

이산수학과 응용 해설

박승안 지음

불법복사는 지적재산을 훔치는 범죄행위입니다.

저작권법 제136조(권리의 침해죄)에 따라 위반자는 5년 이하의 징역 또는
5천만원 이하의 벌금에 처하거나 이를 병과할 수 있습니다.

KM 경문사

박 승 안

해설

1.	[해설102] Peano 의 공리계	9 면
2.	[해설203] 정수의 표준분해	3 면
3.	[해설204] Mersenne 素數	1 면
4.	[해설205] Fibonacci 수와 Lucas 수	7 면
5.	[해설307] 원시근과 이산로그	3 면
6.	[해설308] 전자 서명	5 면
7.	[해설404] 선형점화수열	5 면
8.	[해설504] 형식적 멱급수의 전개	3 면
9.	[해설506] 형식적 멱급수의 곱	5 면
10.	[해설907] 회로판	2 면
11.	[해설1002] 단순 연결그래프의 생성수형도	5 면
12.	[해설1102] 행렬식	16 면
13.	[해설1207] 타원곡선을 이용 정수의 인수분해	5 면
14.	[해설1704] Latin 방진과 Euler 방진	20 면

총 90 면

Peano 의 공리계

여기서는, 자연수에 대한 Peano 의 공리계를 소개한다.

정의 1 (Peano 의 공리계) 자연수 전체의 집합 \mathbb{N} 은 다음 네 조건을 만족시키는 집합이다.

(i) $1 \in \mathbb{N}$

(ii) 집합 \mathbb{N} 위에 일대일 사상 $\mathbb{N} \rightarrow \mathbb{N}$, $x \mapsto x^+$ 가 정의되어 있다. 즉,

$$x \neq y \Rightarrow x^+ \neq y^+, \quad x^+ = y^+ \Rightarrow x = y$$

(iii) 모든 원소 $x \in \mathbb{N}$ 에 대하여 $x^+ \neq 1$ 이다.

(iv) (수학적 귀납법 공리) 집합 \mathbb{N} 의 부분집합 S 에 대하여 다음 두 조건이 성립한다고 가정하자.

(a) $1 \in S$ (b) $x \in S$ 이면, $x^+ \in S$ 이다.

이 때, $S = \mathbb{N}$ 이다.

위의 (ii) 의 사상을 **후자사상**(後者寫像, successor map)이라 하고 x^+ 를 x 의 **후자**(後者, immediate successor)라고 한다. 위의 정의에서

$$1^+ = 2, 2^+ = 3, 3^+ = 4, 4^+ = 5, \dots$$

이라고 하면 $\mathbb{N} = \{1, 2, 3, 4, 5, \dots\}$ 이다.

정리 2 임의의 원소 $x \in \mathbb{N}$ 에 대하여 다음 중에서 하나 그리고 단 하나가 성립한다.

(1) $x = 1$ (2) 적당한 원소 $v \in \mathbb{N}$ 에 대하여 $x = v^+$ 이다.

증명 정리를 만족시키는 원소 $x \in \mathbb{N}$ 전체의 집합을 S 라고 하자.

먼저 정의 1 (iii) 에 의하여 모든 $v \in \mathbb{N}$ 에 대하여 $v^+ \neq 1$ 이므로 1 은 조건 (1) 만을 만족시키므로 $1 \in S$ 이다.

이제 $x \in S$ 이라고 하자. 이 때, $x = 1$ 이면, 정의 1의 (iii)에 의하여 $x^+ \neq 1$ 이지만 $x^+ = 1^+$ 이고 $1 \in N$ 이므로 x^+ 는 조건 (2) 만을 만족시키고 따라서 $x^+ \in S$ 이다. 다음에 $x \neq 1$ 이면, 적당한 $v \in N$ 에 대하여 $x = v^+$ 이므로 $x^+ = (v^+)^+$ 이고 $v^+ \in N$ 이지만, 정의 1의 (iii)에 의하여 $x^+ \neq 1$ 이므로 x^+ 는 조건 (2) 만을 만족시키고 따라서 $x^+ \in S$ 이다. 그러므로, 정의 1의 (iv)에 의하여 $S = N$ 이다.

따라서 모든 $x \in N$ 에 대하여 정리가 성립한다.

정의 3 집합 N 의 임의의 두 원소 x, y 에 대하여 합 $x + y$ 를 다음과 같이 귀납적으로 정의한다.

$$(i) \ x + 1 = x^+ \quad (ii) \ x + y^+ = (x + y)^+$$

위의 정의와 수학적 귀납법 공리(정의 1 (iv))에 의하여 집합 N 위의 덧셈 $+$ 은 잘 정의된다(well-defined).

정리 4 집합 N 위의 덧셈 $+$ 에 관하여 다음이 성립한다.

$$A.1 : (x + y) + z = x + (y + z) \quad (\text{결합법칙})$$

$$A.2 : x + y = y + x \quad (\text{교환법칙})$$

$$A.3 : x + z = y + z \text{ 이면, } x = y \text{ 이다.} \quad (\text{소약법칙})$$

증명 (1) A.1의 증명

이제 $x, y \in N$ 이라고 하자. 먼저 $z = 1$ 일 때, 정의 3에 의하여

$$(x + y) + 1 = (x + y)^+ = x + y^+ = x + (y + 1)$$

이므로, $z = 1$ 일 때 A.1은 성립한다.

다음에 $x, y, z \in N$ 에 대하여 등식 $(x + y) + z = x + (y + z)$ 가 성립한다고 가정하자. 이 때, 정의 3에 의하여

$$\begin{aligned} (x + y) + z^+ &= \{(x + y) + z\}^+ = \{(x + (y + z))\}^+ \\ &= x + (y + z)^+ = x + (y + z^+) \end{aligned}$$

이므로 z^+ 에 대해서도 A.1 은 성립한다.

따라서 모든 원소 $x, y, z \in \mathbb{N}$ 에 대하여 A.1 은 성립한다.

(2) A.2 의 증명

먼저 모든 원소 $x \in \mathbb{N}$ 에 대하여 $x+1 = 1+x$ 임을 증명한다.

분명히 위의 등식은 $x = 1$ 일 때 성립한다.

이제 원소 $x \in \mathbb{N}$ 에 대하여 $x+1 = 1+x$ 라고 가정하면, 정의 3 과 A.1 에 의하여 다음이 성립한다.

$$\begin{aligned} x^+ + 1 &= (x+1) + 1 = (1+x) + 1 \\ &= 1 + (x+1) = 1 + x^+ \end{aligned}$$

따라서 모든 원소 $x \in \mathbb{N}$ 에 대하여 $x+1 = 1+x$ 이다.

이제 임의의 원소 $x, y \in \mathbb{N}$ 에 대하여 등식 $x+y = y+x$ 가 성립함을 y 에 관한 귀납법으로 증명한다.

먼저 위의 결과에 의하여 $y = 1$ 일 때 이 등식은 성립한다.

그리고, $x+y = y+x$ 라고 가정하면, 정의 3 과 A.1 에 의하여 다음이 성립한다.

$$\begin{aligned} x + y^+ &= (x+y)^+ = (y+x)^+ \\ &= y + x^+ = y + (x+1) \\ &= y + (1+x) = (y+1) + x = y^+ + x \end{aligned}$$

따라서 모든 원소 $x, y \in \mathbb{N}$ 에 대하여 $x+y = y+x$ 이다.

(3) A.3 의 증명

먼저 원소 $x, y \in \mathbb{N}$ 에 대하여 $x+1 = y+1$ 이면, 정의 3 에 의하여 $x^+ = y^+$ 이고 따라서 정의 1 (ii) 에 의하여 $x = y$ 이다.

이제 원소 $x, y, z \in \mathbb{N}$ 에 대하여 A.3 가 성립한다고 가정하자.

이 때, $x+z^+ = y+z^+$ 이면, 정의 3 에 의하여 $(x+z)^+ = (y+z)^+$ 이므로 정의 1 (ii) 에 의하여 $x+z = y+z$ 이고 따라서 가정에 의하여 $x = y$ 이다.

그러므로, 모든 원소 $x, y, z \in \mathbb{N}$ 에 대하여 A.3 이 성립한다.

정리 5 모든 원소 $x, y \in \mathbb{N}$ 에 대하여 $x \neq x + y$ 이다.

증명 정의 1 (iii) 에 의하여 $1 \neq y^+ = y + 1 = 1 + y$ 이므로, $x = 1$ 일 때 $x \neq x + y$ 이다.

그리고 $x, y \in \mathbb{N}$ 에 대하여 $x \neq x + y$ 이라고 가정하면, $x^+ \neq x^+ + y$ 이다. 실제로, $x^+ = x^+ + y$ 이면, A.2 와 정의 3 에 의하여

$$x^+ = x^+ + y = y + x^+ = (y + x)^+ = (x + y)^+$$

이므로 $x = x + y$ 로 되어 모순이 생긴다.

따라서 모든 원소 $x, y \in \mathbb{N}$ 에 대하여 $x \neq x + y$ 이다.

정리 6 임의의 두 소 $x, y \in \mathbb{N}$ 에 대하여 다음 중에서 하나 그리고 단 하나가 성립한다.

- (1) $x = y$
- (2) 적당한 원소 $u \in \mathbb{N}$ 에 대하여 $x = y + u$ 이다.
- (3) 적당한 원소 $v \in \mathbb{N}$ 에 대하여 $y = x + v$ 이다.

증명 먼저 (1), (2), (3) 중에서 하나가 성립함을 증명한다.

정리 2 에 의하여 다음 중에서 하나 그리고 단 하나가 성립한다.

(a) $y = 1$

(b) 적당한 원소 $v \in \mathbb{N}$ 에 대하여 $y = v^+ = v + 1 = 1 + v$ 이다.

그러므로, $x = 1$ 일 때 정리는 성립한다.

이제 두 원소 $x, y \in \mathbb{N}$ 에 대하여 (1), (2), (3) 중에서 하나가 성립한다고 가정하면, x^+ 와 y 에 대하여 다음 결과를 얻는다.

① $x = y$ 이면, $x^+ = y^+ = y + 1$ 이므로 (ii) 가 성립한다.

② 적당한 원소 $u \in \mathbb{N}$ 에 대하여 $x = y + u$ 이라고 하자.

이 때, $x^+ = (y + u)^+ = y + u^+$ 이므로 (ii) 가 성립한다.

③ 적당한 원소 $v \in \mathbb{N}$ 에 대하여 $y = x + v$ 이라고 하자.

이 때, $v = 1$ 이면, $y = x + v = x + 1 = x^+$ 이므로 (i) 가 성립한다.

한편, $v \neq 1$ 이면, 정리 2에 의하여 $v = w^+$ 인 $w \in \mathbb{N}$ 가 존재하고 이때

$$\begin{aligned} y &= x + v = x + w^+ = x + (w+1) = x + (1+w) \\ &= (x+1) + w = x^+ + w \end{aligned}$$

이므로 (iii) 가 성립한다.

그러므로 모든 원소 $x, y \in \mathbb{N}$ 에 대하여 (1), (2), (3) 중에서 하나가 성립한다. 한편, (1) 과 (2) 가 동시에 성립하면, $x = y = x + u$ 로 되어 정리 5에 모순된다. 마찬가지로, (1) 과 (3) 이 동시에 성립하면, 정리 5에 모순된다.

그리고, (2) 와 (3) 이 동시에 성립하면,

$$x = y + u = (x + v) + u = x + (v + u)$$

로 되어 정리 5에 모순된다.

따라서 (1), (2), (3) 중에서 하나 그리고 단 하나가 증명한다.

정의 7 집합 \mathbb{N} 의 임의의 두 원소 x, y 에 대하여 곱 $x \cdot y$ 를 다음과 같이 귀납적으로 정의한다.

$$(i) \ x \cdot 1 = x \qquad (ii) \ x \cdot y^+ = x \cdot y + x$$

위의 정의와 귀납법 공리에 의하여 집합 \mathbb{N} 위의 곱셈 \cdot 은 잘 정의된다.

정리 8 집합 \mathbb{N} 위의 곱셈 \cdot 에 관하여 다음이 성립한다.

$$M.1 : (x \cdot y) \cdot z = x \cdot (y \cdot z) \qquad (\text{결합법칙})$$

$$M.2 : x \cdot y = y \cdot x \qquad (\text{교환법칙})$$

$$M.3 : x \cdot z = y \cdot z \text{ 이면, } x = y \text{ 이다.} \qquad (\text{소약법칙})$$

$$D : x \cdot (y+z) = x \cdot y + x \cdot z, \quad (x+y) \cdot z = x \cdot z + y \cdot z \qquad (\text{분배법칙})$$

증명 이 정리를 D, M2, M1, M3 의 순으로 증명한다.

(1) D 의 증명

이제 $x, y \in \mathbb{N}$ 이라고 할 때, 정의 7에 의하여

$$x \cdot (y+1) = x \cdot y^+ = x \cdot y + x = x \cdot y + x \cdot 1$$

이므로 $z = 1$ 일 때 D의 첫째 등식이 성립한다.

다음에 $x, y, z \in \mathbb{N}$ 에 대하여 등식 $x \cdot (y+z) = x \cdot y + x \cdot z$ 가 성립한다고 가정하면, 정의 3, 정의 7과 A.3에 의하여

$$\begin{aligned} x \cdot (y+z^+) &= x \cdot (y+z)^+ \\ &= x \cdot (y+z) + x \\ &= (x \cdot y + x \cdot z) + x \\ &= x \cdot y + (x \cdot z + x) \\ &= x \cdot y + x \cdot z^+ \end{aligned}$$

이므로 z^+ 에 대해서도 D의 첫째 등식은 성립한다.

따라서 모든 $x, y, z \in \mathbb{N}$ 에 대하여 D의 첫째 등식은 성립한다.

마찬가지 방법으로, D의 둘째 등식이 성립함을 증명할 수 있다.

(2) M.2의 증명

분명히 정의 7에 의하여 $1 \cdot 1 = 1$ 이다.

또, 원소 $x \in \mathbb{N}$ 에 대하여 $1 \cdot x = x$ 라고 가정하면, 정의 7과 정의 3에 의하여 $1 \cdot x^+ = 1 \cdot x + 1 = x + 1 = x^+$ 이다.

따라서 모든 원소 $x \in \mathbb{N}$ 에 대하여 $1 \cdot x = x \cdot 1$ 이다.

이제 $x, y \in \mathbb{N}$ 이라고 할 때, 위의 결과에 의하여 $x \cdot 1 = 1 \cdot x$ 이다. 또, $x \cdot y = y \cdot x$ 라고 가정하면, 정의 7과 D에 의하여 다음이 성립한다.

$$\begin{aligned} x \cdot y^+ &= x \cdot y + x = y \cdot x + x \\ &= y \cdot x + 1 \cdot x \\ &= (y+1) \cdot x = y^+ \cdot x \end{aligned}$$

따라서 모든 $x, y \in \mathbb{N}$ 에 대하여 $x \cdot y = y \cdot x$ 이다.

(3) M.1의 증명

먼저 $x, y \in \mathbb{N}$ 이라고 할 때, 정의 7에 의하여 다음이 성립한다.

$$(x \cdot y) \cdot 1 = x \cdot y = x \cdot (y \cdot 1)$$

그리고, $x, y, z \in \mathbb{N}$ 에 대하여 등식 $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ 가 성립한다고 가정하면, 정의 3, D와 정의 7에 의하여

$$\begin{aligned}
(x \cdot y) \cdot z^+ &= (x \cdot y) \cdot (z+1) \\
&= (x \cdot y) \cdot z + (x \cdot y) \cdot 1 \\
&= x \cdot (y \cdot z) + x \cdot y = x \cdot (y \cdot z + y) \\
&= x \cdot (y \cdot z + y \cdot 1) = x \cdot \{y \cdot (z+1)\} \\
&= x \cdot (y \cdot z^+)
\end{aligned}$$

따라서 모든 원소 $x, y, z \in \mathbb{N}$ 에 대하여 M.1 이 성립한다.

(3) M.3 의 증명

원소 $x, y, z \in \mathbb{N}$ 에 대하여 $x \cdot z = y \cdot z$ 일 때, $x \neq y$ 라고 가정하자.

이 때, 정리 6 에 의하여 $x = y + u$ 인 원소 $u \in \mathbb{N}$ 가 존재하거나 또는 $y = x + v$ 인 원소 $v \in \mathbb{N}$ 가 존재한다. 그런데, 첫째 경우에

$$x \cdot z = (y + u) \cdot z = y \cdot z + u \cdot z$$

이므로 정리 6 에 모순되고, 또 둘째 경우에

$$y \cdot z = (x + v) \cdot z = x \cdot z + v \cdot z$$

으로 되어 정리 6 에 모순된다. 따라서 $x = y$ 이다.

정의 9 두 원소 $x, y \in \mathbb{N}$ 에 대하여 $y = x + u$ 인 원소 $u \in \mathbb{N}$ 가 존재할 때, 이 사실을 $x < y$ 로 나타낸다.

그리고, $x = y$ 또는 $x < y$ 일 때, 이 사실을 $x \leq y$ 로 나타낸다.

집합 \mathbb{N} 위에는 위에서와 같이 정의된 순서관계 $<$ 에 대해서는 다음 두 정리가 성립한다.

정리 10 임의의 원소 $x, y, z \in \mathbb{N}$ 에 대하여 다음이 성립한다.

(1) 다음 중에서 하나 그리고 단 하나가 성립한다.

$$(i) \ x < y \quad (ii) \ x = y \quad (iii) \ y < x$$

(2) $x < y$, $y < z$ 이면, $x < z$ 이다.

(3) $x < y$ 이면, $x + z < y + z$, $x \cdot z < y \cdot z$ 이다.

증명 (1) 정리 6 과 정의 9 에 의하여 (1) 이 성립한다.

(2) $x < y$, $y < z$ 이면, 정의 9에 의하여

$$y = x + u, \quad z = y + v$$

인 원소 $u, v \in \mathbb{N}$ 가 존재하고 이때

$$z = y + v = (x + u) + v = x + (u + v)$$

이고 $u + v \in \mathbb{N}$ 이다. 따라서 $x < y$, $y < z$ 이면, $x < z$ 이다.

(3) $x < y$ 이면, $y = x + u$ 인 원소 $u \in \mathbb{N}$ 가 존재하고, 이때

$$\begin{aligned} y + z &= (x + u) + z = x + (u + z) \\ &= x + (z + u) = (x + z) + u, \\ y \cdot z &= (x + u) \cdot z = x \cdot z + u \cdot z \end{aligned}$$

이고 또 $u \in \mathbb{N}$, $u \cdot z \in \mathbb{N}$ 이다.

따라서 $x < y$ 이면, $x + z < y + z$, $x \cdot z < y \cdot z$ 이다.

정리 11 집합 \mathbb{N} 에서 다음이 성립한다.

- (1) 모든 원소 $x \in \mathbb{N}$ 에 대하여 $1 \leq x$ 이다.
- (2) $y \leq x$ 일 때 그리고 이때에만 $y < x^+$ 이다.
- (3) $x < y$ 일 때 그리고 이때에만 $x^+ \leq y$ 이다.
- (4) 모든 원소 $x \in \mathbb{N}$ 에 대하여 $x < x^+$ 이다.

증 명 (1) 원소 $x \in \mathbb{N}$ 에 대하여 $x < 1$ 이라고 가정하자.

이 때, $1 = x + u$ 인 원소 $u \in \mathbb{N}$ 가 존재하고, 여기서 정리 2에 의하여 $u = 1$ 이거나 또는 $u = v^+$ 인 원소 $v \in \mathbb{N}$ 가 존재한다.

그런데, $u = 1$ 이면, $1 = x + u = x + 1 = x^+$ 로 되어 정의 1 (iii)에 모순되고, 또 $u = v^+$ 이면

$$1 = x + u = x + v^+ = (x + v)^+$$

로 되어 정의 1 (iii)에 모순된다.

따라서 모든 원소 $x \in \mathbb{N}$ 에 대하여 $1 \leq x$ 이다(정리 10 참조).

(2) 먼저 $y \leq x$ 이라고 하자. 이 때, $y = x$ 또는 $y < x$ 이다.

그런데 $y = x$ 이면, $x^+ = y^+ = y + 1$ 이므로 $y < x^+$ 이다.

그리고, $y < x$ 이면, $x = y + u$ 인 원소 $u \in \mathbb{N}$ 가 존재하고 이때

$$x^+ = (y + u)^+ = y + u^+$$

이므로 $y < x^+$ 이다. 따라서 $y \leq x$ 이면, $y < x^+$ 이다.

역으로, $y < x^+$ 이라고 하자. 이 때, $x^+ = y + v$ 인 원소 $v \in \mathbb{N}$ 가 존재한다. 그런데, $v = 1$ 이면

$$x^+ = y + v = y + 1 = y^+$$

이므로 $y = x$ 이고, 또 $v \neq 1$ 이면 정리 2 에 의하여 $v = w^+$ 인 $w \in \mathbb{N}$ 가 존재하고 이때

$$x^+ = y + v = y + w^+ = (y + w)^+$$

이므로 $x = y + w$ 이고 따라서 $y < x$ 이다.

(3) 위의 (2) 와 정리 10 에 의하여 (3) 이 성립한다.

(4) 분명히 $x \leq x$ 이므로 (2) 에 의하여 $x < x^+$ 이다.

정리 12 (정수의 整列性) 집합 \mathbb{N} 의 부분집합 $S (\neq \emptyset)$ 에는 가장 작은 원소 l 이 존재한다. 즉, $\emptyset \subsetneq S \subseteq \mathbb{N}$ 일 때, 모든 $s \in S$ 에 대하여 $l \leq s$ 인 원소 $l \in S$ 이 존재한다.

증 명 집합 \mathbb{N} 의 부분집합 T 를 다음과 같이 정하자.

$$T = \{x \in \mathbb{N} \mid \text{모든 원소 } s \in S \text{ 에 대하여 } x \leq s\}$$

이 때, 정리 11 (1) 에 의하여 $1 \in T \neq \emptyset$ 이다. 또, 정리 11 (4) 에 의하여 모든 원소 $s \in S$ 에 대하여 $s < s^+$ 이므로 $s^+ \notin T$ 이다. 그러므로, $T \subsetneq \mathbb{N}$ 이므로 정의 1 (iv) 에 의하여 $l \in T$, $l^+ \notin T$ 인 원소 l 이 존재한다.

이제 l 이 S 에 속하는 가장 작은 원소임을 밝히기로 한다.

먼저 $l \in T$ 이므로, 모든 원소 $s \in S$ 에 대하여 $l \leq s$ 이다.

그런데, $l \notin S$ 이라고 가정하면, 모든 원소 $s \in S$ 에 대하여 $l < s$ 이므로, 정리 11 (3) 에 의하여 모든 $s \in S$ 에 대하여 $l^+ \leq s$ 이고 따라서 $l^+ \in T$ 로 되어 모순이 생긴다. 그러므로, $l \in S$ 이다.

정수의 표준분해 ($10000 \leq n \leq 10269$)

10000	$2^4 \cdot 5^4$	10030	$2 \cdot 5 \cdot 7 \cdot 59$	10060	$2^2 \cdot 5 \cdot 503$
10001	$73 \cdot 137$	10031	$7 \cdot 1433$	10061	10061
10002	$2 \cdot 3 \cdot 1667$	10032	$2^4 \cdot 3 \cdot 11 \cdot 19$	10062	$2 \cdot 3^3 \cdot 13 \cdot 43$
10003	$7 \cdot 1429$	10033	$79 \cdot 127$	10063	$29 \cdot 347$
10004	$2^2 \cdot 41 \cdot 61$	10034	$2 \cdot 29 \cdot 173$	10064	$2^4 \cdot 17 \cdot 37$
10005	$3 \cdot 5 \cdot 23 \cdot 29$	10035	$3^2 \cdot 5 \cdot 223$	10065	$3 \cdot 5 \cdot 11 \cdot 61$
10006	$2 \cdot 5003$	10036	$2^2 \cdot 13 \cdot 193$	10066	$2 \cdot 7 \cdot 719$
10007	10007	10037	10037	10067	10067
10008	$2^3 \cdot 3^2 \cdot 139$	10038	$2 \cdot 3 \cdot 7 \cdot 239$	10068	$2^2 \cdot 3 \cdot 839$
10009	10009	10039	10039	10069	10069
10010	$2 \cdot 5 \cdot 7 \cdot 11 \cdot 13$	10040	$2^3 \cdot 5 \cdot 251$	10070	$2 \cdot 5 \cdot 19 \cdot 53$
10011	$3 \cdot 47 \cdot 71$	10041	$3 \cdot 3347$	10071	$3^3 \cdot 373$
10012	$2^2 \cdot 2503$	10042	$2 \cdot 5021$	10072	$2^3 \cdot 1259$
10013	$17 \cdot 19 \cdot 31$	10043	$11^2 \cdot 83$	10073	$7 \cdot 1439$
10014	$2 \cdot 3 \cdot 1669$	10044	$2^2 \cdot 3^4 \cdot 31$	10074	$2 \cdot 3 \cdot 23 \cdot 73$
10015	$5 \cdot 2003$	10045	$5 \cdot 7^2 \cdot 41$	10075	$5^2 \cdot 13 \cdot 31$
10016	$2^5 \cdot 313$	10046	$2 \cdot 5023$	10076	$2^2 \cdot 11 \cdot 229$
10017	$3^3 \cdot 7 \cdot 53$	10047	$3 \cdot 17 \cdot 197$	10077	$3 \cdot 3359$
10018	$2 \cdot 5009$	10048	$2^6 \cdot 157$	10078	$2 \cdot 5049$
10019	$43 \cdot 233$	10049	$13 \cdot 773$	10079	10079
10020	$2^2 \cdot 3 \cdot 5 \cdot 167$	10050	$2 \cdot 3 \cdot 5^2 \cdot 67$	10080	$2^5 \cdot 3^2 \cdot 5 \cdot 7$
10021	$11 \cdot 911$	10051	$19 \cdot 23^2$	10081	$17 \cdot 593$
10022	$2 \cdot 5011$	10052	$2^2 \cdot 7 \cdot 359$	10082	$2 \cdot 71^2$
10023	$3 \cdot 13 \cdot 257$	10053	$3^2 \cdot 1117$	10083	$3 \cdot 3361$
10024	$2^3 \cdot 7 \cdot 179$	10054	$2 \cdot 11 \cdot 457$	10084	$2^2 \cdot 2521$
10025	$5^2 \cdot 401$	10055	$5 \cdot 2011$	10085	$5 \cdot 2017$
10026	$2 \cdot 3^2 \cdot 557$	10056	$2^3 \cdot 3 \cdot 419$	10086	$2 \cdot 3 \cdot 41^2$
10027	$37 \cdot 271$	10057	$89 \cdot 113$	10087	$7 \cdot 11 \cdot 131$
10028	$2^2 \cdot 23 \cdot 109$	10058	$2 \cdot 47 \cdot 107$	10088	$2^3 \cdot 13 \cdot 97$
10029	$3 \cdot 3343$	10059	$3 \cdot 7 \cdot 479$	10089	$3^2 \cdot 19 \cdot 59$

정수의 표준분해 (2)

10090	$2 \cdot 5 \cdot 1009$	10120	$2^3 \cdot 5 \cdot 11 \cdot 23$	10150	$2 \cdot 5^2 \cdot 7 \cdot 29$
10091	10091	10121	$29 \cdot 349$	10151	10151
10092	$2^2 \cdot 3 \cdot 29^2$	10122	$2 \cdot 3 \cdot 7 \cdot 241$	10152	$2^3 \cdot 3^3 \cdot 47$
10093	10093	10123	$53 \cdot 191$	10153	$11 \cdot 13 \cdot 71$
10094	$2 \cdot 7^2 \cdot 103$	10124	$2^2 \cdot 2531$	10154	$2 \cdot 5077$
10095	$3 \cdot 5 \cdot 673$	10125	$3^4 \cdot 5^3$	10155	$3 \cdot 5 \cdot 677$
10096	$2^4 \cdot 631$	10126	$2^3 \cdot 61 \cdot 83$	10156	$2^2 \cdot 2539$
10097	$23 \cdot 439$	10127	$13 \cdot 19 \cdot 41$	10157	$7 \cdot 1451$
10098	$2 \cdot 3^3 \cdot 11 \cdot 17$	10128	$2^4 \cdot 3 \cdot 211$	10158	$2 \cdot 3 \cdot 1693$
10099	10099	10129	$7 \cdot 1447$	10159	10159
10100	$2^2 \cdot 5^2 \cdot 101$	10130	$2 \cdot 5 \cdot 1013$	10160	$2^4 \cdot 5 \cdot 127$
10101	$3 \cdot 7 \cdot 13 \cdot 37$	10131	$3 \cdot 11 \cdot 307$	10161	$3^2 \cdot 1129$
10102	$2 \cdot 5051$	10132	$2^2 \cdot 17 \cdot 149$	10162	$2 \cdot 5081$
10103	10103	10133	10133	10163	10163
10104	$2^3 \cdot 3 \cdot 421$	10134	$2 \cdot 3^2 \cdot 563$	10164	$2^2 \cdot 3 \cdot 7 \cdot 11^2$
10105	$5 \cdot 43 \cdot 47$	10135	$5 \cdot 2027$	10165	$5 \cdot 19 \cdot 107$
10106	$2 \cdot 31 \cdot 163$	10136	$2^3 \cdot 7 \cdot 181$	10166	$2 \cdot 13 \cdot 17 \cdot 23$
10107	$3^2 \cdot 1123$	10137	$3 \cdot 31 \cdot 109$	10167	$3 \cdot 3389$
10108	$2^2 \cdot 7 \cdot 19^2$	10138	$2 \cdot 37 \cdot 137$	10168	$2^3 \cdot 31 \cdot 41$
10109	$11 \cdot 919$	10139	10139	10169	10169
10110	$2 \cdot 3 \cdot 5 \cdot 337$	10140	$2^2 \cdot 3 \cdot 5 \cdot 13^2$	10170	$2 \cdot 3^2 \cdot 5 \cdot 113$
10111	10111	10141	10141	10171	$7 \cdot 1453$
10112	$2^7 \cdot 79$	10142	$2 \cdot 11 \cdot 461$	10172	$2^2 \cdot 2543$
10113	$3 \cdot 3371$	10143	$3^2 \cdot 7^2 \cdot 23$	10173	$3 \cdot 3391$
10114	$2 \cdot 13 \cdot 389$	10144	$2^5 \cdot 317$	10174	$2 \cdot 5087$
10115	$5 \cdot 7 \cdot 17^2$	10145	$5 \cdot 2029$	10175	$5^2 \cdot 11 \cdot 37$
10116	$2^2 \cdot 3^2 \cdot 281$	10146	$2 \cdot 3 \cdot 19 \cdot 89$	10176	$2^6 \cdot 3 \cdot 53$
10117	$67 \cdot 151$	10147	$73 \cdot 139$	10177	10177
10118	$2 \cdot 5059$	10148	$2^2 \cdot 43 \cdot 59$	10178	$2 \cdot 7 \cdot 727$
10119	$3 \cdot 3373$	10149	$3 \cdot 17 \cdot 199$	10179	$3^3 \cdot 13 \cdot 29$

정수의 표준분해 (3)

10180	$2^2 \cdot 5 \cdot 509$	10210	$2 \cdot 5 \cdot 1021$	10240	$2^{11} \cdot 5$
10181	10181	10211	10211	10241	$7^2 \cdot 11 \cdot 9$
10182	$2 \cdot 3 \cdot 1697$	10212	$2^2 \cdot 3 \cdot 23 \cdot 37$	10242	$2 \cdot 3^2 \cdot 569$
10183	$17 \cdot 599$	10213	$7 \cdot 1459$	10243	10243
10184	$2^3 \cdot 19 \cdot 67$	10214	$2 \cdot 5107$	10244	$2^2 \cdot 13 \cdot 197$
10185	$3 \cdot 5 \cdot 7 \cdot 97$	10215	$3^2 \cdot 5 \cdot 227$	10245	$3 \cdot 5 \cdot 683$
10186	$2 \cdot 11 \cdot 463$	10216	$2^3 \cdot 1277$	10246	$2 \cdot 47 \cdot 109$
10187	$61 \cdot 167$	10217	$17 \cdot 601$	10247	10247
10188	$2^2 \cdot 3^2 \cdot 283$	10218	$2 \cdot 3 \cdot 13 \cdot 131$	10248	$2^3 \cdot 3 \cdot 7 \cdot 61$
10189	$23 \cdot 443$	10219	$11 \cdot 929$	10249	$37 \cdot 277$
10190	$2 \cdot 5 \cdot 1019$	10220	$2^2 \cdot 5 \cdot 7 \cdot 73$	10250	$2 \cdot 5^3 \cdot 41$
10191	$3 \cdot 43 \cdot 79$	10221	$3 \cdot 3407$	10251	$3^2 \cdot 17 \cdot 67$
10192	$2^4 \cdot 7^2 \cdot 13$	10222	$2 \cdot 19 \cdot 269$	10252	$2^2 \cdot 11 \cdot 233$
10193	10193	10223	10223	10253	10253
10194	$2 \cdot 3 \cdot 1699$	10224	$2^4 \cdot 3^2 \cdot 71$	10254	$2 \cdot 3 \cdot 1709$
10195	$5 \cdot 2039$	10225	$5^2 \cdot 409$	10255	$5 \cdot 7 \cdot 293$
10196	$2^2 \cdot 2549$	10226	$2 \cdot 5113$	10256	$2^4 \cdot 641$
10197	$3^2 \cdot 11 \cdot 103$	10227	$3 \cdot 7 \cdot 487$	10257	$3 \cdot 13 \cdot 263$
10198	$2 \cdot 5099$	10228	$2^2 \cdot 2557$	10258	$2 \cdot 23 \cdot 223$
10199	$7 \cdot 31 \cdot 47$	10229	$53 \cdot 193$	10259	10259
10200	$2^3 \cdot 3 \cdot 5^2 \cdot 17$	10230	$2 \cdot 3 \cdot 5 \cdot 11 \cdot 31$	10260	$2^2 \cdot 3^3 \cdot 5 \cdot 19$
10201	101^2	10231	$13 \cdot 787$	10261	$31 \cdot 331$
10202	$2 \cdot 5101$	10232	$2^3 \cdot 1279$	10262	$2 \cdot 7 \cdot 733$
10203	$3 \cdot 19 \cdot 179$	10233	$3^3 \cdot 379$	10263	$3 \cdot 11 \cdot 311$
10204	$2^2 \cdot 2551$	10234	$2 \cdot 7 \cdot 17 \cdot 43$	10264	$2^3 \cdot 1283$
10205	$5 \cdot 13 \cdot 157$	10235	$5 \cdot 23 \cdot 89$	10265	$5 \cdot 2053$
10206	$2 \cdot 3^6 \cdot 7$	10236	$2^2 \cdot 3 \cdot 853$	10266	$2 \cdot 3 \cdot 29 \cdot 59$
10207	$59 \cdot 173$	10237	$29 \cdot 353$	10267	10267
10208	$2^5 \cdot 11 \cdot 29$	10238	$2 \cdot 5119$	10268	$2^2 \cdot 17 \cdot 151$
10209	$3 \cdot 41 \cdot 83$	10239	$3 \cdot 3413$	10269	$3^2 \cdot 7 \cdot 163$

Mersenne 素數 (2019 년 5 월 현재)

크기 순	素數 p	M_p 의 자리수	발견연도 및 발견자	크기 순	素數 p	M_p 의 자리수	발견연도 및 발견자
1	2	1		27	44497	13395	1979 Nelson 등
2	3	1		28	86243	25962	1982 Slowinski
3	5	2		29	110503	33265	1988 Colquitt, Welch
4	7	3		30	132049	39751	1983 Slowinski
5	13	4	1456 미상	31	216091	65050	1985 Slowinski
6	17	6	1588 Cataldi	32	756839	227832	1992 Slowinski, Gage
7	19	6	1588 Cataldi	33	859433	258716	1994 Slowinski, Gage
8	31	10	1772 Euler	34	1257787	378632	1996 Slowinski, Gage
9	61	19	1883 Pervushin	35	1398269	420921	1996 Armengaud 등
10	89	27	1911 Powers	36	2976221	895932	1997 Spence, Woltman
11	107	33	1914 Powers	37	3021377	909526	1998 Clarkson, Woltman, Kurowski 등
12	127	39	1876 Lucas	38	6972593	2098960	1999 Hairatwala, Woltman, Kurowski 등
13	521	157	1952 Robinson	39	13466917	4053946	2001 Cameron, Woltman, Kurowski 등
14	607	183	1952 Robinson	40	20996011	6320430	2003 Schafer
15	1279	386	1952 Robinson	41	24036583	7235733	2004 Findley, Woltman
16	2203	664	1952 Robinson	42	25964951	7816230	2005 Nowak, Woltman
17	2281	687	1952 Robinson	43	30402457	9152052	2005 Cooper, Boone
18	3217	969	1957 Riesel	44	32582657	9808358	2006 Cooper, Boone
19	4253	1281	1961 Hurwitz	45	37156667	11185272	2008 Elvenich, Woltman
20	4423	1332	1961 Hurwitz	46	42643801	12837064	2009 Strindmo, Woltman
21	9689	2917	1963 Gillies	47	43112609	12978189	2008 Smith, Woltman
22	9941	2993	1963 Gillies	48	57885161	17425170	2013 Cooper, Woltman
23	11213	3376	1963 Gilles	49	74207281	22338618	2016 Cooper, Woltman
24	19937	6002	1971 Tucker	50	77232917	23249425	2017 Pace, Woltman
25	21701	6533	1978 Noll, Nickel	51	82589933	24862048	2018 Laroche, Woltman
26	23209	6987	1979 Noll				

Fibonacci 수와 Lucas 수

여기서는 Fibonacci 수와 Lucas 수에 대하여 논하기로 한다.

정리 1 Fibonacci 수열 $\{f_n\}$ 에 대하여 다음이 성립한다 ($n \geq 1$).

- (1) $\binom{n}{1}f_1 + \binom{n}{2}f_2 + \binom{n}{3}f_3 + \cdots + \binom{n}{n}f_n = f_{2n}$
- (2) $-\binom{n}{1}f_1 + \binom{n}{2}f_2 - \binom{n}{3}f_3 + \cdots + (-1)^n \binom{n}{n}f_n = -f_n$

증 명 이제

$$\alpha = \frac{1+\sqrt{5}}{2}, \quad \beta = \frac{1-\sqrt{5}}{2}$$

이라고 하면, Binet 의 공식(정리 2.6.3) 에 의하여 다음이 성립한다.

$$f_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad (n \geq 1)$$

- (1) $\alpha^2 = \alpha + 1$, $\beta^2 = \beta + 1$ 이므로 다음이 성립한다,

$$\begin{aligned} & \binom{n}{1}f_1 + \binom{n}{2}f_2 + \binom{n}{3}f_3 + \cdots + \binom{n}{n}f_n \\ &= \binom{n}{1} \left(\frac{\alpha - \beta}{\alpha - \beta} \right) + \binom{n}{2} \left(\frac{\alpha^2 - \beta^2}{\alpha - \beta} \right) + \binom{n}{3} \left(\frac{\alpha^3 - \beta^3}{\alpha - \beta} \right) \\ & \quad + \cdots + \binom{n}{n} \left(\frac{\alpha^n - \beta^n}{\alpha - \beta} \right) \\ &= \frac{1}{\alpha - \beta} \left\{ \binom{n}{1} \alpha + \binom{n}{2} \alpha^2 + \binom{n}{3} \alpha^3 + \cdots + \binom{n}{n} \alpha^n \right\} \\ & \quad - \frac{1}{\alpha - \beta} \left\{ \binom{n}{1} \beta + \binom{n}{2} \beta^2 + \binom{n}{3} \beta^3 + \cdots + \binom{n}{n} \beta^n \right\} \\ &= \frac{\{-1 + (1 + \alpha)^n\} - \{-1 + (1 + \beta)^n\}}{\alpha - \beta} \\ &= \frac{(1 + \alpha)^n - (1 + \beta)^n}{\alpha - \beta} \\ &= \frac{(\alpha^2)^n - (\beta^2)^n}{\alpha - \beta} = \frac{\alpha^{2n} - \beta^{2n}}{\alpha - \beta} = f_{2n} \end{aligned}$$

(2) $\alpha + \beta = 1$ 이므로 $1 - \alpha = \beta$, $1 - \beta = \alpha$ 이고 따라서 다음이 성립한다.

$$\begin{aligned}
& - \binom{n}{1} f_1 + \binom{n}{2} f_2 - \binom{n}{3} f_3 + \cdots + (-1)^n \binom{n}{n} f_n \\
&= - \binom{n}{1} \left(\frac{\alpha - \beta}{\alpha - \beta} \right) + \binom{n}{2} \left(\frac{\alpha^2 - \beta^2}{\alpha - \beta} \right) - \binom{n}{3} \left(\frac{\alpha^3 - \beta^3}{\alpha - \beta} \right) \\
&\quad + \cdots + (-1)^n \binom{n}{n} \left(\frac{\alpha^n - \beta^n}{\alpha - \beta} \right) \\
&= \frac{1}{\alpha - \beta} \left\{ - \binom{n}{1} \alpha + \binom{n}{2} \alpha^2 - \binom{n}{3} \alpha^3 + \cdots + (-1)^n \binom{n}{n} \alpha^n \right\} \\
&\quad - \frac{1}{\alpha - \beta} \left\{ - \binom{n}{1} \beta + \binom{n}{2} \beta^2 - \binom{n}{3} \beta^3 + \cdots + (-1)^n \binom{n}{n} \beta^n \right\} \\
&= \frac{-\{-1 + (1 - \alpha)^n\} - \{-1 + (1 - \beta)^n\}}{\alpha - \beta} \\
&= \frac{-(1 - \alpha)^n - (1 - \beta)^n}{\alpha - \beta} = \frac{-\beta^n - \alpha^n}{\alpha - \beta} = -f_n
\end{aligned}$$

정리 2 Fibonacci 수열 $\{f_n\}$ 에 대하여 다음이 성립한다.

$$\lim_{n \rightarrow \infty} \frac{f_{n+1}}{f_n} = \frac{1 + \sqrt{5}}{2}$$

증 명 정리 2.6.6 에 의하여 다음이 성립한다,

$$f_n = \frac{1}{\sqrt{5}} \left(\frac{1 + \sqrt{5}}{2} \right)^n + \delta_n, \quad |\delta_n| < \frac{1}{2} \quad (n \geq 1)$$

따라서

$$\begin{aligned}
\frac{f_{n+1}}{f_n} &= \frac{\left(\frac{1 + \sqrt{5}}{2} \right)^{n+1} + \sqrt{5} \delta_{n+1}}{\left(\frac{1 + \sqrt{5}}{2} \right)^n + \sqrt{5} \delta_n} \\
&= \frac{\frac{1 + \sqrt{5}}{2} + \sqrt{5} \left(\frac{1 + \sqrt{5}}{2} \right)^{-n} \delta_{n+1}}{1 + \sqrt{5} \left(\frac{1 + \sqrt{5}}{2} \right)^{-n} \delta_n}
\end{aligned}$$

이므로 $\lim_{n \rightarrow \infty} \frac{f_{n+1}}{f_n} = \frac{1 + \sqrt{5}}{2}$ 이다.

정의 3 다음과 같이 정의된 양의 정수 l_n 을 **Lucas 수**(Lucas number)라고 한다.

$$(i) \quad l_1 = 1, \quad l_2 = 3$$

$$(ii) \quad l_{n+2} = l_n + l_{n+1} \quad (n \geq 1)$$

그리고, 이들 Lucas 수 l_n 으로 이루어진 무한수열 $\{l_n\}$ 을 **Lucas 수열**(Lucas sequence)라고 한다.

다음 정리는 비교적 쉽게 증명할 수 있다.

정리 4 Lucas 수열 $\{l_n\}$ 에 대하여 다음 등식이 성립한다.

- (1) $l_1 + l_2 + l_3 + \cdots + l_n = l_{n+2} - 3 \quad (n \geq 1)$
- (2) $l_1 + l_3 + l_5 + \cdots + l_{2n-1} = l_{2n} - 2 \quad (n \geq 1)$
- (3) $l_2 + l_4 + l_6 + \cdots + l_{2n} = l_{2n+1} - 1 \quad (n \geq 1)$
- (4) $l_n^2 = l_{n+1}l_{n-1} + 5(-1)^n \quad (n \geq 2)$
- (5) $l_1^2 + l_2^2 + l_3^2 + \cdots + l_n^2 = l_n l_{n+1} - 2 \quad (n \geq 1)$
- (6) $l_{n+1}^2 - l_n^2 = l_{n-1}l_{n+2} \quad (n \geq 2)$

정리 5 Lucas 수열 $\{l_n\}$ 에 대하여 다음이 성립한다.

$$l_n < \left(\frac{7}{4}\right)^n \quad (n \geq 1)$$

증명 먼저 $n = 1, n = 2$ 일 때,

$$l_1 = 1 < \frac{7}{4} = \left(\frac{7}{4}\right)^1,$$

$$l_2 = 3 = \frac{48}{16} < \frac{49}{16} = \left(\frac{7}{4}\right)^2$$

이므로 이 경우에 정리의 부등식이 성립한다.

다음에 $k \geq 3$ 일 때, n 이 $1, 2, \dots, k$ 일 때, 정리의 부등식이 성립한다고 가정하자.

이 때,

$$\begin{aligned}
l_{k+1} &= l_k + l_{k-1} < \left(\frac{7}{4}\right)^k + \left(\frac{7}{4}\right)^{k-1} \\
&= \left(\frac{7}{4}\right)^{k-1} \left(\frac{7}{4} + 1\right) \\
&= \left(\frac{7}{4}\right)^{k-1} \frac{11}{4} \\
&< \left(\frac{7}{4}\right)^{k-1} \left(\frac{7}{4}\right)^2 = \left(\frac{7}{4}\right)^{k+1}
\end{aligned}$$

이므로 $n = k+1$ 일 때에도 정리의 부등식이 성립한다.

그러므로 모든 양의 정수 n 에 대하여 정리의 부등식이 성립한다.

정리 6 Lucas 수열 l_n 에 대하여 다음 등식이 성립한다.

- (1) $l_n = f_{n+1} + f_{n-1} \quad (n \geq 2)$
- (2) $l_n = f_n + 2f_{n-1} \quad (n \geq 2)$

증 명 먼저 $n = 2$ 일 때,

$$\begin{aligned}
l_2 &= 3 = 2 + 1 = f_3 + f_1, \\
l_2 &= 3 = 1 + 2 = f_1 + 2f_1
\end{aligned}$$

이므로 이 경우에 두 등식이 성립한다.

다음에 $k \geq 2$ 인 경우에 n 이 $2, \dots, k$ 일 때 두 등식이 성립한다고 가정하자. 이 때,

$$\begin{aligned}
l_{k+1} &= l_k + l_{k-1} = (f_{k+1} + f_{k-1}) + (f_k + f_{k-2}) \\
&= (f_{k+1} + f_k) + (f_{k-1} + f_{k-2}) \\
&= f_{k+2} + f_k = f_{(k+1)+1} + f_{(k+1)-1}, \\
l_{k+1} &= l_k + l_{k-1} = (f_k + 2f_{k-1}) + (f_{k-1} + 2f_{k-2}) \\
&= (f_k + f_{k-1}) + 2(f_{k-1} + f_{k-2}) \\
&= f_{k+1} + 2f_k = f_{k+1} + 2f_{(k+1)-1}
\end{aligned}$$

이므로 두 등식은 $n = k+1$ 일 때에도 성립한다.

그러므로 모든 정수 n (≥ 2)에 대하여 두 등식이 성립한다.

정리 7 Fibonacci 수열 $\{f_n\}$ 과 Lucas 수열 $\{l_n\}$ 사이에는 다음과 같은 관계식이 성립한다.

- (1) $l_n = f_{n+2} - f_{n-2}$ ($n \geq 3$)
- (2) $l_{n+1} + l_{n-1} = 5f_n$ ($n \geq 2$)
- (3) $f_n l_n = f_{2n}$ ($n \geq 1$)
- (4) $l_n^2 = f_n^2 + 4f_{n+1}f_{n-1}$ ($n \geq 2$)
- (5) $2f_{m+n} = f_m l_n + l_m f_n$ ($m, n \geq 1$)
- (6) $(f_n, l_n) = 1$ 또는 $(f_n, l_n) = 2$ ($n \geq 1$)

증명 (1), (2) 정리 6 에 의하여 다음이 성립한다.

$$l_n = f_{n+1} + f_{n-1} \quad (n \geq 2)$$

이 등식을 이용하여 등식 (1), (2) 를 증명한다.

(3) 정리 6 과 정리 2.6.1 에 의하여 다음 두 등식이 성립한다.

$$l_n = f_{n+1} + f_{n-1} \quad (n \geq 2)$$

$$f_{m+n} = f_m f_{n+1} + f_{m-1} f_n \quad (m, n \geq 2)$$

이 두 등식을 이용하여 등식 (3) 을 증명한다.

(4) 정리 6 에 의하여 다음이 성립한다.

$$l_n = f_{n+1} + f_{n-1}, \quad l_n = f_n + 2f_{n-1} \quad (n \geq 2)$$

이 두 등식을 이용하여 등식 (3)을 증명한다.

(5) 정리 2.6.1 에 의하여 다음 등식이 성립한다.

$$f_{m+n} = f_m f_{n+1} + f_{m-1} f_n \quad (m, n \geq 2)$$

$$f_{m+n} = f_n f_{m+1} + f_{n-1} f_m \quad (m, n \geq 2)$$

이 두 등식을 이용하여 등식 (5) 를 증명한다.

(6) 이제 $d = (f_n, l_n)$ 이라고 하자. 이 때, $d | f_n$, $d | l_n$ 이므로

$d | (l_n - f_n)$ 이고 또 정리 6 에 의하여

$$l_n = f_n + 2f_{n-1} \quad (n \geq 2)$$

이므로 $d | 2f_{n-1}$ 이다. 그런데, 정리 2.6.2 에 의하여 $(f_n, f_{n-1}) = 1$ 이다.

따라서 $d | 2$ 이므로, $d = 1$ 또는 $d = 2$ 이다.

정리 8 Lucas 수열 $\{l_n\}$ 에 대하여 다음 등식이 성립한다.

$$l_n = \left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1-\sqrt{5}}{2}\right)^n \quad (n \geq 1)$$

증 명 이제

$$\alpha = \frac{1+\sqrt{5}}{2}, \quad \beta = \frac{1-\sqrt{5}}{2}$$

이라고 하면, $\alpha\beta = -1$ 이고 Fibonacci 수에 대한 Binet 의 공식에 의하여

$$f_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \text{ 이다. 그리고 정리 6 에 의하여}$$

$$l_n = f_{n+1} + f_{n-1} \quad (n \geq 2)$$

이므로 다음이 성립한다.

$$\begin{aligned} l_n &= f_{n+1} + f_{n-1} \\ &= \frac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta} + \frac{\alpha^{n-1} - \beta^{n-1}}{\alpha - \beta} \\ &= \frac{\alpha^{n+1} + \alpha^{n-1}}{\alpha - \beta} + \frac{-\beta^{n+1} - \beta^{n-1}}{\alpha - \beta} \\ &= \frac{\alpha^{n-1}(\alpha^2 + 1)}{\alpha - \beta} + \frac{-\beta^{n-1}(\beta^2 + 1)}{\alpha - \beta} \\ &= \frac{\alpha^{n-1}(\alpha^2 - \alpha\beta)}{\alpha - \beta} + \frac{-\beta^{n-1}(\beta^2 - \alpha\beta)}{\alpha - \beta} \\ &= \frac{\alpha^{n-1}\alpha(\alpha - \beta)}{\alpha - \beta} + \frac{-\beta^{n-1}\beta(\beta - \alpha)}{\alpha - \beta} = \alpha^n + \beta^n \end{aligned}$$

위의 정리를 이용하여 다음 두 정리를 증명할 수 있다.

정리 9 Fibonacci 수열 $\{f_n\}$ 과 Lucas 수열 $\{l_n\}$ 사이에는 다음과 같은 관계식이 성립한다.

$$(1) \quad l_n^2 = l_{2n} + 2(-1)^n \quad (n \geq 1)$$

$$(2) \quad l_n l_{n+1} - l_{2n+1} = (-1)^n \quad (n \geq 1)$$

$$(3) \quad l_n^2 - l_{n-1} l_{n+1} = 5(-1)^n \quad (n \geq 2)$$

$$(4) \quad l_{2n} + 7(-1)^n = l_{n-2} l_{n+2} \quad (n \geq 3)$$

정리 10 Lucas 수열 $\{l_n\}$ 에 대하여 다음 등식이 성립한다.

$$(1) \quad l_n^2 - 5f_n^2 = 4(-1)^n \quad (n \geq 1)$$

$$(2) \quad l_{2n+1} = 5f_n f_{n+1} + (-1)^n \quad (n \geq 1)$$

$$(3) \quad l_n^2 - f_n^2 = 4f_{n-1}f_{n+1} \quad (n \geq 2)$$

$$(4) \quad l_m l_n + 5f_m f_n = 2l_{m+n} \quad (m, n \geq 1)$$

素數와 원시근

(p 는 素數, g 는 p 의 最小 원시근)

p	g	p	g	p	g	p	g	p	g	p	g
2	1	113	3	277	5	457	13	643	11	839	11
3	2	127	3	281	3	461	2	647	5	853	2
5	2	131	2	283	3	463	3	653	2	857	3
7	3	137	3	293	2	467	2	659	2	859	2
11	2	139	2	307	5	479	13	661	2	863	5
13	2	149	2	311	17	487	3	673	5	877	2
17	3	151	6	313	10	491	2	677	2	881	3
19	2	157	5	317	2	499	7	683	5	883	2
23	5	163	2	331	3	503	5	691	3	887	5
29	2	167	5	337	10	509	2	701	2	907	2
31	3	173	2	347	2	521	3	709	2	911	17
37	2	179	2	349	2	523	2	719	11	919	7
41	6	181	2	353	3	541	2	727	5	929	3
43	3	191	19	359	7	547	2	733	6	937	5
47	5	193	5	367	6	557	2	739	3	941	2
53	2	197	2	373	2	563	2	743	5	947	2
59	2	199	3	379	2	569	3	751	3	953	3
61	2	211	2	383	5	571	3	757	2	967	5
67	2	223	3	389	2	577	5	761	6	971	6
71	7	227	2	397	5	587	2	769	11	977	3
73	5	229	6	401	3	593	3	773	2	983	5
79	3	233	3	409	21	599	7	787	2	991	6
83	2	239	7	419	2	601	7	797	2	997	7
89	3	241	7	421	2	607	3	809	3		
97	5	251	6	431	7	613	2	811	3		
101	2	257	3	433	5	617	3	821	2		
103	5	263	5	439	15	619	2	823	3		
107	2	269	2	443	2	631	3	827	2		
109	6	271	6	449	3	641	3	829	2		

[illegible]

전자 서명

공개 열쇠 암호체계는 문서를 인증(authentication)하는 데에도 이용된다. 각 문서에는 그 내용에 근거한 독특한 전자 서명(디지털 서명, digital signature)이 지정된다. 각 문서에 첨부되는 서명은 비밀 열쇠를 이용하여 암호화되며 문서를 수신한 사람은 공개 열쇠를 이용하여 서명이 유효하다는 것을 검증할 수 있다. 이 절에서는 몇 가지 전자 서명에 대하여 논한다(§ 3.3, § 3.4 참조).

[1] RSA 암호체계를 이용한 전자 서명

(1) 서명자 U 는 상당히 큰 서로 다른 素數 p, q 를 택하여 $m = pq$ 의 값을 구하고 m 의 값을 공개하지만 p, q 의 값을 공개하지 않는다.

(2) 서명자 U 는 $\varphi(m) = (p-1)(q-1)$ 의 값을 구한 다음에

$$(e, \varphi(m)) = 1, \quad 1 \leq e < \varphi(m)$$

인 정수 e 를 택하여

$$ed \equiv 1 \pmod{\varphi(m)}, \quad 1 \leq d < \varphi(m)$$

인 정수 d 를 구하고 e 의 값을 공개하지만 d 의 값을 공개하지 않는다.

(3) 서명자 U 는 서명할 평문을 $1 \leq a < m$ 인 정수 a 로 나타낸다.

(4) 서명자 U 는 RSA 암호체계 프로토콜에 따라 A 에게 평문 a 를 전송한다(§ 3.3 참조). 그리고 U 는 자신의 비밀 열쇠 d 를 이용하여

$$s \equiv a^d \pmod{m}, \quad 1 \leq s < m$$

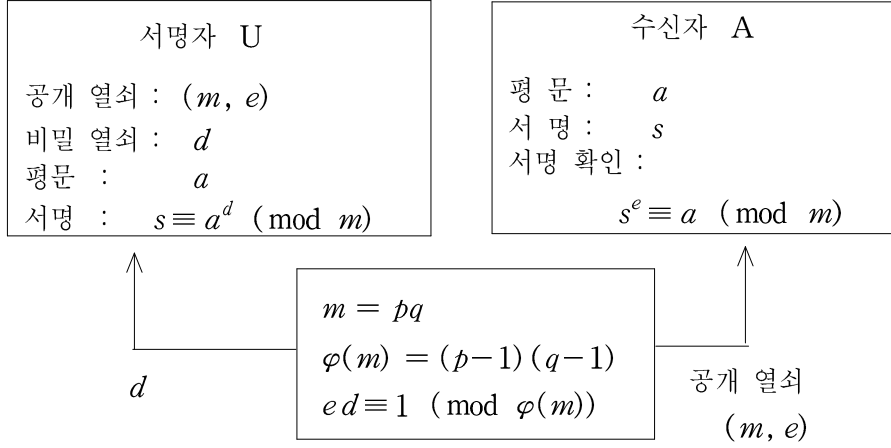
를 계산하여 서명 s 를 A 에게 전송한다.

(5) 수신자 A 는 U 로부터 수신한 평문 a , 서명 s 와 공개 열쇠 (m, e) 를 이용하여, 합동식

$$s^e \equiv a \pmod{m}$$

가 성립하는지를 확인하여 s 가 유효한 서명인지를 검증한다.

여기서 p, q, m, e, d, s 는 서명자 U 에 따라 달라진다. 이러한 의미에서 이들 정수를 각각 $p_U, q_U, m_U, e_U, d_U, s_U$ 로 나타내기도 한다.



앞의 단계 (5)에서

$$s \equiv a^d \pmod{m}, \quad ed \equiv 1 \pmod{\varphi(m)}$$

임을 이용하여 정리 3.3.1의 증명과 마찬가지로 합동식

$$s^e \equiv (a^d)^e \equiv a^{ed} \equiv a \pmod{m}$$

가 성립함을 밝힐 수 있다.

보기 1 서로 다른 두 素數 $p = 11, q = 17$ 에 대하여 $m = pq = 187$ 이라고 하면, $\varphi(m) = (p-1)(q-1) = 10 \cdot 16 = 160$ 이다.

이제 $e = 23$ 일 때, $(23, 160) = 1$ 이고

$$ed \equiv 1 \pmod{\varphi(m)}, \quad 1 \leq d < \varphi(m)$$

인 정수 d 를 구할 수 있다. 실제로,

$$160 \cdot (-1) + 23 \cdot 7 = 1,$$

$$23 \cdot 7 \equiv 1 \pmod{160}$$

이므로 $d = 7$ 이다.

그리고, $a = 5$ 일 때, 다음이 성립한다.

$$s \equiv a^d \equiv 5^7 \equiv 104 \pmod{187},$$

$$s^e \equiv 104^{23} \equiv 5 \equiv a \pmod{187}$$

$$\begin{array}{r|rr|r} 6 & 160 & 23 & 1 \\ & 138 & 22 & \\ 22 & \hline & 22 & 1 & \\ & 22 & & \\ & \hline & 0 & & \end{array}$$

6	1		
1	0	1	-1
0	1	-6	7

[2] ElGamal 암호체계를 이용한 전자 서명

(1) 서명자 U 는 상당히 큰 素數 p 와 범 p 에 관한 원시근 g ($2 \leq g < p$)를 택하고, $1 \leq r < p$ 인 정수 r 를 임의로(randomly) 택하여

$$d \equiv g^r \pmod{p}, \quad 1 \leq d < p$$

인 정수 d 의 값을 구하여 p, g, d 는 공개하지만 r 는 공개하지 않는다.

즉, 사용자 U 의 공개 열쇠는 p, g, d 이고 비밀 열쇠는 r 이다.

(2) 서명자 U 는 평문을 $1 \leq a < p$ 인 정수 a 로 나타낸다.

(3) 서명자 U 는 ElGamal 암호체계 프로토콜에 따라 수신자 A 에게 a 를 전송한다.

(4) 서명자 U 는

$$(k, p-1) = 1, \quad 1 \leq k < p-1$$

인 정수 k 를 임의로 택하여

$$k k^{-1} \equiv 1 \pmod{p-1}, \quad 1 \leq k^{-1} < p-1$$

인 정수 k^{-1} 를 구하고 또

$$\begin{aligned} c &\equiv g^k \pmod{p}, & 1 \leq c < p \\ s &\equiv (a - rc) k^{-1} \pmod{p-1}, & 1 \leq s < p-1 \end{aligned}$$

인 정수 c 와 s 를 계산한다.

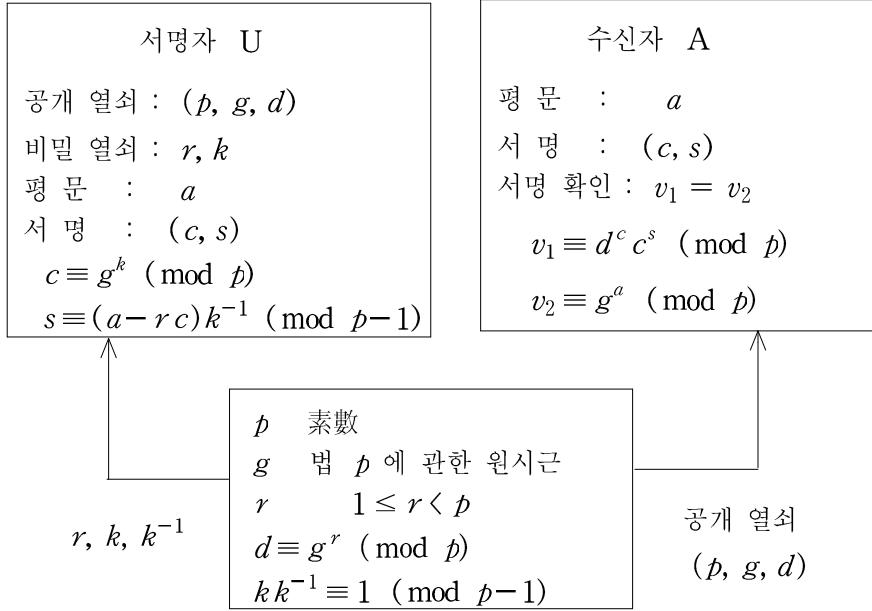
(5) 서명자 U 는 서명 (c, s) 를 A 에게 전송한다.

(6) 수신자 A 는 U 로부터 수신한 평문 a 와 서명 (c, s) 그리고 공개 열쇠 p, g, d 를 이용하여

$$\begin{aligned} v_1 &\equiv d^c c^s \pmod{p}, & 1 \leq v_1 < p \\ v_2 &\equiv g^a \pmod{p}, & 1 \leq v_2 < p \end{aligned}$$

인 정수 v_1, v_2 를 구하고 $v_1 = v_2$ 임을 확인하여 서명이 유효함을 검증한다.

여기서 p, g, k, k^{-1}, c, s 는 서명자 U 에 따라 달라진다. 이러한 의미에서 이들 정수를 각각 $p_U, g_U, k_U, k_U^{-1}, c_U, s_U$ 로 나타내기도 한다.



앞의 단계 (4) 에서, $(k, p-1) = 1$ 이므로

$$kk^{-1} \equiv 1 \pmod{p-1}, \quad 1 \leq k^{-1} < p-1$$

인 정수 k^{-1} 가 존재한다(정리 1.3.6).

단계 (5) 에서 서명 (c, s) 는 임의로 택한 정수 k 의 값에 따라 달라진다.

그리고, 단계 (6) 에서

$$c \equiv g^k \pmod{p}, \quad kk^{-1} \equiv 1 \pmod{p-1}$$

이고 또 $g^{p-1} \equiv 1 \pmod{p}$ 이므로 다음이 성립한다.

$$c^{k^{-1}} \equiv g^{kk^{-1}} \equiv g \pmod{p}$$

또한, $d \equiv g^r \pmod{p}$, $s \equiv (a - rc)k^{-1} \pmod{p-1}$ 이므로

$$\begin{aligned} v_1 &\equiv d^c c^s \equiv g^{rc} (c^{k^{-1}})^{a-rc} \\ &\equiv g^{rc} g^{a-rc} \equiv g^a \equiv v_2 \pmod{p} \end{aligned}$$

이므로 $v_1 = v_2$ 이다.

합동식

$$v_1 \equiv v_2 \pmod{p} \quad \text{즉} \quad d^c c^s \equiv g^a \pmod{p}$$

를 만족시키는 두 정수 c, s 를 결정하는 문제는 상당히 어려우므로, 이 서명 방법은 안전하다고 말할 수 있다.

실제로, $d \equiv g^r \pmod{p}$ 이므로

$$c^s \equiv g^a d^{-c} \equiv g^a g^{-rc} \equiv g^{a-rc} \pmod{p}$$

이고 따라서 c 의 값이 정해지면 이에 따라 위의 합동식을 만족시키는 정수 s 를 구해야 하는데 이것은 이산로그 문제이다. 한편, 합동식

$$d^c c^s \equiv g^a \pmod{p}$$

에서 s 의 값이 정해지면, 이에 따라 이 합동식을 만족시키는 정수 c 를 구하여야 하는데 이것은 엄밀한 의미의 이산로그 문제는 아니지만 흔히 사용하는 방법으로는 풀 수 없다.

보기 2 素數 $p = 16563$ 에 대하여 $g = 2$ 는 법 p 에 관한 원시근이다.

이제 $r = 3457$ 에 대하여

$$d \equiv g^r \pmod{p}, \quad 1 \leq d < p$$

이라고 하면 $d \equiv g^r \equiv 2^{3457} \equiv 12758 \pmod{p}$ 이다. 그리고

$$(k, p-1) = 1, \quad 1 \leq k < p-1$$

인 정수 k 로서 $k = 7841$ 을 택하고 유클리드의 알고리즘을 이용하여

$$k k^{-1} \equiv 1 \pmod{p-1}, \quad 1 \leq k^{-1} < p-1$$

인 정수 k^{-1} 를 구하면 $k^{-1} = 15101$ 이다.

그리고, $a = 2019$ 일 때, 다음이 성립한다.

$$c \equiv g^k \equiv 2^{7841} \equiv 7037 \pmod{p}$$

$$s \equiv (a - rc) k^{-1} \equiv (2019 - 3457 \cdot 7037)^{15101} \equiv 13714 \pmod{p-1}$$

$$d^c c^s \equiv 12758^{7037} \cdot 7037^{13714} \equiv 15057 \pmod{p}$$

$$g^a \equiv 2^{2019} \equiv 15057 \pmod{p}$$

선형점화수열

Gauss 의 정리에 의하면, 실수 또는 복소수를 계수로 가지는 n 차 방정식은 복소수체 \mathbb{C} 안에서 중복을 허락하여 n 개의 근을 가진다. 일반적인, 삼차 방정식과 사차방정식의 근은 각각 Cardano 의 정리와 Ferrari 의 정리를 이용하여 구할 수 있다([1]의 § 4.6 참조). 그러나, 5 차 이상의 방정식에 대한 근의 공식은 없다.

간단한 삼차다항식, 사차다항식은 조립제법을 이용하여 인수분해할 수 있다. 정리 4.4.6 과 마찬가지로 방법으로 다음 정리를 증명할 수 있다.

정리 1 실수체 \mathbb{R} 또는 복소수체 \mathbb{C} 에서의 무한수열 $\{a_t\}$ 가 다음과 같은 3 차의 동차 선형점화식을 만족시키는 동차 선형점화수열이라고 하자.

$$a_{t+3} = c_0 a_t + c_1 a_{t+1} + c_2 a_{t+2} \quad (t = 0, 1, 2, \dots)$$

이 때, $\{a_t\}$ 의 고유방정식

$$x^3 - c_2 x^2 - c_1 x - c_0 = 0$$

이 복소수체 \mathbb{C} 안에서 세 근 α, β, γ 를 가지면 $\{a_t\}$ 는 a_0, a_1, a_2 의 값에 따라 다음과 같이 결정된다.

(1) α, β, γ 가 서로 다른 경우

$$a_t = A\alpha^t + B\beta^t + C\gamma^t \quad (t = 0, 1, 2, \dots)$$

(2) $\alpha \neq \beta, \alpha \neq \gamma, \beta = \gamma$ 인 경우

$$a_t = A\alpha^t + (B + Ct)\beta^t \quad (t = 0, 1, 2, \dots)$$

(3) $\alpha = \beta = \gamma$ 인 경우

$$a_t = (A + Bt + Ct^2)\alpha^t \quad (t = 0, 1, 2, \dots)$$

보기 1 실수체 \mathbb{R} 에서 다음과 같이 정의된 동차 선형점화수열 $\{a_t\}$ 를 생각해 보자.

$$(i) \quad a_0 = 12, \quad a_1 = 18, \quad a_2 = 24$$

$$(ii) \quad a_{t+3} = 16a_t + 12a_{t+1} \quad (t = 0, 1, 2, \dots)$$

먼저 $\{a_t\}$ 의 고유다항식은 다음과 같다.

$$\begin{aligned} f(x) &= x^3 - 12x - 16 \\ &= (x-4)(x^2 + 4x + 4) \\ &= (x-4)(x+2)^2 \end{aligned} \quad \begin{array}{c|cccc} 4 & 1 & 0 & -12 & -16 \\ & & 4 & 16 & 16 \\ \hline & 1 & 4 & 4 & 0 \end{array}$$

따라서 고유방정식 $f(x) = 0$ 의 근은 $x = 4, x = -2$ (이중근) 이므로

$$a_t = A4^t + (B + Ct)(-2)^t \quad (t = 0, 1, 2, \dots)$$

으로 놓을 수 있다. 그런데, $a_0 = 12, a_1 = 18, a_2 = 24$ 이므로

$$A + B = 12$$

$$4A - 2B - 2C = 18$$

$$16A + 4B + 8C = 24$$

이고 따라서 $A = 4, B = 8, C = -9$ 이다.

그러므로 다음이 성립한다.

$$a_t = 4^{t+1} + (8 - 9t)(-2)^t \quad (t = 0, 1, 2, \dots)$$

보기 2 실수체 \mathbb{R} 에서 다음과 같이 정의된 동차 선형점화수열 $\{a_t\}$ 를 생각해 보자.

$$(i) \quad a_0 = 1, \quad a_1 = 0, \quad a_2 = 4$$

$$(ii) \quad a_{t+3} = 8a_t - 12a_{t+1} + 6a_{t+2} \quad (t = 0, 1, 2, \dots)$$

먼저 $\{a_t\}$ 의 고유다항식은 다음과 같다.

$$\begin{aligned} f(x) &= x^3 - 6x^2 + 12x - 8 \\ &= (x-2)(x^2 - 4x + 4) \\ &= (x-2)^3 \end{aligned} \quad \begin{array}{c|cccc} 2 & 1 & -6 & 12 & -8 \\ & & 2 & -8 & 8 \\ \hline & 1 & -4 & 4 & 0 \end{array}$$

따라서 $\{a_t\}$ 의 고유방정식 $f(x) = 0$ 의 근은 $x = 2$ (삼중근) 뿐이므로

$$a_t = (A + Bt + Ct^2)2^t \quad (t = 0, 1, 2, \dots)$$

으로 놓을 수 있다. 그런데, $a_0 = 1$, $a_1 = 0$, $a_2 = 4$ 이므로

$$\begin{aligned} A &= 0, \\ A + B + C &= 0, \\ A + 2B + 4C &= 1 \end{aligned}$$

이고 따라서 $A = 1$, $B = -1$, $C = 1$ 이므로 다음이 성립한다,

$$a_t = (1 - 2t + t^2)2^t \quad (t = 0, 1, 2, \dots)$$

보기 3 실수체 \mathbb{R} 에서 다음과 같이 정의된 동차 선형점화수열 $\{a_t\}$ 를 생각해 보자.

$$(i) \quad a_0 = 1, \quad a_1 = 0, \quad a_2 = 4$$

$$(ii) \quad a_{t+3} = 8a_t - 12a_{t+1} + 6a_{t+2} \quad (t = 0, 1, 2, \dots)$$

먼저 $\{a_t\}$ 의 고유다항식은 다음과 같다.

$$\begin{aligned} f(x) &= x^3 - 6x^2 + 12x - 8 \\ &= (x - 2)^3 \end{aligned}$$

$$\begin{array}{c|cccc} 2 & 1 & -6 & 12 & -8 \\ & & 2 & -8 & 8 \\ \hline & 1 & -4 & 4 & 0 \end{array}$$

따라서 $\{a_t\}$ 의 고유방정식 $f(x) = 0$ 의

근은 $x = 2$ (삼중근) 뿐이므로

$$a_t = (C_1 + C_2t + C_3t^2)2^t \quad (t = 0, 1, 2, \dots)$$

으로 놓을 수 있다. 그런데, $a_0 = 1$, $a_1 = 0$, $a_2 = 4$ 이므로

$$\begin{aligned} C_1 &= 0 \\ 2(C_1 + C_2 + C_3) &= 0 \\ 4(C_1 + 2C_2 + 4C_3) &= 4 \end{aligned}$$

이고 따라서 $C_1 = 1$, $C_2 = -1$, $C_3 = 1$ 이므로 다음이 성립한다.

$$a_t = (1 - 2t + t^2)2^t \quad (t = 0, 1, 2, \dots)$$

보기 4 실수체 \mathbb{R} 에서 다음과 같이 정의된 동차 선형점화수열 $\{a_t\}$ 를 생각해 보자.

$$(i) \quad a_0 = 12, \quad a_1 = 18, \quad a_2 = 24$$

$$(ii) \quad a_{t+3} = 16 a_t + 12 a_{t+1} \quad (t = 0, 1, 2, \dots)$$

먼저 $\{a_t\}$ 의 고유다항식은 다음과 같다.

$$\begin{aligned} f(x) &= x^3 - 12x - 16 \\ &= (x-4)(x+2)^2 \end{aligned} \quad \begin{array}{c|cccc} 4 & 1 & 0 & -12 & -16 \\ & & 4 & 16 & 16 \\ \hline & 1 & 4 & 4 & 0 \end{array}$$

따라서 고유방정식 $f(x) = 0$ 의 근은

$$x = 4, \quad x = -2 \text{ (이중근)}$$

이므로 a_t 는 다음과 같은 꼴로 나타내어진다.

$$a_t = A 4^t + (B_1 + B_2 t) (-2)^t \quad (t = 0, 1, 2, \dots)$$

그런데, $a_0 = 12, \quad a_1 = 18, \quad a_2 = 24$ 이므로

$$A + B_1 = 12$$

$$4A - 2B_1 - 2B_2 = 18$$

$$16A + 4B_1 + 8B_2 = 24$$

이고 따라서 $A = 4, \quad B_1 = 8, \quad B_2 = -9$ 이다.

그러므로 $\{a_t\}$ 의 항은 다음과 같다.

$$a_t = 4^{t+1} + (8 - 9t) (-2)^t \quad (t = 0, 1, 2, \dots)$$

일반적으로 다음 정리가 성립한다.

이 정리의 증명은 생략하기로 한다.

정리 2 실수체 \mathbb{R} 또는 복소수체 \mathbb{C} 에서의 무한수열 $\{a_t\}$ 가 동차 선형 점화식

$$a_{t+n} = c_0 a_t + c_1 a_{t+1} + \cdots + c_{n-1} a_{t+n-1} \quad (t = 0, 1, 2, \dots)$$

에 의하여 정의된 동차 선형 점화수열일 때, 고유다항식

$$f(x) = x^n - c_{n-1}x^{n-1} - \cdots - c_1x - c_0$$

는 복소수체 \mathbb{C} 안에서 다음과 같은 꼴로 인수분해된다.

$$f(x) = (x - a_1)^{e_1} (x - a_2)^{e_2} \cdots (x - a_r)^{e_r} \quad (e_i \geq 1)$$

이 때, $\{a_t\}$ 는 다음과 같은 꼴로 나타내어진다.

$$\begin{aligned} a_t = & (A_1 + A_2 t + A_3 t^2 + \cdots + A_{e_1} t^{e_1-1}) a_1^t \\ & + (B_1 + B_2 t + B_3 t^2 + \cdots + B_{e_2} t^{e_2-1}) a_2^t \\ & \vdots \\ & + (C_1 + C_2 t + C_3 t^2 + \cdots + C_{e_r} t^{e_r-1}) a_r^t \end{aligned}$$

여기서

$$A_1, A_2, \dots, A_{e_1}, B_1, B_2, \dots, B_{e_2}, \dots, C_1, C_2, \dots, C_{e_r}$$

는 a_0, a_1, \dots, a_{n-1} 의 값에 따라 결정되는 실수 또는 복소수이다.

형식적 멱급수의 전개

음이 아닌 정수 r 에 대하여 x_1, x_2, \dots, x_n 에 관한 일차방정식

$$x_1 + x_2 + \dots + x_n = r$$

의 해 중에서

$$x_1 = e_1, x_2 = e_2, \dots, x_n = e_n \quad (e_1, e_2, \dots, e_n \text{은 음이 아닌 정수})$$

와 같은 꼴의 해 전체의 개수는 ${}_n H_r = \binom{n+r-1}{r}$ 이다(보기 5.4.7).

형식적 멱급수 $\sum_{t=0}^{\infty} x^t = 1 + x + x^2 + x^3 + \dots$ 에 대하여 $(\sum_{t=0}^{\infty} x^t)^n$ 을 전개할 때, n 개의 인수

$$\sum_{t=0}^{\infty} x^t, \sum_{t=0}^{\infty} x^t, \dots, \sum_{t=0}^{\infty} x^t$$

에서 각각 $x^{e_1}, x^{e_2}, \dots, x^{e_n}$ 를 택하여 곱한 곱은

$$x^{e_1} x^{e_2} \dots x^{e_n} = x^{e_1 + e_2 + \dots + e_n}$$

이므로 $(\sum_{t=0}^{\infty} x^t)^n$ 은 다음과 같은 항으로 이루어진 형식적 멱급수이다.

$$x^{e_1 + e_2 + \dots + e_n} \quad (e_1, e_2, \dots, e_n \text{은 음이 아닌 정수})$$

여기서 $e_1 + e_2 + \dots + e_n = r$ 라고 하면, r 는 음이 아닌 모든 정수를 움직이므로 위의 결과에 의하여 다음이 성립한다.

$$\left(\sum_{t=0}^{\infty} x^t\right)^n = \sum_{r=0}^{\infty} \binom{n+r-1}{r} x^r = \sum_{t=0}^{\infty} \binom{n+t-1}{t} x^t$$

한편, 보기 4.2.5에 의하여

$$\sum_{t=0}^{\infty} x^t = 1 + x + x^2 + x^3 + \dots = \frac{1}{1-x}$$

이므로 다음 결과를 얻는다.

$$\frac{1}{(1-x)^n} = \left(\frac{1}{1-x}\right)^n = \left(\sum_{t=0}^{\infty} x^t\right)^n = \sum_{t=0}^{\infty} \binom{n+t-1}{t} x^t$$

보기 1 다음 등식이 성립한다.

$$\begin{aligned}\frac{1}{(1-x)^2} &= (1+x+x^2+x^3+\cdots)^2 = \sum_{t=0}^{\infty} \binom{t+1}{t} x^t \\ &= \sum_{t=0}^{\infty} \binom{t+1}{1} x^t = \sum_{t=0}^{\infty} (t+1) x^t\end{aligned}$$

$$\begin{aligned}\frac{1}{(1-x)^3} &= (1+x+x^2+x^3+\cdots)^3 = \sum_{t=0}^{\infty} \binom{t+2}{t} x^t \\ &= \sum_{t=0}^{\infty} \binom{t+2}{2} x^t = \sum_{t=0}^{\infty} \frac{(t+1)(t+2)}{2} x^t\end{aligned}$$

$$\begin{aligned}\frac{1}{(1-x)^4} &= (1+x+x^2+x^3+\cdots)^4 = \sum_{t=0}^{\infty} \binom{t+3}{t} x^t \\ &= \sum_{t=0}^{\infty} \binom{t+3}{3} x^t = \sum_{t=0}^{\infty} \frac{(t+1)(t+2)(t+3)}{6} x^t\end{aligned}$$

보기 2 형식적 멱급수

$$(1+x+x^2+x^3+\cdots)^4 = \sum_{t=0}^{\infty} \frac{(t+1)(t+2)(t+3)}{6} x^t$$

에서 x^r 의 계수는 $\frac{(r+1)(r+2)(r+3)}{6}$ 이다.

따라서 네 미지수 x_1, x_2, x_3, x_4 관한 일차방정식

$$x_1 + x_2 + x_3 + x_4 = r$$

의 해 중에서 x_1, x_2, x_3, x_4 의 값이 음이 아닌 정수인 해 전체의 개수는 다음과 같다.

$$\frac{(r+1)(r+2)(r+3)}{6} = \binom{r+3}{3} = \binom{r+3}{r} = {}_4H_r$$

한편, $0 \leq r \leq k$ 인 경우에 일차방정식

$$(*) \quad x_1 + x_2 + x_3 + x_4 = r$$

의 해 중에서 x_1, x_2, x_3, x_4 의 값이 음이 아닌 정수인 해 전체의 개수를 구하려면,

$$(1+x+x^2+x^3+\cdots+x^k)^4$$

의 전개식에서 x^r 의 계수를 구하면 된다.

예를 들면,

$$\begin{aligned}
 & (1 + x + x^2 + x^3 + \cdots + x^{16})^4 \\
 &= 1 + 4x + 10x^2 + 20x^3 + 35x^4 + 56x^5 + 84x^6 \\
 &+ 120x^7 + 165x^8 + 220x^9 + 286x^{10} + 364x^{11} + 455x^{12} \\
 &+ 560x^{13} + 1680x^{14} + 816x^{15} + 969x^{16} + (x^{64} \text{ 까지의 합})
 \end{aligned}$$

이므로 일차방정식

$$x_1 + x_2 + x_3 + x_4 = 16, \quad x_1 + x_2 + x_3 + x_4 = 15$$

의 해 중에서 x_1, x_2, x_3, x_4 의 값이 음이 아닌 정수인 해 전체의 개수는

각각 위의 전개식에서의 x^{16}, x^{15} 의 계수인 969, 816 이고 또 다음 결과를 얻는다.

$$\binom{16+3}{3} = \binom{16+3}{16} = 969, \quad \binom{15+3}{3} = \binom{15+3}{16} = 816$$

그러나, 일차방정식

$$x_1 + x_2 + x_3 + x_4 = 17$$

의 해 중에서 x_1, x_2, x_3, x_4 의 값이 음이 아닌 정수인 해 전체의 개수는

위의 전개식에서의 x^{17} 의 계수는 아니다.

실제로, 이 값은

$$(1 + x + x^2 + x^3 + \cdots + x^{17})^4$$

의 전개식에서의 x^{17} 의 계수와 다르다.

형식적 멱급수의 곱

다음 세 형식적 멱급수들의 곱을 전개했을 때의 x^3 의 계수를 구해보자.

$$(1+x+x^2+x^3+x^4+\cdots)(1+x^2+x^4+x^6+x^8+\cdots) \\ (1+x^3+x^6+x^9+x^{14}+\cdots)$$

먼저 이 곱을

$$(1+x^{1\cdot 1}+x^{2\cdot 1}+x^{3\cdot 1}+\cdots)(1+x^{1\cdot 2}+x^{2\cdot 2}+x^{2\cdot 3}+\cdots) \\ (1+x^{1\cdot 3}+x^{2\cdot 3}+x^{3\cdot 3}+\cdots)$$

으로 나타내어 전개하면 곱은 다음과 같다.

$$1+x^{1\cdot 1}+(x^{2\cdot 1}+x^{1\cdot 2})+(x^{1\cdot 1}x^{1\cdot 2}+x^{3\cdot 1}+x^{1\cdot 3}) \\ +(x^{2\cdot 2}+x^{1\cdot 1}x^{1\cdot 3}+x^{2\cdot 1}x^{1\cdot 2})+\cdots$$

이 전개식에서, 예를 들어 $x^{2\cdot 1}$ 은 2의 분할

$$2=1+1 \quad (1 \text{ 이 } 2 \text{ 개})$$

에 대응하고 $x^{1\cdot 1}x^{1\cdot 2}$ 은 3의 분할

$$3=1+2 \quad (1 \text{ 이 } 1 \text{ 개, } 2 \text{ 가 } 1 \text{ 개})$$

에 대응한다고 생각하면, 3차 이하의 항에 대하여 다음과 같이 1, 2, 3의 분할이 대응한다.

$$x^{1\cdot 1}$$

$$1=1$$

$$x^{2\cdot 1}+x^{1\cdot 2}$$

$$2=1+1, \quad 2=2$$

$$x^{1\cdot 1}x^{1\cdot 2}+x^{3\cdot 1}+x^{1\cdot 3}$$

$$3=1+2, \quad 3=1+1+1, \quad 3=3$$

이 결과에 의하여 $p(1)=1$, $p(2)=2$, $p(3)=3$ 임을 알 수 있다.

일반적으로, 다음 정리가 성립한다.

정리 1 양의 정수 n 에 대하여 $1 \leq m \leq n$ 인 양의 정수 m 에 대한 $p(m)$ 의 값은 다음 곱을 전개한 식에서의 x^m 의 계수와 같다.

$$\begin{aligned} & \left(\sum_{i=0}^{\infty} x^i \right) \left(\sum_{i=0}^{\infty} x^{2i} \right) \cdots \left(\sum_{i=0}^{\infty} x^{ni} \right) \\ &= (1 + x + x^2 + x^3 + \cdots)(1 + x^2 + x^4 + x^6 + \cdots) \\ & \cdots (1 + x^n + x^{2n} + x^{3n} + \cdots) \end{aligned}$$

증명 양의 정수 r 에 대하여

$$A_r(x) = \sum_{i=0}^{\infty} x^{ir} = 1 + x^r + x^{2r} + x^{3r} + \cdots$$

이라 하고 $1 \leq m \leq n$ 인 정수 m 에 대하여 c_m 을 곱

$$A_1(x) A_2(x) \cdots A_n(x) = \left(\sum_{i=0}^{\infty} x^i \right) \left(\sum_{i=0}^{\infty} x^{2i} \right) \cdots \left(\sum_{i=0}^{\infty} x^{ni} \right)$$

에서의 x^m 의 계수라고 하자. 이 때, c_m 은

$$x^{i_1 \cdot r_1} x^{i_2 \cdot r_2} \cdots x^{i_k \cdot r_k} \quad (m = i_1 r_1 + i_2 r_2 + \cdots + i_k r_k)$$

과 같은 꼴의 항 전체의 개수와 같다. 그런데,

$$x^{i_1 \cdot r_1}, x^{i_2 \cdot r_2}, \cdots, x^{i_k \cdot r_k}$$

은 각각 $A_{r_1}(x)$, $A_{r_2}(x)$, \cdots , $A_{r_k}(x)$ 의 항이므로 r_1, r_2, \cdots, r_k 는 모두 서로 다르고 따라서 이 항에 대하여 다음과 같은 m 의 분할이 대응한다.

$$m = r_1 + \cdots + r_1 + r_2 + \cdots + r_2 + \cdots + r_k + \cdots + r_k$$

$$(\quad r_1 \text{은 } i_1 \text{개, } r_2 \text{는 } i_2 \text{개, } \cdots, r_k \text{는 } i_k \text{개})$$

그런데 또 다른 항 $x^{j_1 \cdot s_1} x^{j_2 \cdot s_2} \cdots x^{j_l \cdot s_l}$ 에 대하여 또 다른 m 의 분할을 얻으므로 $c_m \geq p(m)$ 이다.

한편, m 의 분할은 모두 다음과 같은 꼴이다.

$$m = r_1 + \cdots + r_1 + r_2 + \cdots + r_2 + \cdots + r_k + \cdots + r_k$$

(r_1, r_2, \cdots, r_k 는 서로 다르고 r_1 은 i_1 개, \cdots , r_k 는 i_k 개)

이와 같은 m 의 분할에 대하여 곱 $x^{i_1 \cdot r_1} x^{i_2 \cdot r_2} \cdots x^{i_k \cdot r_k}$ 이 대응하고, 또 $x^{i_1 \cdot r_1}, x^{i_2 \cdot r_2}, \cdots, x^{i_k \cdot r_k}$ 은 각각 $A_{r_1}(x), A_{r_2}(x), \cdots, A_{r_k}(x)$ 의 항이므로 $x^{i_1 \cdot m_1} x^{i_2 \cdot m_2} \cdots x^{i_k \cdot m_k}$ 은 곱 $A_1(x) A_2(x) \cdots A_n(x)$ 를 전개할 때 나타나는 항이므로 $c_m \leq p(m)$ 이다.

그러므로 $p(m) = c_m$ 이고, 따라서 정리가 성립한다.

위의 증명에서 각 항 $x^{i_1 \cdot r_1} x^{i_2 \cdot r_2} \cdots x^{i_k \cdot r_k}$ 에 대하여

$$i_1 r_1 \leq n, \quad i_2 r_2 \leq n, \quad \cdots, \quad i_k r_k \leq n$$

이므로

$$i_1 \leq \left\lfloor \frac{n}{r_1} \right\rfloor, \quad i_2 \leq \left\lfloor \frac{n}{r_2} \right\rfloor, \quad \cdots, \quad i_k \leq \left\lfloor \frac{n}{r_k} \right\rfloor$$

이고, 따라서 다음 따름정리가 성립한다.

따름정리 2 양의 정수 n 에 대하여

$$f_r(x) = 1 + x^r + x^{2r} + x^{3r} + \cdots + x^{nr} \quad (1 \leq r \leq n)$$

이라고 할 때, $1 \leq m \leq n$ 인 정수 m 에 대하여 $p(m)$ 의 값은 다항식의 곱

$$f_1(x) f_2(x) \cdots f_n(x)$$

을 전개한 식에서의 x^m 의 계수와 같다.

여기서, $f_r(x)$ 는 형식적 역급수

$$\sum_{i=0}^{\infty} x^{ir} = 1 + x^r + x^{2r} + x^{3r} + \cdots$$

에서 n 차 이하의 항을 택하여 만든 다항식이다.

보기 1 다음 다항식의 곱을 생각해 보자.

$$\begin{aligned}
 & (1+x+x^2+x^3+x^4)(1+x^2+x^4)(1+x^3)(1+x^4) \\
 &= 1+x+2x^2+3x^3+5x^4 \\
 & \quad +5x^5+6x^6+7x^7+7x^8+6x^9+5x^{10} \\
 & \quad +5x^{11}+3x^{12}+2x^{13}+x^{14}+x^{15}
 \end{aligned}$$

따라서 $p(1) = 1$, $p(2) = 2$, $p(3) = 3$, $p(4) = 5$ 이다.

한편, 위의 다항식으로부터 $n = 5, 6, \dots, 15$ 에 대한 $p(n)$ 의 값을 구할 수는 없다. 실제로, $p(5) = 7$ 이다(보기 2.6.1).

보기 2 다음 다항식의 곱을 생각해 보자.

$$\begin{aligned}
 & (1+x+x^2+x^3+x^4+x^5+x^6)(1+x^2+x^4+x^6) \\
 & (1+x^3+x^6)(1+x^4)(1+x^5)(1+x^6) \\
 &= 1+x+2x^2+3x^3+5x^4+7x^5+11x^6 \\
 & \quad +12x^7+18x^8+\dots
 \end{aligned}$$

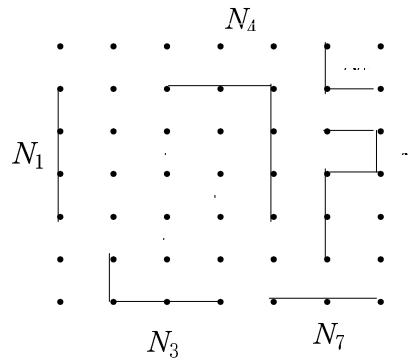
이로부터 다음 결과를 얻는다.

$$\begin{aligned}
 & p(1) = 1, \quad p(2) = 2, \quad p(3) = 3, \quad p(4) = 5, \\
 & p(5) = 7, \quad p(6) = 11
 \end{aligned}$$

한편, 위의 다항식으로부터 $n = 7, 8, \dots, 17$ 에 대한 $p(n)$ 의 값을 구할 수는 없다. 실제로, $p(7) = 15$ 이다(보기 2.6.3).

회로판

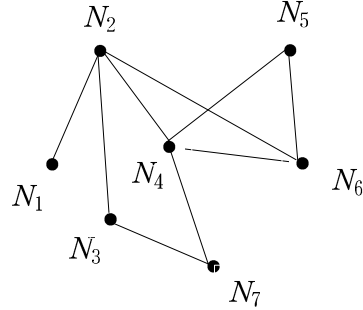
회로판(printed circuit board)은 고르게 배열된 노드(node)라고 부르는 격자점(grid point)으로 이루어져 있으며 이 격자점은 수평 선분 또는 수직 선분으로 연결되어 있다. 이 판 위에서 n 개의 노드는 수평 선분 또는 수직 선분을 따라 서로 교차하지 않는 통로(이것을 net 라고 한다)로 연결되어 있다. 아래 판에는 49 개의 노드와 7 개의 net N_1, N_2, \dots, N_7 가 있다.



이러한 회로판을 제작하는 과정에서 net 와 net 사이에 쓸데없는 쇼트 회로(short circuit)가 있는지를 판정하는 문제를 생각해 보자.

이와 같은 쇼트 회로가 있는지를 결정하는 방법 중의 하나는 서로 다른 net 를 둘씩 택하여 이 중 하나에 전기 신호를 적용시켜 다른 하나에 신호가 나타나면 쇼트 회로가 있음을 알아내는 방법이나, net 가 많을 경우에 이 방법은 시간 낭비이다. 그런데, 예를 들어 N_1, N_3, N_6 사이에는 쇼트 회로가 없다고 볼 수 있으므로, 모든 net 와 net 에 대하여 쇼트 회로가 있는지를 조사할 필요는 없다.

회로판의 net 는 꼭지점으로 나타내고, 또 두 net 사이에 쇼트 회로가 있을 때 그리고 이때에만 이 두 net 에 대응하는 두 꼭지점을 모서리로 이으면 다음 그림을 얻는다.



이 그림이 나타내는 그래프를 G 라고 할 때, 세 꼭지점 N_2, N_4, N_6 에 의하여 결정되는 G 의 부분그래프는 K_3 이고 또 $\chi(K_3) = 3$ 이므로 $\chi(G) \geq 3$ 이다.

한편, 3 가지 색을 사용하여 다음과 같이 지정하면 이웃하는 꼭지점에 다른 색이 지정되므로 $\chi(G) = 3$ 이다.

N_1, N_3, N_6 : 빨강,

N_2, N_5, N_7 : 파랑,

N_4 : 노랑

그러므로 $V = \{N_1, N_2, \dots, N_7\}$ 는 세 부분집합

$$\{N_1, N_3, N_6\}, \{N_2, N_5, N_7\}, \{N_4\}$$

의 합집합으로 분할되고, 또 이들 세 부분집합 안에 있는 두 net 사이에는 쇼트 회로가 없다고 생각할 수 있으므로 쇼트 회로가 있는지를 조사할 때에는

$$N_1 \text{ 과 } N_2, \quad N_1 \text{ 과 } N_4, \quad N_2 \text{ 와 } N_4$$

에 대해서만 조사하면 된다. 집합 V 를 분할하는 방법으로는 V 를

$$\{N_1, N_6\}, \{N_2, N_5, N_7\}, \{N_3, N_4\}$$

의 합집합으로 분할하는 방법도 있다.

단순 연결그래프의 생성 수형도

단순 연결그래프의 생성 수형도의 개수에 대해서는 다음 정리가 성립한다.
이 정리의 증명은 생략하기로 한다.

정리 1 (Kirchoff 의 정리) 단순 연결그래프 $G = (V, E)$, $|V| = n$ 일 때 n 개의 꼭지점에 v_1, v_2, \dots, v_n 과 같이 문자를 붙여 꼭지점을 구별하는 경우에 G 의 인접행렬을 $A = [a_{ij}]_{n \times n}$ 이라 하고 K 를 다음과 같은 n 차의 행렬이라고 할 때, G 의 서로 다른 생성 수형도의 개수는 K 의 한 성분 (따라서 모든 성분)에서의 여인수 $K_{i,j}$ 의 값과 일치한다,

$$K = \begin{bmatrix} k_{11} & k_{12} & \cdots & k_{1n} \\ k_{21} & k_{22} & \cdots & k_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ k_{n1} & k_{n2} & \cdots & k_{nn} \end{bmatrix}, \quad k_{ij} = \begin{cases} -a_{ij} & (i \neq j \text{인 경우}) \\ \deg v_i & (i = j \text{인 경우}) \end{cases}$$

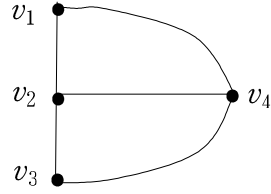
위의 정리에서 K 를 G 의 **Kirchoff 행렬**이라고 하며 K 의 (i, j) 성분에서의 여인수 $K_{i,j}$ 는 다음과 같은 행렬식이다.

$$K_{i,j} = (-1)^{i+j} \begin{vmatrix} k_{11} & k_{12} & \cdots & \boxed{\text{X}} & \cdots & k_{1n} \\ k_{21} & k_{22} & \cdots & \boxed{\text{X}} & \cdots & k_{2n} \\ \vdots & \vdots & \cdots & \vdots & \cdots & \vdots \\ \boxed{\text{X}} & \boxed{\text{X}} & \cdots & \boxed{\text{X}} & \cdots & \boxed{\text{X}} \\ \vdots & \vdots & \cdots & \vdots & \cdots & \vdots \\ k_{n1} & k_{n2} & \cdots & \boxed{\text{X}} & \cdots & k_{nn} \end{vmatrix}$$

위의 행렬식에서 망으를 친 행과 열은 삭제되었음을 뜻한다.

보기 1 오른쪽 그림이 나타내는 단순 연결그래프의 인접행렬은 다음과 같다.

$$A = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$



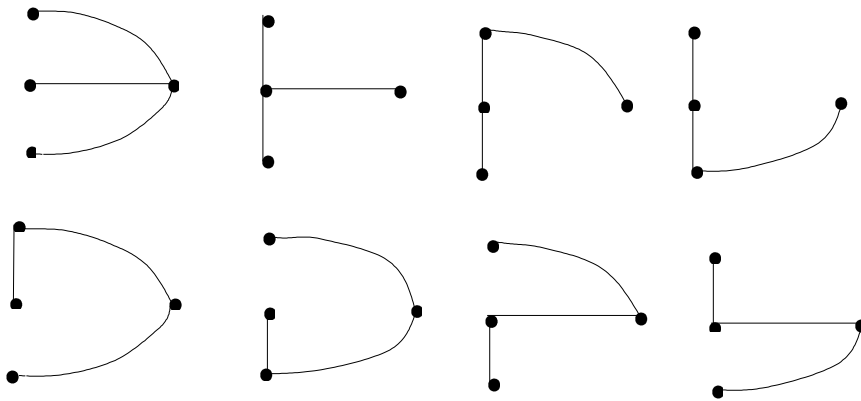
또, 꼭지점 v_1, v_2, v_3, v_4 의 차수는 각각 2, 3, 2, 3 이므로 이 그래프의 Kirchoff 행렬은

$$K = \begin{bmatrix} 2 & -1 & 0 & -1 \\ -1 & 3 & -1 & -1 \\ 0 & -1 & 2 & -1 \\ -1 & -1 & -1 & 3 \end{bmatrix}$$

이고, K 의 $(1, 1)$ 성분에서의 여인수는 다음과 같다.

$$\begin{vmatrix} 3 & -1 & -1 \\ -1 & 2 & -1 \\ -1 & -1 & 3 \end{vmatrix} = 18 - 1 - 1 - 2 - 3 - 3 = 8$$

따라서 G 의 서로 다른 생성 수형도는 모두 8 개 존재한다. 이들 8 개의 생성 수형도는 모두 4 개의 꼭지점과 3 개의 모서리로 이루어져 있다.

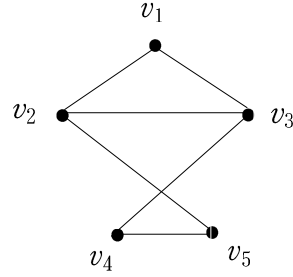


보기 2 오른쪽 그림이 나타내는 그래프

G 를 생각해 보자.

먼저 G 의 인접행렬 A 는 다음과 같다.

$$A = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix}$$



그리고

$$\deg v_1 = 2, \deg v_2 = 3, \deg v_3 = 3, \deg v_4 = 2, \deg v_5 = 2$$

이므로 Kirchoff 행렬 K 는 다음과 같다.

$$K = \begin{bmatrix} 2 & -1 & -1 & 0 & 0 \\ -1 & 3 & -1 & 0 & -1 \\ -1 & -1 & 3 & -1 & 0 \\ 0 & 0 & -1 & 2 & -1 \\ 0 & -1 & 0 & -1 & 2 \end{bmatrix}$$

행렬 K 의 $(1, 1)$ 에서의 여인수는 다음과 같다.

$$\begin{aligned} K_{1,1} &= \begin{vmatrix} 3 & -1 & 0 & -1 \\ -1 & 3 & -1 & 0 \\ 0 & -1 & 2 & -1 \\ -1 & 0 & -1 & 2 \end{vmatrix} \\ &= \begin{vmatrix} 0 & 8 & -3 & -1 \\ -1 & 3 & -1 & 0 \\ 0 & -1 & 2 & -1 \\ 0 & -3 & 0 & 2 \end{vmatrix} \\ &= (-1)^{2+1} (-1) \begin{vmatrix} 8 & -3 & -1 \\ -1 & 2 & -1 \\ -3 & 0 & 2 \end{vmatrix} \\ &= \begin{vmatrix} 0 & 13 & -9 \\ -1 & 2 & -1 \\ 0 & -6 & 5 \end{vmatrix} \\ &= (-1)^{2+1} (-1) \begin{vmatrix} 13 & -9 \\ -6 & 5 \end{vmatrix} = 65 - 54 = 11 \end{aligned}$$

따라서 G 의 서로 다른 생성 수형도는 11 개 존재한다.

앞의 정리 1을 이용하면, 다음 정리를 증명할 수 있다.

정리 2 완전그래프 K_n 의 n 개의 꼭지점에 v_1, v_2, \dots, v_n 과 같은 문자를 붙여 꼭지점을 구별할 때, $n \geq 3$ 인 경우에 K_n 의 서로 다른 생성수형도의 개수는 n^{n-2} 이다.

그리고, $n \geq 3$ 일 때, 꼭지점 v_1, v_2, \dots, v_n 을 가진 서로 다른 수형도의 개수는 n^{n-2} 이다.

증 명 (1) 완전그래프 K_n 의 인접행렬은 n 차의 행렬

$$A = \begin{bmatrix} 0 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 0 & 1 & \cdots & 1 & 1 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 1 & 1 & 1 & \cdots & 0 & 1 \\ 1 & 1 & 1 & \cdots & 1 & 0 \end{bmatrix}$$

이고, 또 K_n 의 각 꼭지점 v_i 에 대하여 $\deg v_i = n-1$ 이므로 K_n 의 Kirchhoff 행렬 K 는 다음과 같은 n 차의 행렬이다.

$$K = \begin{bmatrix} n-1 & -1 & -1 & \cdots & -1 & -1 \\ -1 & n-1 & -1 & \cdots & -1 & -1 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ -1 & -1 & -1 & \cdots & n-1 & -1 \\ -1 & -1 & -1 & \cdots & -1 & n-1 \end{bmatrix}$$

그리고, 행렬 K 에서 $(1,1)$ 성분의 여인수는 다음과 같은 $(n-1)$ 차의 행렬식이다.

$$K_{1,1} = \begin{vmatrix} n-1 & -1 & -1 & \cdots & -1 & -1 \\ -1 & n-1 & -1 & \cdots & -1 & -1 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ -1 & -1 & -1 & \cdots & n-1 & -1 \\ -1 & -1 & -1 & \cdots & -1 & n-1 \end{vmatrix}$$

위의 행렬식에서 제 1 행에 제 2 행, \dots , 제 $n-1$ 행을 더하면

$$K_{1,1} = \begin{vmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ -1 & n-1 & -1 & \cdots & -1 & -1 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ -1 & -1 & -1 & \cdots & n-1 & -1 \\ -1 & -1 & -1 & \cdots & -1 & n-1 \end{vmatrix}$$

이고 또 위의 행렬식에서 제 2행, \cdots , 제 $n-1$ 에 각각 제 1행을 더하면 다음 결과를 얻는다.

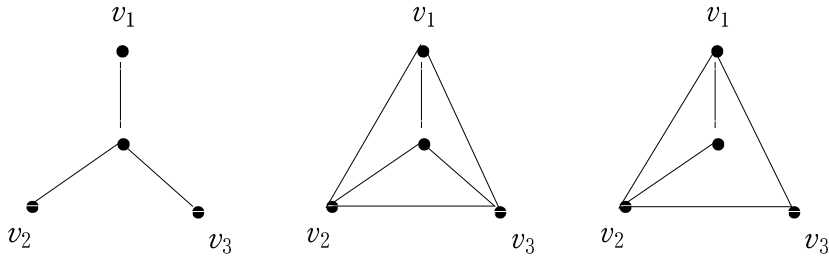
$$K_{1,1} = \begin{vmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 0 & n & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & n & 0 \\ 0 & 0 & 0 & \cdots & 0 & n \end{vmatrix} = n^{n-2}$$

따라서 정리 1에 의하여 완전그래프 G 의 서로 다른 생성 수형도의 개수는 n^{n-2} 이다.

(2) n 개의 꼭지점 v_1, v_2, \cdots, v_n 을 수형도는 완전그래프 K_n 의 한 생성 수형도이고, 또 n 개의 꼭지점 v_1, v_2, \cdots, v_n 을 가진 완전그래프 K_n 의 생성 수형도는 모두 꼭지점 v_1, v_2, \cdots, v_n 을 가진 수형도이다.

따라서 (1)의 결과에 의하여 $n \geq 3$ 일 때, 꼭지점 v_1, v_2, \cdots, v_n 을 가진 서로 다른 수형도의 개수는 n^{n-2} 이다.

위의 (2)의 증명에서 완전그래프가 필요하다. 예를 들어, 아래 그림에서 첫째 그림이 나타내는 수형도는 둘째 그림이 나타내는 완전그래프의 생성 수형도이지만 셋째 그림이 나타내는 그래프의 생성 순형도는 아니다.



행렬식

자연수 $1, 2, \dots, n$ 을 일렬로 늘어놓은 순열(順列, permutation) 전체의 개수는 $n!$ 개이다. 이러한 순열

$$\sigma : j_1, j_2, j_3, \dots, j_n$$

에 대하여 다음과 같은 $\frac{n(n-1)}{2}$ 개의 순서쌍을 생각해 보자.

$$\begin{aligned} (j_1, j_2), (j_1, j_3), \dots, (j_1, j_n), \\ (j_2, j_3), \dots, (j_2, j_n), \\ \dots\dots\dots, \\ (j_{n-1}, j_n) \end{aligned}$$

위의 순서쌍 중에서 크기의 순으로 되어 있지 않은 순서쌍이 있을 때, σ 에 전도(轉倒, inversion)가 있다고 하고, 이러한 전도가 일어난 개수를 $\mu(\sigma)$ 로 나타낸다. 그리고, $\mu(\sigma)$ 가 짝수일 때 σ 를 **우순열**(偶順列, even permutation)이라 하고 $\mu(\sigma)$ 가 홀수일 때 σ 를 **기순열**(奇順列, odd permutation)이라고 하며 다음과 같이 정의된 $\text{sgn } \sigma$ 를 σ 의 **부호**(符號, sign, signum)라고 한다.

$$\text{sgn } \sigma = (-1)^{\mu(\sigma)} = \begin{cases} 1 & (\sigma \text{ 가 우순열일 때}) \\ -1 & (\sigma \text{ 가 기순열일 때}) \end{cases}$$

보기 1 자연수 $1, 2, 3, 4, 5$ 의 한 순열

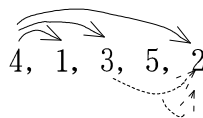
$$\sigma : 4, 1, 3, 5, 2$$

를 생각해 보자.

이 순열에서 전도가 일어난 순서쌍은 다음과 같은 5 개의 순서쌍뿐이다.

$$(4, 1), (4, 3), (4, 2), (3, 2), (5, 2)$$

따라서 $\mu(\sigma) = 5$ 이므로 σ 는 기순열이고 $\text{sgn } \sigma = -1$ 이다.



체 F 위의 n 차의 행렬

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$$

에 대하여, A 의 제 1행, 제 2행, \dots , 제 n 행의 원소 중에서 한 개씩 택하되 제 1열, 제 2열, \dots , 제 n 열에서도 한 개씩만 나오도록 택한 원소를 각각

$$a_{1j_1}, a_{2j_2}, \dots, a_{nj_n}$$

이라고 하면 j_1, j_2, \dots, j_n 는 $1, 2, \dots, n$ 의 순열이다. 역으로, $1, 2, \dots, n$ 의 순열 j_1, j_2, \dots, j_n 에 대하여 $a_{1j_1}, a_{2j_2}, \dots, a_{nj_n}$ 은 A 의 각 행과 각 열에서 한 개씩만 택한 원소들이다.

정의 1 체 F 위의 n 차의 행렬 $A = [a_{ij}]_{n \times n}$ 에 대하여 다음과 같이 정의된 $\det A$ 를 A 의 **행렬식**(行列式, determinant)이라고 한다.

$$\det A = \sum_{\sigma} (\operatorname{sgn} \sigma) a_{1j_1} a_{2j_2} \cdots a_{nj_n}$$

여기서, σ 는 $1, 2, \dots, n$ 의 순열 j_1, j_2, \dots, j_n 을 타나내며 \sum 는 이와 같은 $n!$ 개의 순열 σ 전체에 대한 총합을 나타낸다. 그리고, n 차의 행렬의 행렬식 $\det A$ 를 **n 차의 행렬식**이라 하고 이 행렬식을

$$|A| \quad \text{또는} \quad \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}$$

특히, 1차의 행렬 $[a]$ 의 행렬식은 a 와 동일하다고 생각한다.

보기 2 오른쪽 표는 1, 2의 모든 순열을 분류한 표이며, 이로부터 다음 결과를 얻는다.

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = \sum_{\sigma} a_{1j_1} a_{2j_2} = a_{11}a_{22} - a_{12}a_{21}$$

순열 σ	$\mu(\sigma)$	
1, 2	0	우순열
2, 1	1	기순열

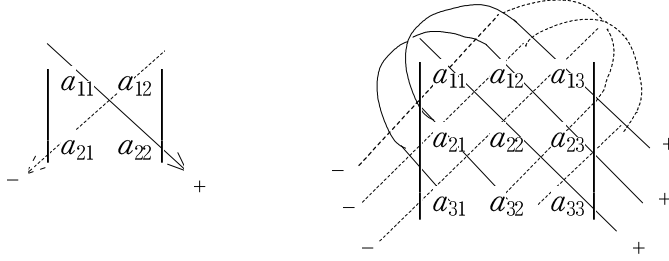
보기 3 다음 표는 1, 2, 3 의 모든 순열을 분류한 표이다.

순열 σ	$\mu(\sigma)$		순열 σ	$\mu(\sigma)$	
1, 2, 3	0	우순열	2, 3, 1	2	우순열
1, 3, 2	1	기순열	3, 1, 2	2	우순열
2, 1, 3	1	기순열	3, 2, 1	3	기순열

체 F 위의 3 차의 행렬식은 다음과 같다.

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = \sum_{\sigma} (\text{sgn } \sigma) a_{1j_1} a_{2j_2} a_{3j_3} \\
 = a_{11} a_{22} a_{33} + a_{12} a_{23} a_{31} + a_{13} a_{21} a_{32} \\
 - a_{11} a_{23} a_{32} - a_{12} a_{21} a_{33} - a_{13} a_{22} a_{31}$$

다음 두 그림은 2 차와 3 차의 행렬식을 구하는 방법을 보여 주고 있다.
그러나, 4 차 이상의 행렬식은 이와 같은 그림으로 구할 수 없다.



보기 4 다음 행렬식의 값을 구해 보자.

$$\begin{vmatrix} 0 & a_{12} & 0 & 0 \\ 0 & 0 & a_{23} & 0 \\ 0 & 0 & 0 & a_{34} \\ a_{41} & 0 & 0 & 0 \end{vmatrix}$$

이 행렬식의 항 중에서 0 이 아닌 항은 다음 항뿐이다.

$$(\text{sgn } \sigma) a_{12} a_{23} a_{34} a_{41} \quad (\text{단, } \sigma : 2, 3, 4, 1)$$

순열 σ 에서 전도가 일어나는 순서쌍은 $(2, 1), (3, 1), (4, 1)$ 뿐이므로 $\mu(\sigma) = 3, \text{sgn } \sigma = -1$ 이고 따라서 이 행렬식의 값은 $-a_{12} a_{23} a_{34} a_{41}$ 이다.

아래에 소개할 네 정리에 대한 증명은 [해설 3]을 참조하기 바란다.

다음 정리에 의하면 행렬식의 행에 대한 성질은 열에 대해서도 성립한다.

정리 2 체 F 위의 n 차의 행렬 A 에 대하여 $\det A^T = \det A$ 이다.

$$\begin{vmatrix} a_{11} & a_{21} & \cdots & a_{n1} \\ a_{12} & a_{22} & \cdots & a_{n2} \\ \vdots & \vdots & \cdots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}$$

정리 3 체 F 위의 행렬 $A = [a_{ij}]_{n \times n}$ 에서 서로 다른 두 행 [두 열] 을 서로 바꾸어 놓은 행렬을 B 라고 하면, $\det B = -\det A$ 이다.

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{s1} & a_{s2} & \cdots & a_{sn} \\ \cdots & \cdots & \cdots & \cdots \\ a_{r1} & a_{r2} & \cdots & a_{rn} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} = - \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{r1} & a_{r2} & \cdots & a_{rn} \\ \cdots & \cdots & \cdots & \cdots \\ a_{s1} & a_{s2} & \cdots & a_{sn} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}$$

$$\text{즉, } \det C_{rs} A = -\det A, \quad \det A C_{rs} = -\det A$$

또, A 의 서로 다른 두 행 [두 열] 의 성분이 일치하면, $\det A = 0$ 이다.

정리 4 체 F 위의 행렬 $A = [a_{ij}]_{n \times n}$ 에 대하여 A 의 한 행 [한 열] 을 k 배 하여 얻은 행렬을 B 이라고 하면 $\det B = k \det A$ 이다.

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ ka_{r1} & ka_{r2} & \cdots & ka_{rn} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} = k \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{r1} & a_{r2} & \cdots & a_{rn} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}$$

$$\text{즉, } \det D_{rr}(k) A = k \det A, \quad \det A D_{rr}(k) = k \det A$$

정리 5 체 F 위의 행렬 A 에서 한 행 [한 열] 의 각 성분이 합의 경우에 $\det A$ 는 두 행렬식의 합으로 분리된다.

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ b_1 + c_1 & b_2 + c_2 & \cdots & b_n + c_n \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ b_1 & b_2 & \cdots & b_n \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} + \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ c_1 & c_2 & \cdots & c_n \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}$$

앞의 정리 3 ~ 정리 5를 이용하면 다음 정리를 증명할 수 있다.

정리 6 체 F 위의 행렬 $A = [a_{ij}]_{n \times n}$ 에 대하여 다음이 성립한다.

- (1) A 의 서로 다른 두 행 [두 열]의 대응하는 성분이 비례하거나 또는 일치하면, $\det A = 0$ 이다.

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{r1} & a_{r2} & \cdots & a_{rn} \\ \cdots & \cdots & \cdots & \cdots \\ ka_{r1} & ka_{r2} & \cdots & ka_{rn} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} = k \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{r1} & a_{r2} & \cdots & a_{rn} \\ \cdots & \cdots & \cdots & \cdots \\ a_{r1} & a_{r2} & \cdots & a_{rn} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} = 0$$

특히, A 의 한 행 [열]의 성분이 0이면, $\det A = 0$ 이다.

- (2) $\det(kA) = k^n \det A$, $\det(-A) = (-1)^n \det A$

- (3) A 의 한 행 [한 열]에 다른 행 [다른 열]의 k 배를 더하여 얻은 행렬을 B 라고 하면, $\det B = \det A$ 이다.

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{r1} + ka_{s1} & a_{r2} + ka_{s2} & \cdots & a_{rn} + ka_{sn} \\ \cdots & \cdots & \cdots & \cdots \\ a_{s1} & a_{s2} & \cdots & a_{sn} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{r1} & a_{r2} & \cdots & a_{rn} \\ \cdots & \cdots & \cdots & \cdots \\ a_{s1} & a_{s2} & \cdots & a_{sn} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}$$

$$\text{즉, } \det E_{rs}(k)A = \det A, \quad \det A E_{rs}(k) = \det A$$

정리 7 체 F 위의 행렬 $A = [a_{ij}]_{n \times n}$ 가 下 삼각행렬이거나 또는 上 삼각행렬이면, $\det A = a_{11}a_{22} \cdots a_{nn}$ 이다. 즉,

$$\begin{vmatrix} a_{11} & 0 & \cdots & 0 \\ a_{21} & a_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_{nn} \end{vmatrix} = a_{11}a_{22} \cdots a_{nn}$$

특히, $A = \text{diag}\{a_{11}, a_{22}, \cdots, a_{nn}\}$ 이면, $\det A = a_{11}a_{22} \cdots a_{nn}$ 이다.

증 명 행렬 A 가 下 삼각행렬이면,

$$\det A = \sum_{\sigma} (\operatorname{sgn} \sigma) a_{1j_1} a_{2j_2} \cdots a_{nj_n}$$

에서 0 이 아닌 항은 $a_{11} a_{22} \cdots a_{nn}$ 뿐이므로 $\det A = a_{11} a_{22} \cdots a_{nn}$ 이다.

그리고, A 가 上 삼각행렬이면, A^T 는 下 삼각행렬이므로 정리 3.1.2 와 위의 결과에 의하여 $\det A = \det A^T = a_{11} a_{22} \cdots a_{nn}$ 이다.

보기 5 실수체 \mathbb{R} 위에서 다음이 성립한다(정리 3, 정리 6).

$$\begin{aligned} \begin{vmatrix} 2 & 8 & 7 \\ 1 & 1 & 2 \\ -3 & 5 & 1 \end{vmatrix} &= - \begin{vmatrix} 1 & 1 & 2 \\ 2 & 8 & 7 \\ -3 & 5 & 1 \end{vmatrix} = - \begin{vmatrix} 1 & 1 & 2 \\ 0 & 6 & 3 \\ 0 & 8 & 7 \end{vmatrix} \\ &= -3 \begin{vmatrix} 1 & 1 & 2 \\ 0 & 2 & 1 \\ 0 & 8 & 7 \end{vmatrix} = -3 \begin{vmatrix} 1 & 1 & 2 \\ 0 & 2 & 1 \\ 0 & 0 & 3 \end{vmatrix} = -18 \end{aligned}$$

보기 6 체 F 위에서 다음이 성립한다(정리 6, 정리 4).

$$\begin{aligned} \begin{vmatrix} 1 & a & b & c+d \\ 1 & b & c & d+a \\ 1 & c & d & a+b \\ 1 & d & a & b+c \end{vmatrix} &= \begin{vmatrix} 1 & a & b & a+b+c+d \\ 1 & b & c & b+c+d+a \\ 1 & c & d & c+d+a+b \\ 1 & d & a & d+a+b+c \end{vmatrix} \\ &= (a+b+c+d) \begin{vmatrix} 1 & a & b & 1 \\ 1 & b & c & 1 \\ 1 & c & d & 1 \\ 1 & d & a & 1 \end{vmatrix} = 0 \end{aligned}$$

정리 8 체 F 위의 n 차의 행렬 A, B 에 대하여 다음이 성립한다.

- (1) $\det I_n = 1$, $\det C_{ij} = -1$, $\det D_{ii}(k) = k$, $\det E_{ij}(k) = 1$
- (2) E 가 기본행렬이면, $\det EA = (\det E)(\det A)$ 이다.
- (3) A 가 정칙행렬일 때 그리고 이때에만 $\det A \neq 0$ 이다.
- (4) $\det AB = (\det A)(\det B)$ 즉 $|AB| = |A||B|$

증 명 (1), (2) 정리 3 ~ 정리 7 에 의하여 (1) 이 성립한다.

(3), (4) 먼저 행렬 A 가 정칙행렬이면, 적당한 기본행렬 E_1, E_2, \dots, E_s 에 대하여 $A = E_1 E_2 \cdots E_s$ 이다(정리 11.1.7).

따라서 (1)에 의하여

$$\begin{aligned}\det A &= \det (E_1 E_2 \cdots E_s) = (\det E_1)(\det E_2 \cdots E_s) \\ &= \cdots = (\det E_1)(\det E_2) \cdots (\det E_s)\end{aligned}$$

이므로 $\det A \neq 0$ 이고, 또 다음이 성립한다.

$$\begin{aligned}\det (AB) &= \det (E_1 E_2 \cdots E_s B) \\ &= (\det E_1)(\det E_2 \cdots E_s B) \\ &= (\det E_1)(\det E_2) \cdots (\det E_s)(\det B) \\ &= (\det A)(\det B)\end{aligned}$$

다음에 A 가 정칙행렬이 아니라고 하자.

이 때, A 에 기본 행 변형을 시행하여 얻은 기약 행 사다리꼴 행렬을 A' 이라고 하면, $A' = PA$ 인 정칙행렬 P 가 존재한다(정리 2.3.5). 그런데, A 는 정칙행렬이 아니므로 $r(A) < n$ 이고 따라서 A' 의 마지막 행은 0 만으로 이루어져 있다(정의 11.1.6). 그러므로, $A'B$ 의 마지막 행도 0 만으로 이루어진 행렬이므로 $\det A' = 0$, $\det A'B = 0$ 이다(정리 6). 그런데, P 는 정칙행렬이므로 앞의 결과에 의하여 $\det P \neq 0$ 이다.

$$\begin{aligned}(\det P)(\det A) &= \det PA = \det A' = 0, \\ (\det P)(\det AB) &= \det P(AB) = \det (PA)B = \det A'B = 0\end{aligned}$$

이므로 $\det A = 0$, $\det AB = 0$ 이고 따라서 다음 등식이 성립한다.

$$\det AB = 0 = 0 \cdot \det B = (\det A)(\det B)$$

그러므로, 정리의 (3), (4) 가 성립한다.

정리 9 체 F 위의 n 차의 행렬 A, B 에 대하여 다음이 성립한다.

- (1) A 가 정칙행렬이면, $\det A^{-1} = (\det A)^{-1}$ 이다.
 - (2) $AB = I_n$ 이면, A 는 정칙행렬이고 $A^{-1} = B$ 이다.
- $BA = I_n$ 이면, A 는 정칙행렬이고 $A^{-1} = B$ 이다.

증 명 (1) A 가 정칙행렬일 때, $AA^{-1} = I_n$ 이므로 정리 8 에 의하여

$$(\det A)(\det A^{-1}) = \det AA^{-1} = \det I_n = 1$$

이고 $\det A \neq 0$ 이고 따라서 $\det A^{-1} = (\det A)^{-1}$ 이다.

(2) $AB = I_n$ 이면, 정리 8에 의하여 $(\det A)(\det B) = \det I_n = 1$

이고, 따라서 $\det A \neq 0$ 이므로 A 는 정칙행렬이고 $A^{-1} = B$ 이다.

마찬가지로, $BA = I_n$ 이면, A 는 정칙행렬이고 $A^{-1} = B$ 이다.

다음 정리가 성립한다.

정리 10 체 F 위의 n 차의 행렬 A ($\neq O_n$) 에 대하여 다음 네 조건은 서로 동치이다.

- (1) A 는 정칙행렬이다.
- (2) $\det A \neq 0$
- (3) $r(A) = n$
- (4) 다음 동차 연립일차방정식의 해는 자명한 해 $(0, 0, \dots, 0)$ 뿐이다.

$$A \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$$

따라서 $\det A = 0$ 일 때 그리고 이때에만 위의 동차 연립일차방정식은 자명한 해 $(0, \dots, 0)$ 이외의 해를 가진다.

보기 7 실수체 \mathbb{R} 위의 다음 연립일차방정식을 생각해 보자.

$$\begin{cases} 3x_1 + x_2 = kx_1 \\ 2x_1 + 2x_2 = kx_2 \end{cases} \quad \Leftrightarrow \quad \begin{cases} (3-k)x_1 + x_2 = 0 \\ 2x_1 + (2-k)x_2 = 0 \end{cases}$$

위의 연립일차방정식에서

$$\begin{vmatrix} 3-k & 1 \\ 2 & 2-k \end{vmatrix} = (3-k)(2-k) - 2 = k^2 - 5k + 4 \\ = (k-1)(k-4)$$

이고 따라서 정리 10에 의하여 위의 연립일차방정식이 자명한 해 이외의 행를 가질 필요충분조건은 $k = 1$ 또는 $k = 4$ 인 것이다.

정리 11 (Vandermonde 의 행렬식) 체 F 위에서 다음이 성립한다.

$$V = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ x_1^2 & x_2^2 & \cdots & x_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1} \end{vmatrix} = (-1)^{\frac{(n-1)n}{2}} \prod_{i < j} (x_i - x_j)$$

즉,
$$V = (-1)^{\frac{(n-1)n}{2}} (x_1 - x_2)(x_1 - x_3) \cdots (x_1 - x_n) \\ (x_2 - x_3) \cdots (x_2 - x_n) \\ \dots\dots\dots (x_{n-1} - x_n)$$

증 명 행렬식 V 는 x_1, x_2, \dots, x_n 에 관한 다항식으로 볼 수 있다. 그런데, $1 \leq i < j \leq n$ 일 때, 행렬식 V 에서 x_i 대신에 x_j 를 대입하면, 정리 6 에 의하여 $V = 0$ 이므로 V 는 $x_i - x_j$ 를 인수로 가진다.

그러므로, 적당한 $k \in F$ 에 대하여 $V = k \prod_{i < j} (x_i - x_j)$ 이고, 이 등식의 양변에서 $x_2 x_3^2 \cdots x_n^{n-1}$ 의 계수를 비교하면 k 는 다음과 같다.

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

보기 8 체 F 의 임의의 원소 a, b, c 에 대하여 다음이 성립한다.

$$\begin{vmatrix} 1 & 1 & 1 \\ a & b & c \\ a^2 & b^2 & c^2 \end{vmatrix} = \begin{vmatrix} 1 & a & a^2 \\ 1 & b & b^2 \\ 1 & c & c^2 \end{vmatrix} = (a-b)(b-c)(c-a)$$

연 습 문 제

1. 실수체 \mathbb{R} 위에서 다음 행렬식의 값을 구하여라.

$$(1) \begin{vmatrix} 1 & 2 & 3 \\ 2 & 4 & 6 \\ 3 & 4 & 2 \end{vmatrix} \quad (2) \begin{vmatrix} 4 & 4 & 0 \\ 2 & 2 & 0 \\ 9 & 7 & 2 \end{vmatrix} \quad (3) \begin{vmatrix} 3 & 4 & 0 \\ 1 & 2 & 0 \\ 9 & 7 & 2 \end{vmatrix}$$

§3.1 행렬식 83

2. 실수체 \mathbb{R} 위에서 다음 행렬식의 값을 구하여라.

$$(1) \begin{vmatrix} 2 & 4 & 6 & 4 \\ 1 & 2 & 3 & 2 \\ 0 & 1 & 1 & 0 \\ 1 & 2 & 0 & 2 \end{vmatrix} \quad (2) \begin{vmatrix} 2 & 1 & 5 & 7 \\ 3 & 0 & 1 & -1 \\ 2 & 0 & 0 & 0 \\ 1 & 0 & 3 & 2 \end{vmatrix} \quad (3) \begin{vmatrix} 1 & 1 & 1 & 1 \\ a & b & c & d \\ a^2 & b^2 & c^2 & d^2 \\ a^3 & b^3 & c^3 & d^3 \end{vmatrix}$$

3. 실수체 \mathbb{R} 위에서 다음 등식이 성립함을 밝혀라.

$$(1) \begin{vmatrix} 1+a & 1 & 1 \\ 1 & 1+b & 1 \\ 1 & 1 & 1+c \end{vmatrix} = abc + ab + ac + bc$$

$$(2) \begin{vmatrix} (b+c)^2 & a^2 & 1 \\ (c+a)^2 & b^2 & 1 \\ (a+b)^2 & c^2 & 1 \end{vmatrix} = -2(a+b+c)(a-b)(b-c)(c-a)$$

4. 실수체 \mathbb{R} 위에서 다음이 성립함을 증명하여라.

$$(1) \begin{vmatrix} a & b & b & b \\ a & b & a & a \\ a & a & b & a \\ b & b & b & a \end{vmatrix} = -(a-b)^4$$

$$(2) \begin{vmatrix} x & a_1 & a_2 & 1 \\ a_1 & x & a_2 & 1 \\ a_1 & a_2 & x & 1 \\ a_1 & a_2 & a_3 & 1 \end{vmatrix} = (x-a_1)(x-a_2)(x-a_3)$$

5. 실수체 \mathbb{R} 또는 복소수체 \mathbb{C} 위의 n 차의 행렬 A 가 교대행렬일 때, n 이 홀수이면 $\det A = 0$ 임을 밝혀라.

6. 체 F 위의 $m \times n$ 행렬 A 와 $n \times m$ 행렬 B 에 대하여 AB 는 m 차의 행렬이므로 $\det AB$ 가 정의된다. 이 경우에 $m > n$ 이면, $\det AB = 0$ 임을 밝혀라.
이 결과에 의하여 $\det AB \neq 0$ 이면, $m \leq n$ 이다.
7. 실수체 \mathbb{R} 위에서의 다음 동차 연립일차방정식이 자명한 해 이외의 해를 가지도록 k 의 값을 정하여라.

$$(1) \begin{cases} x_1 + 4x_2 = kx_1 \\ x_1 + x_2 = kx_2 \end{cases} \quad (2) \begin{cases} kx_1 + x_2 + x_3 = 0 \\ x_1 + kx_2 + x_3 = 0 \\ x_1 + x_2 + kx_3 = 0 \end{cases}$$

연 습 문 제 풀 이

1.

$$(1) \begin{vmatrix} 1 & 2 & 3 \\ 2 & 4 & 6 \\ 3 & 4 & 2 \end{vmatrix} = \begin{vmatrix} 1 & 2 & 3 \\ 0 & 0 & 0 \\ 3 & 4 & 2 \end{vmatrix} = 0$$

$$(2) \begin{vmatrix} 4 & 4 & 0 \\ 2 & 2 & 0 \\ 9 & 7 & 2 \end{vmatrix} = \begin{vmatrix} 0 & 4 & 0 \\ 0 & 2 & 0 \\ 2 & 7 & 2 \end{vmatrix} = 0$$

2.

$$(1) \begin{vmatrix} 2 & 4 & 6 & 4 \\ 1 & 2 & 3 & 2 \\ 0 & 1 & 1 & 0 \\ 1 & 2 & 0 & 2 \end{vmatrix} = \begin{vmatrix} 0 & 0 & 0 & 0 \\ 1 & 2 & 3 & 2 \\ 0 & 1 & 1 & 0 \\ 1 & 2 & 0 & 2 \end{vmatrix} = 0$$

$$\begin{aligned} (2) \begin{vmatrix} 2 & 1 & 5 & 7 \\ 3 & 0 & 1 & -1 \\ 2 & 0 & 0 & 0 \\ 1 & 0 & 3 & 2 \end{vmatrix} &= \begin{vmatrix} 0 & 1 & 5 & 7 \\ 0 & 0 & 1 & -1 \\ 2 & 0 & 0 & 0 \\ 1 & 0 & 3 & 2 \end{vmatrix} \\ &= \begin{vmatrix} 0 & 1 & 5 & 7 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & -6 & 0 \\ 1 & 0 & 3 & 2 \end{vmatrix} = (-6) \begin{vmatrix} 0 & 1 & 5 & 7 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 3 & 2 \end{vmatrix} \\ &= (-6)(-1) \begin{vmatrix} 1 & 0 & 3 & 2 \\ 0 & 1 & 5 & 7 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 1 & 0 \end{vmatrix} = 6 \begin{vmatrix} 1 & 0 & 3 & 2 \\ 0 & 1 & 5 & 7 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{vmatrix} \\ &= 6 \cdot 1 \cdot 1 \cdot 1 = 6 \end{aligned}$$

$$\begin{aligned} 3. (1) \begin{vmatrix} 1+a & 1 & 1 \\ 1 & 1+b & 1 \\ 1 & 1 & 1+c \end{vmatrix} &= \begin{vmatrix} a & 0 & -c \\ 0 & b & -c \\ 1 & 1 & 1+c \end{vmatrix} \\ &= ab(1+c) + bc + ac \\ &= abc + ab + ac + bc \end{aligned}$$

$$\begin{aligned}
 (2) \quad & \begin{vmatrix} (b+c)^2 & a^2 & 1 \\ (c+a)^2 & b^2 & 1 \\ (a+b)^2 & c^2 & 1 \end{vmatrix} = \begin{vmatrix} (b+c)^2 - a^2 & a^2 & 1 \\ (c+a)^2 - b^2 & b^2 & 1 \\ (a+b)^2 - c^2 & c^2 & 1 \end{vmatrix} \\
 & = (a+b+c) \begin{vmatrix} b+c-a & a^2 & 1 \\ c+a-b & b^2 & 1 \\ a+b-c & c^2 & 1 \end{vmatrix} = (a+b+c) \begin{vmatrix} -2a & a^2 & 1 \\ -2b & b^2 & 1 \\ -2c & c^2 & 1 \end{vmatrix}
 \end{aligned}$$

(제3열의 $(a+b+c)$ 배를 제1열에 더한다.)

$$= -2(a+b+c) \begin{vmatrix} a & a^2 & 1 \\ b & b^2 & 1 \\ c & c^2 & 1 \end{vmatrix} = 2(a+b+c) \begin{vmatrix} 1 & a^2 & a \\ 1 & b^2 & b \\ 1 & c^2 & c \end{vmatrix}$$

$$= -2(a+b+c) \begin{vmatrix} 1 & a & a^2 \\ 1 & b & b^2 \\ 1 & c & c^2 \end{vmatrix} = -2(a+b+c)(a-b)(b-c)(c-a)$$

(보기 3.1.8 참조)

$$4. \quad (1) \quad \begin{vmatrix} a & b & b & b \\ a & b & a & a \\ a & a & b & a \\ b & b & b & a \end{vmatrix} = \begin{vmatrix} a-b & 0 & 0 & b-a \\ a-b & 0 & a-b & 0 \\ a-b & a-b & 0 & 0 \\ b & b & b & a \end{vmatrix}$$

(제1행, 제2행, 제3행에서 제4행을 뺀다)

$$= (a-b)^3 \begin{vmatrix} 1 & 0 & 0 & -1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ b & b & b & a \end{vmatrix} = (a-b)^3 \begin{vmatrix} 1 & 0 & 0 & -1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ b & b & b & a \end{vmatrix}$$

(공통인수를 빼낸다) (제2행, 제3행에서 제1행을 뺀다)

$$= (a-b)^3 \begin{vmatrix} 1 & 0 & 0 & -1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & a-b \end{vmatrix} = -(a-b)^3 \begin{vmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & a-b \end{vmatrix}$$

(제4행에서 제1행, 제2행, (제2열과 제3열을 서로 바꾼다)

제3행의 b 배를 뺀다)

$$= -(a-b)^4$$

4. (2) 행렬식

$$D(x) = \begin{vmatrix} x & a_1 & a_2 & 1 \\ a_1 & x & a_2 & 1 \\ a_1 & a_2 & x & 1 \\ a_1 & a_2 & a_3 & 1 \end{vmatrix}$$

을 x 에 관한 다항식으로 생각하고 이 다항식에

$$x = a_1, \quad x = a_2, \quad x = a_3$$

을 대입하면 정리 3.1.6에 의하여

$$D(a_1) = \begin{vmatrix} a_1 & a_1 & a_2 & 1 \\ a_1 & a_1 & a_2 & 1 \\ a_1 & a_2 & a_1 & 1 \\ a_1 & a_2 & a_3 & 1 \end{vmatrix} = 0,$$

$$D(a_2) = \begin{vmatrix} a_2 & a_1 & a_2 & 1 \\ a_1 & a_2 & a_2 & 1 \\ a_1 & a_2 & a_2 & 1 \\ a_1 & a_2 & a_3 & 1 \end{vmatrix} = 0,$$

$$D(a_3) = \begin{vmatrix} a_3 & a_1 & a_2 & 1 \\ a_1 & a_3 & a_2 & 1 \\ a_1 & a_2 & a_3 & 1 \\ a_1 & a_2 & a_3 & 1 \end{vmatrix} = 0$$

이므로 적당한 실수 k 에 대하여 다음이 성립한다.

$$D(x) = k(x-a_1)(x-a_2)(x-a_3)$$

위의 등식의 양변에

$$x = 1, \quad a_1 = a_2 = a_3 = 0$$

을 대입하면, 정리 3.1.7에 의하여

$$k(1-0)(1-0)(1-0) = \begin{vmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{vmatrix} = 1$$

이므로 $k = 1$ 이고 따라서 다음 결과를 얻는다.

$$\begin{vmatrix} x & a_1 & a_2 & 1 \\ a_1 & x & a_2 & 1 \\ a_1 & a_2 & x & 1 \\ a_1 & a_2 & a_3 & 1 \end{vmatrix} = (x-a_1)(x-a_2)(x-a_3)$$

5. 실수체 \mathbb{R} 또는 복소수체 \mathbb{C} 위에서 n 차의 행렬 A 가 교대행렬이면,
 $A^T = -A$ 이고 $\det A = \det A^T$ 이므로 다음이 성립한다(정리 3.1.6).

$$\det A = \det A^T = \det(-A) = (-1)^n \det A$$

따라서 n 이 홀수이면,

$$\det A = -\det A$$

이고 $\det A$ 는 실수 또는 복소수 이므로 $\det A = 0$ 이다.

6. 두 행렬 $A = [a_{ij}]_{m \times n}$, $B = [b_{ij}]_{n \times m}$ 에서 $m > n$ 인 경우에 A, B 에
 적당한 영행렬을 덧붙인 m 차의 행렬

$$A' = \begin{bmatrix} a_{11} & \cdots & a_{1n} & 0 & \cdots & 0 \\ a_{21} & \cdots & a_{2n} & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} & 0 & \cdots & 0 \end{bmatrix}, \quad B' = \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1m} \\ \vdots & \vdots & & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nm} \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}$$

을 생각하면 $A'B' = AB$ 이고 또

$$\det A' = 0, \quad \det B' = 0$$

이므로 정리 3.1.8 에 의하여 다음이 성립한다.

$$\det AB = \det A'B' = (\det A')(\det B') = 0 \cdot 0 = 0$$

따라서 $\det AB \neq 0$ 이면, $m \leq n$ 이다.

7. 연립일차방정식

$$\begin{cases} x_1 + 4x_2 = kx_1 \\ x_1 + x_2 = kx_2 \end{cases} \quad \Leftrightarrow \quad \begin{cases} (1-k)x_1 + 4x_2 = 0 \\ x_1 + (1-k)x_2 = 0 \end{cases}$$

에 대하여 다음이 성립한다.

$$\begin{vmatrix} 1-k & 4 \\ 1 & 1-k \end{vmatrix} = (1-k)^2 - 4 = (k+1)(k-3)$$

따라서 위의 연립일차방정식이 자명한 해 이외의 해를 가질 필요충분 조건은 $k = 1$ 또는 $k = 4$ 인 것이다.

7. (2) 동차 연립일차방정식

$$\begin{cases} kx_1 + x_2 + x_3 = 0 \\ x_1 + kx_2 + x_3 = 0 \\ x_1 + x_2 + kx_3 = 0 \end{cases}$$

에 대하여 다음이 성립한다.

$$\begin{aligned} & \begin{vmatrix} k & 1 & 1 \\ 1 & k & 1 \\ 1 & 1 & k \end{vmatrix} \\ &= k^3 - 3k + 2 \\ &= (k-1)(k^2 + k - 2) \\ &= (k-1)^2(k+2) \end{aligned} \qquad \begin{array}{c|cccc} 1 & 1 & 0 & -3 & 2 \\ & & 1 & 1 & -2 \\ \hline & 1 & 1 & -2 & 0 \end{array}$$

따라서 정리 10에 의하여 주어진 연립일차방정식이 자명한 해 이외의 해를 가질 필요충분조건은 $k = 1$ 또는 $k = -2$ 인 것이다.

타원곡선을 이용한 정수의 인수분해

타원곡선을 이용한 정수의 인수분해 방법은 H.W. Lenstra 가 Pollard 의 $(p-1)$ 방법으로부터着想해낸 방법이다.

Pollard 의 $(p-1)$ 방법은 홀수인 素數 p 에 대하여 체 $\mathbb{Z}_p = \{0, 1, \dots, p-1\}$ 에서 $\mathbb{Z}_p^* = \{1, 2, \dots, p-1\}$ 의 성질을 이용한 인수분해 방법이고, 타원곡선을 이용한 인수분해 방법은 타원곡선 E 에 대한 덧셈군 $G(E, \mathbb{Z}_p)$ 의 성질을 이용한 인수분해 방법이다. 이와 같은 인수분해 방법이 널리 이용되는 이유는 덧셈군 $G(E, \mathbb{Z}_p)$ 의 연산을 상당히 빠른 속도로 행할 수 있기 때문이다.

일반적으로, n 이 양의 정수일 때, 가환환 $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ 에서 원소 $x \in \mathbb{Z}_n$, $x \neq 0$ 의 곱셈에 관한 역원 $x^{-1} \in \mathbb{Z}_n$ 가 존재하기 위한 필요충분조건은 $\gcd(x, n) = 1$ 인 것이다.

가환환 \mathbb{Z}_n 에서의 타원곡선

$$E : y^2 = x^3 + ax^2 + bx + c \quad (a, b, c \in \mathbb{Z}_n)$$

에 대하여

$$G(E, \mathbb{Z}_n) = \{(x, y) \in \mathbb{Z}_n^2 \mid y^2 = x^3 + ax^2 + bx + c\} \cup \{O\}$$

이라고 하자. 이 때, n 이 素數인 경우에 집합 $G(E, \mathbb{Z}_n)$ 은 정리 12.6.1에서와 같이 정의된 덧셈에 관하여 덧셈군을 이룬다. 한편, n 이 합성수인 경우에는 정리 12.6.1에서와 같은 덧셈을 정의할 수 없다. 예를 들어, 집합 $G(E, \mathbb{Z}_n)$ 의 두 점 $P = (x_1, y_1)$, $Q = (x_2, y_2)$, $x_2 \neq x_1$ 에 대하여 $x_2 - x_1 \in \mathbb{Z}_n$ 의 곱셈에 관한 역원이 존재하기 위한 필요충분조건은 $\gcd(x_2 - x_1, n) = 1$ 인 것이고 또 이때에만 $k = (y_2 - y_1)(x_2 - x_1)^{-1} \in \mathbb{Z}_n$ 이다.

정수 n 이 합성수일 때, $G(E, \mathbb{Z}_n)$ 의 두 점 $P = (x_1, y_1)$, $Q = (x_2, y_2)$ 에 대하여 다음과 같이 정의하자.

(1) $x_2 \neq x_1$ 일 때,

(i) $\gcd(x_2 - x_1, n) = 1$ 인 경우에 $P + Q = (x_3, y_3)$ 이다. 여기서

$$k = (y_2 - y_1)(x_2 - x_1)^{-1} \in \mathbb{Z}_n$$

$$x_3 = k^2 - a - (x_1 + x_2) \in \mathbb{Z}_n, \quad y_3 = k(x_3 - x_1) + y_1 \in \mathbb{Z}_n$$

(ii) $\gcd(x_2 - x_1, n) \neq 1$ 인 경우에 $P + Q$ 는 정의되지 않는다.

(2) $y_1 \neq 0$ 일 때,

(i) $\gcd(2y_1, n) = 1$ 인 경우에 $P + P = (x_3, -y_3)$ 이다. 여기서

$$k = (3x_1^2 + 2ax_1 + b)(2y_1)^{-1} \in \mathbb{Z}_n$$

$$x_3 = k^2 - a - 2x_1 \in \mathbb{Z}_n, \quad y_3 = k(x_3 - x_1) + y_1 \in \mathbb{Z}_n$$

(ii) $\gcd(2y_1, n) \neq 1$ 인 경우에 $P + P$ 는 정의되지 않는다.

이제 p 가 n 의 홀수인 소인수일 때, 각 $x \in \mathbb{Z}_n$ 에 대하여 $(x)_p \in \mathbb{Z}_p$ 를

$$x \equiv (x)_p \pmod{p}, \quad 0 \leq (x)_p < p$$

인 정수라고 하 다음이 성립한다.

$$\gcd(x, n) = 1 \Rightarrow \gcd((x)_p, p) = \gcd(x, p) = 1$$

따라서 \mathbb{Z}_n 에서의 타원곡선 E 에 대하여

$$E_p : y^2 = x^3 + (a)_p x^2 + (b)_p x + (c)_p$$

이라고 할 때, $G(E, \mathbb{Z}_n)$ 에 속하는 두 점 $P = (x_1, y_1)$, $Q = (x_2, y_2)$ 에 대

하여 $\overline{P} = ((x_1)_p, (y_1)_p)$, $\overline{Q} = ((x_2)_p, (y_2)_p)$ 라고 하면, $\overline{P}, \overline{Q} \in G(E, \mathbb{Z}_p)$

이고 또 앞서서와 같이 $G(E, \mathbb{Z}_n)$ 에서 $P + Q$, kP 가 정의되는 경우에

덧셈군 $G(E, \mathbb{Z}_p)$ 에서 $\overline{P+Q} = \overline{P} + \overline{Q}$, $\overline{kP} = k\overline{P}$ 이다(k 는 양의 정수).

위의 (1) 에서 $\gcd(x_2 - x_1, n) \neq 1$ 인 경우에는 $1 < \gcd(x_2 - x_1, n) \leq n$

이고, 또 (2) 에서 $\gcd(2y_1, n) \neq 1$ 인 경우에는 $1 < \gcd(2y_1, n) \leq n$ 이다.

그런데

$$1 < \gcd(x_2 - x_1, n) < n, \quad 1 < \gcd(2y_1, n) < n$$

이면, $\gcd(x_2 - x_1, n)$ 과 $\gcd(2y_1, n)$ 은 1 도 아니고 n 도 아닌 n 의 인수이다.

보기 1 양의 정수 $n = 137703491$ 의 인수를 구해보자.

먼저 한 점 $P = (2, 1)$ 을 생각하고 타원곡선

$$E : y^2 = x^3 + bx + c \quad (b, c \in \mathbb{Z}_n)$$

을 생각하자. 이 때, $b = 1$ 인 경우에 $1^2 = 2^3 + 2 + c$ 이므로 $c = -9$ 이고 따라서 타원곡선의 방정식은 $y^2 = x^3 + x - 9$ 이다.

이제 $G(E, \mathbb{Z}_n)$ 에서 $r = 10, 20, 30, \dots$ 에 대하여 차례로 $r!P$ 를 계산하면,

$$20!P = (38765800, 102761480)$$

$$40!P = (73059078, 50101112)$$

이지만, $60!P$ 를 계산하는 과정에서

$$(98622427, 37062796) + (25032179, 18303780)$$

을 계산할 수 없게 된다. 이로부터

$$\gcd(98622427 - 25032179, n) = 17389$$

임을 얻고, 따라서 17389 는 $n = 137703491$ 의 인수이다.

보기 2 양의 정수 $n = 271811237833$ 의 인수를 구해보자.

타원곡선

$$E : y^2 = x^3 + bx + c \quad (b, c \in \mathbb{Z}_n)$$

을 생각하고 이 곡선 위의 점 $P = (2, 1)$ 을 택하자. 먼저 $b = 1$ 부터 시작하면 $b = -9$ 이고 아무런 어려움 없이 $20!P, 40!P, 60!P$ 를 계산할 수 있다.

이 단계에서 좀 더 큰 r 에 대한 $r!P$ 를 구하거나 다른 b 의 값을 정한다. 예를 들어 $b = 2$ 이라고 하면 $c = -11$ 이고, 이때 $G(E, \mathbb{Z}_n)$ 에서 아무런 어려움 없이 $20!P, 60!P, 80!P$ 를 계산할 수 있다.

또 다시 $b = 3$ 인 경우에 $c = -13$ 이고 이때 때 $G(E, \mathbb{Z}_n)$ 에서 $60!P$ 는 계산해낼 수 있으나 $80!P$ 를 계산하는 과정 중에서 덧셈

$$(16755565661, 260664116207) + (229018473606, 100653888225)$$

를 구할 수 없게 된다. 이 사실로부터

$$\gcd(16755565661 - 229018473606, n) = 2595377$$

을 얻게 되고 따라서 2595377 은 n 의 인수이다.

타원곡선을 이용한 정수의 인수분해에서 중요한 사항은 타원곡선을 선택하는 일과 kP 를 계산하는 일이다.

예를 들어, 타원곡선 $y^2 = x^3 + bx + 1$ 을 택하면, $P = (0, 1)$ 는 이 곡선 위에 있는 점이고 이때 b 의 값은 $b = 1$ 부터 시작하여 차례로 늘려간다.

다음에 $G(E, \mathbb{Z}_n)$ 에서 kP 를 계산하기 위하여 정수 k 를 택하는 가장 간단한 방법은 2부터 시작하여 특정한 양의 정수 r 까지의 정수를 정하여 차례로 $2!P, 3!P, 4!P, \dots, r!P$ 를 계산하는 방법이다. 이보다 나은 방법은 특정한 양의 정수 C 보다 작은 素數들의 곱을 k 로 택하는 방법이다. 예를 들어, p_1, p_2, \dots, p_r 가 특정한 정수 C 보다 작은 素數들 전체라고 할 때, $P_1 = p_1 P, P_2 = p_2 P_1, P_3 = p_3 P_2, \dots$ 을 차례로 계산한다.

이 때, 계산에 실패하면 n 의 인수를 구할 수 있으나, 성공적으로 $P_r = p_r P_{r-1}$ 까지 계산할 수 있는 경우에는 b 의 값을 바꾸어 또 다른 타원곡선에 대하여 이와 같은 절차를 되풀이한다.

알고리즘 1 (타원곡선 위의 점 P_1 에 대한 kP_1 구하기)

이 알고리즘은 $G(E, \mathbb{Z}_n)$ 에서 점 P_1 에 대하여 kP_1 을 계산한다.

이 계산이 실패할 때에는 이 알고리즘은 끝이 나고 실패가 일어난 두 점으로 돌아가게 된다. 아래에서 $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ 이라고 하자.

- (1) [시작] $P_2 = O$ 라고 놓는다.
- (2) $k = 0$ 이면 P_2 로 돌아와서 계산을 끝낸다.
- (3) [k 가 홀수인 경우] k 가 홀수이면, $d = \gcd(x_2 - x_1, n)$ 을 계산하고 $k-1$ 을 다시 k 로 놓는다. 여기서 $d = 1$ 일 때에는 $P_2 + P_1$ 을 계산하고 이 결과를 다시 P_2 로 놓은 다음에 단계 (2) 로 간다.

한편, $d \neq 1$ 일 때에는 알고리즘을 끝내고 P_1 과 P_2 로 되돌아간다.

- (4) [k 가 짝수인 경우] k 가 짝수이면, $d = \gcd(2y_1, n)$ 을 계산하고 $\frac{k}{2}$ 를 다시 k 로 놓는다. 여기서 $d = 1$ 일 때에는 $G(E, \mathbb{Z}_n)$ 에서 $2P_1$ 을 계산하고 이 결과를 P_1 으로 놓은 다음에 단계 (2)로 간다. 한편, $d \neq 1$ 일 때에는 알고리즘을 끝내고 P_1 으로 되돌아간다.

타원곡선을 이용한 인수분해에 대한 알고리즘은 다음과 같다.

알고리즘 2 (타원곡선을 이용한 정수 n 의 인수분해 알고리즘)

- (1) [素數 表 작성] 처음 m 개의 素數 전체의 집합 $T = \{p_1, p_2, \dots, p_m\}$ 를 정한다.
- (2) [시작] $b = 1$ 이라고 놓는다.
- (3) [타원곡선의 선택] $P = (0, 1)$, $i = 1$ 이라고 하고 타원곡선의 방정식

$$E : y^2 = x^3 + bx + 1$$
 을 택한다.
- (4) $i \leq m$ 이면, $k = p_i$ 로 놓는다. 한편, $i > m$ 이면, $b+1$ 을 다시 b 로 놓고 단계 (3) 으로 간다.
- (5) [kP 의 계산] $G(E, \mathbb{Z}_n)$ 에서 kP 를 계산하여 이 결과를 다시 P 로 놓는다. 이 때, 계산이 실패하는 경우에는 단계 (6) 으로 가고, 성공하는 경우에는 $i+1$ 을 다시 i 로 놓고 단계 (4)를 되풀이한다.
- (6) [인수 확인] 계산 과정에서 n 과의 최대공약수가 1 이 아닌 정수가 나타났는지를 조사한다.
 정수 n 의 인수를 구한 경우에는 그 인수로 되돌아가서 알고리즘을 끝내고 그렇지 않은 경우에는 단계 (3) 으로 되돌아간다.

보기 3 앞의 알고리즘에 따라 $n = 357564082969$ 의 인수를 구해보자.

먼저 T 를 처음 100 개의 素數 전체의 집합이라 하고 $b = 1$ 이라고 하자.
 다음에 $P = (0, 1)$, $i = 1$ 이라고 하고 타원곡선 $y^2 = x^3 + bx + 1$ 을 택한다.
 그리고 b 의 값은 $b = 1$ 부터 차례로 늘려간다.

이 때, $i = 1$ 및 $i = 2$ 일 때 이 알고리즘으로는 n 의 인수를 구할 수가 없다. 한편, $i = 3$ 인 경우에 $(149 \cdot 139 \cdot \dots \cdot 5 \cdot 3 \cdot 2)P$ 를 계산하는 과정에서

$$2(269927330530, 348260288613)$$

을 계산할 수가 없다. 여기서,

$$\gcd(348260288613, n) = 430811$$

이고, 따라서 430811 인 n 의 인수이다.

Latin 방진과 Euler 방진

농업 연구원이 세 품종의 배추 씨앗과 세 종류의 비료에 대하여 세 가지 토양에서의 씨앗의 발아율을 실험할 때, 세 토양을 1, 2, 3 으로 나타내고 다음과 같은 표를 이용하면 실험하려는 요소를 하나도 빠뜨리지 않고 또 겹치지 않게 조사할 수 있다.

	비료 1	비료 2	비료 3
씨앗 1	1	3	2
씨앗 2	2	1	3
씨앗 3	3	2	1

정의 1 양의 정수 n 에 대하여 $X_n = \{1, 2, \dots, n\}$ 이라고 하자.

그리고, $1, 2, \dots, n$ 의 원소를 성분으로 가지는 n 차의 행렬 중에서 각 행과 각 열에 $1, 2, \dots, n$ 이 꼭 한 번씩 나타나 있는 행렬을 **n 차의 Latin 방진**(方陣, square) 이라고 한다.

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$$

결국 n 차의 Latin 방진은 각 행과 각 열이 $1, 2, \dots, n$ 의 순열인 행렬을 의미한다. 특히, n 차의 Latin 방진 중에서 그 제 1 행의 원소와 제 1 열의 원소가 모두 $1, 2, \dots, n$ 을 크기 순으로 배열해 놓은 방진을 **표준화된** (standardized) **Latin 방진**이라고 한다.

보기 1 분명히 Latin 방진 2 차의 Latin 방진은 다음 두 행렬뿐이다.

$$\begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}, \quad \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$$

보기 2 다음은 모두 3 차의 Latin 방진이다(문제 1 참조).

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 3 & 2 \\ 2 & 1 & 3 \\ 3 & 2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 3 & 2 \\ 3 & 2 & 1 \\ 2 & 1 & 3 \end{bmatrix}$$

이 중에서 처음 행렬은 표준화된 3 차의 Latin 방진이다.

보기 3 표준화된 4 차의 Latin 방진은 다음 네 가지뿐이다.

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \\ 3 & 1 & 4 & 2 \\ 4 & 3 & 2 & 1 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 2 & 1 \\ 4 & 3 & 1 & 2 \end{bmatrix}$$

정리 2 임의의 양의 정수 n 에 대하여 n 차의 Latin 방진이 적어도 존재한다.

실제로, 각 정수 i, j ($1 \leq i, j \leq n$)에 대하여 $i+j-1$ 을 n 으로 나누었을 때의 나머지를 a_{ij} 라고 하면, $A = [a_{ij}]_{n \times n}$ 는 다음과 같은 n 차의 Latin 방진이다.

$$A = \begin{bmatrix} 1 & 2 & \cdots & n-1 & n \\ 2 & 3 & \cdots & n & 1 \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ n & 1 & \cdots & n-2 & n-1 \end{bmatrix}$$

증명 가정에 의하여 $a_{ij} \equiv i+j-1 \pmod{n}$ 이므로 A 는 정리와 같고 또 다음이 성립한다(정리 3.1.3 참조).

$$a_{ij} = a_{ik} \implies i+j-1 \equiv i+k-1 \pmod{n} \implies j=k$$

$$a_{ij} = a_{kj} \implies i+j-1 \equiv k+j-1 \pmod{n} \implies i=k$$

따라서 A 의 각 행과 각 열에는 $1, 2, \dots, n$ 이 꼭 한 번씩 나타나 있으므로 A 는 n 차의 Latin 방진이다.

서로 다른 n 차의 Latin 방진의 개수를 $L(n)$ 으로 나타낼 때, 다음 결과가 알려져 있다.

$$\begin{aligned} L(1) &= 1, & L(2) &= 2, & L(3) &= 12, \\ L(4) &= 576, & L(5) &= 161280, & L(6) &= 812851200 \\ L(n) &\geq n! \cdot (n-1)! \cdot (n-2)! \cdots 3! \cdot 2! \cdot 1 \end{aligned}$$

정의 3 두 n 차의 Latin 방진 $A = [a_{ij}]_{n \times n}$, $B = [b_{ij}]_{n \times n}$ 에 대하여 n^2 개의 순서쌍 (a_{ij}, b_{ij}) 가 모두 서로 다를 때, A 와 B 는 서로 직교한다 (直交, orthogonal)고 하고 또 이때 n 차의 행렬

$$\begin{bmatrix} (a_{11}, b_{11}) & (a_{12}, b_{12}) & \cdots & (a_{1n}, b_{1n}) \\ (a_{21}, b_{21}) & (a_{22}, b_{22}) & \cdots & (a_{2n}, b_{2n}) \\ \vdots & \vdots & \cdots & \vdots \\ (a_{n1}, b_{n1}) & (a_{n2}, b_{n2}) & \cdots & (a_{nn}, b_{nn}) \end{bmatrix}$$

를 n 차의 **오일러 방진**(Euler square)이라고 한다.

보기 4 두 2 차의 Latin 방진

$$\begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}, \quad \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$$

는 서로 직교하지 않으므로, 2 차의 Euler 방진은 존재하지 않는다.

그리고, 다음 두 3 차의 Latin 방진은 서로 직교한다.

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix}$$

따라서 이로부터 다음과 같은 3 차의 Euler 방진을 얻는다.

$$C = \begin{bmatrix} (1,1) & (2,2) & (3,3) \\ (2,3) & (3,1) & (1,2) \\ (3,2) & (1,3) & (2,1) \end{bmatrix}$$

세 종류의 세탁기와 세 가지 세탁기용 세제에 알맞은 온도와 물의 경도를 실험할 때, 세 가지 온도를 1, 2, 3 으로 나타내고 물의 경도를 1, 2, 3 으로 나타내어 보기 4 의 Euler 방진 C 를 이용하면 실험하려는 요소를 하나도 빠짐없이 겹치지 않게 조사할 수 있다.

보기 5 다음 두 3 차의 Latin 방진 A, B 는 서로 직교하지 않는다.

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}, \quad B = \begin{bmatrix} 2 & 1 & 3 \\ 1 & 3 & 2 \\ 3 & 2 & 1 \end{bmatrix}$$

실제로, 이 두 행렬의 대응하는 성분으로 이루어진 순서쌍은

$$(1, 2), (2, 1), (3, 3), (2, 1), (3, 3), (3, 3), (1, 2), (2, 1)$$

과 같이 세 순서쌍 $(1, 2), (2, 1), (3, 3)$ 이 되풀이되어 나타난다.

보기 6 다음 두 행렬 A, B 는 서로 직교하는 4 차의 Latin 방진이다.

$$A = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \end{bmatrix}$$

따라서 이 두 Latine 방진을 이용하여 4 차의 Euler 방진을 얻는다.

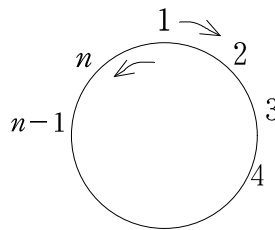
정리 4 모든 홀수 n 에 대하여 서로 직교하는 두 n 차의 Latin 방진 A, B 가 존재하고 따라서 n 차의 Euler 방진이 존재한다.

증 명 오른쪽 그림과 같이 제 1 행에 차례로 $1, 2, \dots, n$ 을 늘어놓고 각 $j = 1, 2, \dots, n$ 에 대하여 제 j 열에는 j 부터 시작하여

$$j, j+1, \dots, n, 1, \dots, j-1$$

을 늘어놓아 만든 n 차의 행렬을 A 라고 하자.

다음에 제 1 행에 차례로 $1, 2, \dots, n$ 을 늘어놓고 각 $j = 1, 2, \dots, n$ 에 대하여 제 j 열에는 j 부터 시작하여



$$j, j-1, \dots, 2, 1, n, \dots, j+1$$

을 늘어놓아 만든 n 차의 행렬을 B 라고 하자. 이 때, 두 Latin 방진 A, B 는 서로 직교하고, 따라서 이로부터 n 차의 Euler 방진을 얻는다.

보기 7 다음은 정리 17.5.4의 증명 방법과 같은 방법으로 서로 직교하는 5 차의 Latin 방진으로 만들어 얻은 5 차의 Euler 방진이다.

$$\begin{bmatrix} (1,1) & (2,2) & (3,3) & (4,4) & (5,5) \\ (2,5) & (3,1) & (4,2) & (5,3) & (1,4) \\ (3,4) & (4,5) & (5,1) & (1,2) & (2,3) \\ (4,3) & (5,4) & (1,5) & (2,1) & (3,2) \\ (5,2) & (1,3) & (2,4) & (3,5) & (4,1) \end{bmatrix}$$

Euler 는 이른바 ‘36 명의 사관의 문제’라고 불리는 6 차의 Euler 방진의 존재에 관한 문제를 1779 년에 제기하였고 이러한 방진이 존재하지 않을 것으로 예상하였으며, Terry 가 1899 년에 이 예상이 옳았음을 증명하였다.

그리고 1959 년에 $n > 6$ 인 모든 정수 n 에 대하여 n 차의 Euler 방진이 적어도 하나 존재한다는 사실이 증명되었다.

정의 5 집합 $X_n = \{1, 2, \dots, n\}$ 에 대하여 사상 $\sigma : X_n \longrightarrow X_n$ 가 일대일 대응일 때, σ 를 X_n 위의 **치환**(置換, permutation) 이라고 한다.
치환 $\sigma : X_n \longrightarrow X_n$ 를 다음과 같이 나타내기로 한다.

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

예를 들면, 치환 $\sigma : \{1, 2, 3\} \longrightarrow \{1, 2, 3\}$ 에 대하여

$$\sigma(1) = 2, \quad \sigma(2) = 3, \quad \sigma(3) = 1$$

일 때, σ 를 다음과 같이 나타낸다.

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

집합 $X_n = \{1, 2, \dots, n\}$ 위의 치환은 모두 $n!$ 개 존재한다(정리 4.3.3).

정의 6 집합 $X_n = \{1, 2, \dots, n\}$ 의 원소를 성분으로 가지는 행렬

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

과 치환 $\sigma : X_n \longrightarrow X_n$ 에 대하여 행렬 $\sigma(A)$ 은 다음과 같은 행렬을 뜻한다.

$$\sigma(A) = \begin{bmatrix} \sigma(a_{11}) & \sigma(a_{12}) & \cdots & \sigma(a_{1n}) \\ \sigma(a_{21}) & \sigma(a_{22}) & \cdots & \sigma(a_{2n}) \\ \vdots & \vdots & \cdots & \vdots \\ \sigma(a_{n1}) & \sigma(a_{n2}) & \cdots & \sigma(a_{nn}) \end{bmatrix}$$

보기 8 다음 두 행렬은 서로 직교하는 3 차의 Latin 방진이다.

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix}$$

그리고 두 치환

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

에 대하여 $\sigma(A)$ 와 $\tau(B)$ 는 다음과 같은 3 차의 Latin 방진이다.

$$\sigma(A) = \begin{bmatrix} 2 & 3 & 1 \\ 3 & 1 & 2 \\ 1 & 2 & 3 \end{bmatrix}, \quad \tau(B) = \begin{bmatrix} 2 & 1 & 3 \\ 3 & 2 & 1 \\ 1 & 3 & 2 \end{bmatrix}$$

여기서, $\sigma(A)$ 와 $\tau(B)$ 는 서로 직교하는 3 차의 Latin 방진이다.

위의 보기에서 본 바와 같이, 일반적으로 서로 직교하는 Latin 방진에 대하여 다음 정리가 성립한다.

정리 7 집합 $X_n = \{1, 2, \dots, n\}$ 의 원소를 성분으로 가지는 n 차의 행렬 $A = [a_{ij}]_{n \times n}$, $B = [b_{ij}]_{n \times n}$ 에 대하여 다음이 성립한다.

- (1) A 가 n 차의 Latin 방진이면, 임의의 치환 $\sigma : X_n \rightarrow X_n$ 에 대하여 $\sigma(A)$ 는 n 차의 Latin 방진이다.
- (2) A, B 가 서로 직교하는 n 차의 Latin 방진일 때, 임의의 두 치환

$$\sigma : X_n \rightarrow X_n, \quad \tau : X_n \rightarrow X_n$$

에 대하여 $\sigma(A), \tau(B)$ 는 서로 직교하는 n 차의 Latin 방진이다.

증명 (1) A 가 n 차의 Latin 방진일 때, 각 정수 i, j ($1 \leq i, j \leq n$)에 대하여 다음이 성립한다.

$$\begin{aligned} \sigma(a_{ij}) = \sigma(a_{ik}) &\Rightarrow a_{ij} = a_{ik} \Rightarrow j = k \\ \sigma(a_{ij}) = \sigma(a_{kj}) &\Rightarrow a_{ij} = a_{kj} \Rightarrow i = k \end{aligned}$$

따라서 $\sigma(A)$ 는 n 차의 Latin 방진이다.

- (2) 두 행렬 A, B 가 서로 직교하는 n 차의 Latin 방진일 때, 각 정수 i, j ($1 \leq i, j \leq n$)에 대하여 다음이 성립한다.

$$\begin{aligned} (\sigma(a_{ij}), \tau(b_{ij})) &= (\sigma(a_{ks}), \tau(b_{ks})) \\ \Rightarrow \sigma(a_{ij}) &= \sigma(a_{ks}), \quad \tau(b_{ij}) = \tau(b_{ks}) \\ \Rightarrow a_{ij} &= a_{ks}, \quad b_{ij} = b_{ks} \Rightarrow i = k, \quad j = s \end{aligned}$$

따라서 $\sigma(A), \tau(B)$ 는 서로 직교하는 n 차의 Latin 방진이다.

정의 8 정수 $n (\geq 2)$ 에 대하여 $t (\geq 2)$ 개의 n 차의 Latin 방진 A_1, A_2, \dots, A_t 가 둘 씩 서로 직교할 때, 즉 모든 i, j ($1 \leq i \neq j \leq t$)에 대하여 A_i, A_j 가 서로 직교할 때, A_1, A_2, \dots, A_t 는 **쌍마다 직교한다** (mutually orthogonal)고 한다.

정리 9 정수 $n (\geq 2)$ 에 대하여 n 차의 Latin 방진

$$A_1 = [a_{1ij}]_{n \times n}, A_2 = [a_{2ij}]_{n \times n}, \dots, A_t = [a_{tij}]_{n \times n}$$

가 쌍마다 서로 직교하면 $2 \leq t \leq n-1$ 이다.

증 명 적당한 치환

$$\sigma_1 : X_n \longrightarrow X_n, \sigma_2 : X_n \longrightarrow X_n, \cdots, \sigma_t : X_n \longrightarrow X_n$$

를 택하여, t 개의 행렬

$$\sigma_1(A_1), \sigma_2(A_2), \cdots, \sigma_t(A_t)$$

의 제 1 행의 성분이 모두 차례로 $1, 2, \cdots, n$ 이 되도록 할 수 있고 이때 정리 7 에 의하여 $\sigma_1(A_1), \sigma_2(A_2), \cdots, \sigma_t(A_t)$ 는 쌍마다 서로 직교하는 Latin 방진이다.

$$\sigma_1(A_1) = \begin{bmatrix} 1 & 2 & \cdots & n \\ * & * & \cdots & * \\ \vdots & \vdots & \cdots & \vdots \\ * & * & \cdots & * \end{bmatrix}, \cdots, \sigma_t(A_t) = \begin{bmatrix} 1 & 2 & \cdots & n \\ * & * & \cdots & * \\ \vdots & \vdots & \cdots & \vdots \\ * & * & \cdots & * \end{bmatrix}$$

한편, 위의 t 개의 행렬의 $(2, 1)$ 성분인 t 개의 원소

$$\sigma_1(a_{121}), \sigma_2(a_{221}), \cdots, \sigma_t(a_{t21})$$

는 모두 서로 다르다. 실제로, 서로 다른 k, s 에 대하여

$$\sigma_k(a_{k21}) = \sigma_s(a_{s21}) = j$$

이라고 가정하면,

$$(\sigma_k(a_{k21}), \sigma_s(a_{s21})) = (j, j) = (\sigma_k(a_{klj}), \sigma_s(a_{slj}))$$

으로 되어 $\sigma_k(A_k), \sigma_s(A_s)$ 가 서로 직교한다는 사실에 모순된다.

그런데, 각 행렬 $\sigma_i(A_i)$ 의 제 1 열에는 $1, 2, \cdots, n$ 이 한 번씩 나타나고 또 $\sigma_i(a_{i11}) = 1$ 즉 $\sigma_i(A_i)$ 의 $(1, 1)$ 성분은 1 이므로

$$2 \leq \sigma_i(a_{i21}) \leq n \quad (1 \leq i \leq t)$$

이어야 하고, 따라서 $2 \leq t \leq n-1$ 이다.

정의 10 정수 n (≥ 2) 에 대하여 $n-1$ 개의 서로 직교하는 n 차의 Latin 방진 $L_1, L_2, \cdots, L_{n-1}$ 이 존재할 때, $L_1, L_2, \cdots, L_{n-1}$ 은 n 차의 Latin 방진의 **완비직교계**(完備直交系, complete orthogonal system)를 이룬다고 한다.

보기 9 다음 세 행렬은 4 차의 Latin 방진의 완비 직교계이다.

$$L_1 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{bmatrix}, \quad L_2 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \end{bmatrix}, \quad L_3 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{bmatrix}$$

정리 11 임의의 素數 p 에 대하여 체 $\mathbb{F}_p = \{0, 1, \dots, p-1\}$ 의 원소를

$$a_0 = 0, a_1, a_2, \dots, a_{p-1}$$

이라고 하면 다음과 같은 체 \mathbb{F}_p 위의 p 차의 행렬 L_1, L_2, \dots, L_{p-1} 은 p 차의 Latin 방진의 완비직교계를 이룬다.

$$L_k = \begin{bmatrix} a_0 & a_1 & \cdots & a_{p-1} \\ a_k a_1 + a_0 & a_k a_2 + a_1 & \cdots & a_k a_{p-1} + a_{p-2} \\ a_k a_2 + a_0 & a_k a_3 + a_1 & \cdots & a_k a_{p-1} + a_{p-2} \\ \vdots & \vdots & \cdots & \vdots \\ a_k a_{p-1} + a_0 & a_k a_{p-1} + a_1 & \cdots & a_k a_{p-1} + a_{p-2} \end{bmatrix} \quad (1 \leq k \leq p-1)$$

증 명 각 k ($1 \leq k \leq p-1$) 에 대하여, $a_k \neq 0$ 이므로 L_k 는 체 \mathbb{F}_p 위의 p 차의 Latin 방진이다. 그리고 각 k ($1 \leq k \leq p-1$) 에 대하여

$$a_{kij} = a_k a_{i-1} + a_{j-1} \quad (1 \leq i \leq p-1, 1 \leq j \leq p)$$

이라고 하면, $1 \leq k \neq r \leq p-1$ 일 때 다음 조건은 서로 동치이다.

- (1) $(a_{kij}, a_{rij}) = (a_{kst}, a_{rst})$
- (2) $(a_k a_{i-1} + a_{j-1}, a_r a_{i-1} + a_{j-1}) = (a_k a_{s-1} + a_{t-1}, a_r a_{s-1} + a_{t-1})$
- (3) $a_k a_{i-1} + a_{j-1} = a_k a_{s-1} + a_{t-1}, \quad a_r a_{i-1} + a_{j-1} = a_r a_{s-1} + a_{t-1}$
- (4) $a_k (a_{i-1} - a_{s-1}) = a_{j-1} - a_{t-1} = a_r (a_{i-1} - a_{s-1})$
- (5) $a_{i-1} = a_{s-1}, \quad a_{j-1} = a_{t-1} \quad \Leftrightarrow \quad i = s, j = t$

따라서 L_1, L_2, \dots, L_{p-1} 은 쌍마다 서로 직교한다.

보기 10 체 $\mathbb{F}_3 = \{0, 1, 2\}$ 에 대하여 정리 11 을 적용하면, 다음과 같은 3 차의 Latin 방진의 완비직교계를 얻는다.

$$A = \begin{bmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{bmatrix}$$

Latin 방진 A 는 그대로 두고, B 의 제 1 행의 성분 $0, 1, 2$ 를 $0, 2, 1$ 로 바꿔 놓기 위하여 B 에 치환 $\sigma = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 2 & 1 \end{pmatrix}$ 을 시행하면

$$A = \begin{bmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{bmatrix}, \quad \sigma(B) = \begin{bmatrix} 0 & 2 & 1 \\ 1 & 0 & 2 \\ 2 & 1 & 0 \end{bmatrix}$$

이고 이때 $A, \tau(B)$ 는 3 차의 Latin 방진의 완비 직교계이다.

보기 11 체 $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$ 에 대하여 정리 11 을 적용하면, 다음과 같은 5 차의 Latin 방진의 완비직교계를 얻는다.

$$L_1 = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \\ 2 & 3 & 4 & 0 & 1 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \end{bmatrix}, \quad L_2 = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 0 & 1 \\ 4 & 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 & 0 \\ 3 & 4 & 0 & 1 & 2 \end{bmatrix}$$

$$L_3 = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 3 & 4 & 0 & 1 & 2 \\ 1 & 2 & 3 & 4 & 0 \\ 4 & 0 & 1 & 2 & 3 \\ 2 & 3 & 4 & 0 & 1 \end{bmatrix}, \quad L_4 = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 4 & 0 & 1 & 2 & 3 \\ 3 & 4 & 0 & 1 & 2 \\ 2 & 3 & 4 & 0 & 1 \\ 1 & 2 & 3 & 4 & 0 \end{bmatrix}$$

그리고 L_1, L_2 로부터 다음과 같은 5 차의 Euler 방진을 얻는다.

$$\begin{bmatrix} (0,0) & (1,1) & (2,2) & (3,3) & (4,4) \\ (1,2) & (2,3) & (3,4) & (4,0) & (0,1) \\ (2,4) & (3,0) & (4,1) & (0,2) & (1,3) \\ (3,1) & (4,2) & (0,3) & (1,4) & (2,0) \\ (4,3) & (0,4) & (1,0) & (2,1) & (3,2) \end{bmatrix}$$

서로 직교하는 두 6 차의 Latin 방진은 존재하지 않으므로 6 차의 Latin 방진의 완비직교계는 존재하지 않는다(보기 7).

그리고, 10 차의 Latin 방진의 완비직교계도 존재하지 않는다는 사실이 알려져 있다.

다음 정리의 증명은 생략한다(정리 10, [9]의 정리 3.7.9, 정리 3.7.13).

정리 12 정수 n ($n \geq 2$)에 대하여 다음 세 조건은 서로 동치이다.

- (1) n 차의 Latin 방진의 완비 직교계가 존재한다.
- (2) 위수 n 인 아핀평면이 존재한다.
- (3) 위수 n 인 사영평면이 존재한다.

연 습 문 제

1. 3 차의 Latin 방진을 모두 12 개 존재한다. 이들을 모두 구하여라.
2. 다음 두 Latin 방진 A, B 가 서로 직교하는지 판정하여라.

$$(1) A = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}, \quad B = \begin{bmatrix} 3 & 1 & 2 \\ 2 & 3 & 1 \\ 1 & 2 & 3 \end{bmatrix}$$

$$(2) A = \begin{bmatrix} 2 & 1 & 3 \\ 3 & 2 & 1 \\ 1 & 3 & 2 \end{bmatrix}, \quad B = \begin{bmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$$

3. 다음 두 Latin 방진 A, B 가 서로 직교함을 확인하여라.

$$A = \begin{bmatrix} 4 & 2 & 3 & 1 \\ 2 & 4 & 1 & 3 \\ 3 & 1 & 4 & 2 \\ 1 & 3 & 2 & 4 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 3 & 4 & 2 \\ 4 & 2 & 1 & 3 \\ 2 & 4 & 3 & 1 \\ 3 & 1 & 2 & 4 \end{bmatrix}$$

그리고 적당한 치환 σ, τ 를 정하여, $\sigma(A)$ 의 제 1 행의 성분과 $\tau(B)$ 의 제 1 행의 성분이 모두 차례로 1, 2, 3, 4가 되도록 변형하여라.

4. 정리 17.5.4를 이용하여 7 차의 Euler 방진을 구하여라.

5. 행렬 A 가 n 차의 Latin 방진일 때, 다음이 성립함을 증명하여라.

- (1) A 의 서로 다른 두 행을 맞바꾸어 얻은 행렬은 Latin 방진이다.
 (2) A 의 서로 다른 두 열을 맞바꾸어 얻은 행렬은 Latin 방진이다.

6. 체 $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ 에 정리 17.5.11 을 적용하여 7 차의 Latin 방진의 완비직교계를 구하여라.

7. 체 $\mathbb{F}_{11} = \{0, 1, 2, 3, \dots, 10\}$ 에 정리 11 을 적용하여 11 차의 Latin 방진의 완비직교계를 구하여라.

8. 다음 두 행렬 A, B 가 서로 직교하는 5 차의 Latin 방진이 되도록 A, B 의 비어 있는 성분을 채워라.

$$A = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & & & & \\ 3 & & & & \\ 4 & & & & \\ 5 & & & & \end{bmatrix}, \quad B = \begin{bmatrix} 1 & & & & \\ & 2 & & & \\ & & 3 & & \\ & & & 4 & \\ & & & & 5 \end{bmatrix}$$

9. 다음 Latin 방진 A 에 대하여 A 와 그 전치행렬 A^T 가 서로 직교하는지를 판정하여라.

$$(1) \quad A = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix} \quad (2) \quad A = \begin{bmatrix} 2 & 1 & 3 \\ 3 & 2 & 1 \\ 1 & 3 & 2 \end{bmatrix}$$

10. 다음 Latin 방진 A 에 대하여 A 와 그 전치행렬 A^T 가 서로 직교하는지를 판정하여라.

$$A = \begin{bmatrix} 1 & 3 & 4 & 2 \\ 4 & 2 & 1 & 3 \\ 2 & 4 & 3 & 1 \\ 3 & 1 & 2 & 4 \end{bmatrix}$$

연 습 문 제 풀 이

1.

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 3 & 2 \\ 2 & 1 & 3 \\ 3 & 2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 3 & 2 \\ 3 & 2 & 1 \\ 2 & 1 & 3 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 1 & 3 \\ 1 & 3 & 2 \\ 3 & 2 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 1 & 3 \\ 3 & 2 & 1 \\ 1 & 3 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 3 & 1 \\ 3 & 1 & 2 \\ 1 & 2 & 3 \end{bmatrix}$$

$$\begin{bmatrix} 3 & 1 & 2 \\ 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}, \begin{bmatrix} 3 & 1 & 2 \\ 2 & 3 & 1 \\ 1 & 2 & 3 \end{bmatrix}, \begin{bmatrix} 3 & 2 & 1 \\ 1 & 3 & 2 \\ 2 & 1 & 3 \end{bmatrix}, \begin{bmatrix} 3 & 2 & 1 \\ 2 & 1 & 3 \\ 1 & 3 & 2 \end{bmatrix}$$

2. 두 행렬

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}, \quad B = \begin{bmatrix} 3 & 1 & 2 \\ 2 & 3 & 1 \\ 1 & 2 & 3 \end{bmatrix}$$

는 직교한다. 그리고,

$$\begin{bmatrix} (1,3) & (2,1) & (3,2) \\ (2,2) & (3,3) & (1,1) \\ (3,1) & (1,2) & (2,3) \end{bmatrix}$$

는 Euler 방진이다.

(2) 두 행렬

$$A = \begin{bmatrix} 2 & 1 & 3 \\ 3 & 2 & 1 \\ 1 & 3 & 2 \end{bmatrix}, \quad B = \begin{bmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$$

은 직교하지 않는다.

$$\begin{bmatrix} (2,2) & (1,3) & (3,1) \\ (3,1) & (2,2) & (1,3) \\ (1,3) & (3,1) & (2,2) \end{bmatrix}$$

3. 두 Latin 방진

$$A = \begin{bmatrix} 4 & 2 & 3 & 1 \\ 2 & 4 & 1 & 3 \\ 3 & 1 & 4 & 2 \\ 1 & 3 & 2 & 4 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 3 & 4 & 2 \\ 4 & 2 & 1 & 3 \\ 2 & 4 & 3 & 1 \\ 3 & 1 & 2 & 4 \end{bmatrix}$$

는 직교한다.

$$\begin{bmatrix} (4,1) & (2,3) & (3,4) & (1,2) \\ (2,4) & (4,2) & (1,1) & (3,3) \\ (3,2) & (1,4) & (4,3) & (2,1) \\ (1,3) & (3,1) & (2,2) & (4,4) \end{bmatrix}$$

그리고, 치환 σ, τ 를

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$$

으로 정하면, $\sigma(A), \tau(B)$ 는 다음과 같다.

$$\sigma(A) = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{bmatrix}, \quad \tau(B) = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{bmatrix}$$

4. 정리 17.5.4를 이용하면 다음과 같은 7차의 Euler 방진을 얻는다.

$$\begin{bmatrix} (1,1) & (2,2) & (3,3) & (4,4) & (5,5) & (6,6) & (7,7) \\ (2,7) & (3,1) & (4,2) & (5,3) & (6,4) & (7,5) & (1,6) \\ (3,6) & (4,7) & (5,1) & (6,2) & (7,3) & (1,4) & (2,5) \\ (4,5) & (5,6) & (6,7) & (7,1) & (1,2) & (2,3) & (3,4) \\ (5,4) & (6,5) & (7,6) & (1,7) & (2,1) & (3,2) & (4,3) \\ (6,3) & (7,4) & (1,5) & (2,6) & (3,7) & (4,1) & (5,2) \\ (7,2) & (1,3) & (2,4) & (3,5) & (4,6) & (5,7) & (6,1) \end{bmatrix}$$

5. (1) 행렬 A 의 제 i 행과 제 j 행을 맞바꾸어 놓은 행렬을 B 라고 하면,
 B 의 제 i 행과 제 j 행은 각각 A 의 제 j 행과 제 i 행이고 나머지 행은
 A 의 행과 일치하므로 B 의 각 행에는 $1, 2, \dots, n$ 이 한 번씩 나타나고,
또 B 의 각 열의 i 번째 성분과 j 번째 성분만이 위치가 바뀌므로 각 열
에는 $1, 2, \dots, n$ 이 한 번씩 나타난다. 따라서 B 는 Latin 방진이다.
(2) 위의 (1)과 마찬가지로, A 의 서로 다른 두 열을 맞바꾸어 얻은
행렬은 Latin 방진임을 알 수 있다.

6. 체 $F_7 = \{0, 1, 2, 3, 4, 5, 6\}$ 에 정리 11을 적용하여 7차의 Latin 방진의
완비직교계를 얻는다.

$$\begin{aligned}
 L_1 &= \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 & 0 \\ 2 & 3 & 4 & 5 & 6 & 0 & 1 \\ 3 & 4 & 5 & 6 & 0 & 1 & 2 \\ 4 & 5 & 6 & 0 & 1 & 2 & 3 \\ 5 & 6 & 0 & 1 & 2 & 3 & 4 \\ 6 & 0 & 1 & 2 & 3 & 4 & 5 \end{bmatrix}, \quad L_2 = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 0 & 1 \\ 4 & 5 & 6 & 0 & 1 & 2 & 3 \\ 6 & 0 & 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 & 6 & 0 \\ 3 & 4 & 5 & 6 & 0 & 2 & 3 \\ 5 & 6 & 0 & 1 & 2 & 3 & 4 \end{bmatrix}, \\
 L_3 &= \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 0 & 1 & 2 \\ 6 & 0 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 0 & 1 \\ 5 & 6 & 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 5 & 6 & 0 \\ 4 & 5 & 6 & 0 & 1 & 2 & 3 \end{bmatrix}, \quad L_4 = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 & 5 & 6 & 0 \\ 5 & 6 & 0 & 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 5 & 6 & 0 & 1 \\ 6 & 0 & 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 6 & 0 & 1 & 2 \end{bmatrix}, \\
 L_5 &= \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 0 & 1 & 2 & 3 & 4 \\ 3 & 4 & 5 & 6 & 0 & 1 & 2 \\ 1 & 2 & 3 & 4 & 5 & 6 & 0 \\ 6 & 0 & 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 6 & 0 & 1 & 2 & 3 \\ 2 & 3 & 4 & 5 & 6 & 0 & 1 \end{bmatrix}, \quad L_6 = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 0 & 1 & 2 & 3 & 4 & 5 \\ 5 & 6 & 0 & 1 & 2 & 3 & 4 \\ 4 & 5 & 6 & 0 & 1 & 2 & 3 \\ 3 & 4 & 5 & 6 & 0 & 1 & 2 \\ 2 & 3 & 4 & 5 & 6 & 0 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 0 \end{bmatrix}
 \end{aligned}$$

9. Latin 방진 A 에 대하여

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}, \quad A^T = A = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}$$

는 서로 직교하지 않는다.

$$\begin{bmatrix} (1,1) & (2,2) & (3,3) \\ (2,2) & (3,3) & (1,1) \\ (3,3) & (1,1) & (2,2) \end{bmatrix}$$

(2) 두 행렬

$$A = \begin{bmatrix} 2 & 1 & 3 \\ 3 & 2 & 1 \\ 1 & 3 & 2 \end{bmatrix}, \quad A^T = \begin{bmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$$

는 서로 직교하지 않는다.

$$\begin{bmatrix} (2,2) & (1,3) & (3,1) \\ (3,1) & (2,2) & (1,3) \\ (1,3) & (3,1) & (2,2) \end{bmatrix}$$

10. 다음 Latin 방진 A 에 대하여

$$A = \begin{bmatrix} 1 & 3 & 4 & 2 \\ 4 & 2 & 1 & 3 \\ 2 & 4 & 3 & 1 \\ 3 & 1 & 2 & 4 \end{bmatrix}, \quad A^T = \begin{bmatrix} 1 & 4 & 2 & 3 \\ 3 & 2 & 4 & 1 \\ 4 & 1 & 3 & 2 \\ 2 & 3 & 1 & 4 \end{bmatrix},$$

는 서로 직교한다.

$$A = \begin{bmatrix} (1,1) & (3,4) & (4,2) & (2,3) \\ (4,3) & (2,2) & (1,4) & (3,1) \\ (2,4) & (4,1) & (3,3) & (1,2) \\ (3,2) & (1,3) & (2,1) & (4,4) \end{bmatrix}$$

Latin 방진과 사영평면

정수 n ($n \geq 2$) 에 대하여 다음 세 조건은 서로 동치이다(정리 10.3.11).

- (1) n 차의 Latin 방진의 완비직교계가 존재한다.
- (2) 위수 n 인 아핀평면이 존재한다.
- (3) 위수 n 인 사영평면이 존재한다.

이제 다음과 같은 n 차의 행렬 L_1, L_2, \dots, L_{n-1} 이 n 차의 Latin 방진의 완비직교계를 이룬다고 하자.

$$L_1 = \begin{bmatrix} a_{1,11} & a_{1,12} & \cdots & a_{1,1n} \\ a_{1,21} & a_{1,22} & \cdots & a_{1,2n} \\ \vdots & \vdots & \cdots & \vdots \\ a_{1,n1} & a_{1,n2} & \cdots & a_{1,nn} \end{bmatrix}, \quad L_2 = \begin{bmatrix} a_{2,11} & a_{2,12} & \cdots & a_{2,1n} \\ a_{2,21} & a_{2,22} & \cdots & a_{2,2n} \\ \vdots & \vdots & \cdots & \vdots \\ a_{2,n1} & a_{2,n2} & \cdots & a_{2,nn} \end{bmatrix},$$

$$\cdots, \quad L_{n-1} = \begin{bmatrix} a_{n-1,11} & a_{n-1,12} & \cdots & a_{n-1,1n} \\ a_{n-1,21} & a_{n-1,22} & \cdots & a_{n-1,2n} \\ \vdots & \vdots & \cdots & \vdots \\ a_{n-1,n1} & a_{n-1,n2} & \cdots & a_{n-1,nn} \end{bmatrix}$$

이 때, 다음 절차에 따라 위수 n 인 아핀평면과 위수 n 인 사영평면을 결정할 수 있다.

단계 1 : 다음과 같이 $n+1$ 개의 행과 n^2 개의 열로 이루어진 표를 만든다.

1	1	\cdots	1	2	2	\cdots	2	\cdots	n	n	\cdots	n
1	2	\cdots	n	1	2	\cdots	n	\cdots	1	2	\cdots	n
$a_{1,11}$	$a_{1,12}$	\cdots	$a_{1,1n}$	$a_{1,21}$	$a_{1,22}$	\cdots	$a_{1,2n}$	\cdots	$a_{1,n1}$	$a_{1,n2}$	\cdots	$a_{1,nn}$
$a_{2,11}$	$a_{2,12}$	\cdots	$a_{2,1n}$	$a_{2,21}$	$a_{2,22}$	\cdots	$a_{2,2n}$	\cdots	$a_{2,n1}$	$a_{2,n2}$	\cdots	$a_{2,nn}$
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\cdots	\vdots	\vdots	\vdots	\vdots
$a_{n-1,11}$	\cdots	$a_{n-1,1n}$	$a_{n-1,21}$	\cdots	$a_{n-1,2n}$	\cdots	$a_{n-1,n1}$	\cdots	$a_{n-1,n1}$	\cdots	$a_{n-1,nn}$	

여기서 제 3 행, ..., 제 $n+1$ 행은 각각 L_1, \dots, L_{n-1} 의 n 개의 행의 성분을 차례로 늘어놓은 것이다.

단계 2 : 위의 표에 열의 번호 $1, 2, \dots, n, \dots, n^2$ 을 추가한다.

1	2	...	n	$n+1$	$n+2$...	$2n$...	$(n-1)n+1$	$n+1$	n^2
1	1	...	1	2	2	...	2	...	n	n	n
1	2	...	n	1	2	...	n	...	1	2	n
$a_{1,11}$	$a_{1,12}$...	$a_{1,1n}$	$a_{1,21}$	$a_{1,22}$...	$a_{1,2n}$...	$a_{1,n1}$	$a_{1,n2}$	$a_{1,nn}$
$a_{2,11}$	$a_{2,12}$...	$a_{2,1n}$	$a_{2,21}$	$a_{2,22}$...	$a_{2,2n}$...	$a_{2,n1}$	$a_{2,n2}$	$a_{2,nn}$
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	...	\vdots	\vdots	\vdots	\vdots	\vdots
$a_{n-1,11}$	$a_{n-1,1n}$	$a_{n-1,21}$	$a_{n-1,2n}$...	$a_{n-1,n1}$	$a_{n-1,nn}$

단계 3 : 각 정수 r, i ($1 \leq r \leq n+1, 1 \leq i \leq n$) 에 대하여 위의 표의 제 r 행에서 i 를 포함하는 열의 번호 전체로 이루어진 집합을 $L_{r,i}$ 로 나타낸다.

단계 4 : 다음과 같이 정의된 결합구조 $\alpha = (\mathcal{P}, \mathcal{L})$ 는 위수 n 인 아핀 평면이다.

$$\mathcal{P} = \{1, 2, \dots, n^2\},$$

$$\mathcal{L} = \{L_{r,i} \mid 1 \leq r \leq n+1, 1 \leq i \leq n\}$$

단계 5 : 다음과 같이 정의된 결합구조 $\pi = (\mathcal{P}', \mathcal{L}')$ 는 위수 n 인 사영 평면이다.

$$\mathcal{P}' = \{1, 2, \dots, n^2, \infty_1, \dots, \infty_n, \infty_{n+1}\},$$

$$\mathcal{L}' = \{L_{r,i}' \mid 1 \leq r \leq n+1, 1 \leq i \leq n\} \cup \{L_\infty\}$$

$$L_{ri}' = L_{ri} \cup \{\infty_i\}, \quad (1 \leq r \leq n+1, 1 \leq i \leq n)$$

$$L_\infty = \{\infty_1, \infty_2, \dots, \infty_n, \infty_{n+1}\}$$

보기 다음 두 행렬 A, B 는 3 차의 Latin 방진의 완비 직교계를 이룬다.

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 3 & 2 \\ 2 & 1 & 3 \\ 3 & 2 & 1 \end{bmatrix}$$

이로부터 다음 절차에 따라 위수 3 인 아핀평면과 위수 3 인 사영평면을 결정할 수 있다.

단계 1 :

$$\begin{array}{ccccc} 1 & 1 & 1 & 2 & 2 & 2 & 3 & 3 & 3 \\ 1 & 2 & 3 & 1 & 2 & 3 & 1 & 2 & 3 \\ 1 & 2 & 3 & 2 & 3 & 1 & 3 & 1 & 2 \\ 1 & 3 & 2 & 2 & 1 & 3 & 3 & 2 & 1 \end{array}$$

단계 2 : 위의 표에 열의 번호 1, 2, 3, ..., 7, 8, 9 를 첨가한다.

$$\begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 1 & 1 & 2 & 2 & 2 & 3 & 3 & 3 \\ 1 & 2 & 3 & 1 & 2 & 3 & 1 & 2 & 3 \\ 1 & 2 & 3 & 2 & 3 & 1 & 3 & 1 & 2 \\ 1 & 3 & 2 & 2 & 1 & 3 & 3 & 2 & 1 \end{array}$$

단계 3 : 각 정수 r, i ($1 \leq r \leq 4, 1 \leq i \leq 3$) 에 대하여 위의 표의 제 r 행에서 i 를 포함하는 열의 번호 전체로 이루어진 집합을 $L_{r,i}$ 로 나타낸다.

$$\begin{aligned} L_{1,1} &= \{1, 2, 3\}, & L_{1,2} &= \{4, 5, 6\}, & L_{1,3} &= \{7, 8, 9\}, \\ L_{2,1} &= \{1, 4, 7\}, & L_{1,2} &= \{2, 5, 8\}, & L_{2,3} &= \{3, 6, 9\}, \\ L_{3,1} &= \{1, 6, 8\}, & L_{3,2} &= \{2, 4, 9\}, & L_{3,3} &= \{3, 5, 7\}, \\ L_{4,1} &= \{1, 5, 9\}, & L_{4,2} &= \{3, 4, 8\}, & L_{4,3} &= \{2, 6, 7\} \end{aligned}$$

단계 4 : 다음과 같이 정의된 결합구조 $\alpha = (\mathcal{P}, \mathcal{L})$ 는 위수 3 인 아핀 평면이다.

$$\begin{aligned} \mathcal{P} &= \{1, 2, 3, 4, 5, 6, 7, 8, 9\}, \\ \mathcal{L} &= \{L_{r,i} \mid 1 \leq r \leq 4, 1 \leq i \leq 3\} \end{aligned}$$

단계 5 : 다음과 같이 정의된 결합구조 $\pi = (\mathcal{P}', \mathcal{L}')$ 는 위수 3인 사영 평면이다.

$$\mathcal{P}' = \{1, 2, 3, 4, 5, 6, 7, 8, 9, \infty_1, \infty_2, \infty_3, \infty_4\},$$

$$\mathcal{L}' = \{L_{1,1}', \dots, L_{1,4}', \dots, L_{4,1}', \dots, L_{4,3}', L_\infty\}$$

$$L_{1,1}' = \{1, 2, 3, \infty_1\}, \quad L_{1,2}' = \{4, 5, 6, \infty_1\},$$

$$L_{1,3}' = \{7, 8, 9, \infty_1\}, \quad L_{2,1}' = \{1, 4, 7, \infty_2\},$$

$$L_{2,2}' = \{2, 5, 8, \infty_2\}, \quad L_{2,3}' = \{3, 6, 9, \infty_2\},$$

$$L_{3,1}' = \{1, 6, 8, \infty_3\}, \quad L_{3,2}' = \{2, 4, 9, \infty_3\},$$

$$L_{3,3}' = \{3, 5, 7, \infty_3\}, \quad L_{4,1}' = \{1, 5, 9, \infty_4\},$$

$$L_{4,2}' = \{3, 4, 8, \infty_4\}, \quad L_{4,3}' = \{2, 6, 7, \infty_4\},$$

$$L_\infty = \{\infty_1, \infty_2, \infty_3, \infty_4\}$$

