2012

24 September 2019 21:33

Relatively prime

$a \equiv b \pmod n$ if n divides $(a-b)$

$8 \equiv 4 \pmod 2$ since 2 divides $8-4=4$

$12 \not\equiv 1 \pmod 3$ since 3 doesn't divide $12-1=11$

$16 \pmod 9 \equiv 7 \pmod 9$

↳ $\mathbb{Z}_9 = \{0, 1, 2, \ldots 8\}$

Evaluate $7^{40} \pmod 9$ $\quad \mathbb{Z}_9 = \{0, 1, 2, \ldots 8\}$

$7^1 = 7 \pmod 9$

$7^2 = 49 \equiv 4 \pmod 9$

$7^3 = (7^2 \times 7) = (4 \times 7) = 28 \equiv 1 \pmod 9$

$7^4 = (7^3 \times 7) = (1 \times 7) = 7 \pmod 9$

$7^5 = (7^4 \times 7) = (7 \times 7) = 49 \equiv 4 \pmod 9$

7^{40}

Evaluate $7^{41} \pmod 9$

$7^3 = 1 \pmod 9$

Since

$7^{41} \equiv (7^3)^{13} (7)^2 \pmod 9$

$7^{41} \equiv (1)^{13} (7)^2 \pmod 9$

$7^{41} \equiv (1)(49) \pmod 9$

$7^{41} \equiv 4 \pmod 9$

Powers Recap

$7^{41} = 7^{39+2}$

$= (7^{39})(7^2)$

$= (7^{3 \times 13})(7^2)$

$= (7^3)^{13} (7^2)$

Fast Exponentiation

Evaluate $3^{10} \pmod{11}$ $\quad (0, 1, 2, \ldots 10)$

① Express the power (10) in terms of powers of 2

2^3 2^2 2^1 2^0

2	10	0
2	5	1
2	2	0
	1	

$10 = 1010$

$10 = 8 + 2$

$\Rightarrow 3^{10} = (3^8)(3^2)$

② Calculate the powers

$3^1 \equiv 3 \pmod{11}$

$3^2 \equiv 9 \pmod{11}$

$3^4 = (9 \times 9) \pmod{11} \equiv 81 \pmod{11} \equiv 4 \pmod{11}$

$3^8 = (3^4 \times 3^4) = 4 \times 4 \pmod{11} \equiv 16 \pmod{11} \equiv 5 \pmod{11}$

$\Rightarrow 3^{10} \pmod{11}$

$= (3^8)(3^2) \pmod{11}$

$\equiv (5)(9) \pmod{11}$

$\equiv 45 \pmod{11}$

$\equiv 1 \pmod{11}$

$\Rightarrow 3^{10} \pmod{11} \equiv 1 \pmod{11}$

Evaluate $2^{644} \pmod{645}$

① Express 644 as a power of 2

2	644	0
2	322	0
2	161	1
2	80	0
2	40	0
2	20	0
2	10	0
2	5	1
2	2	0
	1	

9	8	7	6	5	4	3	2	1	0
1	0	1	0	0	0	0	1	0	0

$644 = 1 0 1 0 0 0 0 1 0 0$

$644 = (1 \times 2^9) + (1 \times 2^7) + (1 \times 2^2)$

$644 = 512 + 128 + 4$

$\Rightarrow 2^{644} = (2^{512}) \times (2^{128}) \times (2^4)$

② Evaluate powers

$2^1 = 2 \pmod{645}$

$2^2 = 4 \pmod{645}$

$2^3 = 8 \pmod{645}$

$2^4 = 16 \pmod{645}$

$\frac{65536}{645} = 101 \cdots$

$101 \times 645 = 65145$

$65536 - 65145 = 391$

$2^4 = 16 \pmod{645}$

$(2^4 \times 2^4) \to 2^8 = (16 \times 16) \pmod{645} \equiv 256 \pmod{645}$

$(2^8 \times 2^8) \to 2^{16} = (256 \times 256) \pmod{645} = 65536 \pmod{645} \equiv 391 \pmod{645}$

$(2^{16} \times 2^{16}) \to 2^{32} = (391 \times 391) \pmod{645} = 152881 \pmod{645} \equiv 16 \pmod{645}$

$(2^{32} \times 2^{32}) \to 2^{64} = (16 \times 16) \pmod{645} \equiv 256 \pmod{645}$

$(2^{64} \times 2^{64}) \to 2^{128} = (256 \times 256) \pmod{645} \equiv 391 \pmod{645}$

$(2^{128} \times 2^{128}) \to 2^{256} = (391 \times 391) \pmod{645} \equiv 16 \pmod{645}$

$(2^{256} \times 2^{256}) \to 2^{512} = (16 \times 16) \pmod{645} \equiv 256 \pmod{645}$

$\Rightarrow 2^{644} = (2^{512})(2^{128})(2^4) \pmod{645}$

$2^{644} = (256)(391)(16) \pmod{645}$

$2^{644} = 1601536 \pmod{645}$

$2^{644} \equiv 1 \pmod{645}$

NNB

Eg2 Calculate $91^{239} \pmod{6731}$

① Convert 239 to binary

239	1
119	1
59	1
29	1
14	0
7	1
3	1
1	

7 6 5 4 3 2 1 0

$239 = 1\,1\,1\,0\,1\,1\,1\,1_2$

$239 = (1\times2^7)+(1\times2^6)+(1\times2^5)+(0\times2^4)+(1\times2^3)+(1\times2^2)+(1\times2^1)+(1\times2^0)$

$239 = 128+64+32+8+4+2+1$

$\Rightarrow 91^{239} = 91^{128+64+32+8+4+2+1}$

$= (91^{128})(91^{64})(91^{32})\cdots(91^{1})$

$91^1 \equiv 91 \pmod{6731}$

$91^2 = 8281 \pmod{6731} \equiv 1550 \pmod{6731}$

$91^4 = (1550)^2 \pmod{6731} = 2402500 \pmod{6731} \equiv 6264 \pmod{6731}$

$2402500 \div 6731 = 356$ r

$356 \times 6731 = 2396236$

$2402500 - 2396236 = 6264$

$91^8 = (6264)^2 \pmod{6731} = 39237696 \pmod{6731} \equiv 2697 \pmod{6731}$

$91^{16} = (2697)^2 \pmod{6731} = 7273809 \pmod{6731} \equiv 4329 \pmod{6731}$

$91^{32} = (4329)^2 \pmod{6731} = 18740241 \pmod{6731} \equiv 1137 \pmod{6731}$

$91^{64} = (1137)^2 \pmod{6731} = 1292769 \pmod{6731} \equiv 417 \pmod{6731}$

$91^{128} = (417)^2 \pmod{6731} = 173889 \pmod{6731} \equiv 5614 \pmod{6731}$

$\Rightarrow 91^{239} = (91)(1550)(6264)(2697)(1137)(417)(5614) \pmod{6731}$

$91^{239} = (883537200)(1278725913)(5614) \pmod{6731}$

$91^{239} = (5947)(4188)(5614) \pmod{6731}$

$91^{239} = (24906036)(5614) \pmod{6731}$

$91^{239} = (1336)(5614) \pmod{6731}$

$91^{239} = 7500304 \pmod{6731}$

$\boxed{91^{239} = 1970 \pmod{6731}}$

FLT: ① $a^{p-1} \equiv 1 \pmod{p}$

② $a^p \equiv a \pmod{p}$

Eg Let $a = 2$ and $p = 5$ ie $\mathbb{Z}_5 \pmod 5$

① $2^{5-1} \equiv 1 \pmod 5$?

↳ $2^4 = 16 \pmod 5 \equiv 1 \pmod 5$

② $2^5 \equiv 2 \pmod 5$?

↳ $32 \equiv 2 \pmod 5$ ✓

Example: Show that $2^{340} \equiv 1 \pmod{11}$

$p = 11$, $p-1 = 10$

Now $2^{340} \pmod{11}$

$2^{340} = (2^{10 \times 34}) = (2^{10})^{34} \pmod{11}$

FLT: $2^{11-1} \equiv 1$ $= (1)^{34} \pmod{11}$

$\Rightarrow 2^{340} \equiv 1 \pmod{11}$ ..... QED

Example 2: Calculate $31^{5323905} \pmod{1039}$

given that 1039 is prime.

Here 1039 is prime $\Rightarrow$ we can use FLT.

$1039 - 1 = 1038$

1038 —

$1039 - 1 = 1038$

$\Rightarrow \quad 31^{1038} \equiv 1 \pmod{1039}$ .... FLT

Now $5323905 = 5129(1038) + 3$

$a^{x+y} = a^x \cdot a^y$

$\Rightarrow \quad 31^{5323905} = 31^{5129(1038)+3}$

$= \left(31^{5129(1038)}\right)\left(31^3\right)$

$a^{xy} = (a^x)^y$ $= \left(31^{(1038)(5129)}\right)\left(31^3\right)$

$= \left(31^{1038}\right)^{5129}\left(31\right)^3$

$= (1)^{5129}(31)^3 \pmod{1039}$

$= 1 \quad (31)^3 \pmod{1039}$

$= (31)^3 \pmod{1039}$

$= 29791 \pmod{1039}$

$31^{5323905} \equiv 699 \pmod{1039}$

Eg 1 : Find $3^{-1} \pmod 7$ by inspection

Mod 7 = {0, 1, 2, 3, 4, 5, 6}

$3 \times 0 = 0 \pmod 7$ ×

$3 \times 1 = 3 \pmod 7$ ×

$3 \times 2 = 6 \pmod 7$ ×

$3 \times 3 = 9 \pmod 7 \equiv 2 \bmod 7$ ×

$3 \times 4 = 12 \pmod 7 \equiv 5 \pmod 7$ ×

$3 \times 5 = 15 \pmod 7 \equiv 1 \pmod 7$ ✓

$3 \times 6 =$

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

Eg2 Find the inverse $5^{-1} \pmod 7$ using FLT

ie Find a number x such that $5x \equiv 1 \pmod 7$

Since the mod is 7 which is prime and $5 \nmid 7$

$\Rightarrow$ Use FLT $\quad a^{p-1} \equiv 1 \pmod p$ $\quad p=7$, $a=5$

$$5^{7-1} \equiv 1 \pmod 7$$

$$5^6 \equiv 1 \pmod 7$$

Multiply both sides by 5^{-1}

$$5^{-1}(5^6) \equiv 5^{-1}(1) \pmod 7$$

$$5^5 \equiv 5^{-1} \pmod 7$$

$$3125 \equiv 5^{-1} \pmod 7$$

$$3 \equiv 5^{-1} \pmod 7$$

$a^{-1} = a^{p-2}$

$\frac{3125}{7} = 446\frac{3}{7}$

$446 \times 7 = 3122$

$3125 - 3122 = 3$

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

Eg3 Solve $3x \equiv 1 \pmod 7$

This can also be written as

$$3x - 7y = 1 \quad \text{... Diophantine Eqn}$$

$3(5) \equiv 1 \pmod 7$

$(3)(5) - 7(y) = 1$

As before, to solve this Diophantine Eqn, use Euclid. Alg

ie Find gcd (3, 7)

$7 = 2(3) + 1 \rightarrow \gcd = 1 \longrightarrow 7 - 2(3) = 1$

~~$3 = 3(1) + 0$~~

Since $1 \mid 1$, solutions exist

Using the reverse Euclidean Alg

$1(7) - 2(3) = 1$

$x = -2$

$\Rightarrow x = -2$ is a solution of $3x \equiv 1 \pmod 7$

But -2 is not in $\pmod 7$, but $-2 + 7 = 5 \pmod 7$

$\Rightarrow x = 5$ is a solution of $3x \equiv 1 \pmod 7$

$\Rightarrow$ $x=5$ is a solution of $3x \equiv 1 \pmod 7$

Eg 4 Solve $81x \equiv 1 \pmod{256}$

ie $81x - 256y = 1$

① Euclidean Alg

$256 = 3(81) + 13$ → $256 - 3(81) = 13$

$81 = 6(13) + 3$ → $81 - 6(13) = 3$ ✓

$13 = 4(3) + 1$ → gcd → $13 - 4(3) = 1$ ✓

~~$3 = 3(1) + 0$~~

Since $1 \mid 1$, solutions exist

② Reverse Euclid Alg

$1(13) - 4(3) = 1$

$1(13) - 4[81 - 6(13)] = 1$

$1(13) - 4(81) + 24(13) = 1$

$25(13) - 4(81) = 1$

$25[256 - 3(81)] - 4(81) = 1$

$25(256) - 75(81) - 4(81) = 1$

mod 256 → ~~$25(256)$~~ $- 79(81) = 1$

$x = -79$

But -79 is not $\pmod{256}$ $\Rightarrow$ $-79 + 256 = 177$

$\Rightarrow$ $(81)(177) \equiv 1 \pmod{256}$ ie $x = 177$

Find the inverse of $A = \begin{pmatrix} 5 & 3 \\ 2 & 1 \end{pmatrix} \pmod{26}$

- $\det(A) = (5)(1) - (3)(2) = 5 - 6 = -1$
- $\text{adj}(A) = \begin{pmatrix} 1 & -3 \\ -2 & 5 \end{pmatrix}$

$A^{-1} = \frac{1}{\det(A)} \cdot \text{adj}(A)$

Since this is a modular Matrix

Find the inverse of $A = \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix}$ mod 5.

- $\det(A) = (3)(1) - (2)(2) = -1$
- $\text{adj}(A) = \begin{pmatrix} 1 & -2 \\ -2 & 3 \end{pmatrix}$

$\Rightarrow$ The usual integer matrix inverse is

$$A^{-1} = \frac{1}{\det(A)} \begin{pmatrix} 1 & -2 \\ -2 & 3 \end{pmatrix} = \frac{1}{-1} \begin{pmatrix} 1 & -2 \\ -2 & 3 \end{pmatrix} = \begin{pmatrix} -1 & 2 \\ 2 & -3 \end{pmatrix} \text{ mod 5}$$

But we are working (mod 5)

$$\Rightarrow A^{-1} = \begin{pmatrix} 4 & 2 \\ 2 & 2 \end{pmatrix} \pmod 5$$

* Check: $A \cdot A^{-1} = \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 4 & 2 \\ 2 & 2 \end{pmatrix} \pmod 5$

$$= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod 5$$

If $A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}$ then find A^{-1} (mod 26)

- $\det(A) = (2)(8) - (3)(7) = 16 - 21 = -5$
- $\text{adj}(A) = \begin{pmatrix} 8 & -3 \\ -7 & 2 \end{pmatrix}$

→ We cannot use the same formula for finding A^{-1} as before

Instead we need $(-5)^{-1} \pmod{26}$ → $\{0, 1, 2, \ldots 25\}$

$-5 + 26 = 21$ ie $(21)^{-1} \pmod{26}$ ie $21x \equiv 1 \pmod{26}$

$26 = 1(21) + 5$ $\quad 26 - 1(21) = 5$ ✓

$21 = 4(5) + 1$ → gcd $\quad 21 - 4(5) = 1$ ✓

$1(21) - 4(5) = 1$

$1(21) - 4[26 - 1(21)] = 1$

$1(21) - 4(26) + 4(21) = 1$

$5(21) - 4(26) = 1 \pmod{26}$

$1(21) - 4(26) + 4(21) = 1$

$5(21) - 4(26) = 1 \pmod{26}$

$\Rightarrow (5)(21) = 1 \pmod{26}$

$\Rightarrow 21^{-1} = 5 \pmod{26}$

Check:

$21 \times 5 = 105 \pmod{26}$

$\frac{105}{26} \approx 4$

$26 \times 4 = 104$

$105 - 104 = 1 \pmod{26}$

So, we now this 5 as our 'determinant part'

$\Rightarrow A^{-1} = 5 \begin{pmatrix} 8 & -3 \\ -7 & 2 \end{pmatrix} \pmod{26}$ (adj(A))

$A^{-1} = \begin{pmatrix} 40 & -15 \\ -35 & 10 \end{pmatrix} \pmod{26}$

$A^{-1} = \begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix} \pmod{26}$

* Check: $A \cdot A^{-1} = I \pmod{26}$

$\begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix} = \begin{pmatrix} (2)(14)+(3)(17) & 2(11)+3(10) \\ 7(14)+8(17) & 7(11)+8(10) \end{pmatrix} \pmod{26}$

$= \begin{pmatrix} 79 & 52 \\ 234 & 157 \end{pmatrix} \pmod{26}$

$= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{26}$ ✓

Let $A = \begin{pmatrix} 5 & 3 \\ 2 & 1 \end{pmatrix}$. Find A^{-1} and use it to decode the message NOIJ.

A^{-1}:

- $\det(A) = (5)(1) - (3)(2) = 5 - 6 = -1$
- $\text{adj}(A) = \begin{pmatrix} 1 & -3 \\ -2 & 5 \end{pmatrix}$

we need $(-1)^{-1} \pmod{26}$

ie we need $(25)^{-1} \pmod{26}$ .... $25x \equiv 1 \pmod{26}$

$26 = 1(25) + 1$ → gcd

$1(26) - 1(25) = 1 \pmod{26}$

$25^{-1} = -1 \pmod{26}$ But $-1 + 26 = 25$

$\Rightarrow (25)^{-1} \equiv 25 \pmod{26}$

$\Rightarrow A^{-1} = 25\begin{pmatrix} 1 & -3 \\ -2 & 5 \end{pmatrix} \pmod{26}$

$A^{-1} = \begin{pmatrix} 25 & -75 \\ -50 & 125 \end{pmatrix} \pmod{26}$

$$A^{-1} = \begin{pmatrix} 25 & 3 \\ 2 & 21 \end{pmatrix} \pmod{26}$$

0	1	2	3	4	5	6	7	8	9	10	11	...	25
a	b	c	d	e	f	g	h	i	j	k	l	...	z

To decode

N	O	I	J
13	14	8	9

$\begin{pmatrix} 13 \\ 14 \end{pmatrix} \quad \begin{pmatrix} 8 \\ 9 \end{pmatrix}$

$$\Rightarrow \begin{pmatrix} 25 & 3 \\ 2 & 21 \end{pmatrix}\begin{pmatrix} 13 \\ 14 \end{pmatrix} = \begin{pmatrix} 25(13) + 3(14) \\ 2(13) + 21(14) \end{pmatrix} \bmod 26 = \begin{pmatrix} 367 \\ 320 \end{pmatrix} \bmod 26 = \begin{pmatrix} 3 \\ 8 \end{pmatrix} = \begin{pmatrix} D \\ I \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} 25 & 3 \\ 2 & 21 \end{pmatrix}\begin{pmatrix} 8 \\ 9 \end{pmatrix} = \begin{pmatrix} 25(8) + 3(9) \\ 2(8) + 21(9) \end{pmatrix} \bmod 26 = \begin{pmatrix} 227 \\ 205 \end{pmatrix} \bmod 26 = \begin{pmatrix} 19 \\ 23 \end{pmatrix} = \begin{pmatrix} T \\ X \end{pmatrix}$$

NOIJ → DITX

Eg The ciphertext WKFT was encrypted using a Hill Digraph Cipher using $A = \begin{pmatrix} 4 & 1 \\ 3 & 2 \end{pmatrix}$.

Find A^{-1} and retrieve the plaintext.

- $\det(A) = (4)(2) - (1)(3) = 8 - 3 = 5$
- $\text{adj}(A) = \begin{pmatrix} 2 & -1 \\ -3 & 4 \end{pmatrix}$

We need $(5)^{-1} \pmod{26}$ ... use Euclid

$26 = 5(5) + 1$

$1(26) - 5(5) = 1 \pmod{26}$

$5^{-1} = -5 \pmod{26}$

$\Rightarrow S^{-1} = \boxed{21} \pmod{26}$

$\Rightarrow A^{-1} = 21 \begin{pmatrix} 2 & -1 \\ -3 & 4 \end{pmatrix} \pmod{26}$

$A^{-1} = \begin{pmatrix} 42 & -21 \\ -63 & 84 \end{pmatrix} \bmod 26 = \boxed{\begin{pmatrix} 16 & 5 \\ 15 & 6 \end{pmatrix} \bmod 26}$

W	K	F	T
22	10	5	19

$\begin{pmatrix} 22 \\ 10 \end{pmatrix} \quad \begin{pmatrix} 5 \\ 19 \end{pmatrix}$

Decode

$\Rightarrow \begin{pmatrix} 16 & 5 \\ 15 & 6 \end{pmatrix} \begin{pmatrix} 22 \\ 10 \end{pmatrix} = \begin{pmatrix} 402 \\ 390 \end{pmatrix} \bmod 26 = \begin{pmatrix} 12 \\ 0 \end{pmatrix}$ M A

$\Rightarrow \begin{pmatrix} 16 & 5 \\ 15 & 6 \end{pmatrix} \begin{pmatrix} 5 \\ 19 \end{pmatrix} = \begin{pmatrix} 175 \\ 189 \end{pmatrix} \bmod 26 = \begin{pmatrix} 19 \\ 7 \end{pmatrix}$ T H

* NB *

WKFT ⟶ MATH

Chinese Remainder Theorem

Use CRT to solve $x \equiv 2 \pmod 3$ $r_1 = 2$ $n_1 = 3$

$x \equiv 4 \pmod 5$ $r_2 = 4$ $n_2 = 5$

$x \equiv 6 \pmod 7$ $r_3 = 6$ $n_3 = 7$

Step 1: 3, 5 & 7 are relatively prime ✓

$M = n_1 \cdot n_2 \cdot n_3 = 3 \cdot 5 \cdot 7 = \boxed{105}$

$M_1 = \frac{M}{n_1} = \frac{105}{3} = \boxed{35}$

$M_2 = \frac{M}{n_2} = \frac{105}{5} = \boxed{21}$

$M_3 = \frac{M}{n_3} = \frac{105}{7} = \boxed{15}$

Step 2: Solve ① $M_1 x \equiv 1 \pmod 3$

$35x \equiv 1 \pmod 3$

$2x \equiv 1 \pmod 3$ → 0, 1, 2

By inspection $x = 2 \Rightarrow \boxed{S_1 = 2}$

② $M_2 x \equiv 1 \pmod 5$

$21x \equiv 1 \pmod 5$ → 0, 1, 2, 3, 4

$1x \equiv 1 \pmod 5$

By inspection $x = 1 \Rightarrow \boxed{S_2 = 1}$

③ $M_3 x \equiv 1 \pmod 7$

$15x \equiv 1 \pmod 7$ → 0, 1, 2, 3, 4, 5, 6

$1x \equiv 1 \pmod 7$

By inspection $x = 1 \Rightarrow \boxed{s_3 = 1}$

The solution to the system is

$$x = M_1 r_1 s_1 + M_2 r_2 s_2 + M_3 r_3 s_3$$

$$x = (35)(2)(2) + (21)(4)(1) + (15)(6)(1)$$

$$x = 140 + 84 + 90$$

$$x = 314 \pmod{105}$$

$$\boxed{x \equiv 104 \pmod{105}}$$

Check:

① $x \equiv 2 \pmod 3$
$104 \equiv 2 \pmod 3$ ✓

② $x \equiv 4 \pmod 5$
$104 \equiv 4 \pmod 5$ ✓

③ $x \equiv 6 \pmod 7$
$104 \equiv 6 \pmod 7$ ✓

Eg2: Use CRT to solve

$x \equiv 2 \pmod 3$ $r_1 = 2$ $n_1 = 3$

$x \equiv 3 \pmod 5$ $r_2 = 3$ $n_2 = 5$

$x \equiv 4 \pmod{11}$ $r_3 = 4$ $n_3 = 11$

Step1: 3, 5 & 11 are relatively prime ✓

$M = n_1 \cdot n_2 \cdot n_3 = 3 \cdot 5 \cdot 11 = 165$

$M_1 = \frac{165}{3} = \boxed{55}$

$M_2 = \frac{165}{5} = \boxed{33}$

$M_3 = \frac{165}{11} = \boxed{15}$

Step2: Solve ① $55x \equiv 1 \pmod 3$

$1x \equiv 1 \pmod 3$

By inspection $x = 1 \Rightarrow \boxed{s_1 = 1}$

② $33x \equiv 1 \pmod 5$

$3x \equiv 1 \pmod 5$

By inspection $x = 2 \Rightarrow \boxed{s_2 = 2}$

By inspection $x = 2 \Rightarrow \boxed{S_2 = 2}$

③ $15x \equiv 1 \pmod{11}$

$4x \equiv 1 \pmod{11}$

By inspection $x = 3 \Rightarrow \boxed{S_3 = 3}$

The overall solution

$$x = M_1 r_1 s_1 + M_2 r_2 s_2 + M_3 r_3 s_3$$

$$x = (55)(2)(1) + (33)(3)(2) + (15)(4)(3)$$

$$x = 110 + 198 + 180$$

$$x = 488 \pmod{165}$$

$$\boxed{x = 158 \pmod{165}}$$

Proof By Induction

Step1 : Show the predicate is true for $n=1$

Step2: Assume the predicate is true for $n=k$

Step3: Show the predicate is true for $n=k+1$

Eg: use proof by induction to show that for all $n \in \mathbb{N}$

$$\underbrace{1+2+3+4+\cdots n}_{\text{LHS}} = \underbrace{\frac{n(n+1)}{2}}_{\text{RHS}}$$

Step1 : Show true for $n=1$

$$1$$

$$1$$

$$1$$

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

$$= \frac{2}{2}$$

$$= 1 \quad \checkmark$$

Step2 : Assume true for $n=k$

$$1+2+3+4+\cdots k = \frac{k(k+1)}{2}$$

Step3 : Prove true for $n=(k+1)$

ie Show that

$$1+2+3+4+\cdots k+(k+1) = \frac{(k+1)(k+2)}{2}$$

Sub in $(k+1)$ for n

ie Show that $1+2+3+4+\ldots k+(k+1) = \frac{(k+1)(k+2)}{2}$

LHS: $\underbrace{1+2+3+4+\ldots k}_{\frac{k(k+1)}{2}} + \underbrace{(k+1)}_{1}$

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

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

$= \frac{k^2+3k+2}{2}$

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

Prove by induction that $3+6+9+\ldots+(3n) = \frac{3n(n+1)}{2}$

Step1: True for $n=1$

3

3

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

$= \frac{3(2)}{2}$ ✓

Step2: Assume true for $n=k$

$3+6+9+\ldots (3k) = \frac{3k(k+1)}{2}$

Step3: Show true for $n=k+1$

ie Show $3+6+9+\ldots+3k+3(k+1) = \frac{3(k+1)(k+2)}{2}$

LHS $\underbrace{3+6+9+\ldots 3k}_{\frac{3k(k+1)}{2}} + \underbrace{3(k+1)}_{1}$

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

$= \frac{3k(k+1) + 6(k+1)}{2}$

$= \frac{3k^2+3k+6k+6}{2}$

$= 3k^2+9k+6$

$$= \frac{3k^2 + 9k + 6}{2}$$

$$= \frac{3(k^2 + 3k + 2)}{2} = \frac{3(k+1)(k+2)}{2} = \text{RHS}$$

Prove by induction that

$$1^2 + 2^2 + 3^2 + \ldots n^2 = \frac{n(n+1)(2n+1)}{6}$$

Step 1: Show true for $n=1$

$1^2 = \frac{1(2)(3)}{6}$ ✓

Step 2: Assume true for $n=k$

$1^2+2^2+3^2+\ldots k^2 = \frac{k(k+1)(2k+1)}{6}$

Step 3: Show true for $n=k+1$

ie LHS $1^2+2^2+3^2+\ldots k^2+(k+1)^2 = \frac{(k+1)(k+2)(2k+3)}{6}$ RHS

$2(k+1)+1$

$2k+2+1$

LHS $1^2+2^2+3^2+\ldots k^2+(k+1)^2$

$$\frac{k(k+1)(2k+1)}{6} + (k+1)^2$$

$$\frac{k(k+1)(2k+1)+6(k+1)^2}{6}$$

$$\frac{(k+1)[k(2k+1)+6(k+1)]}{6}$$

$$\frac{(k+1)[2k^2+k+6k+6]}{6}$$

$$\frac{(k+1)(2k^2+7k+6)}{6}$$

$$\frac{(k+1)(k+2)(2k+3)}{6} = \text{RHS}$$

$15 \equiv 3 \pmod 4 \longrightarrow 4 \mid (15-3)$

$3(1) \equiv 3(5) \pmod 6$

$1 + 5 \pmod 6 \longrightarrow 6 \mid (1-5) = -4$

$1 \not\equiv 5 \pmod 6$ → $6 \nmid (1-5) = -4$

$6 \equiv 36 \pmod{10}$ → $10 \mid 6-36$

If divide by 6 $\quad 1 \equiv 6 \pmod{10}$ which is incorrect!

→ $10 \mid (1-6)$

⇒ Cannot divide by 6

But if we divide by 3: $3(2) \equiv 3(12) \pmod{10}$

because 3 and 10 are relatively prime ie $\gcd(3,10) = 1$

$2 \equiv 12 \pmod{10}$

---

find all incongruent solutions of

$119x \equiv 133 \pmod{217}$

$217 = 1(119) + 98$

$119 = 1(98) + 21$

$98 = 4(21) + 14$

$21 = 1(14) + \boxed{7}$ → gcd

~~$14 = 2(7) + 0$~~

→ Since $7 \mid 133$ $(7 \times 19 = 133)$

⇒ There are incongruent solutions.

$7(17x) \equiv 7(19) \pmod{\left(\frac{217}{7}\right)}$

Since 7 and 217 are relatively prime ie $\gcd(7,217) = 7$

⇒ Cancel 7.

$17x \equiv 19 \pmod{31}$

To solve this we look for a solution to

$17x \equiv 1 \pmod{31}$

ie $17x + 31y = 1$

$31 = 1(17) + 14$ $\quad 31 - 1(17) = 14$

$17 = 1(14) + 3$ $\quad 17 - 1(14) = 3$ ✓

$14 = 4(3) + 2$ $\quad 14 - 4(3) = 2$ ✓

$3 = 1(2) + \boxed{1}$ → gcd $\quad 3 - 1(2) = 1$ ✓

$1(3) - 1(2) = 1$

$1(3) - 1(2) = 1$

$1(3) - 1[14 - 4(3)] = 1$

$1(3) - 1(14) + 4(3) = 1$

$5(3) - 1(14) = 1$

$5[17 - 1(14)] - 1(14) = 1$

$5(17) - 6(14) = 1$

$5(17) - 6[31 - 1(17)] = 1$

$11(17) - 6(31) = 1$

$17x \equiv 19 \pmod{31}$

$17x + 31y = 19$

$x_0 = 11$ (x19) $\quad y_0 = -6$ (x19) $\quad$ x19

$x_0 = 209 \quad y_0 = -114 \pmod{31}$

$x_0 = 23 \quad$ ~~$y_0 = 10$~~

* Check $17(23) \equiv 19 \pmod{31}$?

$391 \equiv 19 \pmod{31}$ ✓

$x \equiv 8 \pmod{9}$

$x \equiv 7 \pmod{20}$

$x \equiv 5 \pmod{7}$

$N = 1260$

$N_1 = 1260/9 = 140$

$N_2 = 1260/20 = 63$

$N_3 = 1260/7 = 180$

Solve $140x \equiv 1 \pmod{9}$ → 0, 1, 2, 3, 4,

$1794x \equiv 184\ 644$

$1794x + 644y = 184$

$x =$

Solve $140x \equiv 1 \pmod 9$

$x = 2$

$63x \equiv 1 \pmod{20}$

$180x \equiv 1 \pmod 7$

Toss a coin : $S = \{H, T\}$ $\#S = 2$

Toss 2 coins : $S = \{HH, HT, TH, TT\}$ $\#S = 4$

Roll a dice : $S = \{1, 2, 3, 4, 5, 6\}$ $\#S = 6$

Roll 2 dice : $S = \{11, 12, 13, 14, 15, 16, 21, 22, 23, 24, 25, 26, 31, 32, 33, 34, 35, 36, 41, 42, 43, 44, 45, 46, 51, 52, 53, 54, 55, 56, 61, 62, 63, 64, 65, 66\}$ $\#S = 36$

Urn – 1 red, 1 green, 1 blue

Without Replacement

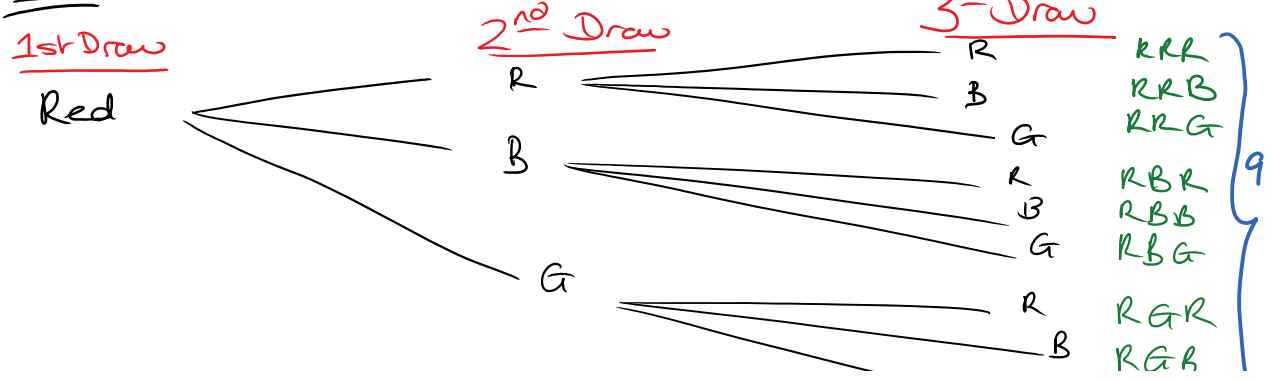
$S = \{RGB, RBG, GRB, GBR, BRG, BGR\}$

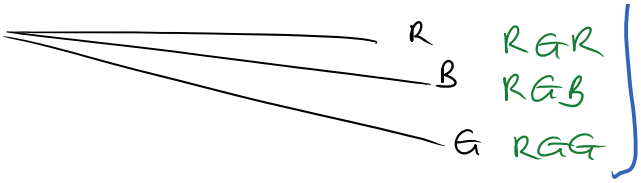
$\#S = 6$

With Replacement

$S = \{RRR, RRG, RRB, RGR, \ldots\}$

Tree





$\#S = 9 \times 3 = 27$

Eg1 How many ways can 4 people be arranged

$4 \times 3 \times 2 \times 1 = 24 \quad (= 4!)$

Eg2 How many ways can a deck of cards be arranged?

$52 \times 51 \times 50 \cdots 3 \times 2 \times 1 = 52!$

52

Eg3 Roll a fair dice $S = \{1, 2, 3, 4, 5, 6\}$

Let

A = Getting an even number $= \{2, 4, 6\}$

B = Getting an odd number $= \{1, 3, 5\}$

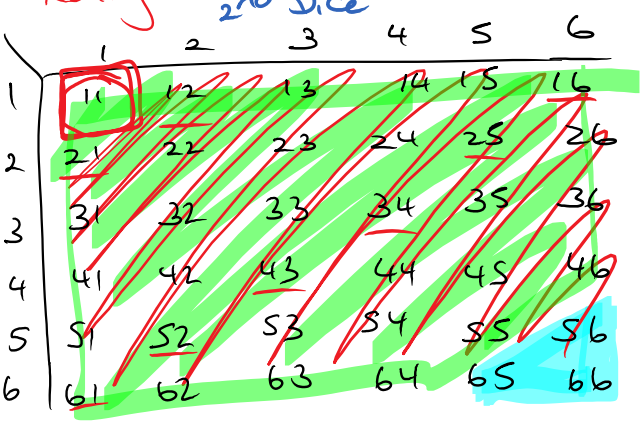
Eg4 Toss a fair coin twice

$S = \{HH, HT, TH, TT\} \quad \#S = 4$

Let

A = Getting at least 1 Head $= \{HH, HT, TH\}$

Eg5 Rolling 2 dice



F = Not 11

F^C = Everything else except 11

$\#S = 36$

Let

A = Sum is 3 $= \{12, 21\}$ $\#A = 2$

B = Sum is 7 $= \{16, 25, 34, 43, 52, 61\}$ $\#B = 6$

C = Sum is greater than 10 $= \{56, 65, 66\}$ $\#C = 3$

D = Sum is less than or equal to 10 = {11, 12, ... 64}

#D = 33

Eg1 Roll 2 dice. Want to look at an outcome being, both numbers even or having a sum greater than 6. #S = 36

E = {22, 24, 26, 42, 44, 46, 62, 64, 66} #E = 9

F = {16, 25, 26, 34, 35, 36, 43, 44, 45, 46, 52, 53, 54, 55, 56, 61, 62, 63, 64, 65, 66} #F = 21

AND

E ∩ F = {26, 44, 46, 62, 64, 66} #E∩F = 6

D = Event where one number is even and one is odd (A)

OR

whose sum is 7 (B)

A = {12, 14, 16, 21, 23, 25, 32, 34, 36, 41, 43, 45, 52, 54, 56, 61, 63, 65}

#A = 18

B = {16, 25, 34, 43, 52, 61} #B = 6

D = A ∪ B = {12, 14, 16, 21, 23, 25, 32, 34, 36, 41, 43, 45, 52, 54, 56, 61, 63, 65}

OR

Eg3 Roll a dice S = {1, 2, 3, 4, 5, 6} #S = 6

Probability of

(i) a 1 E = {1} #E = 1 ⇒ $p(1) = \frac{1}{6}$

(i) a 1 or 2 F = {1, 2} #F = 2 ⇒ $p(1 \text{ or } 2) = \frac{2}{6} = \frac{1}{3}$

(iii) odd and less than 4

G = {1, 3} #G = 2 ⇒ $p(\text{odd or Less than } 4) = \frac{2}{6} = \frac{1}{3}$

(iv) not a 4 or 5 → {1, 2, 3, 6}

$p(4 \text{ or } 5) = \frac{2}{6} = \frac{1}{3}$

$p(\text{not } 4 \text{ or } 5) = 1 - \frac{1}{3} = \frac{2}{3}$

$p(4 \text{ or } 5) = \frac{2}{6} = \frac{1}{3}$

$p(\text{Not } 4 \text{ or } 5) = 1 - \frac{1}{3} = \frac{2}{3}$

(v) Even or less than 3

$P = \{2, 4, 6\}$ $\#P = 3$

$G = \{1, 2\}$ $\#G = 2$

$P \cup G = \{1, 2, 4, 6\}$ $\#P \cup G = 4$

$\Rightarrow p(\text{Even No or less than } 3) = \frac{4}{6} = \frac{2}{3}$

Eg 2 Roll 2 fair dice and add the numbers.

Find the probability:

(i) 2

(ii) 3

(iii) Num less than 5

(iv) Even No

(v) Even no. less than 6

(vi) No less than or equal to 10

2nd dice

1st dice	1	2	3	4	5	6
1	2	3	4	5	6	7
2	3	4	5	6	7	8
3	4	5	6	7	8	9
4	5	6	7	8	9	10
5	6	7	8	9	10	11
6	7	8	9	10	11	12

(i) $p(2) = \frac{1}{36}$

(ii) $p(3) = \frac{2}{36} = \frac{1}{18}$

(iii) $p(\text{No} < 5) = \frac{6}{36} = \frac{1}{6}$

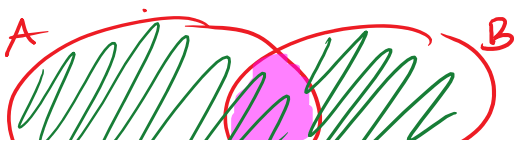
(iv) $p(\text{Even No}) = \frac{18}{36} = \frac{1}{2}$

$p^c = 1 - p$

(v) $p(\text{Even No} \& \text{less than } 6) = \frac{4}{36} = \frac{1}{9}$ ($\rightarrow 10$)

(vi) $p(\text{Num} \leq 10) = 1 - p(\text{Not} \leq 10)$

$= 1 - \frac{3}{36} = \frac{33}{36} = \frac{11}{12}$



$$|A \cup B| = |A| + |B| - |A \cap B|$$

Also

$$p(A \cup B) = p(A) + p(B) - p(A \cap B)$$

Eg 4 Roll 2 fair dice.

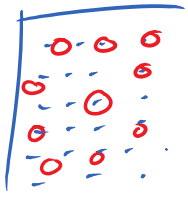
Let A = Sum is 8

B = Both numbers are even

what is the prob. of an 8 or an even number?

$A = \{26, 35, 44, 53, 62\}$ $\#A = 5$

$B = \{22, 24, 26, 42, 44, 46, 62, 64, 66\}$ $\#B = 9$



$A \cap B = \{26, 44, 62\}$ $\#A \cap B = 3$

$$p(A \cup B) = p(A) + p(B) - p(A \cap B)$$

$$= \frac{5}{36} + \frac{9}{36} - \frac{3}{36} = \boxed{\frac{11}{36}}$$

Problem Sheet Probability (Bernoulli Trials)

$$\boxed{P(X = r) = \binom{n}{r} p^r q^{n-r}}$$ where p = prob. of success

Q1 $p = 0.2$ $q = 0.8$ $n = 7$

(i) $P(X = 0) = \binom{7}{0}(0.2)^0(0.8)^7$

$= (1)(1)(0.2097) = 0.2097$

$= \boxed{20.97\%}$

(ii) $P(X = 5, 4, 3, 2, 1, 0)$

$= 1 - P(X = 6, 7)$

$= 1 - \left[\underbrace{\binom{7}{6}(0.2)^6(0.8)^1}_{P(X=6)} + \underbrace{\binom{7}{7}(0.2)^7(0.8)^0}_{P(X=7)} \right]$

$$= 1 - \left[\binom{7}{6}(0.2)^6(0.8)^1 + \binom{7}{7}(0.2)^7(0.8)^0 \right]$$

$$= 1 - [\,0.0003584 + 0.0000128\,]$$

$$= 0.9996 = \boxed{99.96\,\%}$$

Quiz 2

Q5 $P(\text{Attended}) = 0.83$ $\quad P(\text{Ndr attended}) = 0.17$

$P(\text{Passed} \mid \text{Attended}) = 0.95$ $\quad P(\text{Passed} \mid \text{Ndr attend}) = 0.13$

$P(\text{Didn't pass} \mid \text{Attended}) = 0.05$ $\quad P(\text{Didn't Pass} \mid \text{Ndr attend}) = 0.87$

a) $\Rightarrow P(\text{Student Passed}) =$

$$(0.83 \times 0.95) + (0.17 \times 0.13)$$

$$= 0.7885 + 0.0221 = \boxed{0.8106}$$

(b) $P(\text{Attended} \mid \text{Passed}) = \dfrac{P(\text{Attended} \cap \text{Passed})}{P(\text{Passed})}$

$P(A \mid B) = \dfrac{P(A \cap B)}{P(B)}$

$$= \frac{(0.83 \times 0.95)}{0.8106} = \frac{0.7885}{0.8106}$$

$$= \boxed{0.9727}$$

	Attended	Didn't attend	
Passed	0.95	0.13	
Didn't pass	0.05	0.87	
	0.83	0.17	

Modular Matrices - PS8

Q1 GRTM

GREEN EGGS AND HAM X

6 17 4 4 13 | 4 6 6 18 | 0 13 3 | 7 0 12 | 23

a b c d e f g h i j k l m n o p q r s t u v w x y z

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

$$(3\ 10)\begin{pmatrix} 6 \\ \end{pmatrix} = \begin{pmatrix} 18 + 170 \\ \end{pmatrix} = \begin{pmatrix} 188 \\ 173 \end{pmatrix} \text{ Mod } 26 = \begin{pmatrix} 6 \\ 17 \end{pmatrix} \begin{matrix} \to G \\ \to R \end{matrix}$$

$$\begin{pmatrix}3 & 10\\ 9 & 7\end{pmatrix}\begin{pmatrix}6\\17\end{pmatrix} = \begin{pmatrix}18+170\\54+119\end{pmatrix} = \begin{pmatrix}188\\173\end{pmatrix} \bmod 26 = \begin{pmatrix}6\\17\end{pmatrix} \to G,\ R$$

$$\begin{pmatrix}3 & 10\\ 9 & 7\end{pmatrix}\begin{pmatrix}4\\4\end{pmatrix} = \begin{pmatrix}12+40\\36+28\end{pmatrix} = \begin{pmatrix}52\\64\end{pmatrix} \bmod 26 = \begin{pmatrix}0\\12\end{pmatrix} \to A,\ M$$

FLT - PS 9

Q1 (i) $3^{302} \pmod 5$

FLT: $a^{p-1} = 1 \pmod p$

Here $a = 3 \quad p = 5$

FLT: $3^{5-1} = 1 \pmod 5$

$3^4 = 1 \pmod 5$

$(3^{302}) = (3^{300})(3^2) \pmod 5$

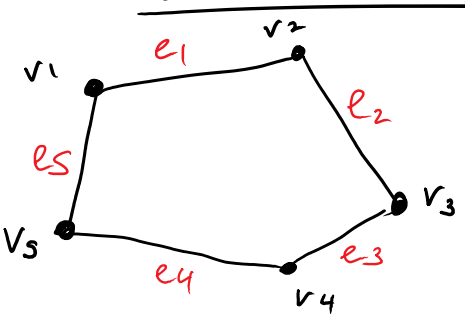
$3^{302} = (3^4)^{75}(3^2) \pmod 5$

$3^{302} = (1)^{75}(9) \pmod 5$

$3^{302} = 9 \pmod 5$

$\boxed{3^{302} = 4 \pmod 5}$

GRAPH THEORY



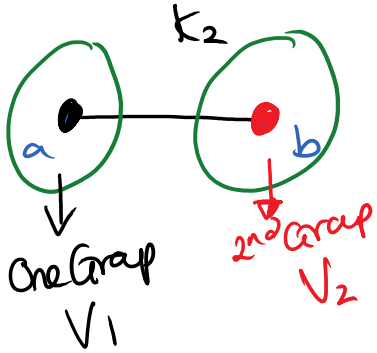
$G = (V, E)$

Complete Graph: Graph in which every pair of vertices has an edge between them. Denoted, K_n

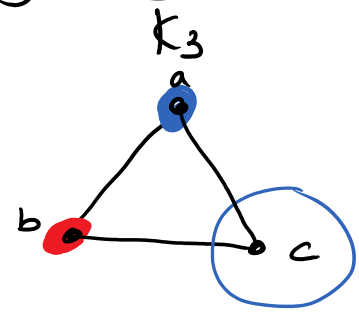
K_1 K_2 K_3 K_4

c c d

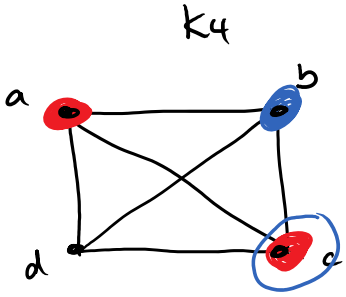
Bipartite Graph: is a graph which can be split into 2 groups in the following way



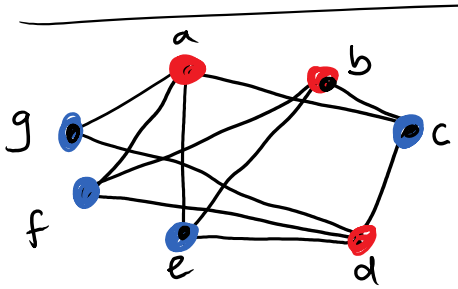
K_2 is bipartite



K_3 is not bipartite.



K_4 is not bipartite



Yes, this graph is bipartite because we can split the vertices into 2 groups

$V_1 = \{a, b, d\}$ and $V_2 = \{c, e, f, g\}$

a b

g c

f

e d

PROBLEM SHEET BERNOULLI

$$P(X=r) = \binom{n}{r} p^r q^{n-r}$$

p = prob. of success.

Q1) $n = 7$

$p = 0.2$

$q = 1 - p = 0.8$

(i) $P(X=0) = \binom{7}{0}(0.2)^0(0.8)^7$

$= (1)(1)(0.2097 = 0.2097 =$ **20.97%**

(ii) $P(X = 5,4,3,2,1,0) = 1 - P(X = 6,7)$

$= 1 - [P(X=6) + P(X=7)]$

$= 1 - \left[\binom{7}{6}(0.2)^6(0.8)^1 + \binom{7}{7}(0.2)^7(0.8)^0\right]$

$= 1 - [(7)(0.000064)(0.8) + (1)(0.0000128)(1)]$

$= 1 - [0.0003712]$

$= 0.9996 =$ **99.96%**

Q5) $n = 6$

$p = 5\% = 0.05$ = prob a transistor is 'bad'.

$q = 95\% = 0.95$ = " " " 'good'.

(i) P(All 6 are good)

(ie 0 are bad)

$P(X = 0) = \binom{6}{0}(0.05)^0(0.95)^6$

$= (1)(1)(0.95)^6$

$= 0.7351$

$=$ **73.51%**

$P(X = 1) = \binom{6}{1}(0.05)^1(0.95)^5$

(ii) $P(X=1) = \binom{6}{1}(0.05)^1(0.95)^5$

$= (6)(0.05)(0.95)^5 = 0.232$

$= 23.2\%$

(iii) P(At least 2 'bad')

$P(X=2,3,4,5,6) = 1 - P(X=1,0)$

$= 1 - [P(X=1) + P(X=0)]$

$= 1 - [0.232 + 0.7351]$

$= 0.0329$

$= 3.29\%$

PROBLEM SHEET 8 - Modular Matrices

Q2 $\begin{pmatrix} 13 & 4 \\ 9 & 1 \end{pmatrix}$

$\det = (13)(1) - (4)(9) = 13 - 36 = -23 \equiv 3 \pmod{26}$

(i) we need to find the inverse of 3 (mod 26)

ie $3x = 1 \pmod{26}$

I $26 = 8(3) + 2$

$3 = 1(2) + 1$

II $1(3) - 1(2) = 1$

$1(3) - 1[26 - 8(3)] = 1$

$9(3) - 1(26) = 1 \pmod{26}$

$(9)(3) = 1 \pmod{26}$

$x = 9$

$\Rightarrow$ The inverse of the determinant is 9

(ii) $adj = \begin{pmatrix} 1 & -4 \\ -9 & 13 \end{pmatrix}$

$\Rightarrow A^{-1} = 9\begin{pmatrix} 1 & -4 \\ -9 & 13 \end{pmatrix} \pmod{26}$

a b c d e f g h i j k l m n o p

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

$$A^{-1} = \begin{pmatrix} 9 & -36 \\ -81 & 117 \end{pmatrix} \pmod{26}$$

q r s t u v w x y z
16 17 18 19 20 21 22 23 24 25

$$A^{-1} = \begin{pmatrix} 9 & 16 \\ 23 & 13 \end{pmatrix} \pmod{26}$$

R	D	R	S	Q	Q	V	U	Q	B	.....
17	3	17	18	16	14	21	20	16	1	

$$\begin{pmatrix} 9 & 16 \\ 23 & 13 \end{pmatrix}\begin{pmatrix} 17 \\ 3 \end{pmatrix} = \begin{pmatrix} 153+48 \\ 391+39 \end{pmatrix} = \begin{pmatrix} 201 \\ 430 \end{pmatrix} = \begin{pmatrix} 19 \\ 14 \end{pmatrix} \to T, O$$

$$\begin{pmatrix} 9 & 16 \\ 23 & 13 \end{pmatrix}\begin{pmatrix} 17 \\ 18 \end{pmatrix} = \begin{pmatrix} 153+288 \\ \end{pmatrix} = \begin{pmatrix} 441 \\ 625 \end{pmatrix} = \begin{pmatrix} 25 \\ 1 \end{pmatrix} \to Z, B$$

$$\begin{pmatrix} 9 & 16 \\ 23 & 13 \end{pmatrix}\begin{pmatrix} 16 \\ 14 \end{pmatrix} = = \begin{pmatrix} 368 \\ 580 \end{pmatrix} = \begin{pmatrix} 4 \\ 4 \end{pmatrix} \to E, E$$

$$\begin{pmatrix} 9 & 16 \\ 23 & 13 \end{pmatrix}\begin{pmatrix} 21 \\ 20 \end{pmatrix} = \begin{pmatrix} 509 \\ 743 \end{pmatrix} = \begin{pmatrix} 15 \\ 15 \end{pmatrix} \to P, P$$

$$\begin{pmatrix} 9 & 16 \\ 23 & 13 \end{pmatrix}\begin{pmatrix} 16 \\ 1 \end{pmatrix} = \begin{pmatrix} 160 \\ 381 \end{pmatrix} = \begin{pmatrix} 4 \\ 17 \end{pmatrix} \to E, R$$

PROB SHEET 9 – FLT

(iv) $5^{2003} \pmod 7$

FLT: $a^{p-1} = 1 \pmod p$

Here $a = 5 \quad p = 7$

$\Rightarrow$ FLT: $5^{7-1} = 5^6 = 1 \pmod 7$

$$5^{2003} = (5^{1998})(5^5) \pmod 7$$
$$= (5^6)^{333}(5^5) \pmod 7$$
$$= (1)^{333}(5^5) \pmod 7$$
$$= (1)(5^5) \pmod 7$$
$$= 3125 \pmod 7$$

$= 3125 \pmod 7$

$\Rightarrow \boxed{5^{2003} = 3 \pmod 7}$

(ix) $5^{2000} \pmod{17}$

Here $a=5$ $p=17$ $\Rightarrow$ FLT: $5^{16} = 1 \pmod{17}$

$5^{2000} = (5^{16})^{125} \pmod{17}$

$= (1)^{125} \pmod{17}$

$\boxed{5^{2000} = 1 \mod 17}$

(xi) $2^{100} \pmod{29}$

$a=2$ and $p=29$ $\Rightarrow$ FLT: $2^{28} = 1 \pmod{29}$

$2^{100} = (2^{84})(2^{16}) \mod 29$

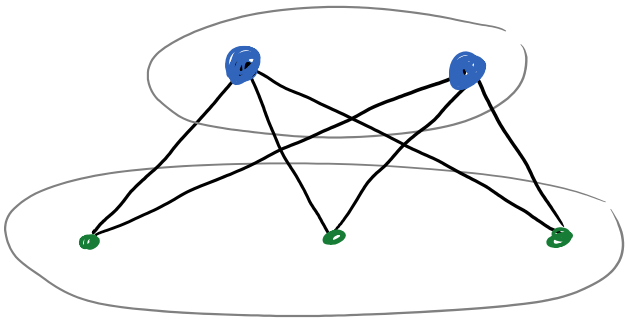
$= (2^{28})^3 (2^{16}) \mod 29$

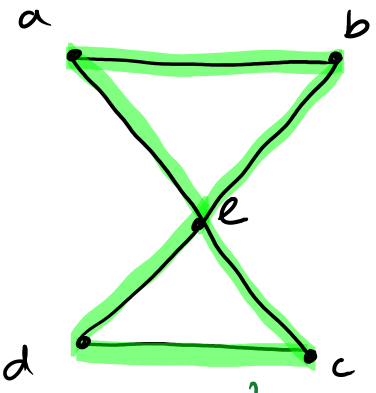
$= (1)^3 (2^{16}) \mod 29$

$= 65536 \mod 29$

$\boxed{2^{100} = 25 \mod 29}$

Complete Bipartite Graph : $K_{2,3}$

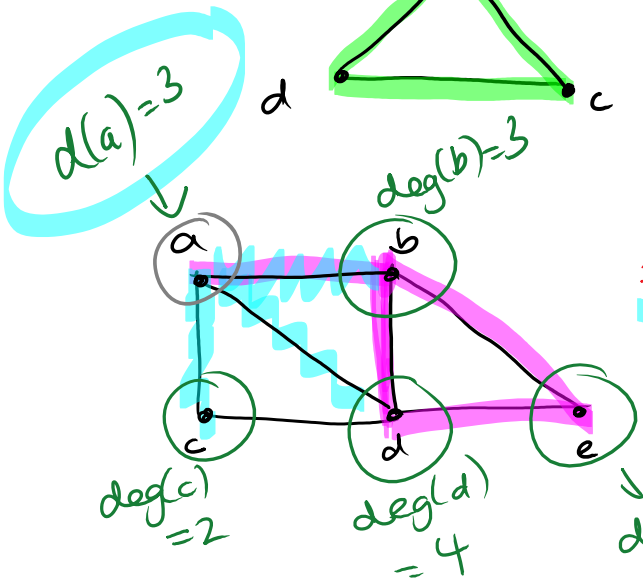




Does this graph have an Euler Cycle.

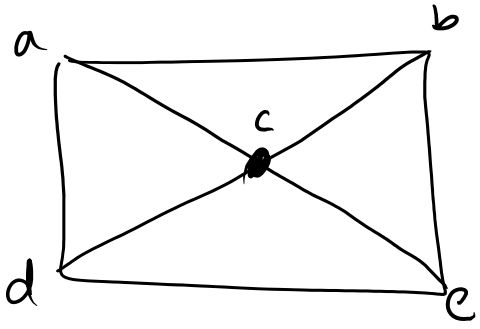
a, b, e, d, c, e, a

Euler cycle - contains every edge and starts/ends at same vertex



Does this graph have an Euler cycle? No

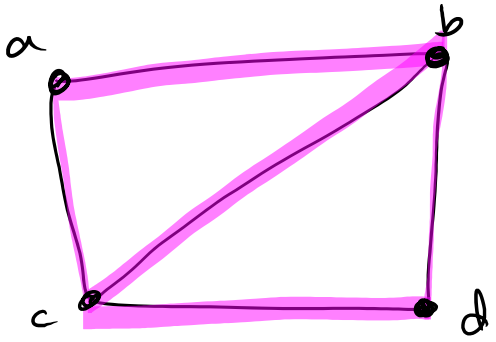
Does this graph have an Euler path? Yes



Does this graph have an Euler Cycle?

Vertex	a	b	c	d	e
Degree	3	3	4	3	3

No, Euler cycle because at least one vertex has odd deg



Does this graph have an Euler Cycle? No

Find an Euler path.

c, b, d, c, a, b

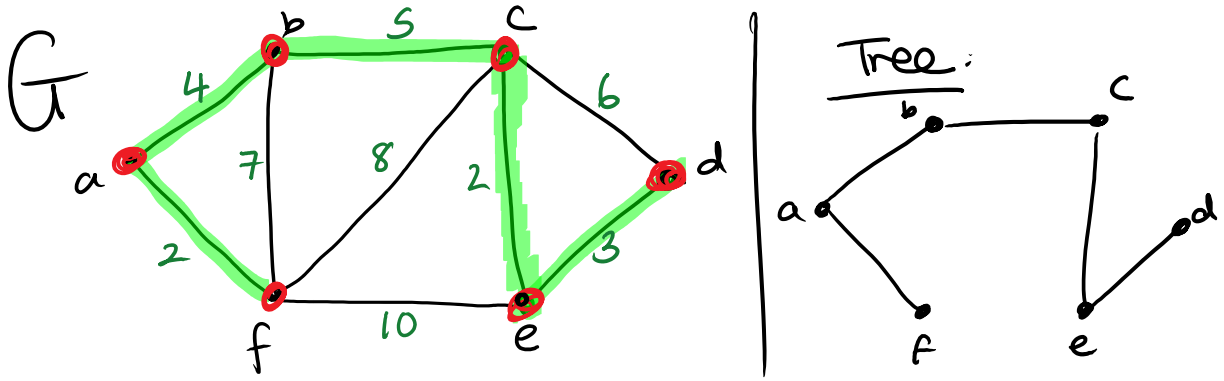
Every edge.

Vertex	a	b	c	d
Degree	2	3	3	2

odd degree

⇒ No Euler Cycle

Kruskal's Algorithm



Step 1 : Choose edge af (because it has smallest weight 2).

Step 2 : Choose edge ce (because it has wght 2)

Step 3 : Choose edge ed (because it has weight 3)

Step 4 : Choose edge ab (" " " 4)

Step 5 : Choose edge bc (" " " 5)

Minimal weight Spanning Tree has weight = 16.

Predicate Logic

$P(x)$: $x > x^2$ $\quad D = \mathbb{R}$

$P(0)$: $0 > 0^2$ False because $0 \not> 0$

$P(\frac{1}{2})$: $\frac{1}{2} > (\frac{1}{2})^2$ True because $\frac{1}{2} > \frac{1}{4}$

$P(2)$: $2 > 2^2$ False because $2 \not> 4$

$Q(x,y)$: $x > y$ $\quad D = \mathbb{Z}$

$Q(3,1)$: $3 > 1$ True ✓

$Q(5,5)$: $5 \not> 5$ False

$Q(6,-6)$: $6 > -6$ True ✓

$Q(2^8, 256)$: $2^8 \not> 256$ False

$\forall x\, P(x)$ → Means that $P(x)$ is true for every possible x in the domain.

$\exists x\, P(x)$ → means there exists <u>some</u> x for which $P(x)$ is true.

$Q(x)$: $x+1 > 2x$ $\quad D = \mathbb{Z}$

Then $\exists x\, Q(x)$ is true because if $x=0$, we get

$Q(0)$: $0+1 > 2(0)$

$1 > 0$ ✓

$Q(x)$: $x+1 > 2x$

- $\forall x\, Q(x)$ is false because we can find (at least) 1 value of x $(x=2)$ for which Q is false

ie $2+1 \not> 2(2)$

$3 \not> 4$

- $\neg Q(x) = x+1 \leq 2x$

$\exists x(\neg Q(x))$ is <u>false</u> because if we let $x=0$

then $\neg Q(0)$: $0+1 \leq 2(0)$

$1 \not\leq 0$

$\exists x(\neg Q(x))$ is <u>true</u> because if we let $x=1$

then $\neg Q(1)$: $1+1 \leq 2(1)$ ✓

$\exists x$ ([illegible]

then $\neg Q(1)$: $1 + 1 \leq 2(1)$

$2 \leq 2$ ✓

Eg 1 Turn this proposition into English. Is it true or false?

$$\exists m \in \mathbb{Z} \; \forall n \in \mathbb{Z} \; (m = n+5)$$

↳ There is an integer m such that adding 5 to any integer gives m.

This proposition is false.

	$\forall X \subseteq \mathbb{N} \; (X \subseteq \mathbb{R})$	$\forall x \in \mathbb{R} \; (x^2 \geq 0)$	
① The cube of any real number is greater than 0			
② A subset of the natural numbers is a subset of the real numbers			
③ For every integer p there is a subset of $\mathbb{Z}$ with less than p members.			

Problem Sheet - Predicate Logic

Q1) $P(x)$ = x spends more than 5 hrs in class

D = {students in DIT}

(a) $\exists x \; P(x)$ – There is at least one student in DIT who spends more than 5 hrs in class

(b) $\forall x \; P(x)$ – Every student in DIT spends more

than 5 hrs in class

(c) $\exists x (\neg P(x))$ = There is at least one student in DIT who does not spend more than 5hrs in class.

(d) $\forall x (\neg P(x))$ = Every student in DIT spends less than 5 hrs in class

---

Q5 Let $Q(x)$: $x+1 > 2x$ $\quad D = \mathbb{Z}$

$\neg Q(x)$: $x+1 \leq 2x$

$Q(0)$ => True since $0+1 > 2(0)$ ✓

$Q(-1)$ => True since $-1+1 > 2(-1)$ ✓

$Q(1)$ => False since $1+1 \not> 2(1)$ ✗

$\exists x\, Q(x)$ => True since if we take $x=0$: $0+1 > 2(0)$

$\forall x\, Q(x)$ => False since if we take $x=1$: $1+1 \not> 2(1)$

$\exists x (\neg Q(x))$ => True since if take $x=2$: $2+1 \leq 2(2)$ ✓

$\forall x (\neg Q(x))$ => False since if we take $x=-3$: $-3+1 \leq 2(-3)$ ✗

Q7 (a) All dogs have fleas. $\quad D = \{\text{All dogs}\}$

$F(x) = x$ has fleas

$\boxed{\forall x\, F(x)}$

(c) Every koala can climb. $\quad D = \{\text{All koalas}\}$

$C(x) = x$ can climb

$\boxed{\forall x\, C(x)}$

(e) There exists a pig that can swim and catch fish $\quad D = \{\text{All pigs}\}$

$S(x) = x$ can swim

$F(x) = x$ can catch fish

$\boxed{\exists x (S(x) \wedge F(x))}$

Q9 $C(x) = x$ has a cat $\quad D = \{\text{All students in the class}\}$

$D(x) = x$ has a dog

$B(x) = x$ has a budgie

(b) All students have a cat $\wedge$ (OR) a dog $\vee$ a budgie

$$\forall x \left(C(x) \vee D(x) \vee B(x) \right)$$

(d) No student has a cat $\wedge$ (AND) a dog and a budgie

$$\neg \exists x \left(C(x) \wedge D(x) \wedge B(x) \right)$$

(e) For each animal type, there is a student in the class who has a pet of that type.

$$\left(\exists x \; C(x) \right) \wedge \left(\exists y \; D(y) \right) \wedge \left(\exists z B(z) \right)$$

Q11 $L(x,y)$ = x likes y $\quad D = \{$all people$\}$

(a) Everyone likes everyone

$$\forall x \forall y \; L(x,y)$$

(c) Someone does not like anyone

$$\exists x \forall y \left(\neg L(x,y) \right)$$

(e) There is someone whom everyone likes

$$\forall x \exists y \left(L(x,y) \right)$$

(g) Everyone does not like someone.

$$\forall x \exists y \left(\neg L(x,y) \right)$$

Eg1 Write the following as a quantified statement

Everyone likes either Microsoft or Apple.

Jill does not like Microsoft.

Therefore Jill likes Apple.

Soln

$L(x,y)$ = x likes Microsoft

Soln

Let $M(x)$ = x likes Microsoft

Let $A(x)$ = x likes Apples.

$\neg M(x)$ = x does not like Microsoft.

$$\forall x \left(M(x) \vee A(x) \right)$$

$\neg M(\text{Jill})$

$\Rightarrow A(\text{Jill})$

Eg2 write the following as a quantified statement.

Every student is intelligent.

$S(x)$ = x is a student

$I(x)$ = x is intelligent

$D = \{$ All students in UT $\}$

A	B	$A \Rightarrow B$
0	0	1
0	1	1
1	0	0
1	1	1

$$\forall x \left(S(x) \rightarrow I(x) \right)$$

Some student(s) are intelligent

$$\exists x \left(S(x) \wedge I(x) \right)$$

Eg3 In a group with members x and y, we let

$P(x,y)$ = x talks to y

$$\forall x \exists y \left(P(x,y) \right)$$

Everyone talks to someone.

$$\exists x \forall y \left(\neg P(x,y) \right)$$

There is at least one person who does not talk to anybody else.

$$\exists x \exists y \left(P(y,x) \wedge P(x,y) \right)$$

there are at least 2 people who talk each other.

---

with members x and y, let

other.

Eg2 In a group with members x and y, let $P(x,y)$ = x knows the name of y

Negate each of the following sentences and write the quantified statement for the negated proposition

(i) Everyone knows at least one other persons name.

↳ There is at least one person who doesn't know everyones name.

$$\exists x \, \forall y \, (\neg P(x,y))$$

(ii) There is someone who knows everyones name

↳ Everyone does not know at least one persons name.

$$\forall x \, \exists y \, (\neg P(x,y))$$

Online Quiz 1 - Number Theory

$$x \equiv 11 \mod 14$$
$$x \equiv 4 \mod 15$$
$$x \equiv 2 \mod 11$$

$m = 14 \cdot 15 \cdot 11 = 2310$

$m_1 = 2310/14 = 165$ → ① $m_1 x \equiv 1 \mod 14$

$m_2 = 2310/15 = 154$ → ② $m_2 x \equiv 1 \mod 15$

$m_3 = 2310/11 = 210$ → ③ $m_3 x \equiv 1 \mod 11$

① $165x \equiv 1 \mod 14$

$11x \equiv 1 \mod 14$

$s_1 = 9$

② $154x \equiv 1 \mod 15$

$4x \equiv 1 \mod 15$

$s_2 = 4$

③ $210x \equiv 1 \mod 11$

$1x \equiv 1 \mod 11$

$s_3 = 1$

$$x = m_1 r_1 s_1 + m_2 r_2 s_2 + m_3 r_3 s_3$$

$$x = (165)(11)(9) + (154)(4)(4) + (210)(2)(1) \pmod{2310}$$

$x = 16335 + 2464 + 420 \pmod{2310}$

$x = 19219 \pmod{2310}$

$x = 739 \pmod{2310}$

Quiz 1

Q6 $d = \gcd(11589240, 136344)$

(i) $11589240 = 85(136344) + 0$

$\Rightarrow d = 136344$

(ii) $11589240s + 136344t = d$ (0) (1) (136344)

$+(11589240) - 85(136344) = 0$

$s = 1$ $t = -85$

(ii) $11589240x \equiv 681720 \pmod{136344}$

$\hookrightarrow 11589240x + 136344y = 681720$

$11589240 = 85(136344) + 0$

$\Rightarrow \gcd = 136344$

Since $136344 \mid 681720$, three are solutions.

Probability Quiz

Q4 15% - walk to college. $p = 0.15$

Sample, $n = 11$

Prob. not walking to college, $q = 0.85$

(a) $P(X=0)$

$= \binom{11}{0}(0.15)^0(0.85)^{11}$

$= (1)(1)(0.167)$

$= \boxed{0.167}$

(b) P(At least 3 of the 11 students walk to college)

$= P(3) + P(4) + P(5) + P(6) \cdots + P(11)$

$= 1 - [P(2) + P(1) + P(0)]$

$= 1 - \left[\binom{11}{2}(0.15)^2(0.85)^9 + \binom{11}{1}(0.15)^1(0.85)^{10} + \binom{11}{0}(0.15)^0(0.85)^{11}\right]$

$= 1 - [0.287 + 0.325 + 0.167]$

$= 1 - [0.778]$

$= \boxed{0.221}$

Predicate Logic Quiz

Q5

p = It is snowing

q = I will go skiing

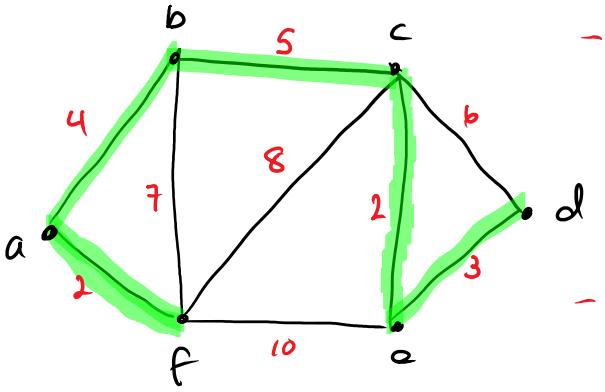
It will snow if I don't go skiing $\neg p \rightarrow q$

I will go skiing if it is snowing $p \rightarrow q$

It is snowing and I may or may not go skiing

$(q \vee \neg q) \wedge p$

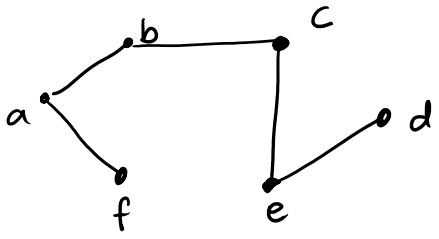
As it is not snowing I will go skiing $\neg p \wedge q$



- Use Kruskal's Algorithm to find a minimum weight spanning tree for this graph.
- What is the weight?

Step1 : |af| = 2
Step2 : |ce| = 2
Step3 : |ed| = 3
Step4 : |ab| = 4
Step5 : |bc| = 5

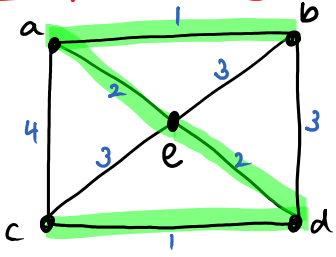
Spanning Tree



weight = 16

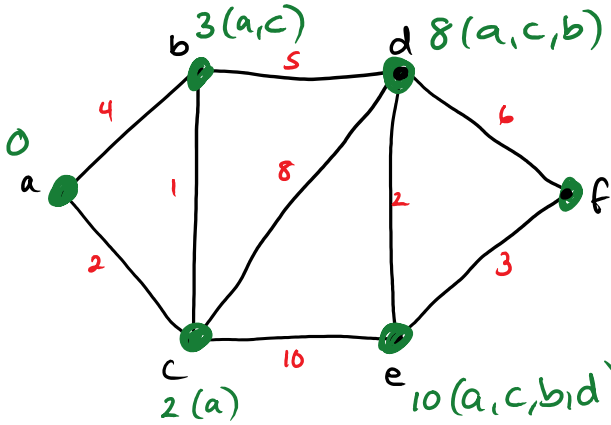
Graph Theory P.S

Q5 (ii)



Edge 1 : |ab| = 1
Edge 2 : |cd| = 1
Edge 3 : |ed| = 2
Edge 4 : |ae| = 2

6 = weight



Use Dijkstra's Algorithm to find the shortest path

⇒ Using Dijkstra's Alg, the shortest path from a to f is

Step1 : $\circlearrowleft = \{a\}$

2 (a) 10 (a, c, b, d)

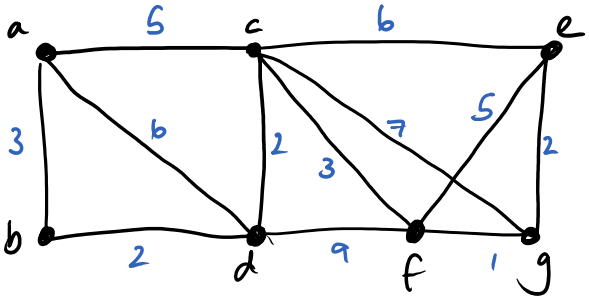
Step 1: D = {a}
Step 2 D = {a, c}
Step 3 D = {a, c, b}
Step 4 D = {a, c, b, d}
Step 5 D = {a, c, b, d, e}
Step 6: D = {a, c, b, d, e, f}

a to f is
a → c → b → d → e → f
which has a weight/distance of 13

Dijkstra's Algorithm

① mark your selected initial node with a current distance of 0 and the rest with infinity.
② Set the non-visited node with the smallest current distance as the current node (c)
③ For each neighbour (n) of the current node (c), add the current distance of c with the weight of the edge connecting c → n. If it is smaller than the current distance of n, set it as the new current distance of n.
④ mark the current node (c) as visited.
⑤ If there are non-visited nodes, go back to step 2.

Eg 1: Find the shortest path from a to all other vertices (particularly g) using Dijkstra's Algorithm



v	a	b	c	d	e	f	g
a	0a	3a	5a	6a	∞a	∞a	∞a
b	0a	3a	5a	5b	∞a	∞a	∞a
c	0a	3a	5a	5b	11c	8c	12c
d	0a	3a	5a	5b	11c	8c	12c
f	0a	3a	5a	5b	11c	8c	9f

Bottom row is the shortest distance from a to each of the vertices
a → b = 3

$a \to c = 5$

$a \to d = 5$

$a \to e = 11$

$a \to f = 8$

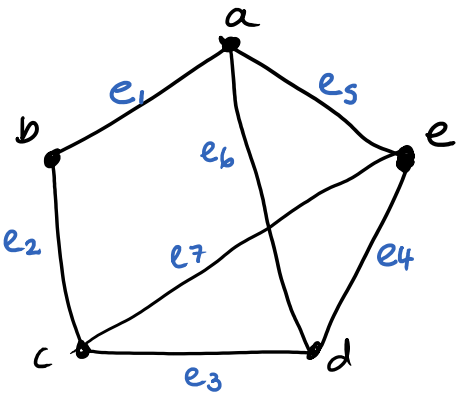
$a \to g = \boxed{9}$

At g (which has a distance of 9) you came through f (9_f) f came through c (8_c) and c came from a (5_a).

So the shortest from a to g is:

$a \xrightarrow{5} c \xrightarrow{3} f \xrightarrow{1} g.$

Shortest distance $= 5+3+1 = \boxed{9}$



(Vertices → Edges)

(Vertices → Vertices)

Adjacency Matrix (nxn)

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

Incidence Matrix (nxm)

	e_1	e_2	e_3	e_4	e_5	e_6	e_7
a	1	0	0	0	1	1	0
b	1	1	0	0	0	0	0
c	0	1	1	0	0	0	1
d	0	0	1	1	0	1	0
e	0	0	0	1	1	0	1

Supplemental 2018-2019

CmPU2012

Q1 (a) $933^{497} \pmod{345}$

$497 = 111110001_2$ from calculator

$497 = (1\times2^8)+(1\times2^7)+(1\times2^6)+(1\times2^5)+(1\times2^4)+(0\times2^3)+(0\times2^2)+(0\times2^1)+(1\times2^0)$

$497 = 256 + 128 + 64 + 32 + 16 + 1$

$933^1 = 933 \pmod{345} \equiv 243 \pmod{345}$

$933^2 = 59049 \pmod{345} \equiv 54 \pmod{345}$

$933^4 = (54)^2 = 2916 \equiv 156 \pmod{345}$

$933^8 = (156)^2 = 24336 \equiv 186 \pmod{345}$

$933^{16} = (186)^2 = 34596 \equiv 96 \pmod{345}$

$933^{32} = (96)^2 = 9216 \equiv 246 \pmod{345}$

$933^{64} = (246)^2 = 60516 \equiv 141 \pmod{345}$

$933^{128} = (141)^2 = 19881 \equiv 216 \pmod{345}$

$933^{256} = (216)^2 = 46656 \equiv 81 \pmod{345}$

(5)

$\Rightarrow 933^{497} = (933^1)(933)^{16}(933)^{32}(933)^{64}(933)^{128}(933)^{256}$

$= (243)(96)(246)(141)(216)(81) \pmod{345}$ (3)

$= 23328 \cdot 34686 \cdot 17496 \pmod{345}$

$= 213 \cdot 186 \cdot 246 \pmod{345}$

$\equiv \boxed{123 \pmod{345}}$

(6) $x \equiv 1 \pmod 5 \quad r_1 = 1$

$x \equiv 2 \pmod 6 \quad r_2 = 2$

$x \equiv 3 \pmod 7 \quad r_3 = 3$

$M = (5)(6)(7) = 210$

$M_1 = 42$ → (1) Solve $42x \equiv 1 \pmod 5$

$2x \equiv 1 \pmod 5$

$x = 3$

$\boxed{s_1 = 3}$

(2)

$M_2 = 35$ → (2) Solve $35x \equiv 1 \pmod 6$

$5x \equiv 1 \pmod 6$

$x = 5$

$\boxed{s_2 = 5}$

$M_3 = 30$ → (3) Solve $30x \equiv 1 \pmod 7$

$2x \equiv 1 \pmod 7$ (by inspection)

$\boxed{s_3 = 4}$

Solve $30x = 1 \pmod{7}$

$2x \equiv 1 \pmod 7$ (by inspection)

$s_3 = 4$ (2)

The soln to the system is

$s = M_1 r_1 s_1 + M_2 r_2 s_2 + M_3 r_3 s_3$

$s = (42)(1)(3) + (35)(2)(5) + (30)(3)(4) \pmod{210}$

$s = 836 \pmod{210}$

$s = 206 \pmod{210}$

(c) $D = \{x : x \text{ is a climber}\}$

(i) Every climber is either a mountaineer or rock climber

$\forall x \ (M(x) \vee R(x))$ (1)

(ii) Some climbers are mountaineers and some are rock climbers

$\exists x \ M(x) \wedge \exists y \ R(y)$ (2)

(iii) $\forall x \ (R(x) \rightarrow E(x)) \wedge \exists y \ (M(y) \rightarrow \neg E(y))$ (2)

(iv) $\forall x \ (\neg R(x) \longrightarrow M(x))$ (2)

(d)

(i) $7! = 5040$ (1)

(ii) County A – 4!

County B – 3!

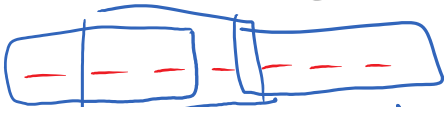
There are 2! ways to arrange 2 groups

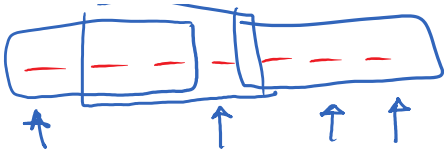
$2! \times 4! \times 3! = 288$ (2)

(iii) County B – 3!

There are 5! ways to arrange the 4 people from county A together with the group of B people

$3! \times 5! = 720$ (2)





(c)(iv) $\binom{4}{1}\binom{3}{1} = 4 \times 3 = 12$ (1)

(v) $\binom{4}{2}\binom{3}{2} = 6 \times 3 = 18$ (2)

(e) $1 + 3 + 9 + 27 + \ldots 3^n = \frac{3^{n+1} - 1}{2}$ (n=0, n=1, n=2, n=3)

$3^0 + 3^1 + 3^2 + 3^3 + \ldots 3^n$

$n=1$ LHS $3^0 + 3^1 = 1 + 3 = 4$

RHS $\frac{3^{1+1} - 1}{2} = \frac{3^2 - 1}{2} = \frac{9-1}{2} = \frac{8}{2} = 4$ ✓ (1)

True for $n=k$

$1 + 3 + 9 + 27 + \ldots 3^k = \frac{3^{k+1} - 1}{2}$

Show true for $n=k+1$

ie $1 + 3 + 9 + 27 + \ldots + 3^k + 3^{k+1} = \frac{3^{(k+1)+1} - 1}{2}$ (3)

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

LHS $1 + 3 + 9 + 27 + \ldots 3^k + 3^{k+1}$

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

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

$= \frac{3^1(3^{k+1}) - 1}{2} = \frac{3^{k+2} - 1}{2}$ = RHS ✓

Q2

(a) $\square \_ \square$ 2, 3, 5, 6, 7, 9

(i) $6 \times 5 \times 4 = 120$ (1)

(ii) $2 \times 5 \times 4 = \boxed{40}$ (1)

(iii) $4 \times 5 \times 2 = \boxed{40}$ (2)

(iv) $4 \times 5 \times 4 = \boxed{80}$ (2)

(v) $4 \times 5 \times 1 = \boxed{20}$ (2)

(b)

$A^c = \{11, 22, 33, 44, 55, 66\}$

$P(A) = 1 - P(A^c) = 1 - \frac{6}{36} = \boxed{\frac{5}{6}}$ (1)

$B = \{16, 25, 34, 43, 52, 61\}$

$P(B) = \frac{6}{36} = \boxed{\frac{1}{6}}$ (1)

$C = \{13, 22, 31\}$

$P(C) = \frac{3}{36} = \boxed{\frac{1}{12}}$ (1)

$D = \{66\}$

$P(D) = \boxed{\frac{1}{36}}$ (1)

- $A \cap B = B$

$P(A \cap B) = P(B) = \frac{1}{6}$

- $A \cap C = \{13, 31\}$

$\Rightarrow P(A \cap C) = \frac{2}{36} = \frac{1}{18}$

- $A \cap D = \phi$

$\Rightarrow P(A \cap D) = P(\phi) = 0$

(i) $P(B|A) = \frac{P(A \cap B)}{P(A)} = \frac{1/6}{5/6} = \boxed{\frac{1}{5}}$ (2)

(ii) $P(C|A) = \frac{P(A \cap C)}{P(A)} = \frac{1/18}{5/6} = \boxed{\frac{1}{15}}$ (2)

(iii) $P(D|A) = \frac{P(A \cap D)}{P(A)} = \frac{0}{5/6} = \boxed{0}$ (2)

(c) $P(X = r) = \binom{n}{r} p^r (1-p)^{n-r}$ $n = 6$

(c) $P(X=r) = \binom{n}{r} p^r (1-p)^{n-r}$

$n = 6$

$p = 0.6$

(i) $P(X=0) = \binom{6}{0}(0.6)^0(0.4)^6 = \frac{64}{15625}$ (2)

(ii) $P(X=1) = \binom{6}{1}(0.6)^1(0.4)^5 = \frac{576}{15625}$ (2)

(iii) $P(X=3) = \binom{6}{3}(0.6)^3(0.4)^3 = \frac{864}{3125}$ (2)

(iv) $P(X \leq 2) = P(X=0) + P(X=1) + P(X=2)$

$= \frac{64}{15625} + \frac{576}{15625} + \frac{432}{3125} = \frac{112}{625}$ (2)

(v) $P(X \geq 3) = P(X=3,4,5,6)$

$= 1 - P(X=2,1,0)$

$= 1 - \frac{112}{625} = \frac{513}{625}$ (3)