VE 203 Hw 6 周维凯 518021911039

Ex 8.2 $n = pq = 77$

$c \equiv m^e \bmod n$

$c \equiv 23^7 \equiv ((23)^2)^3 \cdot 23 \equiv 67^3 \cdot 23 \equiv 23 \times 67 \times 23 \equiv 67^2 \equiv 23 \bmod 77$

Therefore, the encryption message is 23.

Ex 8.4 $3^a \bmod 7 = 6$

$3^b \bmod 7 = 5$

We can get $a = 3$, $b = 5$

$5^3 \equiv 6^5 \equiv 6 \bmod 7$

Therefore, common secret key is 6.

Ex 8.5 i). vertices: 6

edges: 6

degree of a_1: 2

degree of a_2: 4

degree of a_3: 1

degree of a_4: 3

degree of a_5: 2

degree of a_6: 0

isolated vertices: a_6

pendant vertices: a_3

simple graph

$$\begin{array}{c} \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \end{array}
\begin{array}{c} \begin{array}{cccccc} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \end{array} \\
\begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \end{array}$$

ii) vertices: 6

edges: 12

degree of a_1: 6

degree of a_2: 5

degree of a_3: 0

degree of a_4: 3

degree of a_5: 5

degree of a_6: 5

isolated vertices: a_3

No pendant vertices

pseudo graph

$$\begin{array}{c} \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \end{array}
\begin{array}{c} \begin{array}{cccccc} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \end{array} \\
\begin{pmatrix} 1 & 3 & 0 & 1 & 0 & 0 \\ 3 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 3 \\ 0 & 0 & 0 & 0 & 3 & 1 \end{pmatrix} \end{array}$$

iii) vertices: 9

edges: 10

degree of a_1: 2

degree of a_2: 2

degree of a_3: 2

degree of a_4: 0

degree of a_5: 0

degree of a_6: 3

degree of a_7: 2

degree of a_8: 4

degree of a_9: 5

isolated vertices: a_4, a_5

No pendant vertices

multigraph

$$\begin{array}{c} \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \\ a_8 \\ a_9 \end{array}
\begin{array}{c} \begin{array}{ccccccccc} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_8 & a_9 \end{array} \\
\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 3 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 3 & 0 \end{pmatrix} \end{array}$$

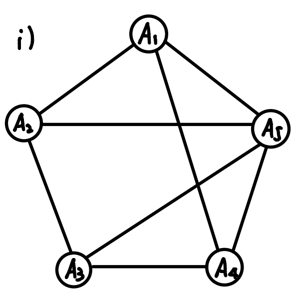
Ex 8.6 i) b, d, e and a, c are the two sets of vertices

Therefore, it is bipartite.

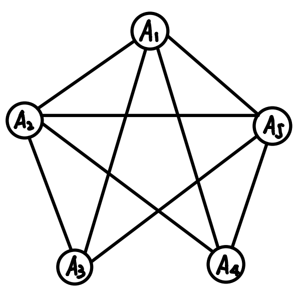
ii) b, c, f forms a triangle, which is an odd circle. therefore, it is not bipartite.

iii) b, d, e forms a triangle, which is an odd circle. therefore, it is not bipartite.

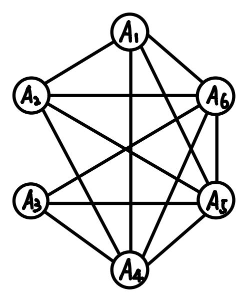
Ex 8.7 i)



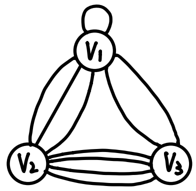
ii)



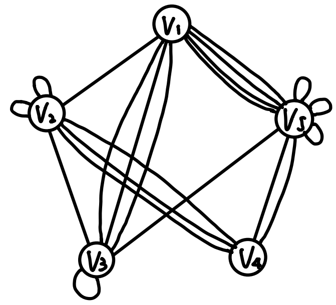
iii)



Ex 9.1 i)



ii)



Ex 9.2 i) $\varphi: u_1 \to v_1,\ u_2 \to v_4,\ u_3 \to v_2,\ u_4 \to v_5,\ u_5 \to v_3$

Let $G_1(U,E)$ denote the first graph, $G_2(V,F)$ denote the second graph.

$E = \{\{u_1,u_2\}, \{u_1,u_5\}, \{u_4,u_5\}, \{u_3,u_4\}, \{u_2,u_3\}\}$

$\varphi_* E = \{\{v_1,v_4\}, \{v_1,v_3\}, \{v_5,v_3\}, \{v_2,v_5\}, \{v_4,v_2\}\}$

$= F$

Therefore, G_1 and G_2 are isomorphic.

ii) $\varphi: u_1 \to v_1,\ u_2 \to v_3,\ u_3 \to v_2,\ u_4 \to v_5,\ u_5 \to v_4$

Let $G_1(U,E)$ denote the first graph, $G_2(V,F)$ denote the second graph.

$E = \{\{u_1,u_5\}, \{u_1,u_4\}, \{u_1,u_2\}, \{u_2,u_5\}, \{u_4,u_5\}, \{u_2,u_4\}, \{u_2,u_3\}, \{u_3,u_4\}\}$

$\varphi_* E = \{\{v_1,v_4\}, \{v_1,v_5\}, \{v_1,v_3\}, \{v_3,v_4\}, \{v_5,v_4\}, \{v_3,v_5\}, \{v_3,v_2\}, \{v_2,v_5\}\}$

$= F$

Therefore, G_1 and G_2 are isomorphic.

Ex 9.3 i) It means that every two vertices are connected.

For graph with n vertices, every vertex with $n-1$ degree

If it is Euler circuit, $n-1$ should be even.

Therefore, $n \in \{2k+1,\ k \in \mathbb{N}\}$.

ii) For graph with n vertices, there is one vertex is with $n-1$ degree while other vertices are with 3 degree.

We know 3 is odd, therefore, it cannot be an Euler circuit.

iii) For cycle graph, every vertex is with 2 degree.

Therefore, cycle graph is always an Euler circuit.

And for cycle graph, $n \geq 3$.

Ex 9.8 ⓪ $S_0 = \phi$ U:0

① $S_1 = \{U\}$ U:0 Q:4 Z:6 D:7 E:10

② $S_2 = \{U,Q\}$ U:0 Q:4 Z:6 D:7 P:9 E:10 T:11 F:14

③ $S_3 = \{U,Q,Z\}$ U:0 Q:4 Z:6 D:7 P:9 E:10 T:11 F:14

④ $S_4 = \{U,Q,Z,D\}$ U:0 Q:4 Z:6 D:7 P:9 E:10 T:11 F:14 C:17

⑤ $S_5 = \{U,Q,Z,D,P\}$ U:0 Q:4 Z:6 D:7 P:9 E:10 T:11 F:14 S:15 O:15

⑥ $S_6 = \{U,Q,Z,D,P,E\}$ U:0 Q:4 Z:6 D:7 P:9 E:10 T:11 F:14 S:15 O:15 C:16

⑦ $S_7 = \{U,Q,Z,D,P,E,T\}$ U:0 Q:4 Z:6 D:7 P:9 E:10 T:11 F:14 X:14 O:15 C:16 S:15

⑧ $S_8 = \{U,Q,Z,D,P,E,T,F,X\}$ U:0 Q:4 Z:6 D:7 P:9 E:10 T:11 F:14 X:14 O:15 S:15 C:16 H:17 G:20 W:23

⑨ $S_9 = \{U,Q,Z,D,P,E,T,F,X,O,S\}$ U:0 Q:4 Z:6 D:7 P:9 E:10 T:11 F:14 X:14 O:15 S:15 C:16 H:17 G:20 W:23
Y:18 N:20 R:22

⑩ $S_{10} = \{U,Q,Z,D,P,E,T,F,X,O,S,C\}$ U:0 Q:4 Z:6 D:7 P:9 E:10 T:11 F:14 X:14 O:15 S:15 C:16 H:17 Y:18 N:20 G:20 R:22 W:23
B:24

⑪ $S_{11} = \{U,Q,Z,D,P,E,T,F,X,O,S,C,H\}$ U:0 Q:4 Z:6 D:7 P:9 E:10 T:11 F:14 X:14 O:15 S:15 C:16 H:17 Y:18 N:20 G:20 R:22 W:23
B:24 I:28

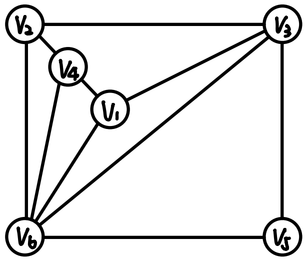
⑫ $S_{12} = \{U,Q,Z,D,P,E,T,F,X,O,S,C,H,Y\}$ U:0 Q:4 Z:6 D:7 P:9 E:10 T:11 F:14 X:14 O:15 S:15 C:16 H:17 Y:18 N:20 G:20 R:22 W:23
B:24 I:28 V:24

⑬ $S_{13} = \{U,Q,Z,D,P,E,T,F,X,O,S,C,H,Y,N,G\}$ U:0 Q:4 Z:6 D:7 P:9 E:10 T:11 F:14 X:14 O:15 S:15 C:16 H:17 Y:18 N:20 G:20 R:22
W:23 B:24 V:24 I:28 A:27

(14) $S_{14} = \{U, Q, Z, D, P, E, T, F, X, O, S, C, H, Y, N, G, R\}$ U: 0 Q: 4 Z: 6 D: 7 P: 9 E: 10 T: 11 F: 14 X: 14 O: 15 S: 15 C: 16 H: 17 Y: 18 N: 20 G: 20 R: 22
W: 23 B: 24 V: 24 M: 24 A: 27 L: 27 I: 28

Finally, we have $U \to Z \to P \to S \to Y \to W$, $U \to Q \to P \to S \to Y \to W$, $U \to Q \to T \to X \to W$
and the length is 23.

Ex 10.1 ii)

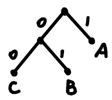


ii) $e=18$, $v=7$

$e > 3v-6$

Therefore, by Corollary 3.3.5, it is non-planar

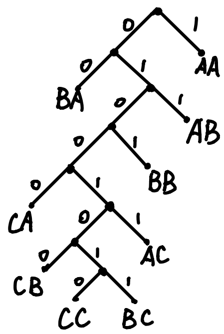
Ex 10.5 i)



A: 1
B: 01
C: 00

ii)

AA: 0.64	AB: 0.152	AC: 0.008
BA: 0.152	BB: 0.0361	BC: 0.0019
CA: 0.008	CB: 0.0019	CC: 0.0001



AA: 1	AB: 011	AC: 010011
BA: 00	BB: 0101	BC: 01001011
CA: 01000	CB: 0100100	CC: 01001010