ex: $y=4 \rightarrow x=2$

$\rightarrow x=-2$



- vertical-line test
  ↳ proves if it's a function
- horizontal-line test
  ↳ proves if it's 1-1

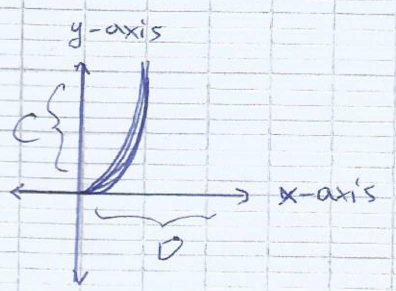
Practice Q:

Q_1: $f: [0, \infty) \rightarrow [0, \infty)$

$f(x) = x^2$

Is f 1-1? Yes

Is f onto? Yes



Definition: If a function f is 1-1 and onto, we say f is a bijective function ⇒ (invertible)

Result: A function f is invertible (f^{-1} exists) iff it is bijective.

6/24/2021

- A function f has an inverse iff f is 1-1 and onto. (bijective)

Assume f is invertible

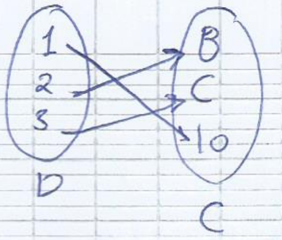
Thus f^{-1} (inverse of f) exists ⇒ $(f \circ f^{-1})(x) = x$

↓ composition

↳ $f(f^{-1}(x)) = x$

↳ does not mean $\frac{1}{f}$.

ex: f:

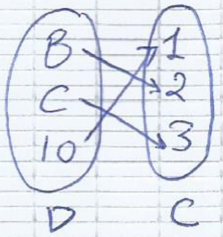


f is 1-1 and onto

f is bijective

f^{-1} exists: Find f^{-1}:

f^{-1}:



$(f \circ f^{-1})(B) = f(f^{-1}(B)) = f(2) = B$ ✓

$(f \circ f^{-1})(10) = f(f^{-1}(10)) = f(1) = 10$ ✓

$(f^{-1} \circ f)(3) = f^{-1}(f(3)) = f^{-1}(C) = 3$ ✓

$(f \circ f^{-1})(2) = f(f^{-1}(2)) =$ undefined

Note: $(f \circ f^{-1}) \to$ Domain of f^{-1} (input)

↳ Codomain of f (output)

~~(Domain of f)~~

$(f^{-1} \circ f) \to$ Domain of f (input)

↳ Codomain of f^{-1} (output)

f

ex: $f: \mathbb{R} \to [0,\infty)$

$f(x) = e^x$

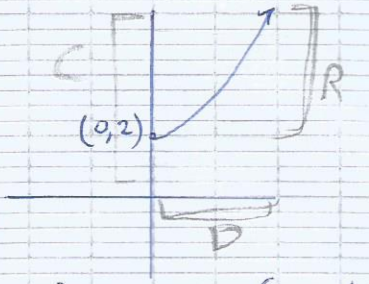
f is 1-1, f is NOT onto.

[0,∞)

ex: $f: \cancel{\mathbb{R}} \to [1,\infty)$

$f(x) = x^2+2$

Does f^{-1} exist?



f is 1-1: (by H.L.T)

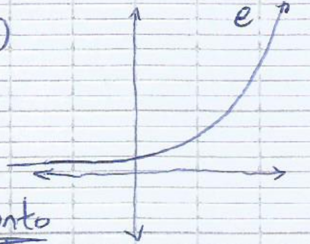
Range $= [2,\infty) \neq C$

f is not onto

(for every y in codomain, say $y = b$. Then $y = b$ intersect the curve.)

ex: $f: \underset{D}{\mathbb{R}} \to \underset{C}{(0,\infty)}$

$f(x) = e^x$



f is 1-1 and onto

(By H.L.T)

(By V.L.T)

ignore ↳ [select y in the ~~Co-domain~~ (range) and draw vertical line at y, then the line intersects the ~~curve~~ domain at exactly 1 pt.]

Find f^{-1} for $f(x) = e^x$:

$f^{-1}: (0,\infty) \to \mathbb{R}$.

now $y = e^x$

1) substitute y for x & x for y

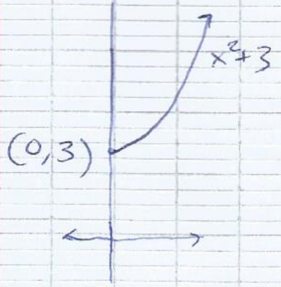
$x = e^y$

$\ln x = y \to f^{-1}$.

ex: $f:[0,\infty)\to[3,\infty)$

$f(x)=x^2+3$

Is f invertible? (Does f^{-1} exist?)



f is 1-1 by H.L.T.

Range $=[3,\infty)=C\to$ onto

so f is bijective (f^{-1} exists)

$f^{-1}:[3,\infty)\to[0,\infty)$

f^{-1}: $y=x^2+3$

$x=y^2+3$

$y^2=x-3$

$y=\pm\sqrt{x-3}$

Co-domain $[0,\infty)\to f^{-1}$

since ~~[illegible]~~ y is in Range ~~[illegible]~~

then we choose $\boxed{y=+\sqrt{x-3}}\to f^{-1}$.

Least Common Multiple:

(remove repeated common factors)

ex $\text{LCM}[30,25]=\dfrac{30\times25}{\gcd(30,25)}$

$=\dfrac{750}{5}=\boxed{150}$

ex: $\text{LCM}[24,13]=\dfrac{13\times24}{\gcd(13,24)}$

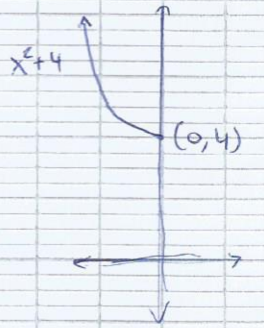
$=\dfrac{312}{1}=\boxed{312}$

ex: $\text{LCM}[24,18]=\dfrac{24\times18}{\gcd(24,18)}$

$=\dfrac{432}{6}=\boxed{72}$

ex: $f:(-\infty,0]\to[4,\infty)$

$f(x)=x^2+4$



f is 1-1 (by H.L.T)

Range: $[4,\infty)=C\to$ onto

$f^{-1}:[4,\infty)\to(-\infty,0)$

f^{-1}: $y=x^2+4$

$x=y^2+4$

$y^2=x-4$

$y=\pm\sqrt{x-4}$

since y is in co-domain ~~[illegible]~~ of f^{-1} $(-\infty,0)$

we choose $\boxed{y=-\sqrt{x-4}}$

Q: $\underset{D}{f:\{1,2,3\}}\to\underset{C}{\{1,2,3\}}$

$D=C$

$f=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\to$ codomain $=$ range

$1\to3,\ 2\to1,\ 3\to2$

f: 1-1, onto

Find smallest positive integer n s.t $f^n=I$

$\underbrace{(f\circ f\ldots\circ f)}_{n\text{ times}}$ $I\to$ Identity map

$f=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ $I=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$

$f=(1\ 3\ 2)\to$ the smallest positive integer where $f^n=I$ is $\boxed{n=3}$.

s.t $(f\circ f\circ f)(1)=1$, $(f\circ f\circ f)(2)=2$ ... etc.

ex: $f: \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 2 & 1 & 6 & 5 \end{pmatrix} \begin{matrix} \to \text{Domain} \\ \to \text{Range} \end{matrix}$

Find smallest +ve integer n

$$\text{s.t } \underbrace{f^n}_{(f \circ f \circ \dots f)} = I = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$$

$$(\underbrace{f \circ f \circ \dots f}_{n \text{ times}})$$

$$f = \underbrace{(1,3,2,4)}_{4\text{-cycle}} \circ \underbrace{(5,6)}_{2\text{-cycle}}$$

smallest +ve integer $= LCM(4,2)$

$$= \frac{4 \times 2}{\gcd(4,2)} = \frac{8}{2} = \boxed{4}$$

ex: Imagine f:

$$f = \underbrace{(1\ 2\ 3\ 4\ 5\ 6)}_{6\text{-cycles}} \circ \underbrace{(7\ 8\ 9\ 10)}_{4 \text{ cycles}}$$

$$n = LCM(6,4) = \frac{6 \times 4}{\gcd(6,4)} = \frac{24}{2} = \boxed{12}$$

6/28/2021

Q. Find the smallest +ve integer n s.t $\underbrace{f^n}_{} = \underbrace{I}_{}$

$$\underbrace{f \circ f \dots \circ f}_{n \text{ times}} = \begin{pmatrix} 1 & 2 & 3 & \dots & 8 \\ 1 & 2 & 3 & \dots & 8 \end{pmatrix}$$

$$f: \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 5 & 1 & 3 & 7 & 8 & 6 & 2 \end{pmatrix}$$

$$\therefore f = \underbrace{(1\ 4\ 3)}_{3\text{-cycle}} \circ \underbrace{(2\ 5\ 7\ 6\ 8)}_{5\text{-cycle}}$$

$$n = LCM[3,5] = \frac{3 \times 5}{\gcd(3,5)} = \frac{15}{1} = \boxed{15}$$

Q.

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 2 & 5 & 6 \end{pmatrix} \begin{matrix} D \\ C \end{matrix}$$

Find least +ve integer s.t $f^n = I$.

it is understood without showing that 5-5 & 6-6:

$$f = \underbrace{(1\ 3)}_{2\text{-c}} \circ \underbrace{(2\ 4)}_{2\text{-c}} \boxed{\cancel{\circ (5) \circ (6)}}$$

so $n = LCM[2,2] = \boxed{2}$

ex: $f: \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 2 & 1 & 6 & 5 \end{pmatrix}$ → Domain / → Range

Find smallest +ve integer n

$$\text{s.t } \underbrace{f^n}_{(f\circ f\circ \ldots f)} = I = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$$

$(\underbrace{f\circ f\circ \ldots f}_{n \text{ times}})$

$$f = \underbrace{(1,3,2,4)}_{4\text{-cycle}} \circ \underbrace{(5,6)}_{2\text{-cycle}}$$

$$\text{smallest +ve integer} = LCM(4,2) = \frac{4\times 2}{gcd(4,2)} = \frac{8}{2} = \boxed{4}$$

ex: Imagine f:

$$f = \underbrace{(1\ 2\ 3\ 4\ 5\ 6)}_{6\text{-cycles}} \circ \underbrace{(7\ 8\ 9\ 10)}_{4 \text{ cycles}}$$

$$n = LCM(6,4) = \frac{6\times 4}{gcd(6,4)} = \frac{24}{2} = \boxed{12}$$

6/2~~7~~8/2021

Q. Find the smallest +ve integer n s.t $\underbrace{f^n}_{} = \underbrace{I}_{}$

$$\underbrace{f\circ f\ldots\circ f}_{n \text{ times}} = \begin{pmatrix} 1 & 2 & 3 & \ldots & 8 \\ 1 & 2 & 3 & \ldots & 8 \end{pmatrix}$$

$$f: \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 5 & 1 & 3 & 7 & 8 & 6 & 2 \end{pmatrix}$$

$$\therefore f = \underbrace{(1\ 4\ 3)}_{3\text{-cycle}} \circ \underbrace{(2\ 5\ 7\ 6\ 8)}_{5\text{-cycle}}$$

$$n = LCM[3,5] = \frac{3\times 5}{gcd(3,5)} = \frac{15}{1} = \boxed{15}$$

Q.

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 2 & 5 & 6 \end{pmatrix} \begin{matrix} D \\ C \end{matrix}$$

Find least +ve integer s.t $f^n = I$.

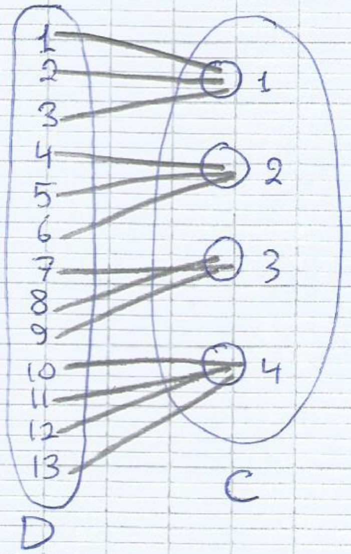
it is understood without showing that 5-5 & 6-6:

$$f = \underbrace{(1\,3)}_{2\text{-c}} \circ \underbrace{(2\,4)}_{2\text{-c}} \boxed{\cancel{\circ (5) \circ (6)}}$$

so $n = LCM[2,2] = \boxed{2}$

Pigeon Hole Principle:

Q. 13 pigeons and 4 holes.
At least m pigeon share the same hole. → Must be correct in all case
(Find the max value of m)

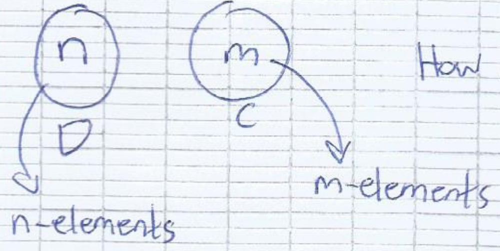


- At least 5 pigeon in the same hole is wrong
- At least 4 pigeon in the same hole in all cases.

In this example, there are $4^{13} = 67108864$ (possibilities) ~~of~~ or functions

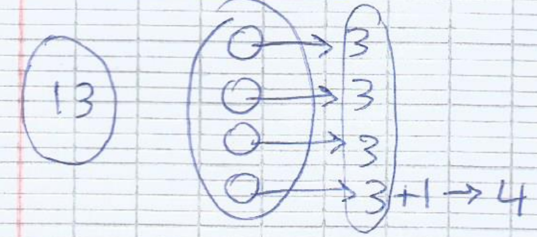
- Thus, At least 4 pigeons share the same hole is correct in all 4^{13} possibilitie

ex:



How many functions can we construct?
m^n different functions

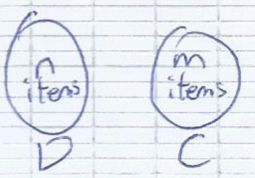
Fair Distribution



Know:

- Assume we want to distribute n items in m holes s.t $n > m$.
- At least k items share same hole is true for all possibilities (m^n) iff $k \leq \lceil \frac{n}{m} \rceil$ (max value of $k = \lceil \frac{n}{m} \rceil$).

Another Way:



We can construct m^n diff. functions. At least k elements in D share the same value in C iff $k \leq \lceil \frac{n}{m} \rceil$ (max value of k) = $\lceil \frac{n}{m} \rceil$

$\downarrow$

Ceiling Function: $\rightarrow$ round it up

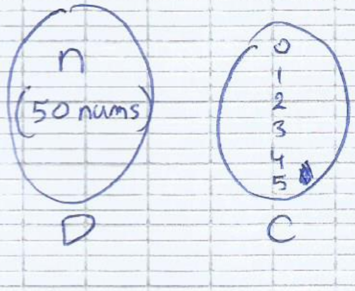
ex: $\lceil \frac{3}{2} \rceil = \lceil 1.5 \rceil$ = least integer $\geq 1.5 = 2$

ex: $\lceil \frac{5}{4} \rceil = \lceil 1.25 \rceil = 2$ ex: $\lceil \frac{13}{4} \rceil = \lceil 3.25 \rceil = 4$

ex: $\lceil \frac{37}{6} \rceil = \lceil 6.16 \rceil = 7$

Q. 50 positive integers:
At least $\underline{\underline{k}}$ numbers, say $n_1, n_2, \cdots, n_k$ satisfy
$n_1 \pmod 6) = (n_2 \bmod 6) = \ldots = n_k \pmod 6$
Find max value of k:

S. we view it as:

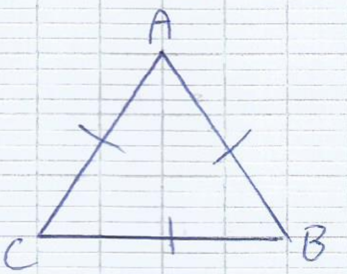


6^{50} possible functions

$k = \lceil \frac{50}{6} \rceil = \lceil 8.33 \rceil = 9$

If we choose 50 +ve integers, we are sure there are at $\underline{\text{least}}$ $\underline{\underline{9}}$ numbers, say $n_1, n_2, \ldots, n_9$ where:
$n_1 \pmod 6 = n_2 \pmod 6 = \ldots n_9 \pmod 6$.
_Statement is also true for any number less than 9 (k).

Q. Geometry:



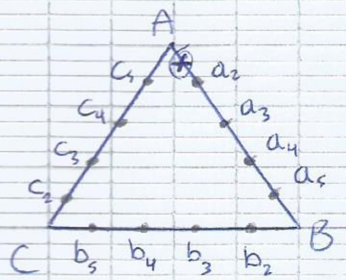
$|AB| = 1$ (length of AB)

Randomly: put points on the sides of $\triangle$. Find min # of points that we can 'put' on the sides of $\underline{\underline{\triangle}}$ s.t. at least there are 2 points, Q_1, Q_2 where distance $(Q_1, Q_2) \leq \frac{1}{5}$.

- Imagine the answer is 30:

If I put 30 points randomly on the sides of the $\triangle$, then I know for sure there are two points say Q_1, Q_2 s.t distance $(Q_1, Q_2) \leq \frac{1}{5} = \underline{20\text{ cm}}$ (let's say)

How to solve:



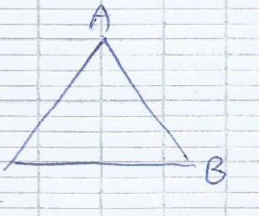
① start putting points exactly distance of $\frac{1}{5}$ so $|Aa_2| = \frac{1}{5}$, continue for other sides (split each side into 5 equal pieces)

② Total points $= (4 \times 3) = \underbrace{12}_{\text{"put"}}$

③ Since Question asks for strictly less than $\frac{1}{5}$, we need to place 1 point between any 2 points.

④ Thus, $12 + 1 = \underbrace{13}_{\text{"put"}}$ so at least 13 points are placed to ensure there are at least 2 points where (Q_1, Q_2) distance is $< \frac{1}{5}$.

Q. Find the min # of point s.t at least 2 points (Q_1, Q_2) distance $< \frac{1}{12}$.



S. $(12 - 1) \times 3 + 1$

$= (11 \times 3) + 1$

$= 33 + 1 =$ At least $\underline{34 \text{ points}}$

6/28/2021

Sets:

Notation: $\{\ \}$

ex: $B = \{3, 4, \phi, \{A\}\}$ → order is not important

B is a set, $3, 4, \phi, \{A\}$ are elements of B.

- 4 is an element of B
- $\{A\}$ is an element of B
- $3 \in B$ ✓
- $\{A\} \in B$ ✓ * $\in$ = "is an element of "
- $4 \in B$ ✓

ex: $A = \{3, \{2\}, 2, 5, \{3,5\}, 7\}$

elements of A: $3, \{2\}, 2, 5, \{3,5\}, 7$

- $\{3,5\} \in A$ ✓ - $3 \in A$ ✓
- $\{3\} \in A$ X - $2 \in A$ ✓

Relation between Sets:

ex: $F = \{\ \} \subseteq H = \{\ \}$

* where $\subseteq$ = "is a subset (each element of 'F' is an element of 'H') or 'F' is equal to 'H'

$F = \{\ \} \subset H = \{\ \}$

* where $\subset$ = " is a (proper) subset of... (each element of 'F' is an element of 'H') but $F \neq H$ (not necesarily).

ex: $B = \{ \{3,A\}, A, 3, \{5,7\}, 5, 7, 0 \}$

- $\{3,A\} \in B$ ($\{3,A\}$ is an element of B) ✓
- $\{3,A\} \subset B$ (3 and A are elements of B so $\{3,A\}$ is a subse ✓
- $\{\{3,A\}\} \subset B$ ($\{3,A\}$ is an element of B so $\{\{3,A\}\}$ is a subset) ✓

* Phi: $\emptyset = \{ \}$ (empty set) is always $\subset$ (a subset) of any set.

ex: $A = \{ \{3\}, 3, 5, B, \{B, 3\}, \emptyset \}$

- $\{\{3\}, 3\} \subset A$ ($\{3\}$ and 3 are elements of A so $\{\{3\},3\}$ is a subset of A) ✓
- $\{3,5\} \subseteq A$ (3 and 5 are elements of B so $\{3,5\}$ is a subset) ✓
  ($\{3,5\}$ is not equal A but statement is still true)
- $\emptyset \in A$ ($\emptyset$ is an element of A) ✓
- $\{\emptyset\} \subset A$ ($\emptyset$ is an element of A so $\{\emptyset\}$ is a subset of A} ✓

* Power Set: Let A be a set. The set of all subsets of A is called the power set of A.

ex: $A = \{0,1,2\}$. Find p(A) "power set of A"

$p(A) = \{ \emptyset, \{0,1,2\}, \{0\}, \{1\}, \{2\}, \{0,1\}, \{0,2\}, \{1,2\} \}$

- $\{0,2\} \subset p(A)$ (0 and 2 are not elements of power set of A) X

- $\{0,2\} \subset A$ (0 and 2 are elements of A so $\{0,2\}$ is a subset of A) ✓

- $\{0,2\} \in p(A)$ ($\{0,2\}$ is an element of $p(A)$) ✓

- $\{\phi\} \subset p(A)$ (ϕ is an element of $p(A)$ so $\{\phi\}$ is a subset of $p(A)$) ✓

* For Power Sets:

- Each subset of A is an element of $p(A)$.
- # of the elements in $p(A) = 2^n$ where $n =$ # of elements in set A.

ex: $A = \{2, 4, \{D\}, 7\}$

$p(A)$ will have $2^4 = 16$ elements.

- $\{D\} \in p(A)$ ($\{D\}$ is not an element of $p(A)$). X
- $\{\{D\}\} \in p(A)$ ($\{\{D\}\}$ is an element of $p(A)$) ↑ ✓
- $\{D\} \in A$ ($\{D\}$ is an element of A) ✓
- $\{2\} \in p(A)$ ($\{2\}$ is an element of $p(A)$) ✓

Summary:

- $B \in p(A)$ is true iff B is a subset of A (elements of B are elements of A).
- $H = \{\ \} \subseteq p(A)$ is true iff each element in H is a subset of set A.

ex: $A = \{2, \{2\}, \{F\}, 0\}$

- $\{2\} \in p(A)$ ($\{2\}$ is an element of $p(A)$) ✓ it is a subset of A.

- $H = \{2, \{2\}\} \subset p(A)$ (2 is not an element in $p(A)$, $\{2\}$ is an element of $p(A)$, so whole statement False) X

- $\{0,2\} \in p(A)$ ($\{0,2\}$ is an element of $p(A)$) ✓

- $\{\phi, \{F\}\} \in p(A)$ ($\{\phi, \{F\}\}$ is not an element of $p(A)$ since ϕ is not an element of A) X

* Universal Sets: (the main set)

ex: $A = \{1,2,3\}$ $B = \{5,6,3,2,1\}$ $U = \{1,3,2,5,6,10,F,0\}$

* where A and B are subsets of universal set U.

- $A \cup B = \{1,2,3,5,6\}$ - $A \cap B = \{1,2,3\}$

'A' union 'B' 'A' intersection 'B'

* Union is the combination of elements between sets with no repetitio
* Intersection is the set of common elements between sets.

- $\bar{A} = U - A = \{5,6,10,F,0\}$

Complement of 'A'.

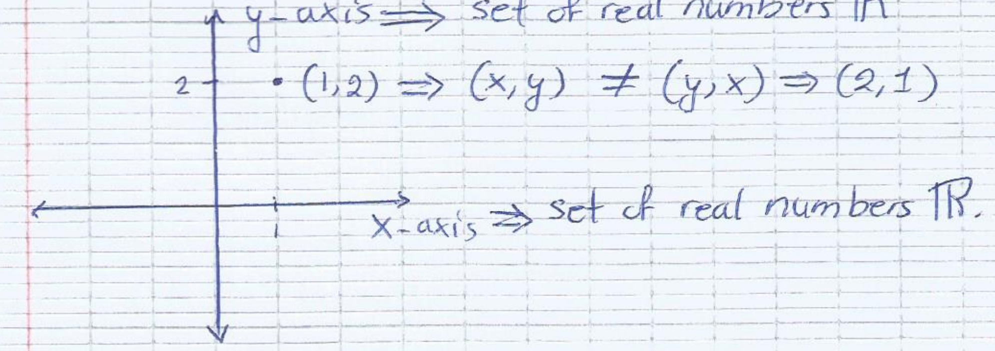
* Complement is the ~~set~~ universal set excluding the elements of 'A'.

ex: $A = \{3,0,1,2\}$ $B = \{2,1,F,5,7,8\}$

* A-B (set of elements that are in A but not in B)
- $A - B = \{3,0\}$

- B-A (set of elements in B but not in A)
- $B - A = \{F,5,7,8\}$

Cartesian Product:



y-axis ⇒ set of real numbers $\mathbb{R}$

• $(1,2) \Rightarrow (x,y) \neq (y,x) \Rightarrow (2,1)$

x-axis ⇒ set of real numbers $\mathbb{R}$.

Product: $\mathbb{R} \times \mathbb{R}$

ex:

$A = \{1,2,3\}$ $B = \{2,5\}$

Q. Find AXB:

Note: order is important, $A \times B = \{(a,b) \text{ where } a \in A, b \in B\}$

$A \times B = \{(1,2), (1,5), (2,2), (2,5), (3,2), (3,5)\}$

Each element of AXB is an ordered pair (a,b) s.t. $a \in A$, $b \in B$.

- $(5,1) \in A \times B$ is False
- $(1,5) \in A \times B$ is True
- $(5,1) \in B \times A$ is True

} order matters!

6/29/2021

ex $A = \{1,3,4\}$ $B = \{a,c,5,6\}$

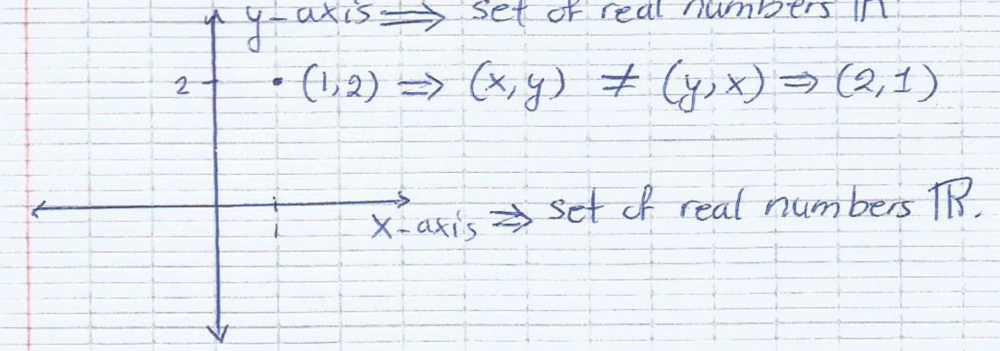
$A \times B = \{(a,b) \mid a \in A, b \in B\}$

AXB need not = BXA

$A \times B = \{(1,a), (1,c), (1,5), (1,6), (3,a), (3,c), (3,5), (3,6), (4,a),$
$(4,c), (4,5), (4,6)\}$

- $(c,1) \in A \times B$ → False
- $\{(1,5), (a,3)\} \subset A \times B$ → False
  ($(a,3)$ is not an element)
  $(a,3) \notin A \times B$

Cartesian Product:


y-axis ⇒ set of real numbers ℝ
2
• (1,2) ⇒ (x,y) ≠ (y,x) ⇒ (2,1)
1
x-axis ⇒ set of real numbers ℝ.

Product: $\mathbb{R} \times \mathbb{R}$

ex:

$A = \{1,2,3\}$ $B = \{2,5\}$

Q. Find $A \times B$:

Note: order is important, $A \times B = \{(a,b) \text{ where } a \in A, b \in B\}$

$A \times B = \{(1,2), (1,5), (2,2), (2,5), (3,2), (3,5)\}$

Each element of $A \times B$ is an ordered pair (a,b) s.t. $a \in A, b \in B$.

- $(5,1) \in A \times B$ is False
- $(1,5) \in A \times B$ is True
- $(5,1) \in B \times A$ is True

order matters!

6/29/2021

ex $A = \{1,3,4\}$ $B = \{a,c,5,6\}$

$A \times B = \{(a,b) \mid a \in A, b \in B\}$

$A \times B$ need not $=$ $B \times A$

$A \times B = \{(1,a), (1,c), (1,5), (1,6), (3,a), (3,c), (3,5), (3,6), (4,a), (4,c), (4,5), (4,6)\}$

- $(c,1) \in A \times B$ → False
- $\{(1,5), (a,3)\} \subset A \times B$ → False

((a,3) is not an element)

$(a,3) \notin A \times B$

ex: $A \times A$ where $A = \{1,2,3\}$

$A \times A = \{(1,1), (1,2), (1,3), (2,1), (2,2), (2,3), (3,1), (3,2), (3,3)\}$

Let $B = A \times A$, $p(B)$ has 2^9 elements.

Notation:

Let F be a set:

$|F|$ (Cardinality of F) = # of elements in F

ex: $A = \{2, 3, \{5\}, 7\}$

$|A| = 4$

$|p(A)| = 2^4 = 16$

ex: If A, B are sets then:

$|A \times B| = |A||B|$

$$\begin{tikzcd}
\text{Cardinality} \arrow[r] \arrow[d] & \text{Countable} \curvearrowright \text{ex: } \mathbb{Z}, \mathbb{Z}^+, \mathbb{Q}, \mathbb{N} \\
\text{Uncountable} \curvearrowright \text{ex: } \mathbb{R} &
\end{tikzcd}$$

Fact: Every finite set is countable

ex:

$A = \{a, b, c, 1, 5, 7\}$ with 6 elements.

ex: $|\mathbb{N}| = |\mathbb{Q}| = |\mathbb{Z}^+| = |\mathbb{Z}| = \infty$

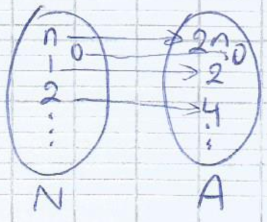
ex: $|\mathbb{R}| = \infty$ but not $= |\mathbb{N}| \ldots$

Definition: A, B $f: A \to B$ is a bijective function (1-1, onto) implies $|A| = |B|$

ex: $A = \{\overset{0,}{\curvearrowright} 2, 4, 6, 8, 10, 12, \ldots\}$ = set of all even integers

$f: \mathbb{N} \to A$

$f(n) = 2n$



f is 1-1 and onto so f is bijective

Thus $|\mathbb{N}| = |A|$

- We show f is 1-1 ($n_1, n_2 \in N$)

Assume $f(n_1) = f(n_2)$

$\boxed{\text{show } n_1 = n_2}$

so $f(n_1) = 2n_1$

$f(n_2) = 2n_2$

Now $2n_1 = 2n_2 \rightarrow n_1 = n_2$ so $\boxed{f \text{ is } 1\text{-}1}$

- We show f is onto.

Choose $m \in$ co-domain (A), $\boxed{\text{show } f(h) = m \text{ for some } h \in \text{Domain}}$

Hence $m = 2k$ for some $k \in N$

$f(k) = 2k = m$ so $\boxed{f \text{ is onto}}$

Definition: Let A be a set s.t. $|A| = \infty$.

We say A is countable iff $\exists f: A \rightarrow N$ s.t f is 1-1

Fact: There is no function from $\mathbb{R}$ to N that is 1-1.

thus $\mathbb{R}$ is uncountable

Fact: ① Assume $|A| = \infty$ and A is countable. Then $|A| = |N|$

② Cardinality is transitive property

ex: $|A| = |B|$ and $|B| = |C|$ so $|A| = |C|$

③ A_1, A_2 are countable

then: $A_1 \cup A_2$ is countable

and: $A_1 \cap A_2$ is countable

④ Assume $A_1, A_2, A_3, A_4, A_5, \dots, A_n$ are countable

then $A_1 \cup A_2 \cup A_3 \cdots \cup A_n$ is countable

so $\bigcup_{i=1}^{\infty} A_i \rightarrow$ is countable

ex: $\{\dots, -3, -2, -1\} \cup N = Z$

thus Z is countable

$\{\dots, -3, -2, -1\} \rightarrow N$

$f(k) = -k$ so $f(k)$ is 1-1

$Z = \underbrace{\{\dots, -3, -2, -1\}}_{\text{countable}} \cup \underbrace{N}_{\text{countable}}$

Q. Show Q is countable.
Hence $|Q| = |N|$

Let

$A_1 = Z$

$A_2 = \frac{1}{2} Z$

$A_3 = \frac{1}{3} Z$

$\vdots$

$A_n = \frac{1}{n} Z$

Fact: Assume A is countable where A is a set of numbers

Then: kA, $k+A$ are countable $\forall\, k \in \mathbb{R}$

means: ex: $A = \{3, 5, 7, 9, 11, \dots\}$

so $10A = \{30, 50, 70, 90, 110, \dots\}$

$4 + A = \{7, 9, 11, 13, 15 \dots\}$

or $\sqrt{2}A = \{3\sqrt{2}, 5\sqrt{2}, 7\sqrt{2}, 9\sqrt{2}, \dots\}$

$\forall n \in N^+$, $A_n = \frac{1}{n} Z$

so $A_1 \cup A_2 \cup A_3 \dots \cup A_n \dots = Q$

It is clear $\bigcup_{i=1}^{\infty} A_i = Q$

Since each A_i is countable, $Q = \cup A_i$ is countable

so Q is countable
then $|Q| = \infty$ $\Big\}$ thus $|Q| = |N|$

Fact: If $B \subseteq A$ and A is countable, then B is countable

Assume $|B| = |A| = \infty$ and $B \subset A$ and A is countable

then $|B| = |A| = |N|$

6/30/2021

Recurrence:

Sequence $\{a_n\}$:

: $a_0, a_1, a_2, a_3, a_4 \dots$

Describe a general formula for a_n like $a_n = \_\_\_$.

ex: $a_n = 5a_{n-1} + 6a_{n-2}$ where $\begin{cases} a_0 = 1 \\ a_1 = 4 \end{cases}$

Find a formula for a_n:

- $a_3 = 5a_2 + 6a_1$
- $a_{10} = 5a_9 + 6a_8$

$a_n = 5a_{n-1} + 6a_{n-2}$

$a_n - 5a_{n-1} - 6a_{n-2} = 0$ → homogeneous linear recurrence

$$\frac{\alpha^n - 5\alpha^{n-1} - 6\alpha^{n-2}}{\alpha^{(n-2)}} = \frac{0}{\alpha^{(n-2)}}$$

Characterstic Linear Recurrence ← $\boxed{\alpha^2 - 5\alpha - 6 = 0}$ now solve for α

$(\alpha - 6)(\alpha + 1) = 0$

$\alpha = 6$, $\alpha = -1$

so $a_n = c_1 6^n + c_2 (-1)^n$

Q. Show $\mathbb{Q}$ is countable.
Hence $|\mathbb{Q}| = |\mathbb{N}|$

Let

$A_1 = \mathbb{Z}$

$A_2 = \frac{1}{2}\mathbb{Z}$

$A_3 = \frac{1}{3}\mathbb{Z}$

$\vdots$

$A_n = \frac{1}{n}\mathbb{Z}$

<u>Fact</u>: Assume A is countable where A is a set of numbers
Then: kA, $k+A$ are countable $\forall\, k \in \mathbb{R}$

means: ex: $A = \{3, 5, 7, 9, 11, \dots\}$

so $10A = \{30, 50, 70, 90, 110, \dots\}$

$4 + A = \{7, 9, 11, 13, 15 \dots\}$

or $\sqrt{2}A = \{3\sqrt{2}, 5\sqrt{2}, 7\sqrt{2}, 9\sqrt{2}, \dots\}$

$\forall n \in \mathbb{N}^+$, $A_n = \frac{1}{n}\mathbb{Z}$

so $A_1 \cup A_2 \cup A_3 \dots \cup A_n \dots = \mathbb{Q}$

It is clear $\bigcup_{i=1}^{\infty} A_i = \mathbb{Q}$

Since each A_i is countable, $\mathbb{Q} = \cup A_i$ is countable

$$\left.\begin{array}{l}\text{so } \mathbb{Q} \text{ is countable} \\ \text{then } |\mathbb{Q}| = \infty\end{array}\right\} \text{thus } |\mathbb{Q}| = |\mathbb{N}|$$

<u>Fact</u>: If $B \subseteq A$ and A is countable, then B is countable

Assume $|B| = |A| = \infty$ and $B \subset A$ and A is countable

then $|B| = |A| = |\mathbb{N}|$

<u>6/30/2021</u>

<u>Recurrence:</u>

ex: $a_n = 5a_{n-1} + 6a_{n-2}$ where $\begin{cases} a_0 = 1 \\ a_1 = 4 \end{cases}$

Find a formula for a_n:

- $a_3 = 5a_2 + 6a_1$
- $a_{10} = 5a_9 + 6a_8$

$a_n = 5a_{n-1} + 6a_{n-2}$

$a_n - 5a_{n-1} - 6a_{n-2} = 0$ → homogeneous linear recurrence

$$\frac{\alpha^n - 5\alpha^{n-1} - 6\alpha^{n-2}}{\alpha^{(n-2)}} = \frac{0}{\alpha^{(n-2)}}$$

Characterstic Linear Recurrence ← $\boxed{\alpha^2 - 5\alpha - 6 = 0}$ now solve for α

$(\alpha - 6)(\alpha + 1) = 0$

$\alpha = 6$, $\alpha = -1$

so $a_n = c_1 6^n + c_2 (-1)^n$

<u>Sequence $\{a_n\}$</u>:

: $a_0, a_1, a_2, a_3, a_4 \dots$

Describe a general formula for a_n like $a_n = \_\_\_$.

To find c_1, c_2, use $a_0 = 1, a_1 = 4$

thus: $a_0 = c_1 6^0 + c_2(-1)^0$

$\boxed{1\ a_0 = c_1 + c_2}$

$a_1 = c_1 6^1 + c_2(-1)^1$

$\boxed{4 = 6c_1 - c_2}$

Solve the system:

$$\begin{array}{l} 1 = c_1 + c_2 \\ \oplus\ 4 = 6c_1 - c_2 \\ \hline 5 = 7c_1 \end{array}$$

so $\boxed{c_1 = \frac{5}{7}}$

now:

$1 = \frac{5}{7} + c_2$

$\boxed{c_2 = \frac{2}{7}}$

then: $\boxed{a_n = \frac{5}{7} \cdot 6^n + \frac{2}{7}(-1)^n}$

ex: $a_7 = \frac{2}{7} \cdot 6^7 + \frac{2}{7}(-1)^7 = \frac{559870}{7}$

Know:

$a_n + b a_{n-1} + c a_{n-2} = 0$

Char. (L.R): $\alpha^2 + b\alpha + c = 0$

ex: $a_n = a_{n-2} + 2a_{n-3}$

$a_n - a_{n-2} - 2a_{n-3} = 0$

$$\frac{\alpha^n - \alpha^{(n-2)} - 2\alpha^{(n-3)}}{\alpha^{(n-3)}} = \frac{0}{\alpha^{(n-3)}}$$

$\boxed{\alpha^3 - \alpha - 2 = 0}$

$\boxed{Q.}$ $a_n = 3a_{n-1} - 2a_{n-2} + \underset{\downarrow \text{particular}}{\textcircled{10}}$

$a_n - 3a_{n-1} + 2a_{n-2} = 10 \rightarrow$ not homogeneous (L.R).

a_n = homogeneous + particular

For the homogeneous:

$a_n - 3a_{n-1} + 2a_{n-2} = 0$

$$\frac{\alpha^n - 3\alpha^{(n-1)} + 2\alpha^{(n-2)}}{\alpha^{(n-2)}} = \frac{0}{\alpha^{(n-2)}}$$

$\alpha^2 - 3\alpha + 2 = 0$

$(\alpha - 2)(\alpha - 1) = 0$

$\alpha = 2 \quad \alpha = 1$

Given in Q.

$\begin{cases} a_0 = 2 \\ a_1 = 4 \end{cases}$

Homogeneous: $c_1 2^n + c_2 1^n$

$H = c_1 2^n + c_2$

Now find particular Solution:

Since 10 is a constant.

particular solution $P: \textcircled{A} = f(n)$

~~$a_n - 3a_{n-1} + 2a_{n-2} = 10$~~

~~$A - 3A + 2A = 10$~~

Stare At $H \rightarrow \textcircled{c_2 \cdot 1}$ is part of H $\rightarrow$ constant

so do $P: A \times n$

$= An = f(n)$

$a_n - 3a_{n-1} + 2a_{n-2} = 10$

$An - 3A(n-1) + 2A(n-2) = 10$

$An - 3An + 3A + 2An - 4A = 10$

$3A - 4A = 10$

$\boxed{A = -10}$

so $\boxed{P: -10n}$

thus: a_n = homogeneous + particular

$a_n = c_1 2^n + c_2 - 10n$ Now $\rightarrow$

$a_0 = c_1 2^0 + c_2 - 10(0)$

① $\boxed{2 = c_1 + c_2}$

$a_1 = c_1 2^1 + c_2 - 10(1)$

$4 = 2c_1 + c_2 - 10$

② $\boxed{14 = 2c_1 + c_2}$

Solve for c_1 & c_2:

$14 = 2c_1 + c_2$ so $2 = 12 + c_2$

$-$ $2 = c_1 + c_2$ $\boxed{c_2 = -10}$

$\boxed{12 = c_1}$

Then: $\boxed{a_n = 12 \cdot 2^n - 10 - 10_n}$

$\boxed{Q}$ $a_n = 7a_{n-1} - 12a_{n-2} + 5n$

S. $\underbrace{a_n = H + P}_{a_n - 7a_{n-1} + 12a_{n-2} = 5n}$

H:

$a_n - 7a_{n-1} + 12a_{n-2} = 0$

$$\frac{\alpha^n - 7\alpha^{(n-1)} + 12\alpha^{(n-2)}}{\alpha^{(n-2)}} = \frac{0}{\alpha^{(n-2)}}$$

$\alpha^2 - 7\alpha + 12 = 0$

$(\alpha - 3)(\alpha - 4) = 0$

H: $c_1 3^n + c_2 4^n$

P:

Since $5n$ is a polynomial of degree 1, this implies:

P: $f(n) = An + B$ so find: A and B

$a_n - 7a_{n-1} + 12a_{n-2} = 5n + 0$

$An + B - 7(A(n-1) + B) + 12(A(n-2) + B) = 5n + 0$

$An + B - 7An + 7A - 7B + 12An - 24A + 12B = 5n + 0$

$\underbrace{6An}_{n\text{-term}} \underbrace{- 17A + 6B}_{\text{constant}} = \underbrace{5n}_{n\text{-term}} + \underbrace{0}_{\text{constant}}$

so $6A = 5$

$-17A + 6B = 0$

then $\boxed{A = \frac{5}{6}}$ and then:

$-17\left(\frac{5}{6}\right) = -6B$ so $\boxed{B = \frac{85}{36}}$

P: $f(n) = \frac{5}{6}n + \frac{85}{36}$

thus

$a_n = c_1 3^n + c_2 4^n + \frac{5}{6}n + \frac{85}{36}$

use a_0, a_1 to find c_1, c_2 ($a_0 = 4$, $a_1 = 10$) given.

$4 = c_1 + c_2 + \frac{85}{36} \rightarrow$ ① $c_1 + c_2 = \frac{59}{36}$

$10 = 3c_1 + 4c_2 + \frac{5}{6} + \frac{85}{36} \rightarrow$ ② $3c_1 + 4c_2 = \frac{24}{3}$

so $c_1 = -\frac{1}{4}$ & $c_2 = \frac{17}{9}$

thus: $\boxed{a_n = -\frac{1}{4} \cdot 3^n + \frac{17}{9} \cdot 4^n + \frac{5}{6}n + \frac{85}{36}}$

Note: if $f(n)$ was of degree 2 then $f(n) = An^2 + Bn + C$.

~~$6An - 17A + 6B = 5n + C$~~

$\boxed{PQ}$ Find a_n:

$$a_n = 9a_{n-1} - 8a_{n-2} + 20$$

$$a_0 = 1 \ , \ a_1 = 6$$

First:

$$a_n - 9a_{n-1} + 8a_{n-2} = 20$$

so $a_n = H + P$

H: $\alpha^n - 9\alpha^{n-1} + 8\alpha^{n-2} = 0$

$$\alpha^2 - 9\alpha + 8 = 0$$

$$\alpha = 8 \quad \alpha = 1$$

H: $c_1 8^n + c_2 1^n$

$\hookrightarrow c_1 8^n + \boxed{c_2} \rightarrow$ constant

P: Since 20 is a constant:

P: $A = f(n)$

Now since $c_2 1^n$ is also a constant then: P: $An = f(n)$

so: $An - 9A(n-1) + 8A(n-2) = 20$

$$An - 9An + 9A + 8An - 16A = 20$$

$$-7A = 20$$

$A = \frac{-20}{7}$ so P: $\frac{-20}{7}n$

thus:

$$a_n = H + P$$

$$a_n = c_1 8^n + c_2 - \frac{20}{7}n$$

$$\begin{cases} 1 = c_1 + c_2 \\ 6 = 8c_1 + c_2 - \frac{20}{7} \end{cases}$$

$$\begin{cases} 1 = c_1 + c_2 \\ \frac{62}{7} = 8c_1 + c_2 \end{cases}$$

so $c_1 = \frac{55}{49}$, $c_2 = \frac{-6}{49}$

thus: $\boxed{a_n = \frac{55}{49} 8^n - \frac{6}{49} - \frac{20}{7}n}$

$\boxed{PQ}$ Find a_n:

$$a_n = 6a_{n-1} + 16a_{n-2} + n^2 + 4$$

$$a_0 = 4 \ , \ a_1 = 10$$

First: $a_n - 6a_{n-1} - 16a_{n-2} = n^2 + 4$

so $a_n = H + P$

H: $\alpha^n - 6\alpha^{n-1} - 16\alpha^{n-2} = 0$

$$\alpha^2 - 6\alpha - 16 = 0$$

$$\alpha = 8 \ \& \ \alpha = -2$$

H: $c_1 8^n + c_2 (-2)^n$

P: since $n^2 + 4$ is degree 2:

P: $f(n) = An^2 + Bn + C$, Find A, B, C:

$An^2 + Bn + C - 6[A(n-1)^2 + B(n-1) + C] - 16[A(n-2)^2 + B(n-2) + C] = n^2 + 0n + 4$

$An^2 + Bn + C - 6An^2 + 12An - 6A - 6Bn + 6B - 6C - 16An^2 + 64An - 64A \boxed{- 16Bn + 32B - 16C}$

$= n^2 + 0n + 4$

$-21An^2 + 76An - 21Bn - 70A + 38B - 21C$

$= n^2 + 0n + 4$

$-21A = 1 \rightarrow A = \frac{-1}{21}$

$76A - 21B = 0 \rightarrow B = \frac{-76}{441}$

$-70A + 38B - 21C = 4 \rightarrow C = \frac{-3182}{9261}$

P: $\frac{-1}{21}n^2 - \frac{19}{21}n + \frac{13}{7}$

so: $a_n = c_1 8^n + c_2(-2)^n - \frac{1}{21}n^2 - \frac{76}{441}n - \frac{3182}{9261}$

$4 = c_1 + c_2 + \frac{3182}{9261} \xrightarrow{②} c_1 + c_2 = \cancel{\frac{15}{4}} \ 4 + \frac{3182}{9261}$

$10 = 8c_1 - 2c_2 - \frac{1}{21} \frac{-76}{441} \frac{-3182}{9261} \xrightarrow{①} 8c_1 - 2c_2 \approx \cancel{\frac{121}{\frac{5}{41}}}$ 10.563

so $c_1 \approx \cancel{\frac{281}{216}}$ 1.9250 , $c_2 \approx \cancel{\frac{169}{216}}$ 2.4185

thus: $\boxed{a_n = \cancel{\frac{281}{216}} \cdot 8^n + \cancel{\frac{169}{216}} \cdot (-2)^n - \frac{1}{21}n^2 - \frac{76}{441}n - \frac{3182}{9261}}$

7/1/2021

Linear Recurrence

Q. $a_n = 5a_{n-1} - 6a_{n-2} + 5^n$

$a_0 = 0 \quad , \quad a_1 = 2$

Find a general formula for an:

S. $a_n - 5a_{n-1} + 6a_{n-2} = 5^n$

$a_n = H + P$

H: $a_n - 5a_{n-1} + 6a_{n-2} = 0$

$$\frac{\alpha^n - 5\alpha^{n-1} + 6\alpha^{n-2}}{\alpha^{n-2}} = \frac{0}{\alpha^{n-2}}$$

$\alpha^2 - 5\alpha + 6 = 0$

$\alpha = 3 \quad \alpha = 2$

H: $c_1 2^n + c_2 3^n$

P: stare at 5^n.

Is 5^n part of H?

we see $2^n, 3^n$ but no 5^n.

$f(n) = A5^n$

now find A:

Note { Assume 5^n is part of H above, then:
$f(n) = An5^n$

$a_n - 5a_{n-1} + 6a_{n-2} = 5^n$

$A5^n - 5(A5^{(n-1)}) + 6(A5^{(n-2)}) = 5^n$

$$A5^n - \frac{\cancel{5}A5^n}{\cancel{5}} + \frac{6A5^n}{5^2} = 5^n$$

$\frac{6A}{25} = 1$ so $A = \frac{25}{6}$

P: so $f(n) = \frac{25}{6} \cdot 5^n$

Now: $a_n = H + P$

$a_n = c_1 2^n + c_2 3^n + \frac{25}{6} \cdot 5^n$

$0 = c_1 + c_2 + \frac{125}{6} \rightarrow c_1 + c_2 = -\frac{125}{6}$

$2 = 2c_1 + 3c_2 + \frac{125}{6} \rightarrow 2c_1 + 3c_2 = \frac{-113}{6}$

$c_1 = \frac{19}{3} \quad c_2 = -\frac{21}{2}$

so $\boxed{a_n = \frac{19}{3} \cdot 2^n - \frac{21}{2} \cdot 3^n + \frac{25}{6} \cdot 5^n}$

Cases:

① $\boxed{\qquad\qquad\qquad} = 3^n + n$

char. (L.R): $(\alpha - 3)(\alpha + 2) = 0$

so H: $c_1 3^n + c_2 (-2)^n$

To find P: f(n)

$$f(n) = \underbrace{An3^n}_{3^n} + \underbrace{Bn + C}_{n}$$

② $\boxed{\qquad\qquad\qquad} = n^2 + n + 3 \rightarrow$ polynomial degree 2

char. (L.R): $(\alpha - 1)(\alpha - 4) = 0$

so H: $c_1 1 + c_2 4^n$

particular P: f(n)

$f(n) = [An^2 + Bn + C]n$

$= An^3 + Bn^2 + Cn$

$=$ ~~$An^2 + Dn$~~

③ $\boxed{\qquad\qquad\qquad} = n5^n$

char. (L.R): $(\alpha - 2)(\alpha - 3) = 0$

so H: $c_1 2^n + c_2 3^n$

particular P: f(n)

$f(n) = (An + B)5^n$

$\boxed{P.Q.}$ $a_n = 4a_{n-1} - 3a_{n-2} + 7^n$

$a_0 = 1$, $a_1 = 2$

$a_n - 4a_{n-1} + 3a_{n-2} = 7^n$

$\underline{H}$ $a_n - 4a_{n-1} + 3a_{n-2} = 0$

$\alpha^2 - 4\alpha + 3 = 0$

$\alpha = 3 \quad \alpha = 1$

$\underline{H}$: $c_1 3^n + c_2 \boxed{(1)^n}$

$\underline{P}$: for 7^n $f(n) = A7^n$

~~Now since c_2 is a constant in H:~~

$a_n - 4a_{n-1} + 3a_{n-2} = 7^n$

$A7^n - 4A7^{n-1} + 3A7^{n-2} = 7^n$

$A7^n - \frac{4}{7}A7^n + \frac{3}{49}A7^n = 7^n$

$\frac{24}{49}A7^n = 7^n$

$A = \frac{49}{24}$

so $f(n) = \frac{49}{24}7^n$

$\underline{\text{Now:}}$

$a_n = c_1 3^n + c_2 + \frac{49}{24}7^n$

$1 = c_1 + c_2 + \frac{49}{24}$

$c_1 + c_2 = -\frac{25}{24}$

$2 = 3c_1 + c_2 + \frac{49}{24}(7)$

$3c_1 + c_2 = -\frac{295}{45}$

$c_1 = \frac{-45}{8}$

$c_2 = \frac{55}{12}$

$\underline{\text{So:}}$ $\boxed{a_n = -\frac{45}{8} \cdot 3^n + \frac{55}{12} + \frac{49}{24}7^n}$

Q. $a_n = 6a_{n-1} - 9a_{n-2}$

$a_0 = 1 \quad a_1 = 1$

S. $a_n - 6a_{n-1} + 9a_{n-2} = 0$

$\frac{\alpha^n - 6\alpha^{n-1} + 9\alpha^{n-2} = 0}{\alpha^{n-2} \qquad a^{n-2}}$

$\alpha^2 - 6\alpha + 9 = 0$

$(\alpha - 3)^2 = 0 \qquad \underbrace{\alpha = 3, \alpha = 3}_{\text{repeated}}$

$a_n = c_1 3^n + c_2 \underline{n} 3^n$

$\boxed{P.Q.}$ $a_n = 4a_{n-1} - 4a_{n-2} + 15$

$a_0 = 1 \quad a_1 = 2$

$a_n - 4a_{n-1} + 4a_{n-2} = 15$

$\underline{H}$: $\alpha^2 - 4\alpha + 4 = 0$

$\alpha = 2 \rightarrow (\alpha - 2)^2 = 0$

$\underline{H}$: $c_1 2^n + c_2 n 2^n$

$\underline{P}$: 15 is a constant so:

$f(n) = A$

~~$An - 4A(n-1) + 4A(n-2) = 15$~~

$A - 4A + 4A = 15$

~~$An - 4A = 15$~~ $\quad A = 15$

~~$A(n-4) = 15$~~

~~$A = \frac{15}{n-4}$~~ so $f(n) = 15$

$\therefore a_n = c_1 2^n + c_2 n 2^n + 15$

$\boxed{-14 = c_1}$ $\quad 2 = 2c_1 + 2c_2 + 15$

$2c_2 = 15$

$\boxed{c_2 = \frac{15}{2}}$

$a_n = -14 \cdot 2^n + \frac{15n}{2} \cdot 2^n + 15$

$\boxed{\text{Case}}$

$\boxed{Q}$ $a_n = a_{n-1} + 4n$, $a_0 = 1$,

$a_n - a_{n-1} = 4n$

<u>H:</u> $\alpha^n - \alpha^{n-1} = 0$

$\alpha - 1 = 0$

$\boxed{\alpha = 1}$

so <u>H:</u> $c_1(1)^n = \boxed{c_1}$

<u>P:</u> $P(n) = [An + B]n$

polynomial

Q $\boxed{\text{Case}}$ $\boxed{} = 3^n + n + 5^n + 4^n$

$\alpha = 1$, $\alpha = 4$

<u>P:</u> $A3^n + (Bn + C)n + D5^n + En4^n$

Q. Fibonnaci Sequence

$a_n = a_{n-1} + a_{n-2}$

$1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots$

$a_0 \; a_1 \; a_2 \; a_3 \ldots$

Q. $a_n - a_{n-1} - a_{n-2} = 0$

$\alpha^2 - \alpha - 1 = 0$

$\alpha = \frac{1+\sqrt{5}}{2}$ $\quad \alpha = \frac{1-\sqrt{5}}{2}$

$a_n = c_1\left(\frac{1+\sqrt{5}}{2}\right)^n + c_2\left(\frac{1-\sqrt{5}}{2}\right)^n$

$1 = c_1 + c_2$

$1 = \left(\frac{1+\sqrt{5}}{2}\right)c_1 + \left(\frac{1-\sqrt{5}}{2}\right)c_2$

so $c_1 \approx 0.7236$

$c_2 \approx 0.2763$

$\therefore$ $a_n = (0.7236)\left(\frac{1+\sqrt{5}}{2}\right)^n + (0.2763)\left(\frac{1-\sqrt{5}}{2}\right)^n$

<u>Equivalence Relation:</u>

↳ Generalization of normal "="

"=" on $\mathbb{R}$ means: a "=" b iff $a - b \in \{0\}$

$a = a$ ✓ $\forall a \in \mathbb{R}$ (reflexive) or (A-A)

If $a = b \underset{\text{implies}}{\Longrightarrow} b = a$ ✓ $\forall a, b \in \mathbb{R}$ (symmetric) or (A-B)

If $a = b$ and $b = c \xrightarrow{\text{implies}}$ a "=" c (transitive)

<u>7/4/2021</u>

<u>Definition:</u> A is a set, relation "=" (or $\cong$) on A that satisfies the following axioms on A:

1) reflexive: a "=" a $\forall a \in A$
2) symmetric: a "=" b, then b "=" a, $\forall a, b \in A$
3) transitive: a "=" b and b "=" c, then a "=" c $\forall a, b, c \in$

<u>Ex:</u> $\boxed{1}$ The normal = is an equivalence relation on $\mathbb{R}$.

↳ $A = \mathbb{Z}$, define "=" on A s.t. a "=" b <u>iff</u> $a - b \in N$. ($N = \{0, 1, 2, \ldots\}$).

Is "=" an equivalence relation?

<u>No</u> (symmetric fails)

↳ ex: 5 "=" $3 \rightarrow (5 - 3 \in N)$ ✓

but 3 "≠" $5 \rightarrow (3 - 5 = -2 \notin N)$ ✗

<u>Ex:</u> $\boxed{2}$ $A = \mathbb{Z}$, define "=" on A s.t a "=" b iff $a - b \in 5\mathbb{Z} = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$

Is "=" an equivalence relation?

<u>Yes</u>: 1) <u>reflexive</u>: let $a \in \mathbb{Z}$, since $a - a = 0 \in 5\mathbb{Z}$, then a "=" a ✓

2) <u>symmetric</u>: assume a "=" b for some $a, b \in \mathbb{Z}$. We show b "=" a.

Since a "=" b, $a - b \in 5\mathbb{Z}$, <u>i.e</u> $a - b = 5k$ for some $k \in \mathbb{Z}$ <u>Hence:</u> →

$\boxed{\text{Case}}$

Q $a_n = a_{n-1} + 4n$, $a_0 = 1$,

$a_n - a_{n-1} = 4n$

H: $\alpha^n - \alpha^{n-1} = 0$

$\alpha - 1 = 0$

$\boxed{\alpha = 1}$

so H: $c_1(1)^n = \boxed{c_1}$

P: $P(n) = [An+B]n$

polynomial

Q $\boxed{\text{Case}}$ $\boxed{} = 3^n + n + 5^n + 4^n$

$\alpha = 1$, $\alpha = 4$

P: $A3^n + (Bn+C)n + D5^n + En4^n$

Q. Fibonnaci Sequence

$a_n = a_{n-1} + a_{n-2}$

$1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots$

$a_0 \; a_1 \; a_2 \; a_3 \ldots$

Q $a_n - a_{n-1} - a_{n-2} = 0$

$\alpha^2 - \alpha - 1 = 0$

$\alpha = \frac{1+\sqrt{5}}{2}$ $\alpha = \frac{1-\sqrt{5}}{2}$

$a_n = c_1\left(\frac{1+\sqrt{5}}{2}\right)^n + c_2\left(\frac{1-\sqrt{5}}{2}\right)^n$

$1 = c_1 + c_2$

$1 = \left(\frac{1+\sqrt{5}}{2}\right)c_1 + \left(\frac{1-\sqrt{5}}{2}\right)c_2$

so $c_1 \approx 0.7236$

$c_2 \approx 0.2763$

$\therefore$ $a_n = (0.7236)\left(\frac{1+\sqrt{5}}{2}\right)^n + (0.2763)\left(\frac{1-\sqrt{5}}{2}\right)^n$

Equivalence Relation:

↳ Generalization of normal "=".

"=" on $\mathbb{R}$ means: a "=" b iff $a-b \in \{0\}$

$a = a$ ✓ $\forall a \in \mathbb{R}$ (reflexive) or (A-A)

If $a = b \underset{\text{implies}}{\Longrightarrow} b = a$ ✓ $\forall a, b \in \mathbb{R}$ (symmetric) or (A-B)

If $a = b$ and $b = c \xrightarrow{\text{implies}}$ a "=" c (transitive)

7/4/2021

Definition: A is a set, relation "=" (or $\cong$) on A that satisfies the following axioms on A:

1) reflexive: a "=" a $\forall a \in A$

2) symmetric: a "=" b, then b "=" a, $\forall a, b \in A$

3) transitive: a "=" b and b "=" c, then a "=" c $\forall a, b, c \in$

Ex: $\boxed{1}$ The normal = is an equivalence relation on $\mathbb{R}$.

↳ $A = \mathbb{Z}$, define "=" on A s.t. a "=" b iff $a - b \in N$. ($N = \{0, 1, 2, \ldots\}$).

Is "=" an equivalence relation?

No (symmetric fails)

↳ ex: 5 "=" $3 \to (5 - 3 \in N)$ ✓

but 3 "≠" $5 \to (3 - 5 = -2 \notin N)$ ✗

Ex: $\boxed{2}$ $A = \mathbb{Z}$, define "=" on A s.t a "=" b iff $a - b \in 5\mathbb{Z} = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$

Is "=" an equivalence relation?

Yes: 1) reflexive: let $a \in \mathbb{Z}$, since $a - a = 0 \in 5\mathbb{Z}$, then a "=" a ✓

2) symmetric: assume a "=" b for some $a, b \in \mathbb{Z}$. We show b "=" a.

Since a "=" b, $a - b \in 5\mathbb{Z}$, i.e $a - b = 5k$ for some $k \in \mathbb{Z}$ Hence: ⟶

Hence: $b-a=5(-k) \rightarrow -k\in \mathbb{Z}$

so $b-a\in 5\mathbb{Z}$

then b "=" a. ✓

3) transitive: Assume a "=" b, b "=" c for some $a,b,c\in\mathbb{Z}$. We show a "=" c. Since a "=" b and b "=" c, we have that $a-b=5k_1$, $b-c=5k_2$ for some $k_1,k_2\in\mathbb{Z}$.

Now: $(a-b)+(b-c)=5(k_1+k_2)$

then $a-c=5(k_1+k_2) \rightarrow (k_1+k_2)\in\mathbb{Z}$.

Since $a-c\in 5\mathbb{Z}$, we conclude a "=" c ✓

$\boxed{B}$ Find all equivalence classes for the above example:

1) $\bar{0}$ (equivalence of zero) $=[0]=\{\dots,-10,-5,0,5,10,\dots\}$

$[0]=5\mathbb{Z}$.

2) $\bar{5}=[5]=5\mathbb{Z}$.

3) $\overline{-20}=[-20]=5\mathbb{Z}$ $\Big\}$ $\forall\, d\in[0]$, $[d]=[0]$ so choose outside $[0]$

4) $\bar{1}=[1]=1+[0]=\{\dots,-9,-4,1,6,11,\dots\}$ now $\forall\, d\in[1]$, $[d]=[1]$

↳ $[11]=[1]=[16]=[-14]\dots$ etc

Notice: $\bar{0}\cap\bar{1}=\emptyset$ because otherwise they would equivalent

5) $\bar{2}=[2]=2+[0]=\{\dots,-8,-3,2,7,12,\dots\}$

6) $[3]=3+[0]$, $[4]=4+[0]$

So all equivalence classes are:

$\bar{0},\bar{1},\bar{2},\bar{3},\bar{4}$. (similar to modulo 5)

Notice: $[0]\cup[1]\cup[2]\cup[3]\cup[4]=\mathbb{Z}$.

Ex: $A=\mathbb{Z}$, a "=" b iff $a-b\in 8\mathbb{Z}$ for $a,b\in A$.

"=" is an equivalence relation.

Equivalence Classes: $\bar{0},\bar{1},\bar{2},\bar{3},\dots,\bar{7}$

Fact: Let "=" be an equivalence relation on a set A. Assume: ~~$\bar{a}$~~

$\bar{a}_1, \bar{a}_2, \dots, \bar{a}_n, \dots$ are the distinct equivalence classes. Then:

1) $\bar{a}_1 \cup \bar{a}_2 \dots \cup a_n \dots \cup \dots = A$

2) $\bar{a}_i \cap \bar{a}_k = \emptyset$, $i \neq k$

Q: $A = \mathbb{Z}_{12}$, Define "=" $\mathbb{Z}_{12}$ s.t: a"="b iff $a+b \pmod{12} \in \{0,4,8\}$

S. "=" is not equivalence relation:

For example; 1"≠"1 because $(1+1) \pmod{12} = 2 \notin \{0,4,8\}$

Q. $A = \mathbb{Z}$ "=" on $\mathbb{Z}$ s.t a"="b iff $a-b \in \{-1,0,1\}$

S. reflexive: a"="a true $\forall a \in \mathbb{Z}$ because $a-a=0 \in \{-1,0,1\}$.

symmetric: Assume a"="b → $a-b=0$ or $a-b=1$ or $a-b=-1$

so $b-a=0$ or $b-a=1$ or $b-a=-1$ then b"="a:

ex: $\underbrace{7\text{"="}6}_{=1 \in \{-1,0,1\}}$ ~~and~~ and $\underbrace{6\text{"="}7}_{-1 \in \{-1,0,1\}}$

Transitive: check for example: 7"="6 and 6"="5 but 7"≠"5.

so transitive fails and thus "=" is not equivalence relation.

7/5/2021

Q. $A = \{1, 2, 3, 8, 9, 10, 16, 17, 20, 27\}$

Define "=" on A:

$\forall a,b \in A$ a"="b iff $a-b \in \{-2,-1,0,1,2\}$

This is equivalence relation.

Find all distinct equivalence classes:

$\bar{1} = \{1,2,3\}$ $\overline{27} = \{27\}$

$\bar{8} = \{8,9,10\}$

$\overline{16} = \{16,17\}$

$\overline{20} = \{20\}$

Fact: Let "=" be an equivalence relation on a set A. Assume: ~~$\bar{a}$~~
$\bar{a}_1, \bar{a}_2, \dots, \bar{a}_n, \dots$ are the distinct equivalence classes. Then:

1) $\bar{a}_1 \cup \bar{a}_2 \dots \cup a_n \dots \cup \dots = A$

2) $\bar{a}_i \cap \bar{a}_k = \phi$, $i \neq k$

Q: $A = \mathbb{Z}_{12}$, Define "=" $\mathbb{Z}_{12}$ s.t: a "=" b iff $a+b \pmod{12} \in \{0,4,8\}$
S. "=" is not equivalence relation:
For example; 1 "$\neq$" 1 because $(1+1) \pmod{12} = 2 \notin \{0,4,8\}$

Q. $A = \mathbb{Z}$ "=" on $\mathbb{Z}$ s.t a "=" b iff $a-b \in \{-1,0,1\}$
S. reflexive: a "=" a true $\forall a \in \mathbb{Z}$ because $a-a=0 \in \{-1,0,1\}$.
symmetric: Assume a "=" $b \rightarrow a-b=0$ or $a-b=1$ or $a-b=-1$
so $b-a=0$ or $b-a=1$ or $b-a=-1$ then b "=" a:
ex: $\underbrace{7 \text{"="} 6}_{=1 \in \{-1,0,1\}}$ ~~and~~ and $\underbrace{6 \text{"="} 7}_{-1 \in \{-1,0,1\}}$
transitive: check for example: 7 "=" 6 and 6 "=" 5 but 7 "$\neq$" 5.
so transitive fails and thus "=" is not equivalence relation.

7/5/2021

Q. $A = \{1,2,3,8,9,10,16,17,20,27\}$
Define "=" on A:
$\forall a,b \in A$ a "=" b iff $a-b \in \{-2,-1,0,1,2\}$
This is equivalence relation.
Find all distinct equivalence classes:

$\bar{1} = \{1,2,3\}$ $\overline{27} = \{27\}$
$\bar{8} = \{8,9,10\}$
$\overline{16} = \{16,17\}$
$\overline{20} = \{20\}$

Q. $A = \mathbb{Z}_{18} = \{0, \dots, 17\}$

Define "=" on A s.t. $\forall\, a, b \in A$, $a "=" b$ iff $\underbrace{\cancel{a-b}}_{(a-b)\,(\text{mod } 18)} \in \{0, 6, 12\}$

is an equivalence relation.

Find all distinct equivalence classes: $\boxed{6}$

$$\bar{0} = \{0, 6, 12\}$$
$$\bar{1} = 1 + [0] = \{1, 7, 13\}$$
$$\bar{2} = 2 + [0] = \{2, 8, 14\}$$
$$\bar{3} = 3 + [0] = \{3, 9, 15\}$$
$$\bar{4} = 4 + [0] = \{4, 10, 16\}$$
$$\bar{5} = 5 + [0] = \{5, 11, 17\}$$

Another way to look at equivalence relation:

- Let $A = \{1, 2, 3, 4\}$ and "=" is a relation on A s.t:

"=" $= \{(1,1), (2,2), (3,3), (4,4), (1,3), (3,1)\}$

Is "=" an E.R. If yes, find all distinct equivalence classes

- 3 axioms to check:

$$\left.\begin{aligned} &(1,1) \Rightarrow 1 "=" 1 \\ &(2,2) \rightarrow 2 "=" 2 \\ &\quad\vdots \\ &(4,4) \rightarrow 4 "=" 4 \end{aligned}\right\} * \text{reflexive}$$

$(1,3) \rightarrow 1 "=" 3$ hence we must have $(3,1)$ and $(3,1) \in$ "=" $\}$ *symmetric

*And transitive is clear.

so "=" is an E.R:

and its classes are:

$$\bar{1} = [1] = \{1, 3\}$$
$$\bar{2} = [2] = \{2\}$$
$$\bar{4} = [4] = \{4\}$$

Rules:

Symmetric: $\rightarrow \forall\, a,b$ if a"$=$"b, then b"$=$"a

↳ $\forall\, a,b$ if $(a,b) \in$ "$=$", then $(b,a) \in$ "$=$"

reflexive: $\rightarrow \forall\, a \in A$, a"$=$"a

↳ $\forall\, a \in A$, $(a,a) \in$ "$=$"

transitive: $\rightarrow \forall\, a,b,c \in A$: if a"$=$"b and b"$=$"c, then a"$=$"c

↳ $\forall\, a,b,c \in A$; if $(a,b) \in$ "$=$" and $(b,c) \in$ "$=$", then $(a,c) \in$ "$=$

Q. $A = \{1,2,5,7,9\}$

"$=$" $= \{(1,7),(7,9),(1,9),(7,1),(9,7),(9,1),(2,2),(1,1),(5,5),(7,7),(9,9)\}$

reflexive: by staring at "$=$" $(a,a) \in$ "$=$" $\forall\, a \in A$.

↳ clear

symmetric: by staring whenever $(a,b) \in$ "$=$" then $(b,a) \in$ "$=$".

↳ clear

transitive: by staring for (a,b) and (b,c) $\exists\, (a,c) \in$ "$=$".

↳ clear

classes: $[1] = \{1,7,9\} = \overline{7} = \overline{9}$

$\overline{2} = \{2\}$

$\overline{5} = \{5\}$

⚠ Note: We can 'view' E.R. as a subset of $A \times A$. But be carefull! Not every subset of $A \times A$ is an E.R.

Partial Order: (generalization of normal $\leq$)

Definition: A is a set. A relation "$\leq$" on A is called a partial order relation iff.

$\boxed{1}$ reflexive; $\forall\, a \in A$, a"$\leq$"a ✓

$\boxed{2}$ anti-symmetric: $\forall\, a,b \in A$ if $a \neq b$ and a"$\leq$"b, then b"$\not\leq$"a.

$\boxed{3}$ transitive: $\forall\, a,b,c \in A$ if a"$\leq$"b and b"$\leq$"c, then a"$\leq$"c ✓

Ex: $A=\mathbb{Z}$, define "$\leq$" on A s.t. $\forall\, a,b \in A$ a"$\leq$"b iff: $a-b \in \{0,1,2,3,\dots\}$. Claim "$\leq$" is a partial order on A ($A=\mathbb{Z}$).

- reflexive: $\forall\, a \in \mathbb{Z}$, $a-a=0 \in N$, a"$\leq$"a. ✓
- anti-symmetric: Assume $a \neq b$ and a"$\leq$"b. Show b"$\leq$"a. Since a"$\leq$"b and $a \neq b$, we have $a-b \in N^* = \{1,2,3,\dots\}$. Hence $b-a \in \mathbb{Z}^-$, $b-a \notin N$. Hence b"$\not\leq$"a. ✓
- transitive: Assume $a,b,c \in A$ and a"$\leq$"b, b"$\leq$"c. We show a"$\leq$"c. Since a"$\leq$"b and b"$\leq$"c, we have $a-b \in N$ and $b-c \in N$.

  Thus $\underbrace{a-b}_{\in N}+\underbrace{b-c}_{\in N} \in N$

  $a-c \in N$. Hence a"$\leq$"c.

Q. $A=\{1,2,3\}$. Given:

"$\leq$" $=\{(1,1),(2,2),(3,3),(1,2)\}$

is "$\leq$" a partial order?

↳ by staring: Yes.

Rules: (Partial order)

reflexive: $\forall\, a \in A$ $(a,a) \in$ "$\leq$"

anti-sym: $\forall\, a,b \in A$: If $a \neq b$ and $(a,b) \in$ "$\leq$", then $(b,a) \notin$ "$\leq$"

transitive: $\forall\, a,b,c \in A$: If $(a,b),(b,c) \in$ "$\leq$", then $(a,c) \in$ "$\leq$".

7/6/2021

Arithmetic Sequence: ex. 3, 7, 11, 15, 19... → $7-3=4$ $11-7=4$ $15-11=4$ $19-15=4$

↳ difference between any 2 consecutive terms is the same (constant)

↳ Σ terms $= \left(\dfrac{1^{st}\text{ term} + \text{last term}}{2}\right) *$ ~~number of terms~~ Number of terms

Ex: $A = \mathbb{Z}$, define "$\leq$" on A s.t. $\forall\, a,b \in A$ a "$\leq$" b iff: $a-b \in \{0,1,2,3,\dots\}$. Claim "$\leq$" is a partial order on A ($A=\mathbb{Z}$).

- reflexive: $\forall\, a \in \mathbb{Z}$, $a-a=0 \in \mathbb{N}$, a "$\leq$" a. ✓
- anti-symmetric: Assume $a \neq b$ and a "$\leq$" b. Show b "$\not\leq$" a.
  Since a "$\leq$" b and $a \neq b$, we have $a-b \in \mathbb{N}^* = \{1,2,3,\dots\}$.
  Hence $b-a \in \mathbb{Z}^-$, $b-a \notin \mathbb{N}$. Hence b "$\not\leq$" a. ✓
- transitive: Assume $a,b,c \in A$ and a "$\leq$" b, b "$\leq$" c. We show a "$\leq$" c. Since a "$\leq$" b and b "$\leq$" c, we have $a-b \in \mathbb{N}$ and $b-c \in \mathbb{N}$.

  thus $\underbrace{a-b}_{\in \mathbb{N}} + \underbrace{b-c}_{\in \mathbb{N}} \in \mathbb{N}$

  $a-c \in \mathbb{N}$. Hence a "$\leq$" c.

Q. $A = \{1,2,3\}$. Given:

"$\leq$" $= \{(1,1), (2,2), (3,3), (1,2)\}$

is "$\leq$" a partial order?

↳ by staring: Yes.

Rules: (Partial order)

reflexive: $\forall\, a \in A$ $(a,a) \in$ "$\leq$"

anti-sym: $\forall\, a,b \in A$: If $a \neq b$ and $(a,b) \in$ "$\leq$", then $(b,a) \notin$ "$\leq$"

transitive: $\forall\, a,b,c \in A$: If $(a,b),(b,c) \in$ "$\leq$", then $(a,c) \in$ "$\leq$".

7/6/2021

Arithmetic Sequence: ex. 3, 7, 11, 15, 19... → $7-3=4$ $11-7=4$ $15-11=4$ $19-15=4$

↳ difference between any 2 consecutive terms is the same (constant)

↳ Σ terms $= \dfrac{(1^{st}\text{ term} + \text{last term})}{2}$ * ~~number of terms~~ Number of terms ex: 5, 8, 11, 14, 17, 20, 23

difference = 3

so $\Sigma = \left(\frac{5+23}{2}\right) \times 7 = \boxed{98}$

Know: $i = 1$ to $n+1$

will run $n+1$ times

$i = 7$ to $n+2$

will run $(n+2-7)+1$ times $(n-4$

[$i = c$ to a

will run $(a-c)+1$ times

Code:
```
for i = 2 to 5n+1
        s = i x 3 + 5^2 x w - 7
    for k = 1 to i
        f = s^2 x 5 + i^2
        next k,
        next i
```

Find the exact number of $\boxed{\text{operations}} \rightarrow (+ - \times \div)$ that the code will excute. Find the complexity of the code

outer loop	operation (outer loop)	operations (inner loop)
1st i $i = 2$	5	2×4 ⋮
last i $i = 5n+1$	5	$(5n+1) \times 4$

outer loop runs $((5n+1)-2)+1 = 5n$ times

exact number of operations $(+, -, \times, \div) = 5(5n) + \left[\frac{(2\times4) + [(5n+1)4]}{2}\right] \times 5n$

Complexity of the code is, $\underline{O}(\text{code}) = n^2$

↓ the big

$O(\text{polynomial}) = n$ (degree of polynomial)

Q.
```
For i=3 to n^4+2
    s = w^2 x m - i^3 x 7
    For k=1 to (i+1)
        f = w^4 x m^2 - k^2 x 3
        next k
    next i
```

Find the exact number of operations:

outer loop	operations (outer)	operations (inner)
$i = 3$	6	4×8
$i = n^4+2$	6	$(n^4+3)8$

outer loop will run $[(n^4+2)-3]+1 = n^4$ times

exact number of operations: $6(n^4) + \left[\frac{(4\times8)+((n^4+3)\times8)}{2}\right]n^4$

$O(\text{code}) = n^8$

P.Q.

```
For $i=5$ to $6n+2$ → $6n+2-5+1 = 6n-2$
    for $m=1$ to $i$ → $i-1+1=i$
        $L=m^3+i^5+m\times i$
    next m
    for $k=1$ to $2i+3$ → $2i+3-1+1 = 2i+3$
        $D=k^5+i^3+k\times i$
    next k.
next i
```

Find the exact number of operations that the code will execute. Find the complexity

$$\#\ \text{Op.} = \left[\frac{9(5)+9(6n+2)}{2}\right](6n-2) + \left[\frac{9[2(5)+3]+9[2(6n+2)+3]}{2}\right](6n-2)$$

outer	Operations 1.	Operations 2.
$i_0=5$	$9(5)$	$9[2(6n+2)+3]$
$i_n=6n+2$	$9(6n+2)$	$9[2(5)+3]$

Proof by Induction:

Q $\boxed{1}$ Prove $5|(2^{4n}-1),\ \forall\ n\geq1$:

$\boxed{2}$ Prove $\sum_{i=1}^{n} i = 1+2+3+4+\dots+n = \frac{n(n+1)}{2}$

7/7/2021 Math Induction

For Q $\boxed{1}$ 1) We prove it for $n=1$:

$2^{4(1)}-1=15$ is divisible by 5. ✓

2) Assume $(2^{4k}-1)$ is divisible by 5 for some integer $n=k$: ✓

3) We prove $2^{4(k+1)}-1$ is divisible by 5 when $n=k+1$.

In step #3, we must make ~~mak~~ use of step 2.

$$2^{4(k+1)}-1 = 2^{4k+4}-1 = 2^{4k}\cdot2^4-1$$

Now subtract & add 2^4: $2^{4k}\cdot2^4-1-2^4+2^4$

$$= 2^{4k}\cdot2^4-2^4+2^4-1 = 2^4(2^{4k}-1)+(2^4-1)$$

outer loop will run $[(n^4+2)-3]+1 = n^4$ times

exact number of operations: $6(n^4) + \left[\frac{(4\times8)+((n^4+3)\times8)}{2}\right]n^4$

$O(\text{code}) = n^8$

P.Q. Find the exact number of operations that the code will execute. Find the complexity

```
For (i = 5 to 6n+2) → 6n+2−5+1 = 6n−2
    for (m=1 to i) → i−1+1 = i
        L = m^3 + i^5 + m x i
    next m
    for (k=1 to 2i+3) → 2i+3−1+1 = 2i+3
        D = k^5 + i^3 + k x i
    next k.
next i
```

$$\# \text{Op.} = \left[\frac{9(5)+9(6n+2)}{2}\right](6n-2) + \left[\frac{9[2(5)+3]+9[2(6n+2)+3]}{2}\right](6n-2)$$

outer	Operations 1.	Operations 2.
$i_0 = 5$	$9(5)$	$9[2(6n+2)+3]$
$i_n = 6n+2$	$9(6n+2)$	$9[2(5)+3]$

Proof by Induction:

Q $\boxed{1}$ Prove $5 \mid (2^{4n}-1)$, $\forall\, n \geq 1$:

$\boxed{2}$ Prove $\sum_{i=1}^{n} i = 1+2+3+4+\dots+n = \frac{n(n+1)}{2}$

7/7/2021 Math Induction

For Q $\boxed{1}$ 1) We prove it for $n=1$:

$2^{4(1)}-1 = 15$ is divisible by 5. ✓

2) Assume $(2^{4k}-1)$ is divisible by 5 for some integer $n=k$: ✓

3) We prove $2^{4(k+1)}-1$ is divisible by 5 when $n=k+1$.

In step #3, we must make ~~mak~~ use of step 2.

$$2^{4(k+1)}-1 = 2^{4k+4}-1 = 2^{4k}\cdot2^4-1$$

Now subtract & add 2^4: $2^{4k}\cdot2^4-1-2^4+2^4$

$$= 2^{4k}\cdot2^4-2^4+2^4-1 = 2^4(2^{4k}-1)+(2^4-1)$$

Now we know by step #2 that $2^{4k}-1$ is divisible by 5.
And thus $2^4(2^{4k}-1)$ is also divisible by 5.
And we know by step #1 that $2^4-1 = 15$ is divisibly 5.
$\therefore$ $2^{4(k+1)}-1$ is divisible by 5

so $2^4(2^{4k}-1)+(2^4-$ is divisib by 5

Q $\boxed{2}$ Use Math Induction to prove $\sum_{i=1}^{n} i = 1+2+3+\cdots+n = \frac{n(n+1)}{2}$

$\boxed{S}$:

1) We prove it for $n=1$:

$$\sum_{i=1}^{1} i = 1 \overset{?}{=} \frac{1(1+1)}{2} \quad \text{yes} ✓$$

2) Assume $\sum_{i=1}^{k} i = 1+2+\cdots+k = \frac{k(k+1)}{2}$ for $\underline{\text{some}}$ $n=k$ ✓

3) We prove $\sum_{i=1}^{k+1} i = 1+2+\cdots+\boxed{k+1}$:

$$= \frac{(k+1)(k+1+1)}{2} \quad \text{when } n=k+1$$

$$= \frac{(k+1)(k+2)}{2} ✓$$

$$\sum_{i=1}^{k+1} i = \underbrace{1+2+\cdots+k}_{\text{from step \#2}} + k+1$$

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

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

Q $\boxed{3}$ Use Math Induction and prove that n^3+2n is divisible by 3 $\forall n \geq$

1) we prove it for $n=1$ $(1)^3+2(1)=3$ is divisible by 3. ✓

2) Assume k^3+2k is divisible by 3 for $\underline{\text{some}}$ $n=k$ ✓.

3) We prove $\underline{(k+1)^3}+2(k+1)$ ~~whic~~ is divisible by 3:

Now: $\underbrace{(k+1)^3}+2k+2 = \underbrace{k^3+3k^2+3k+1}+2k+2$

so $\underbrace{k^3+2k}_{\text{by step \#2 it is } |3} + \underbrace{3k^2+3k+3}$

$$= 3(k^2+k+1)$$
which is $|3$

$\therefore$ $(k+1)^3+2(k+1)$ is divisible by 3

Q$\boxed{4}$ Use math Induction & prove that n^5+4n is divisible by $5 \ \forall \ n \geq 1$
(Hint: $(k+1)^5 = k^5+5k^4+10k^3+10k^2+1$)

1) For $n=1$: $(1)^5+4(1) = 1+4 = 5$ which is div. by 5 ✓

2) Assume k^5+4k is div. by 5 for some $n=k$

3) Prove $(k+1)^5+4(k+1)$ is div. by 5 for $n=k+1$:

$$k^5+5k^4+10k^3+10k^2+1+4k+4$$

$$\underbrace{5k^4+10k^3+10k^2+5+k^5+4k}$$

$$\underbrace{5(k^4+2k^3+2k^2+1)}_{\text{factor of } 5} + \underbrace{k^5+4k}_{\text{by step \#2}}$$

so whole statement is div. by 5.

<u>Counting:</u>

ex: $\binom{5}{3} = 5C3$

↳ 5 choose 3 (order not important)

$\{P_1, P_2, P_3, P_4, P_5\}$

↳ $\{P_1, P_2, P_5\} = \{P_2, P_1, P_5\}$ otherwise $\overset{\text{order matters}}{(P_1, P_2, P_5) \neq (P_2, P_1, P_5)}$

<u>Binomial Expansion</u>

ex: $(x+2)^5 = \binom{5}{0}x^5\cdot 2^0 + \binom{5}{1}x^4\cdot 2^1 + \binom{5}{2}x^3\cdot 2^2 + \binom{5}{3}x^2\cdot 2^3 + \binom{5}{4}x\cdot 2^4 + \binom{5}{5}x^0\cdot 2^5 = x^5+10x^4+40x^3+80x^2+80x+32$

<u>General Formula:</u>

$$\binom{n}{k} = nCk = \frac{n!}{(n-k)!\,k!}$$

ex: $\binom{10}{3} = 10C3 = \dfrac{10!}{7!\,3!} = 120$ ex: $\binom{7}{4} = \dfrac{7\times 6\times 5}{3!} = 35$

Q. A is a set with 10 elements. $|A| = 10$.
How many subsets of $\underbrace{\text{order } 3}_{(\text{size}=3)}$ does A have?

Definition:
A set D of order k
means $|D| = k$.

so $10C3 = 120$

Q. Passwords consist of 5 distinct digits and each digit is a number between 2 & 8. How many passwords can you construct?

$8-2+1 = 7$ digits. No repeating digits

□ □ □ □ □
↓ ↓ ↓ ↓ ↓
$7 \times 6 \times 5 \times 4 \times 3 = 2520 = 7P5 = \frac{7!}{(7-5)!}$
possibilities

If repeating digits is allowed then:
□ □ □ □ □
↓ ↓ ↓ ↓ ↓
$7 \times 7 \times 7 \times 7 \times 7 = 7^5$
$= 16807$

General Formula:

$nCk = \frac{n!}{(n-k)!\,k!}$ & $nPk = \frac{n!}{(n-k)!}$

7/8/2021

~~Induction Practice:~~

~~Q. $n^5 + 4n$ is divisible by $5 \ \forall \ n \geq 1$~~

Direct Proof:

Q. Prove $\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{n} = 2^n$

proof:
$$2^n = (\underset{x}{1} + \underset{a}{1})^n = \binom{n}{0} 1^n \cdot 1^0 + \binom{n}{1} 1^{n-1} \cdot 1^1 + \binom{n}{2} 1^{n-2} \cdot 1^2 + \dots + \binom{n}{n} 1^0 \cdot 1^n$$
$$= \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \dots + \binom{n}{n} \checkmark$$

Q. A is a set with 10 elements. $|A| = 10$.
How many subsets of $\underbrace{\text{order } 3}_{(\text{size}=3)}$ does A have?

Definition:
A set D of order k
means $|D| = k$.

so $10C3 = 120$

Q. Passwords consist of 5 distinct digits and each digit is a number between 2 & 8. How many passwords can you construct?

$8-2+1 = 7$ digits. No repeating digits

□ □ □ □ □
↓ ↓ ↓ ↓ ↓
$7 \times 6 \times 5 \times 4 \times 3 = 2520 = 7P5 = \frac{7!}{(7-5)!}$
possibilities

If repeating digits is allowed then:
□ □ □ □ □
↓ ↓ ↓ ↓ ↓
$7 \times 7 \times 7 \times 7 \times 7 = 7^5$
$= 16807$

General Formula:

$nCk = \frac{n!}{(n-k)!\,k!}$ & $nPk = \frac{n!}{(n-k)!}$

7/8/2021

~~Induction Practice:~~

~~Q. $n^5 + 4n$ is divisible by $5 \ \forall \ n \geq 1$~~

Direct Proof:

Q. Prove $\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{n} = 2^n$

proof:

$$2^n = (\underset{\downarrow x}{1} + \underset{\downarrow a}{1})^n = \binom{n}{0} 1^n \cdot 1^0 + \binom{n}{1} 1^{n-1} \cdot 1^1 + \binom{n}{2} 1^{n-2} \cdot 1^2 + \dots + \binom{n}{n} 1^0 \cdot 1^n$$

$$= \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \dots + \binom{n}{n} \ \checkmark$$

Equivalence Relation:

$A = \{1, 2, 3, 4, 7, 9, 10\}$

& "$=$" is an E.R:

The classes are:

$[1] = \{1, 3\} \nearrow (2,2) = 2^2$ $\quad [1] \cup [2] \cup [4] = A$

$[2] = \{2, 7, 9\} \nearrow (3,3) \hookrightarrow 3^2$ $\quad$ "$=$" can be viewed as subset of $A \times A$

How many elements does "$=$" have?

$[4] = \{4, 10\} \nearrow (2,2) \hookrightarrow 2^2$

Give me the elements of "$=$" as a subset of $A \times A$. ←

$$\text{"="} = \{(1,1), (3,3), (1,3), (3,1), (2,2), (7,7), (9,9), (2,7), (7,2), (2,9), (9,2), (7,9), (9,7), (4,4), (10,10), (4,10), (10,4)\}$$

$\#$ of elements $= 2^2 + 3^2 + 2^2 = 17$

Counting:

Helpful Facts:

1) $\binom{n}{k} = \binom{n}{n-k}$

ex: $\binom{13}{4} = \binom{13}{9}$

ex: $\binom{7}{3} = \binom{7}{4}$

Q. 10 men, 8 women,

$\boxed{1}$ Select 7 randomly:

Find # of all possible selections where exactly 1 female is in the selection.

S. $\binom{10}{6}\binom{8}{1} = 10C6 \times 8C1 = 1680$

$$\underbrace{\underset{\text{6 men}}{\binom{10}{6}} \underset{\text{1 female}}{\binom{8}{1}}}_{\substack{\text{multiply} \\ \text{(and)}}}$$

$\boxed{2}$ Find all possible selection where <u>at least</u> <u>3 men</u> are selected:

S. $\binom{10}{3}\binom{8}{4} + \binom{10}{4}\binom{8}{3} + \binom{10}{5}\binom{8}{2} + \binom{10}{6}\binom{8}{1} + \binom{10}{7}\binom{8}{0}$

$$\underbrace{\underset{\text{3 men}}{\binom{10}{3}} \underset{\text{4 female}}{\binom{8}{4}}}_{\substack{\text{multiply} \\ \text{(and)}}} \quad \underset{\text{(Or)}}{+}$$

Q. P, V, S

In how many ways can we select such committee where F, M, F?

$$\underbrace{\text{Female P}}_{\downarrow \atop 5}, \underbrace{\text{Male V}}_{\downarrow \atop 6}, \underbrace{\text{Female S}}_{\downarrow \atop 4}$$

$$5 \times 6 \times 4$$

Fact: $\overset{a_5}{4}x^5 + 7x + \overset{a_0}{10} = 0$

Find all $\underbrace{\text{rational}}_{\frac{\text{integer}}{\text{integer}}}$ roots:

rational root = $\dfrac{\text{factor of } a_0}{\text{factor of } a_5}$

Fact: $a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 = 0$

where $a_0, a_1, \dots, a_n \in \mathbb{Z}$

If we have a rational root, then

the rational root = $\dfrac{\text{factor of } a_0}{\text{factor of } a_n}$

(Not every rational # in this form is a root!)

Q. Does $x^4 + 2x - 4$ have rational roots?

possible rational roots:

$\frac{-4}{1}$ → sub. -4 for x & check if $=0$.

$\frac{4}{1}$ → " 4 "

$\frac{2}{1}$ → " 2 "

$\frac{-2}{1}$ → " -2 "

$\frac{-1}{1}$ → " -1 "

$\frac{1}{1}$ → " 1 "

Q. $3x^5 - 2x - 1 = 0$

Find all rational roots if possible

$\frac{1}{1}$, $f(1) = 0$ ✓ $\quad$ $\frac{-1}{1}$, $f(-1) \neq 0$

$\frac{1}{3}$, $f(\frac{1}{3}) \neq 0$ $\quad$ so 1 is the only rational root. All other roots are irrational.

$\frac{-1}{3}$, $f(\frac{-1}{3}) \neq 0$

Fact: $a_0, a_1, \cdots, a_n \in \mathbb{Z}$

and $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 = 0$

If $\exists$ a prime number q, s.t $\left[\begin{array}{l} q | a_0, q | a_1, q | a_2, \cdots q | a_{n-1} \\ q \nmid a_n, q^2 \nmid a_0 \end{array}\right.$

then there is no rational roots

Q. $3x^5 + 6x^3 + 8x + 10 = 0$

This polynomial has no rational roots.

Why? $q=2$, $q|10$, $q|8$, $q|6$, $q \nmid 3$, $q^2 \nmid 10$

$2|10 \quad 2|8 \quad 2|6 \quad 2 \nmid 3 \quad 4 \nmid 10$

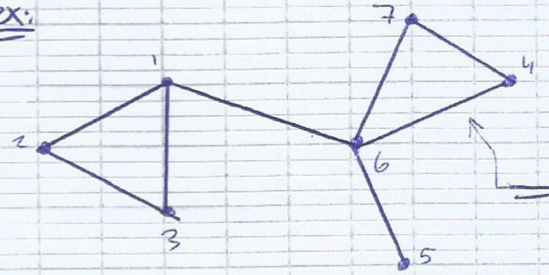
So by the theorem, no rational roots.

7/12/2021

Definition: $G(V, E)$
- V is set of all vertices,
- E is set of all edges (edge is undirecte line segment)

- We say G is a graph of order $\underline{n}$ and size m, where $n = |V|$ and $m = |E|$

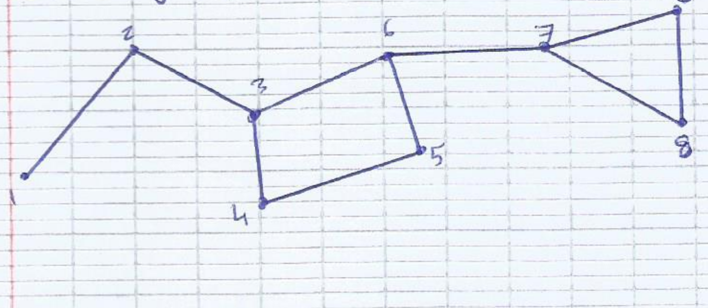
ex:



Graph of order 7 (num. of vertices) and size 8 (num of edges)

$\Rightarrow$ Simple Undirected
- We do not allow multiple edges between 2 vertices

ex: (edge, path)



- order 9
- 1-2 → edge, 7-8 edge
  3-4 edge
- 1-2-3-4-5 path
  (sequence of edges)

Fact: $a_0, a_1, \dots, a_n \in \mathbb{Z}$

and $a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 = 0$

If $\exists$ a prime number q, s.t $\left[\begin{array}{l} q \mid a_0, q \mid a_1, q \mid a_2, \cdots q \mid a_{n-1} \\ q \nmid a_n, q^2 \nmid a_0 \end{array}\right.$
then there is no rational roots

Q. $3x^5 + 6x^3 + 8x + 10 = 0$

This polynomial has no rational roots.

Why? $q = 2$, $q \mid 10$, $q \mid 8$, $q \mid 6$, $q \nmid 3$, $q^2 \nmid 10$

$2 \mid 10$ $2 \mid 8$ $2 \mid 6$ $2 \nmid 3$ $4 \nmid 10$

So by the theorem, no rational roots.

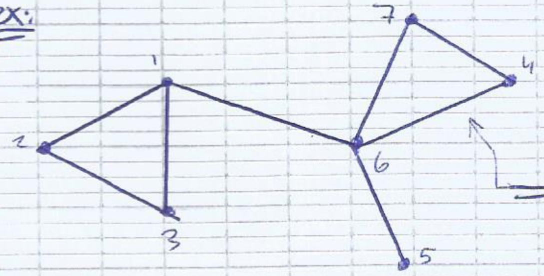
7/12/2021

Definition: $G(V, E)$ • V is set of all vertices,

• E is set of all edges (edge is undirecte line segment)

- We say G is a graph of order $\underline{n}$ and size m, where $n = |V|$ and $m = |E|$

ex:

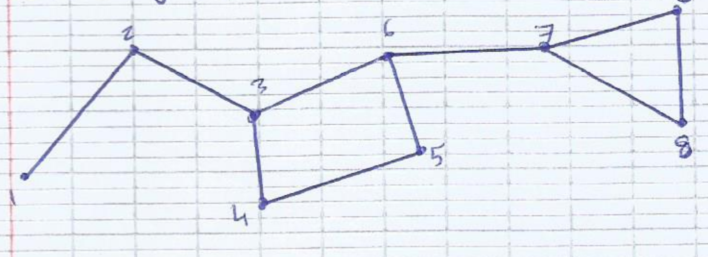


Graph of order 7 (num. of vertices) and size 8 (num of edges)

$\Longrightarrow$ Simple Undirected

- We do not allow multiple edges between 2 vertices

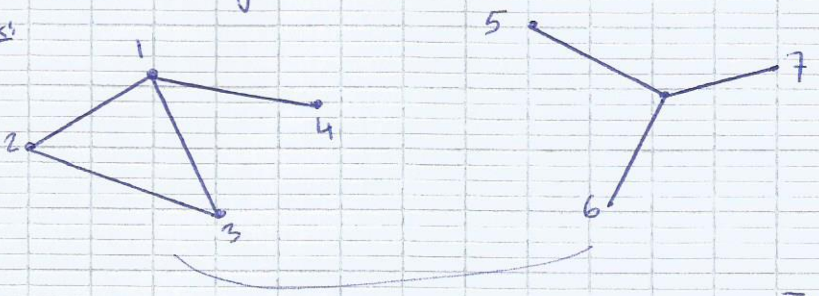
ex: (edge, path)



- order 9
- 1-2 → edge, 7-8 edge
  3-4 edge
- 1-2-3-4-5 path
  (sequence of edges)

Definition: A graph is connected if $\exists$ a path between every 2 vertices.

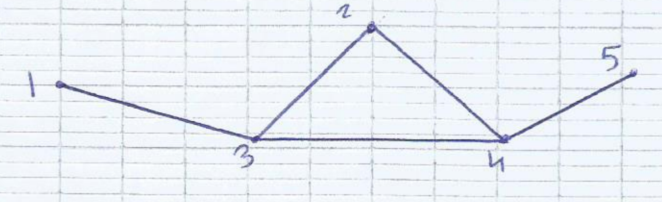
ex:



It is not connected

Why? No path b/w 1 & 5.

ex:



It is connected

1-3-4-5 path   1-3-2 path

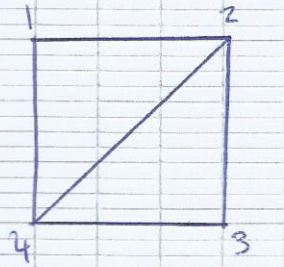
1-3 path   ⋮

1-3-2-4 path

Note: every edge is a path, but not every path is an edge!

Definition: Complete graph is a connected graph s.t $\exists$ an edge b/w every 2 vertices.

ex:

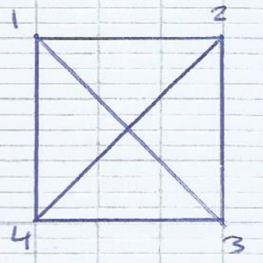


It is connected but not complete.

There is no edge between 1 & 3.

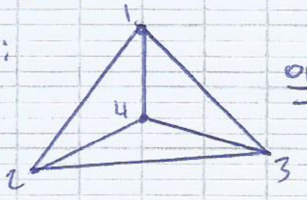
Notation: A complete graph of order n is denoted by K_n

ex: K_4: (don't count the middle or else it will be K_5)

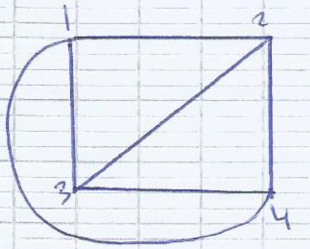


complete graph with order 4.

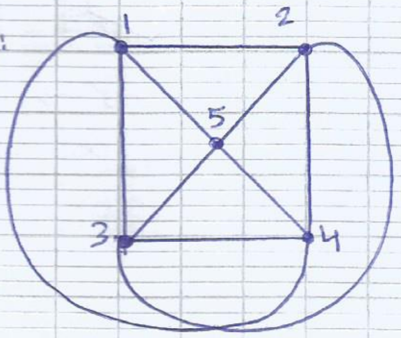
or K_4:



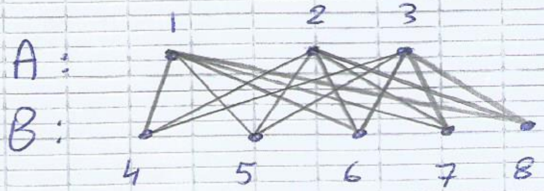
or K_n



ex: K_5:

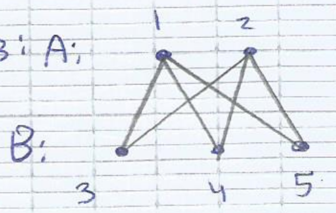


ex: $K_{3,5}$: complete bipartite graph (connected).



Every 2 vertices in A or B are not connected by an edge but every vertex in A is connected by an edge to every vertex in B.

ex: $K_{2,3}$: A:



for 1 to 2:	for 3 to 5:
1-3-2	3-1-5
1-4-2	3-2-5
1-5-2	

for 1 to 5:

1-5

1-3-2-5

1-4-2-5

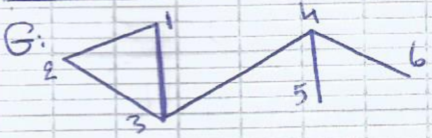
- $K_{n,m}$: Complete Bipartite graph of order n+m.

A: 1 ... n → n vertices

B: n+1 ... n+m. → m vertices

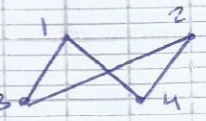
Definition: A connected graph with no cycles is called a tree

ex: G:



G is of order 6 but not a tree: because 1-2-3-1 is a cycle of G

ex: $K_{2,2}$:

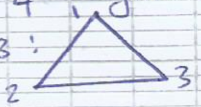


Not a tree: 1-3-2-4-1 is a cycle

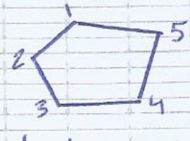
Definition: A cycle is a sequence of edges, initial vertex = terminal vertex.

ex: C_4: cycle of order 4, C_n: cycle of order n

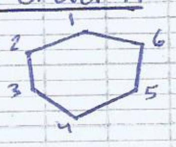
C_3:



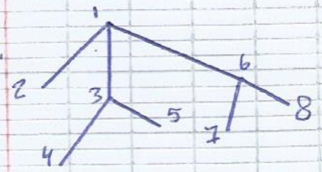
, C_5:



, C_6:

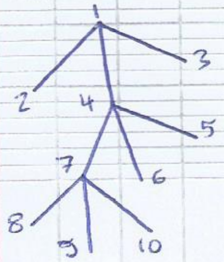


ex:



Connected graph with no cycles → Tree

ex:



1-4-7-10

1-4-6

→ order 10, size 9

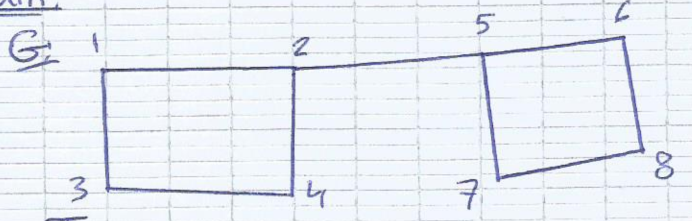
Big Result (Trees)

Let G be a connected graph of order n. The following are equivalent:

1) G is tree
2) size of G n-1
3) G has no cycles
4) ∃! path between every 2 vertices

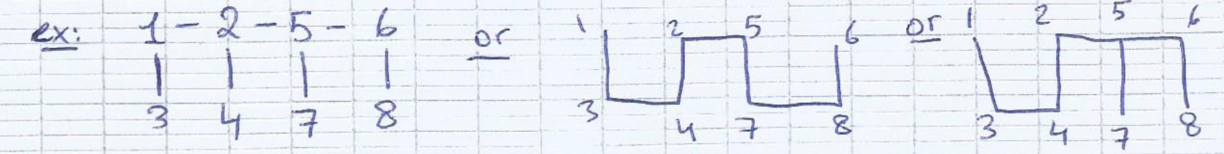
Big Theorem: Every connected graph has a spanning tree

Explain:

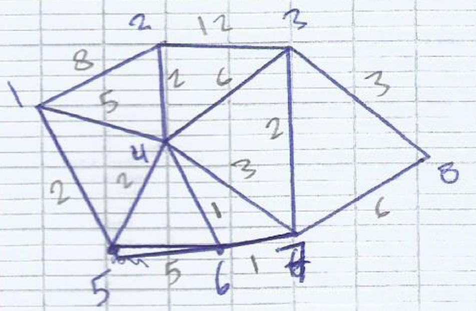


Spanning Tree:
subgraph of G has same order as G but it is a tree

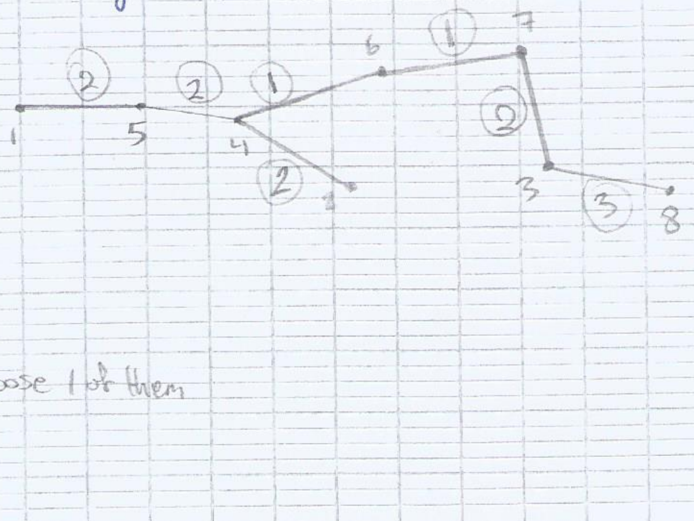
ex:



Dijkstra algorithm:

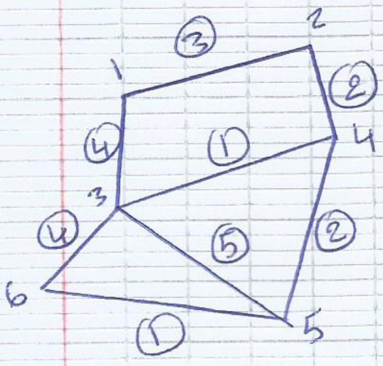


Weighted Graph:
Find minimum spanning tree.
↳ Construct a tree s.t the weighted distance between any 2 vertices is minimum

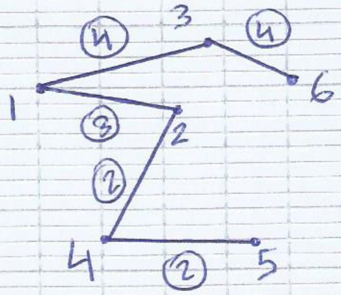


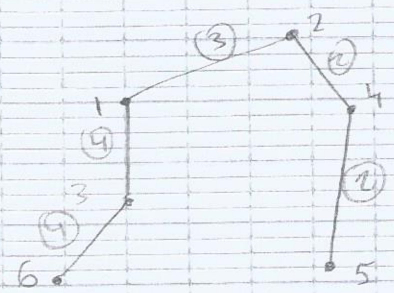
V	1	2	3	4	5	6	7	8
1	$\boxed{0}$	8	∞	5	2	∞	∞	∞
5	X	8^1	∞	2+2 4^5	$\boxed{2}^1$	5+2=7 7^5	∞	∞
4	X	2+4=6 6^4	6+4 10^4	$\boxed{4}^5$	X	1+4 5^4	3+4 7^4	∞
6	X	6	10^4	X	X	$\boxed{5}^4$	1+5 6^6	∞ → choose 1 of them
2	X	$\boxed{6}^4$	12+6 10^4	X	X	X	6^6	∞
7	X	X	2+6 8^7	X	X	X	$\boxed{6}^6$	12^7
3	X	X	$\boxed{8}^7$	X	X	X	X	3+8 11^3
8	X	X	X	X	X	X	X	$\boxed{11}^3$

ex:

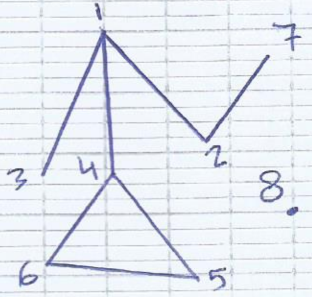


V	1	2	3	4	5	6
1	$\boxed{0}$	3^1	4^1	∞	∞	∞
2	X	$\boxed{3}^1$	4^1	5^2	∞	∞
3	X	X	$\boxed{4}^1$	5^2	9^3	8^3
4	X	X	X	$\boxed{5}^2$	7^4	8^3
5	X	X	X	X	$\boxed{7}^4$	8^3
6	X	X	X	X	X	$\boxed{8}^3$





Q.



degree(1) = 3
degree(4) = 3
degree(6) = 2
degree(3) = 1
degree(8) = 0

Degree of A Vertex:

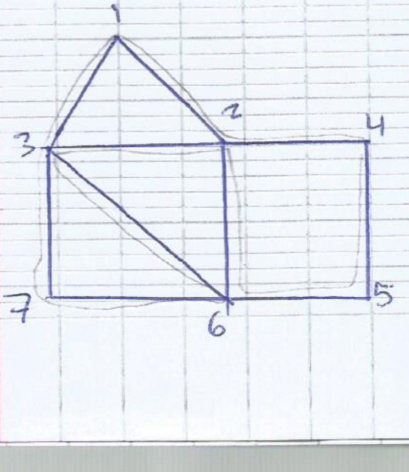
deg$\underbrace{\text{(vertex)}}_{v}$ = # of edges connected to v.

Big Result: Σ degrees = 2× Size
= 2×(# of edges)

Definition: Eulerian (Euler Circuit)

A connected graph is Eulerian iff we can start at a vertex V_0 and visit each edge exactly once and come back to V_0.
(It is possible that you visit a vertex more than once)

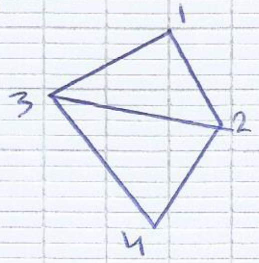
ex:



4-2-1-3-7-6-3-2-6-5-4

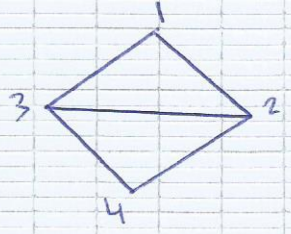
Big Result: A connected graph is Eulerian iff deg(each vertex) is an even integer)

ex:



Not Eulerian:
deg(2) = 3 is not even.

Euler Trail: start at a vertex v_0 visit each edge exactly once then ~~edge~~ end up at a vertex diff. from v_0



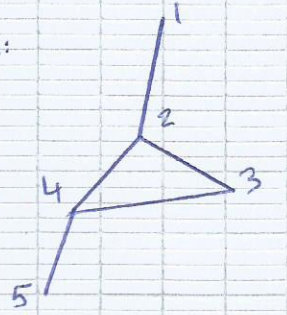
Euler Trail (but not Eulerian)

②-1-3-4-2-③ { start from the vertex of odd degree

→ doesn't work from 1.

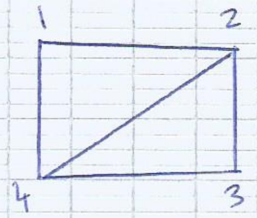
Big Result: A connected graph is Euler Trail iff exactly 2 vertices are of odd degree

ex:



Not Eulerian
Not Euler Trail

ex:



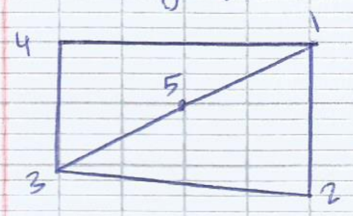
Not Eulerian

②-3-4-2-1-④

Euler Trail

Hamiltonian: A connected graph of order n is Hamiltonian iff C_n is a subgrap of the graph.

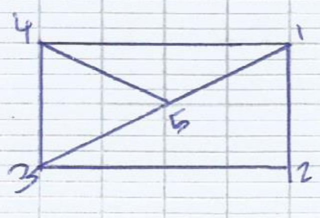
ex:



1-2-3-5-1 ⇒ C_4
Not Hamiltonian

visit each V once

ex:



5-1-2-3-4-5 ⇒ C_5
Yes Hamiltonian.
or 1-2-3-5-4-1

→ Not Eularian
Not Euler Trail