# 2021학년도 1학기 기말시험(온라인평가)

**교과목명 : 이산수학**
**학 번 : 202034-153746**
**성 명 : 이동열**
**연 락 처 : 010-5264-5565**
**평가유형 :주관식형**

---

o 주관식형 : ※ 주관식일 경우 문제번호 표기 후 답안 작성
o 과제물유형 : 공통형
o 과제명 :

1. 2019학년도 『이산수학』의 기말시험 기출문제 중 6개 문제(55번~60번)에 대해 풀이를 해설하시오. 단, 문제에서 다루는 주요 용어에 대해 설명하고, 정답은 왜 정답인지, 오 답은 왜 오답인지를 상세히 설명할 것. (참고: 이산수학 워크북의 해설) [30점]

2. 교재 제10장의 연구과제 14번(교재 p.268)을 푸시오. [10점]

3. 교재 제12장의 연구과제 15번(교재 p.325)을 푸시오. [10점]

4. RSA 암호화와 복호화 과정에 대해 다음 순서에 따라 설명하시오. [20점]
(1) 암호화를 위한 공개키를 임의로 정하고 왜 적합한지 밝히시오.
(2) 학생의 영문 성과 학번의 끝 3자리를 암호문으로 만드는 과정을 설명하시오. (예를 들어 학생 홍길동의 학번이 ******-***123이면 HONG123이 평서문임. 필요한 경우 space를 26번으로 정함).
(3) 복호화를 위한 비밀키를 임의로 정하고 왜 적합한지 밝히시오.
(4) 단계(2)번에서 구한 암호문을 평서문으로 복호화하는 과정을 설명하시오.

1. 202034-153746 이동열

(55)

그래프는 점과 점 사이를 잇는 선으로 이루어진 도형을 말한다. 이 도형에서 점은 꼭지점(vertex), 선은 변(edge)이라고 부르며 꼭지점 집합 V와 변 집합 E를 가지는 그래프를 G=(V,E)로 표현한다. 이 변e를 통해 두 꼭지점 v1과 v2가 연결되었을 경우 v1과 v2가 변 e를 통해 발생되었다고 하며 두 꼭지점 v1과 v2는 인접하다고 표현한다. 그리고 v1과 v2를 잇는 변이 2개 이상일 경우 각 변들을 병렬 변이라고 하며 변에 연결되어 있지 않은 꼭지점들을 고립되었다고 표현한다. ① 그래프는 방향 그래프와 무향 그래프로 나눌수 있는데 방향 그래프는 변이 방향성을 가지고 있는 그래프를 말하며 무향 그래프는 변에 방향성이 없는 그래프를 말한다. 고속도로와 인도의 차이를 생각하면 된다. 위 그래프에서는 각 변이 방향성을 가지고 있지 않으므로 방향그래프가 아니다. ② 이분 그래프는 그래프 G내 꼭지점 부분 집합 v1과 v2로 분할 되어 있을 경우 각 부분 집합 내 꼭지점들은 인접해 있지 않고 다른 집합의 꼭지점에만 인접해 있는 그래프를 말한다. 각 변의 양끝은 각각 v1의 꼭지점과 v2의 꼭지점이어야 하며 (v1-v2) 변 양끝이 같은 집합의 꼭지점일 경우 이분 그래프가 아니게 된다. 위 그래프의 경우 어떤 방식으로 꼭지점 부분 집합을 나누더라도 같은 집합 내 꼭지점이 인접하게 되므로 이분그래프라고 할 수 없다. ③ 완전 그래프는 각 꼭지점들이 인접해 있는 그래프를 말한다. 즉, 모든 꼭지점들이 자기 자신을 제외한 나머지 꼭지점들과 변으로 연결되어 있는 그래프이다. 위 그래프는 각 꼭지점들이 자기 자신을 제외한 다른 꼭지점들과 변으로 연결되어 인접해 있으므로 완전그래프이다. 차수는 각 꼭지점에 연결된 변의 수를 말한다. 무향 그래프의 경우 연결되어 있는 변의 수가 차수가 되고 방향 그래프의 경우 연결되어 있는 변의 인접 부분이 변의 머리인지 꼬리인지에 따라 진입차수와 진출차수로 나뉘게 된다. 위 그래프의 경우 모든 꼭지점의 차수가 2이다.

(56)

그림에 나와있는 그래프는 4개의 꼭지점을 가지고 있는 무향 그래프이다. ① 완전 그래프란 각 꼭지점이 자기자신을 제외한 모든 꼭지점과 인접해 있는 그래프를 말하며 꼭지점 개수를 n이라고 한다면 $K_n$으로 표현할 수 있다. 위 그래프는 꼭지점이 4개인 완전 그래프 $K_4$이다. ② 정규 그래프란 각 꼭지점이 동일한 수의 인접 꼭지점을 갖는 그래프를 말한다. 꼭지점의 차수에 따라 k-정규 그래프(k는 차수)라고 표현하며 그 중에서도 차수가 3인 정규 그래프는 삼차 그래프 및 큐빅 그래프(cubic graph)라고도 한다. 위 그래프는 각 꼭지점의 차수가 3인 3-정규 그래프이며 큐빅 그래프이다. ③ 오일러 투어는 그래프의 모든 변을 한번씩만 통과해 시작지점으로 되돌아오는 탐색방법을 말한다. 오일러 투어는 한 붓그리기, 오일러 회로라고도 불리며 각 꼭지점의 차수가 짝수이면 오일러 투어를 가지게 된다. 오일러의 투어를 구하는 방법은 각 차수가 짝수라는 가정하에 임의의 꼭지점에서 출발하여 다른 꼭지점을 경유해 다시 원래 꼭지점으로 돌아오는 작은 사이클을 구한후 이 사이클이 오일러 투어이면 종료 아니라면 거쳐갔던 꼭지점 중 사용하지 않은 다른 변이 존재하는 꼭지점으로 이동해 방금 진행했던 것과 같은 사이클을 재귀적으로 반복한다. 전부 반복하고 나면 두 번째부터 진행된 사이클을 앞서 진행한 사이클 내에 삽입해 오일러의 투어를 완성한다. 사이클 삽입은 전체 꼭지점 집합 V={A,B,C,D,E,F,G}라고 가정할 때 k-1번째 사이클 B→C→G→F→B가 존재할 경우 k번째 사이클 G→D→E→A→G를 k-1번째 사이클의 G(k번째 시작점)에 삽입해 B→C→G→D→E→A→G→F→B를 완성하는 방법이다.

(56 - 이어서)

2020134 - 153746 이동열

이 그래프의 경우 각 차수가 홀수이므로 오일러의 투어가 존재하지 않는다. ④ 해밀턴 사이클이란 각 꼭지점을 별로 통해 한번씩만 거쳐서 시작 꼭지점으로 되돌아오는 경로를 말한다. 오일러의 투어랑 다른 점은 모든 변을 거칠 필요가 없고 시작 꼭지점과 종료꼭지점이 겹쳐서 중복되는 것이에 꼭지점을 중복해서 방문하면 안된다는 점이다. 해밀턴 사이클을 구하는 알고리즘은 난제로 남아 있으며 위 그래프의 경우 abcda의 해밀턴 사이클을 구할 수 있다.

(57)

트리란 계층 구조를 표현하기 위한 그래프의 일종으로 사이클이 존재하지 않는 그래프를 말하며, 각 꼭지점을 노드라고 표현한다. 트리안에 노드가 한개일 경우 자명한 트리라고 하며, 노드가 존재하지 않으면 공백노드, 그래프 내 트리가 1개이상 존재하면 포레스트라고 한다. 이 트리는 여러노드가 한 노드를 가리킬수 없고 각각의 노드들을 잇는 변이 하나 뿐이다. 이 트리중 최상위 노드를 루트 노드라고 부르며 두 노드 A, B가 존재하고 A노드가 B노드를 가리키고 있을경우 A노드를 부모 노드, B노드를 자식노드 칭한다. 또한 자식노드가 없을 경우 잎노드, 잎노드의 나머지 노드를 내부노드라고 한다. ① 트리는 사이클이 존재하지 않는 연결 그래프를 말하므로 맞다. ② n개의 노드를 가지는 연결 그래프의 경우 변이 n-1개라면 트리가 된다. 즉, n개의 노드에 n개의 변을 가지는 연결 그래프는 트리가 아니다. ③ 차수는 노드가 가지는 자식노드의 개수를 차수로 하며 트리의 차수는 각노드의 차수중 최대값이다. ④ 트리의 높이란 트리내 잎노드들의 총개수를 말한다.

(58)

이 트리는 모든 노드의 최대 수가 2인 이진트리로 공집합을 허용하고 각 자식노드들을 왼쪽자식 노드 오른쪽 자식노드라고 부른다. 허프만 코딩이란 최소합을 사용해 파일을 압축하는 방법이다. 여기서 합이란 완전이진트리를 기본으로 하는 자료구조를 말하며, 부모노드의 값이 자식노드의 값보다 큰 합을 최대합이다. ② 트리의 높이는 루트노드 부터 잎노드 까지의 거리로 변의 개수에 해당한다. 위트리의 경우 높이는 3이다. ③ 트리내 노드의 차수는 자식노드의 개수이고 트리의 차수는 노드차수 중 최대값이다. 위 트리의 경우 최대 노드 차수가 2이므로 트리차수는 2이다. ④ 허프만 코딩이란 문자 발생 빈도수가 존재할경우 빈도수를 가지고 최소합을 갖는 이진트리로 만들어 이진화된 값을 얻는 방식이다. 위와 발생 빈도수를 가지고 예를들면 최소 발생 빈도수를 갖는 두 문자를 선택해 두 문자의 빈도수의 합을 갖는 부모노드를 만들고 그 위에 자식노드로 넣는다. 이 때 두노드중 큰 빈도수를 오른쪽에 두고 두 노드와 부모 노드를 잇는 변에 각각 0과 1을 부여한다. 이 때 0은 왼쪽 1은 오른쪽이다. 이런식으로 계속 반복해서 이진트리를 만들고 나면 각 잎노드에서부터 루트노드 까지의 변에 부여된 이진코드가 허프만코딩 값이 된다. 즉, 빈도수가 많은 문자는 짧은 이진코드를 갖게되고 빈도수가 적은 문자는 긴 이진코드를 결과적으로 위트리에서 E의 코딩값은 E에서 루트까지의 변의 이진값 11이된다.

202034-153746 이동열

(59)

함수는 두 집합 A, B가 존재할 경우 A의 각원소에 대응하는 B의 원소가 한개만 존재하며 A집합을 정의역 B집합을 공역이라고 한다. 모든 함수를 구해야하며 다른 조건은 존재하지 않으므로 함수는 가정하여 모든 경우의 수를 구하면된다. 즉, a가 1~3일 경우, b가 1~3일 경우 두 사건이 동시에 일어날 모든 경우의 수를 구하면 된다. 두 사건이 동시에 일어날 경우의 수를 구하는 계수의 곱셈 법칙을 이용하면 a=3(개), b=3(개) 이므로 3×3=9, 1번이 답이 된다.

(60)

유한 오토마타란 정규문법에 의해 생성된 정규언어를 해석하는 오토마타로 유한한 상태를 가진다고 해서 유한오토마타이다. 결정적 유한 오토마타는 유한 오토마타에서 출력을 제거하고 수락상태 집합을 추가한 형태의 유한오토마타를 말한다. 수락상태는 (reject, accept), (0, 1), (no, yes) 등으로 표현할 수 있다. 위 문제를 표로 나타내면

| | 0 | 1 |
|---|---|---|
| $S_0$ | $S_1(a)$ | $S_0(a)$ |
| $S_1$ | $S_1(b)$ | $S_0(b)$ |

로 나타낼수 있다. 그리고 011000은

| 0 | 1 | 1 | 0 | 0 | 0 |
|---|---|---|---|---|---|
| $S_1(a)$ | $S_0(b)$ | $S_0(a)$ | $S_1(a)$ | $S_1(b)$ | $S_1(b)$ |

로 답은 abaabb ②번이다. ①번의 경우

| 0 | 0 | 1 | 1 | 1 | 1 |
|---|---|---|---|---|---|
| $S_1(a)$ | $S_1(b)$ | $S_0(b)$ | $S_0(a)$ | $S_0(a)$ | $S_1(a)$ |

로 001111에 대응된다. ③번은 b로 시작하는데 해당 결정적 유한 오토마타는 a로만 시작하므로 정답이 아니다. ④번도 b로 시작하므로 정답이 아니다.

202034 - 153746 서동빈

2.

데이크스트라 알고리즘은 양의 값을 가지는 방향 그래프에서 출발지점과 도착지점 사이의 최단거리를 구해주는 알고리즘이며 최소값 갱신을 통해 최단거리를 구할 수 있다.

①
d[b] = 2
d[c] = 4
d[d] = 1
d[e] = ∞
⋮
d[Z] = ∞

②
d[b] = 2
d[c] = 4
d[e] = ∞
d[f] = d[d] + 5 = 6 (a -> d -> f)
d[g] = d[d] + 4 = 5 (a -> d -> g)
⋮
d[Z] = ∞

③
d[c] = 4
d[e] = d[b] + 1 = 3 (a -> b -> e)
d[f] = d[d] + 5 = 6 ~~(a -> d -> g)~~ (a -> d -> f)
d[g] = d[d] + 4 = 5 ~~(a -> b -> e -> h)~~ (a -> d -> g
⋮
d[Z] = ∞

④
d[c] = 4
d[f] = d[d] + 5 = 6 (a -> d -> f)
d[g] = d[d] + 4 = 5 (a -> d -> g)
d[h] = d[e] + 3 = 6 (a -> b -> e -> h)
⋮
d[Z] = ∞

⑤
d[f] = d[d] + 5 = 6 (a -> d -> f)
d[g] = d[d] + 4 = 5 (a -> d -> g)
d[h] = d[e] + 3 = 6 (a -> b -> e -> h)
⋮
d[Z] = ∞

⑥
d[f] = d[d] + 5 = 6 (a -> d -> f)
d[h] = d[e] + 3 = 6 (a -> b -> e -> h)
d[i] = ∞
d[j] = ∞
d[k] = d[g] + 2 = 7 (a -> d -> g -> k)
⋮
d[Z] = ∞

⑦
d[h] = d[e] + 3 = 6 (a -> b -> e -> h)
d[i] = d[f] + 2 = 8 (a -> d -> f -> i)
d[j] = d[f] + 4 = 10 (a -> d -> f -> j)
d[k] = d[g] + 2 = 7 (a -> d -> g -> k)
⋮
d[Z] = ∞

⑧
d[i] = d[f] + 2 = 8 (a -> d -> f -> i)
d[j] = d[f] + 4 = 10 (a -> d -> f -> j)
d[k] = d[g] + 2 = 7 (a -> d -> g -> k)
d[l] = d[h] + 1 = 7 (a -> b -> e -> h -> l)
d[m] = ∞
d[n] = ∞
d[o] = d[h] + 8 = 14 (a -> b -> e -> h -> o)
⋮
d[Z] = ∞

⑨
d[i] = d[f] + 2 = 8 (a -> d -> f -> i)
d[j] = d[f] + 4 = 10 (a -> d -> f -> j)
d[l] = d[h] + 1 = 7 (a -> b -> e -> h -> l)
d[m] = ∞
d[n] = d[k] + 4 = 11 (a -> d -> g -> k -> n)
d[o] = d[h] + 8 = 14 (a -> b -> e -> h -> o)
d[p] = ∞
d[q] = ∞
d[r] = d[k] + 2 = 9 (a -> d -> g -> k -> r)
⋮
d[Z] = ∞

202034-153741 이동열

(10)

d[m] = d[l] + 3 = 10 (a→b→e→h→l→m)
d[n] = d[k] + 4 = 11 (a→d→g→k→n)
d[o] = d[l] + 6 = 13 (a→b→e→h→l→o)
d[p] = ∞
d[q] = ∞
d[r] = d[k] + 2 = 9 (a→d→g→k→r)
⋮
d[z] = ∞

(11)

d[m] = d[l] + 3 = 10 (a→b→e→h→l→m)
d[n] = d[r] + 1 = 10 (a→d→g→k→r→n)
d[o] = d[l] + 6 = 13 (a→b→e→h→l→o)
d[p] = ∞
d[q] = d[r] + 8 = 17 (a→d→g→k→r→q)
d[s] = ∞
d[t] = d[r] + 5 = 14 (a→d→g→k→r→t)
⋮
d[z] = ∞

(12)

d[m] = d[l] + 3 (a→b→e→h→l→m) = 10
d[o] = d[l] + 6 (a→b→e→h→l→o) = 13
d[p] = ∞
d[q] = d[n] + 2 (a→d→g→k→r→n→q) = 12
d[s] = ∞
d[t] = d[r] + 5 (a→d→g→k→r→t) = 14
⋮
d[z] = ∞

(13)

d[o] = d[l] + 6 = 13 (a→b→e→h→l→o)
d[p] = d[q] + 1 = 13 (a→d→g→k→r→n→q→p)
d[s] = ∞
d[t] = d[r] + 5 = 14 (a→d→g→k→r→t)
⋮
d[z] = ∞

(14)

d[p] = d[q] + 1 = 13 (a→d→g→k→r→n→q→p)
d[s] = d[o] + 6 = 19 (a→b→e→h→l→o→s)
d[t] = d[r] + 5 = 14 (a→d→g→k→r→t)
⋮
d[z] = ∞

(15)

d[s] = d[p] + 2 = 15 (a→d→g→k→r→n→q→p→s)
d[t] = d[p] + 1 = 14 (a→d→g→k→r→n→q→p→t)
⋮
d[z] = ∞

(16)

d[s] = d[p] + 2 = 15 (a→d→g→k→r→n→q→p→s)
d[z] = d[t] + 8 = 22 (a→d→g→k→r→n→q→p→t→z)

(17)

d[z] = d[s] + 2 = 17 (a→d→g→k→r→n→q→p→s→z) ← 정답

202034-153746 이동열

3.

이항정리 시 표현되는 계수의 값이 파스칼 삼각형의 값과 일치하는 점을 이용해 조합으로 표현할수 있다.

$(x+y)^n = \sum_{k=0}^{n} C(n,k)\, x^{n-k} y^k$ 에서 계수만을 표현하므로 $x^{n-k}y^k$ 을 제거하면 파스칼 삼각형에 대응하는 조합을 표현할 수 있으며 n은 층수 R은 순서에 해당한다.

즉,

$C_{(1,0)}$ $C_{(1,1)}$

$C_{(2,0)}$ $C_{(2,1)}$ $C_{(2,2)}$

$C_{(3,0)}$ $C_{(3,1)}$ $C_{(3,2)}$ $C_{(3,3)}$

⋮

$C_{(n,0)}$ $C_{(n,1)}$ $C_{(n,2)}$ $C_{(n,3)}$ ⋯ $C_{(n,n)}$

로 표현할 수 있다.

이 상태에서 문제의 그림처럼 피보나치 수열을 표현하면

$F_0 = 1$ ( $C_{(0,0)}$을 조합식에서 분모가 0이 되므로 제외)

$F_1 = C_{(1,0)}$

$F_2 = C_{(2,0)} + C_{(1,1)}$

$F_3 = C_{(3,0)} + C_{(2,1)}$

$F_4 = C_{(4,0)} + C_{(3,1)} + C_{(2,2)}$

⋮

$F_n = C_{(n,0)} + C_{(n-1,1)} + C_{(n-2,2)}, \cdots C_{(n-\lfloor \frac{n}{2} \rfloor, \lfloor \frac{n}{2} \rfloor)}$

(n이 홀수일 경우 소수가 되므로 반드시 바닥함수를 사용)

위와 같으며

$F_n = \sum_{i=0}^{k} C(n-i, i)$ 를 증명하게 된다. ($k$는 $\lfloor \frac{n}{2} \rfloor$)

202034-153746 이동열

4.

(1)

공개키란 (n,e)로 표현하며 n은 두 소수의 곱으로 표현한다. e의 경우 n을 설정할 때 사용한 두 소수 p,q가 존재할 경우 (p-1)(q-1)의 서로소 값으로 설정할 수 있다. 임의의 공개키 (3139, 19)를 설정했을 경우 3139는 43과 73 두 소수의 곱으로 표현 가능하고 e는 (43-1)(73-1)의 서로소이기 때문에 적합한 암호화 키이다.

(2)

Space를 26

0부터 9까지를 27~36으로 임의로 설정한다.

위에서 설정한 공개키 (3139, 19)를 통해 LEE746을 암호화 한다고 하면

먼저 LEE746을 수열로 변경한다. LEE746 → 11 4434 3133

이 수열을 블록으로 나누게 되면 $9=36<3139<99<3636$ 이므로 2자리 블록으로 분리한다.

(11 04 04 34 31 33)

각 블록을 $C=m^e \bmod n$ 계산을 통해 나머지 거듭제곱 알고리즘을 이용해서 암호화 한다.

첫번째 블록을 암호화 한다면

$11^2 \bmod 3139 = 121$

$11^4 \bmod 3139 = (11^2 \bmod 3139)(11^2 \bmod 3139) \bmod 3139$
$= 121^2 \bmod 3139$
$= 2085$

$11^8 \bmod 3139 = (11^4 \bmod 3139)(11^4 \bmod 3139) \bmod 3139$
$= 2085^2 \bmod 3139$
$= 2849$

$11^{16} \bmod 3139 = (11^8 \bmod 3139)(11^8 \bmod 3139) \bmod 3139$
$= 2849^2 \bmod 3139$
$= 2486$

$11^{19} \bmod 3139 = (11^{16} \bmod 3139)(11^3 \bmod 3139) \bmod 3139$
$= (2486 \times 121 \times 11) \bmod 3139$
$= 360$

360이 암호문이 된다.

위와 같은 방법을 나머지 블록에도 적용하면

$4^{19} \bmod 3139 = 2486$, $34^{19} \bmod 3139 = 2305$, $31^{19} \bmod 3139 = 2302$, $33^{19} \bmod 3139 = 2497$

이 되며 암호문 = (360 2486 2481 2305 2302 2497)

(3)

평서문을 공개키 $(n,e)$로 암호화 했다면 복호화는 개인키 $d$를 통해서 진행할 수 있다. $d$는 $e \bmod (p-1)(q-1)$의 역으로 $de \equiv 1 \pmod{(p-1)(q-1)}$로 표현 가능하다. 즉, $de$를 $(p-1)(q-1)$로 나눌 경우 나머지 $d$를 구하면 된다. 위 (2)번에서 $e=19, p=43, q=73$으로 설정했으므로 $(p-1)(q-1)=3024$, $1 \equiv d \times 19 \pmod{3024}$로 표현할 수 있고 확장된 유클리드 알고리즘을 사용해서 $d$를 구할 수 있다.

$3024 = 19 \times 159 + 3$

$19 = 6 \times 3 + 1$

---

$1 = 19 - 6 \times 3$

$= 19 - 6(3024 - 19 \times 159)$

~~$= 19 + 6(19 \times 159)$~~ $19 + 6 \times 19 \times 159 - 6 \times 3024$

$= 19 \times \boxed{955} - 6 \times 3024$

↑ 개인키

이렇게 해서 $955 \times 19 = 3024 \times 6 + 1$로 표현이 가능하게 되고 개인키는 955가 된다.

(4)

(3)에서 구한 개인키를 통해 복호화를 할 수 있다. 평서문 $m$은 $m = C^d \bmod pq$ 모듈러 함수를 통해 구할 수 있다. $p=43, q=73, d=955$ 이므로 식에 대입하면 $m = c^{955} \bmod 3139$이고 여기에 암호문을 대입해서 평서문을 구할 수 있다. [310, 2486, 2486, 2305, 2302, 2497]

첫 번째 블록을 구해보면

$360^{955} \bmod 3139$

$360^2 \bmod 3139 = 901$

$360^4 \bmod 3139 = 901^2 \bmod 3139$

$= 1939$

$360^8 \bmod 3139 = 1939^2 \bmod 3139$

$= 2338$

$360^{16} \bmod 3139 = 2338^2 \bmod 3139$

$= 1245$

$\vdots$

$360^{512} \bmod 3139 = 1638^2 \bmod 3139$

$= 2338$

$360^{955} \bmod 3139 = (360^{512} \bmod 3139)(360^{256} \bmod 3139)(360^{128} \bmod 3139)(360^{32} \bmod 3139)(360^{8} \bmod 3139)(360^{2} \bmod 3139)(360 \bmod 3139) \bmod 3139 = 11$ 이된다.

위와같은 방법으로 나머지 암호문을 복호화 하면

$2486^{955} \bmod 3139 = 4 = E$, $2486^{955} \bmod 3139 = 4E$, $2305^{955} \bmod 3139 = 34 = 7$, $2302^{955} \bmod 3139 = 31 = 4$

$2497^{955} \bmod 3139 = 33 = 9$ 로 복호화되며 모두 연결하면 LEE749 가 된다.