2016학년도 과제연구논문

$GL(n, Z_p)$에서 원소의 위수의 최댓값에 대한 연구

Research about the maximum value of the order of elements in $GL(n, Z_p)$

강수민(Sumin Kang)

김주영(Juyoung Kim)

박성우(Sungwoo Park)

창원과학고등학교

$GL(n, Z_p)$에서 원소의 위수의 최댓값에 대한 연구

강수민 · 김주영 · 박성우
창원과학고등학교

Research about the maximum value of the order of elements in $GL(n, Z_p)$

Sumin Kang · Juyoung Kim · Sungwoo Park
Changwon Science High School

연구요약

우리는 정수론을 바탕으로 행렬의 위수와 다항식의 위수를 정의하고, 행렬의 위수는 그 행렬의 특성다항식의 위수의 약수이며, 특히 특성다항식과 최소다항식이 서로 일치할 경우 행렬의 위수와 특성다항식의 위수가 일치함을 밝혔다. 또한, 라그랑주의 정리에 따르면 $GL(3, Z_p)$의 원소의 위수는 $GL(3, Z_p)$의 원소의 개수의 약수라는 사실을 쉽게 추론할 수 있다. 그러나 $GL(3, Z_p)$의 원소는 $(p^3-1)(p^3-p)(p^3-p^2)$개이므로 p의 값에 따라 매우 큰 수가 되기 때문에 위수를 구함에 있어 원소의 위수가 의 약수라는 정보는 효율적이지 못하다. 그래서 우리는 $GL(3, Z_2)$의 각 원소의 위수를 구하여 각 원소를 그 특성다항식과 위수에 따라 분류하였고, 이를 통하여 실제 원소가 가질 수 있는 최대 위수를 예들을 통해 관찰 및 추측하였다. 그 결과, $GL(n, Z_p)$의 원소의 최대 위수는 p^n-1임을 증명하였다.

중심어 : 위수
위수, 행렬, 특성다항식, 일반선형군 $GL(3, Z_p)$

Ⅰ. 서론

연립방정식의 해를 구하는 과정을 간소화하기 위하여 고안된 행렬은, 현재는 단순히 연립방정식의 해를 구하는 데 이용되는 것뿐만 아니라 매우 높은 활용도를 가지고 있어 그 자체로도 중요한 의미가 있다. 특히 행렬은 역사적으로 많은 수학자들의 연구 주제가 되어왔던 만큼 행렬에서도 의미 있는 연구들이 활발하게 진행되었으며, 그 결과 케일리-해밀턴의 정리 등 다양한 정리가 연구되었고, 그러한 성과들은 현재 암호학, 경제학, 통계학 등 다양한 분야에서 활용되고 있다.

이렇듯 행렬과 행렬식에 대한 연구는 오랜 역사를 가지고 있으나, 여러 가지 독립적인 성과들이 하나의 엄밀한 체계로 통합된 것은 두 대상의 연구에 대한 역사에 비하여 상대적으로 최근에 이루어졌다. 1888년 페아노에 의해 도입된 벡터공간이라는 개념은 독립적으로 발전하고 있던 선형대수학의 많은 결과들을 다른 분야들과 하나의 연결고리로 합쳐지게 하였다. 이후 선형대수학의 근간으로서의 행렬의 역할이나 특징에 대해 알아보는 연구가 활발히 이루어지고 있다.

이러한 추세에 발맞추어, 본 연구에서는 행렬을 정수론에서 정의된 위수로부터 행렬의 위수와 다항식의 위수를 정의하고, 특성다항식의 위수를 이용하여 행렬의 위수를 알 수 있는 효율적인 방법에 대하여 연구하였다. 또한, 행렬의 특성다항식과 위수를 통해 행렬을 분류하고, 이렇게 분류한 행렬들의 집합이 어떠한 성질을 만족하는지 연구하여 $GL(3, Z_2)$의 대수적 성질을 분석하였고, 이로부터 $GL(n, Z_p)$의 원소 A가 가질 수 있는 위수의 최댓값을 발견하였다.

행렬의 위수 탐색을 통하여, 행렬의 연산을 간소화할 수 있고, 행렬에 이산로그를 적용하는 등 수학 연구에 있어 더욱 다양한 시도를 할 수 있을 것으로 생각된다. 또한, $GL(3, Z_p)$의 원소의 위수에 대하여 p가 증가할수록 행렬의 수가 급격히 증가하므로, 암호학에도 응용할 수 있을 것이다.

Ⅱ. 이론적 배경

1. 위수

우리는 어떤 행렬 A에 대하여 $A^n = E$인 정수 n이 존재하지 않을까 하는 생각을 하여, 이에 관련한 정의나 개념을 탐색하던 중, 정수론에서 이와 유사한 개념인 위수를 도입하고 있었음을 발견하였다. 정수론에서 위수란, 법 n에 대하여 어떤 정수 a가 n과 서로소일 때, $a^r \equiv 1 \pmod{n}$인 최소의 자연수 r을 법 n에 대한 a의 위수라 하고 $r = \mathrm{ord}_n(a)$으로 표기한다.

2. 군과 라그랑주의 정리

집합 $G(\neq \varnothing)$ 위에 이항연산 $\circ$와 임의의 원소 $a, b, c \in G$에 대하여 다음과 같은 성질이 성립할 때, $(G, \circ)$를 군이라 한다.

<Table 1> Definition of group

1. 닫혀 있음 ($a \circ b \in G$)
2. 결합법칙이 성립함 ($(a \circ b) \circ c = a \circ (b \circ c)$)
3. 항등원이 존재함[1]
4. 모든 원소가 가역원임[2]

라그랑주(Lagrange)의 정리의 따름정리에 의하여, 유한군 G의 각 원소에 대하여 a의 위수는 $|G|$의 약수이다. 즉, $a^{|G|} = e$이다. 이때, $|GL(n, Z_p)| = \prod_{k=0}^{n-1}(p^n - p^k)$으로 선행연구에서 알려져 있다.

$GL(3, Z_2)$의 원소는 각 성분이 Z_2의 원소이고 $Det(A) \neq 0$인 3차 정사각행렬이어야 한다. 그런데 행렬식이 0이 되지 않으려면 첫째, 각 열이 서로 배수 관계가 되지 않아야 하며, 둘째, 모든 성분이 0인 열이 없어야 한다. 따라서 $|GL(3, Z_2)| = (2^3 - 1)(2^3 - 2)(2^3 - 2^2) = 168$이므로 라그랑주의 정리에 의하여 $GL(3, Z_2)$의 각 원소의 위수는 168의 약수이다.

3. 특성다항식

행렬의 특성다항식(characteristic polynomial)은 행렬을 연산하는 데 있어 큰 도움을 주기 때문에 행렬의 위수를 구할 때도 유용하다. 행렬 $A \in GL(3, Z_k)$에 대하여 행렬 A의 특성다항식을 $p(x) = |xE - A|$라고 한다. 그리고 만약 최고차항의 계수가 1인 다항식 $p_m(x) \in Z_k[x]$가 $p_m(A) = O$를 만족하는 최소차수의 다항식이면 행렬 A의 최소다항식(minimum polynomial)이라 한다.
그리고 특성다항식을 이용하여 위수를 구하는데 있어 중요하게 사용될 케일리-해밀턴(Cayley-Hamilton) 정리는 행렬 A의 특성다항식 $p(x)$에 대하여 $p(A) = O$이 성립한다는 것이다.

---

1) 특정한 원소 $e \in G$가 존재하여 모든 원소 $a \in G$에 대하여 등식 $e \circ a = a \circ e = a$가 성립할 때, 이 원소 $e \in G$를 G의 연산 $\circ$에 대한 항등원이라 한다.

2) 각 원소 $a \in G$에 대하여 $a \circ b = b \circ a = e$를 만족하는 원소 $b \in G$가 존재할 때, 이 원소 b를 a의 연산 $\circ$에 대한 역원이라 하고 a^{-1}로 나타낸다.

Ⅲ. 연구 방법 및 절차

본 연구는 일반선형군 $GL(3, Z_2)$ 내의 원소들의 위수와 $GL(3, Z_2)$의 대수적 성질에 대한 연구이다. 이에 따라 연구 방법 및 절차는 다음과 같이 구성된다.

첫째, 행렬 및 위수에 대한 국내외의 다양한 문헌을 조사하여 관련된 기반 자료를 수집한다.

둘째, $GL(3, Z_2)$에서 행렬의 위수와 다항식의 위수를 정의하여, 특성다항식을 기반으로 하여 행렬의 위수를 알 수 있는 방법에 대하여 연구한다. 이를 통해 $GL(n, Z_p)$의 원소의 위수의 최댓값을 연구한다.

셋째, 군 $GL(3, Z_2)$와 집합 K_p^n을 정의하고 특성다항식에 따라 행렬을 이 집합들에 적절히 분류하여 집합 K_p^n의 대수적 성질을 살펴본다.

1. 개념 정의 및 연구 범위 설정

가. 행렬 및 다항식의 위수의 정의

우리는 앞으로의 연구에서 행렬에서의 위수를 명확히 할 필요가 있었다. 따라서 앞으로의 연구에서는 정수론에서의 위수의 정의를 참고하여, 행렬 A의 위수를 다음과 같이 사용하기로 한다.

<Table 2> Definition of order of a matrix

[정의 1] 어떤 행렬 A에 대하여 $A^n = E$를 만족하는 최소의 양의 정수 n이 존재할 때, n을 행렬 A의 위수라고 한다.

또한, 우리는 행렬의 위수가 특성다항식과 관계가 있으므로, 특성다항식을 이용하여 행렬을 분류하고, 특성다항식에 따른 위수를 확인하여 행렬의 위수를 간접적으로 구하기로 하였다. 이를 위해서는 특성다항식의 위수가 정의되어 있어야 하므로, 다음과 같이 일반적인 다항식의 위수를 정의하였다.

<Table 3> Definition of order of a polynomial

[정의 2] 어떤 다항식 $p(x)$에 대하여 $p(x) \mid x^n - 1$을 만족하는 최소의 양의 정수 n이 존재할 때, n을 다항식의 위수라고 한다.

나. 집합 K_p^n의 정의

우리는 특성다항식에 따라 위수를 구할 수 있다면 특성다항식이 같은 행렬을 원소로 가지는 집합의 특성을 파악하여도 의미 있는 결과를 얻을 수 있을 것이라 예측하였다. 따라서 다음과 같이 특성다항식을 기반으로 한 집합 K_p^n을 정의하였다.

<Table 4> Definition of K_p^n

[정의 3] $K_p^n = \{A \mid A \in GL(3, Z_2), A$의 특성다항식 : $p(x), A$의 위수 : $n\} \cup \{E\}$
[정의 4] $K_p = \{A \mid A \in GL(3, Z_2), A$의 특성다항식 : $p(x)\} \cup \{E\}$
[정의 5] $K^n = \{A \mid A \in GL(3, Z_2), A$의 위수 : $n\} \cup \{E\}$

다. 연구 범위 설정

위수가 존재하지 않는 행렬도 있기 때문에, 위수의 존재 조건을 파악하기 위해서는 먼저 대상을 명확히 할 필요가 있다. 즉, 행렬의 각 원소의 값을 일정한 범위 내로 제한할 필요가 있다. 또한 행렬 A가 비가역이면, 즉 $\mathrm{Det(A)}=0$이면 행렬 A의 위수는 없으므로([2]), $\mathrm{Det(A)}\neq 0$이어야 한다.

따라서 우리는 연구 범위를 좁히기 위하여 일반선형군 $GL(3, Z_p)$를 앞으로의 연구 대상으로 삼았다. $GL(n, Z_p)=\{A|A=(a_{ij})\,(1\leq i, j\leq n), a_{ij}\in Z_p, Det(A)\neq 0\}$으로 알려져 있다.

2. $GL(3, Z_2)$의 원소의 특성다항식

가. 프로그래밍을 통한 $GL(3, Z_2)$의 원소의 위수 판정

우리는 $GL(2, Z_2)$의 행렬의 위수를 프로그램을 제작하여 확인하였으며, 이를 확장할 수 있는지 확인하기 위해 $GL(3, Z_2)$에서도 행렬의 위수를 프로그램을 통하여 구하였다. 다음은 그 결과를 표로 정리한 것이다.

<Table 5> The order of matrices of $GL(3, Z_2)$

위수	1	2	3	4	7	계
행렬의 수	1	21	56	42	48	168

따라서 우리는 $GL(3, Z_2)$에 속하는 새로운 집합 K_p^n을 정의하여, 이 집합의 원소에 대해 위수를 구해 보고자 하였다.

나. $GL(3, Z_2)$의 원소의 특성다항식

삼차 정사각행렬의 특성다항식은 최고차항의 계수가 1인 삼차 식이므로, 행렬 A가 $GL(3, Z_2)$의 원소이면 A의 특성다항식은 다음 4개 중 하나이다. (단, $P(x)\in Z_2[x]$)

<Table 6> Characteristic polynomials of $GL(3, Z_2)$

$p_1(x)=x^3+1$
$p_2(x)=x^3+x^2+1$
$p_3(x)=x^3+x+1$
$p_4(x)=x^3+x^2+x+1$

그리고 $|GL(3, Z_2)|=168$이므로 라그랑주의 정리에 의하여 각 행렬의 위수는 168의 약수이다. 따라서 행렬 $A\in GL(3, Z_2)$의 특성다항식은 $x^{168}-1$의 인수가 되어야 한다. $x^{168}-1$의 가능한 인수들을 정리한 것은 다음과 같다.

<Table 7> Factors of $x^{168}-1$

차수	1	2	3	6
인수($Z_2[x]$)	$(x+1)^8$	$(x^2+x+1)^8$	$(x^3+x^2+1)^8$ $(x^3+x+1)^8$	$(x^6+x^4+x^2+x+1)^8$ $(x^6+x^5+x^4+x^2+1)^8$

우리는 이렇게 얻은 특성다항식에 어떤 원소가 속하는지 알고자 하게 되었다. 즉, $GL(3, Z_2)$의 원소의 목록을 특성다항식을 이용하여 분류할 수 있도록, $GL(3, Z_2)$에서 위수가 존재하는 모든 원소와 그 각각의 특성다항식의 자료를 필요로 하게 되었다. 따라서 우리는 $GL(3, Z_2)$의 모든 원소와 그 각각의 특성다항식을 출력하는 프로그램을 제작하였다. 다음은 그 결과를 표로 정리한 것이다.

<Table 8> Number of matrices which have specific characteristic polynomial

특성다항식	x^3+1	x^3+x^2+1	x^3+x+1	x^3+x^2+x+1	계
행렬의 수	56	24	24	64	168

3. 특성다항식에 따른 $GL(3, Z_2)$의 원소의 위수

가. 특성다항식이 $p_1(x) = x^3 + 1$인 경우

행렬 A가 x^3+1을 특성다항식으로 가지면 $A^3 + E = O$을 만족하므로 A의 위수는 3의 약수이다. 그러나 만약 A의 위수가 1이면 $A = E$이므로 x^3+1을 특성다항식으로 가지지 않는다. 따라서 x^3+1을 특성다항식으로 가지는 행렬의 위수는 3이며, 다음과 같이 총 56가지이다.

<Table 9> Matrices which have x^3+1 for their characteristic polynomial

특성다항식 (최소다항식)	위수	행렬
x^3+1 (x^3+1)	3	$\begin{pmatrix}0&0&1\\0&1&0\\1&0&1\end{pmatrix}$ $\begin{pmatrix}0&0&1\\0&1&0\\1&1&1\end{pmatrix}$ $\begin{pmatrix}0&0&1\\0&1&1\\1&0&1\end{pmatrix}$ $\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix}$ $\begin{pmatrix}0&0&1\\1&0&1\\1&1&0\end{pmatrix}$ $\begin{pmatrix}0&0&1\\1&1&0\\1&0&1\end{pmatrix}$ $\begin{pmatrix}0&0&1\\1&1&1\\0&1&1\end{pmatrix}$ $\begin{pmatrix}0&0&1\\1&1&1\\1&0&1\end{pmatrix}$ $\begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}$ $\begin{pmatrix}0&1&0\\0&1&1\\1&1&1\end{pmatrix}$ $\begin{pmatrix}0&1&0\\1&0&1\\1&1&0\end{pmatrix}$ $\begin{pmatrix}0&1&0\\1&1&0\\0&0&1\end{pmatrix}$ $\begin{pmatrix}0&1&0\\1&1&0\\0&1&1\end{pmatrix}$ $\begin{pmatrix}0&1&0\\1&1&0\\1&0&1\end{pmatrix}$ $\begin{pmatrix}0&1&0\\1&1&0\\1&1&1\end{pmatrix}$ $\begin{pmatrix}0&1&0\\1&1&1\\0&0&1\end{pmatrix}$ $\begin{pmatrix}0&1&1\\0&0&1\\1&1&0\end{pmatrix}$ $\begin{pmatrix}0&1&1\\0&1&0\\1&0&1\end{pmatrix}$ $\begin{pmatrix}0&1&1\\0&1&0\\1&1&1\end{pmatrix}$ $\begin{pmatrix}0&1&1\\1&0&0\\1&1&0\end{pmatrix}$ $\begin{pmatrix}0&1&1\\1&0&1\\0&1&0\end{pmatrix}$ $\begin{pmatrix}0&1&1\\1&0&1\\1&0&0\end{pmatrix}$ $\begin{pmatrix}0&1&1\\1&1&0\\0&0&1\end{pmatrix}$ $\begin{pmatrix}0&1&1\\1&1&1\\0&0&1\end{pmatrix}$ $\begin{pmatrix}1&0&0\\0&0&1\\0&1&1\end{pmatrix}$ $\begin{pmatrix}1&0&0\\0&0&1\\1&1&1\end{pmatrix}$ $\begin{pmatrix}1&0&0\\0&1&1\\0&1&0\end{pmatrix}$ $\begin{pmatrix}1&0&0\\0&1&1\\1&1&0\end{pmatrix}$ $\begin{pmatrix}1&0&0\\1&0&1\\0&1&1\end{pmatrix}$ $\begin{pmatrix}1&0&0\\1&0&1\\1&1&1\end{pmatrix}$ $\begin{pmatrix}1&0&0\\1&1&1\\0&1&0\end{pmatrix}$ $\begin{pmatrix}1&0&0\\1&1&1\\1&1&0\end{pmatrix}$ $\begin{pmatrix}1&0&1\\0&0&1\\0&1&1\end{pmatrix}$ $\begin{pmatrix}1&0&1\\0&1&0\\1&0&0\end{pmatrix}$ $\begin{pmatrix}1&0&1\\0&1&0\\1&1&0\end{pmatrix}$ $\begin{pmatrix}1&0&1\\0&1&1\\0&1&0\end{pmatrix}$ $\begin{pmatrix}1&0&1\\0&1&1\\1&0&0\end{pmatrix}$ $\begin{pmatrix}1&0&1\\1&0&0\\1&1&1\end{pmatrix}$ $\begin{pmatrix}1&0&1\\1&1&0\\1&0&0\end{pmatrix}$ $\begin{pmatrix}1&0&1\\1&1&1\\1&0&0\end{pmatrix}$ $\begin{pmatrix}1&1&0\\0&0&1\\0&1&1\end{pmatrix}$ $\begin{pmatrix}1&1&0\\0&1&1\\0&1&0\end{pmatrix}$ $\begin{pmatrix}1&1&0\\1&0&0\\0&0&1\end{pmatrix}$ $\begin{pmatrix}1&1&0\\1&0&0\\0&1&1\end{pmatrix}$ $\begin{pmatrix}1&1&0\\1&0&0\\1&0&1\end{pmatrix}$ $\begin{pmatrix}1&1&0\\1&0&0\\1&1&1\end{pmatrix}$ $\begin{pmatrix}1&1&0\\1&0&1\\0&0&1\end{pmatrix}$ $\begin{pmatrix}1&1&0\\1&1&1\\0&0&1\end{pmatrix}$ $\begin{pmatrix}1&1&1\\0&0&1\\0&1&1\end{pmatrix}$ $\begin{pmatrix}1&1&1\\0&0&1\\1&0&1\end{pmatrix}$ $\begin{pmatrix}1&1&1\\0&1&0\\1&0&0\end{pmatrix}$ $\begin{pmatrix}1&1&1\\0&1&0\\1&1&0\end{pmatrix}$ $\begin{pmatrix}1&1&1\\0&1&1\\0&1&0\end{pmatrix}$ $\begin{pmatrix}1&1&1\\1&0&0\\0&0&1\end{pmatrix}$ $\begin{pmatrix}1&1&1\\1&0&1\\0&0&1\end{pmatrix}$ $\begin{pmatrix}1&1&1\\1&1&0\\0&1&0\end{pmatrix}$

나. 특성다항식이 $p_2(x)=x^3+x^2+1$인 경우

행렬 A가 x^3+x^2+1을 특성다항식으로 가지면 이 특성다항식은 $Z_2[x]$ 상의 다항식이므로 이를 이용하면 $x^7-1=x^7+1=(x+1)(x^6+x^5+x^4+x^3+x^2+x+1)=(x+1)(x^3+x^2+1)(x^3+x+1)=0$이다. 따라서 이 특성다항식을 가지는 행렬의 위수는 7의 약수이다. 그러나 만약 A의 위수가 1이면 $A=E$이므로 이를 특성다항식으로 가지지 않는다. 따라서 이를 특성다항식으로 가지는 행렬의 위수는 7이며, 다음과 같이 총 24가지이다.

<Table 10> Matrices which have x^3+x^2+1 for their characteristic polynomial

특성다항식 (최소다항식)	위수	행렬
x^3+x^2+1 (x^3+x^2+1)	7	$\begin{pmatrix}0&0&1\\0&1&1\\1&1&0\end{pmatrix}$ $\begin{pmatrix}0&0&1\\1&0&0\\0&1&1\end{pmatrix}$ $\begin{pmatrix}0&0&1\\1&0&1\\1&1&1\end{pmatrix}$ $\begin{pmatrix}0&0&1\\1&1&0\\0&1&0\end{pmatrix}$ $\begin{pmatrix}0&1&0\\0&0&1\\1&0&1\end{pmatrix}$ $\begin{pmatrix}0&1&0\\0&1&1\\1&0&0\end{pmatrix}$ $\begin{pmatrix}0&1&0\\1&0&1\\0&1&1\end{pmatrix}$ $\begin{pmatrix}0&1&0\\1&1&1\\1&1&0\end{pmatrix}$ $\begin{pmatrix}0&1&1\\0&0&1\\1&1&1\end{pmatrix}$ $\begin{pmatrix}0&1&1\\1&0&0\\1&0&1\end{pmatrix}$ $\begin{pmatrix}0&1&1\\1&1&0\\1&0&0\end{pmatrix}$ $\begin{pmatrix}0&1&1\\1&1&1\\0&1&0\end{pmatrix}$ $\begin{pmatrix}1&0&1\\0&0&1\\1&1&0\end{pmatrix}$ $\begin{pmatrix}1&0&1\\1&0&0\\0&1&0\end{pmatrix}$ $\begin{pmatrix}1&0&1\\1&1&0\\1&1&1\end{pmatrix}$ $\begin{pmatrix}1&0&1\\1&1&1\\0&1&1\end{pmatrix}$ $\begin{pmatrix}1&1&0\\0&0&1\\1&0&0\end{pmatrix}$ $\begin{pmatrix}1&1&0\\0&1&1\\1&1&1\end{pmatrix}$ $\begin{pmatrix}1&1&0\\1&0&1\\0&1&0\end{pmatrix}$ $\begin{pmatrix}1&1&0\\1&1&1\\1&0&1\end{pmatrix}$ $\begin{pmatrix}1&1&1\\0&1&1\\1&0&1\end{pmatrix}$ $\begin{pmatrix}1&1&1\\1&0&0\\1&1&0\end{pmatrix}$ $\begin{pmatrix}1&1&1\\1&0&1\\1&0&0\end{pmatrix}$ $\begin{pmatrix}1&1&1\\1&1&0\\0&1&1\end{pmatrix}$

다. 특성다항식이 $p_3(x)=x^3+x+1$인 경우

행렬 A가 x^3+x+1을 특성다항식으로 가지면, 이 특성다항식은 x^3+x^2+1의 경우와 같이 x^7-1의 인수이다. 그러나 만약 A의 위수가 1이면 $A=E$이므로 이를 특성다항식으로 가지지 않는다. 따라서 이를 특성다항식으로 가지는 행렬의 위수는 7이며, 다음과 같이 총 24가지이다.

<Table 11> Matrices which have x^3+x+1 for their characteristic polynomial

특성다항식 (최소다항식)	위수	행렬
x^3+x+1 (x^3+x+1)	7	$\begin{pmatrix}0&0&1\\0&1&1\\1&1&1\end{pmatrix}$ $\begin{pmatrix}0&0&1\\1&0&0\\1&1&0\end{pmatrix}$ $\begin{pmatrix}0&0&1\\1&0&1\\0&1&0\end{pmatrix}$ $\begin{pmatrix}0&0&1\\1&1&0\\0&1&1\end{pmatrix}$ $\begin{pmatrix}0&1&0\\0&0&1\\1&1&0\end{pmatrix}$ $\begin{pmatrix}0&1&0\\0&1&1\\1&0&1\end{pmatrix}$ $\begin{pmatrix}0&1&0\\1&0&1\\0&1&0\end{pmatrix}$ $\begin{pmatrix}0&1&0\\1&1&1\\0&1&1\end{pmatrix}$ $\begin{pmatrix}0&1&1\\0&0&1\\1&0&0\end{pmatrix}$ $\begin{pmatrix}0&1&1\\1&0&0\\0&1&0\end{pmatrix}$ $\begin{pmatrix}0&1&1\\1&1&0\\1&0&1\end{pmatrix}$ $\begin{pmatrix}0&1&1\\1&1&1\\1&0&1\end{pmatrix}$ $\begin{pmatrix}1&0&1\\0&0&1\\1&1&1\end{pmatrix}$ $\begin{pmatrix}1&0&1\\1&0&0\\1&1&1\end{pmatrix}$ $\begin{pmatrix}1&0&1\\1&1&0\\0&1&0\end{pmatrix}$ $\begin{pmatrix}1&0&1\\1&1&1\\1&1&0\end{pmatrix}$ $\begin{pmatrix}1&1&0\\0&0&1\\1&0&1\end{pmatrix}$ $\begin{pmatrix}1&1&0\\0&1&1\\1&0&0\end{pmatrix}$ $\begin{pmatrix}1&1&0\\1&0&1\\0&1&1\end{pmatrix}$ $\begin{pmatrix}1&1&0\\1&1&1\\0&1&0\end{pmatrix}$ $\begin{pmatrix}1&1&1\\0&1&1\\1&1&0\end{pmatrix}$ $\begin{pmatrix}1&1&1\\1&0&0\\1&0&1\end{pmatrix}$ $\begin{pmatrix}1&1&1\\1&0&1\\0&1&1\end{pmatrix}$ $\begin{pmatrix}1&1&1\\1&1&0\\1&0&0\end{pmatrix}$

라. 특성다항식이 $p_4(x)=x^3+x^2+x+1$인 경우

행렬 A가 x^3+x^2+x+1을 특성다항식을 가지면, 이 특성다항식은 $Z_2[x]$ 상의 다항식이므로 이를 이용하면 $x^4-1=(x+1)(x^3+x^2+x+1)=(x+1)^2(x^2+1)=(x+1)^4$이다. 따라서 이를 특성다항식으로 가지는 행렬의 위수는 4의 약수이다. x^3+x^2+x+1을 특성다항식으로 가지는 행렬 중에는 위수가 1, 2, 4인 것이 모두 있으며, 특성다항식이 x^3+x^2+x+1인 경우는 다음과 같이 총 64가지이다.

<Table 12> Matrices which have x^3+x^2+x+1 for their characteristic polynomial

특성다항식 (최소다항식)	위수	행렬
x^3+x^2+x+1 $(x+1)$	1	$\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}$
x^3+x^2+x+1 (x^2+1)	2	$\begin{pmatrix}0&0&1\\0&1&0\\1&0&0\end{pmatrix}$ $\begin{pmatrix}0&0&1\\1&1&1\\1&0&0\end{pmatrix}$ $\begin{pmatrix}0&1&0\\1&0&0\\0&0&1\end{pmatrix}$ $\begin{pmatrix}0&1&0\\1&0&0\\1&1&1\end{pmatrix}$ $\begin{pmatrix}0&1&1\\0&1&0\\1&1&0\end{pmatrix}$ $\begin{pmatrix}0&1&1\\1&0&1\\0&0&1\end{pmatrix}$ $\begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix}$ $\begin{pmatrix}1&0&0\\0&1&0\\0&1&1\end{pmatrix}$ $\begin{pmatrix}1&0&0\\0&1&0\\1&0&1\end{pmatrix}$ $\begin{pmatrix}1&0&0\\0&1&0\\1&1&1\end{pmatrix}$ $\begin{pmatrix}1&0&0\\0&1&1\\0&0&1\end{pmatrix}$ $\begin{pmatrix}1&0&0\\1&0&1\\1&1&0\end{pmatrix}$ $\begin{pmatrix}1&0&0\\1&1&0\\0&0&1\end{pmatrix}$ $\begin{pmatrix}1&0&0\\1&1&0\\1&0&1\end{pmatrix}$ $\begin{pmatrix}1&0&0\\1&1&1\\0&0&1\end{pmatrix}$ $\begin{pmatrix}1&0&1\\0&1&0\\0&0&1\end{pmatrix}$ $\begin{pmatrix}1&0&1\\0&1&1\\0&0&1\end{pmatrix}$ $\begin{pmatrix}1&1&0\\0&1&0\\0&0&1\end{pmatrix}$ $\begin{pmatrix}1&1&0\\0&1&0\\1&0&1\end{pmatrix}$ $\begin{pmatrix}1&1&1\\0&1&0\\0&1&1\end{pmatrix}$ $\begin{pmatrix}1&1&1\\0&0&1\\0&1&0\end{pmatrix}$ $\begin{pmatrix}1&1&1\\0&1&0\\1&0&0\end{pmatrix}$ $\begin{pmatrix}1&1&1\\0&1&0\\1&0&1\end{pmatrix}$
x^3+x^2+x+1 (x^3+x^2+x+1)	4	$\begin{pmatrix}0&0&1\\0&1&0\\1&1&0\end{pmatrix}$ $\begin{pmatrix}0&0&1\\0&1&1\\1&0&0\end{pmatrix}$ $\begin{pmatrix}0&0&1\\1&0&0\\1&1&1\end{pmatrix}$ $\begin{pmatrix}0&0&1\\1&0&1\\0&1&1\end{pmatrix}$ $\begin{pmatrix}0&0&1\\1&1&0\\1&0&0\end{pmatrix}$ $\begin{pmatrix}0&0&1\\1&1&1\\0&1&0\end{pmatrix}$ $\begin{pmatrix}0&1&0\\0&0&1\\1&1&1\end{pmatrix}$ $\begin{pmatrix}0&1&0\\0&1&1\\1&1&0\end{pmatrix}$ $\begin{pmatrix}0&1&0\\1&0&0\\0&1&1\end{pmatrix}$ $\begin{pmatrix}0&1&0\\1&0&0\\1&0&1\end{pmatrix}$ $\begin{pmatrix}0&1&0\\1&0&1\\0&0&1\end{pmatrix}$ $\begin{pmatrix}0&1&0\\1&1&1\\1&0&0\end{pmatrix}$ $\begin{pmatrix}0&1&1\\0&0&1\\1&0&1\end{pmatrix}$ $\begin{pmatrix}0&1&1\\0&1&0\\1&0&0\end{pmatrix}$ $\begin{pmatrix}0&1&1\\1&0&0\\0&0&1\end{pmatrix}$ $\begin{pmatrix}0&1&1\\1&0&1\\1&1&1\end{pmatrix}$ $\begin{pmatrix}0&1&1\\1&1&0\\1&1&0\end{pmatrix}$ $\begin{pmatrix}0&1&1\\1&1&1\\1&1&0\end{pmatrix}$ $\begin{pmatrix}1&0&0\\0&0&1\\1&1&0\end{pmatrix}$ $\begin{pmatrix}1&0&0\\0&1&1\\1&0&1\end{pmatrix}$ $\begin{pmatrix}1&0&0\\1&0&1\\0&1&0\end{pmatrix}$ $\begin{pmatrix}1&0&1\\0&0&1\\0&1&1\end{pmatrix}$ $\begin{pmatrix}1&0&1\\0&1&0\\0&1&1\end{pmatrix}$ $\begin{pmatrix}1&0&1\\0&1&1\\1&0&0\end{pmatrix}$ $\begin{pmatrix}1&0&1\\1&0&0\\1&1&0\end{pmatrix}$ $\begin{pmatrix}1&0&1\\1&1&1\\0&0&1\end{pmatrix}$ $\begin{pmatrix}1&1&0\\0&0&1\\0&1&0\end{pmatrix}$ $\begin{pmatrix}1&1&0\\0&1&0\\1&0&1\end{pmatrix}$ $\begin{pmatrix}1&1&0\\0&1&0\\1&1&1\end{pmatrix}$ $\begin{pmatrix}1&1&0\\0&1&1\\0&0&1\end{pmatrix}$ $\begin{pmatrix}1&1&0\\1&0&1\\1&0&0\end{pmatrix}$ $\begin{pmatrix}1&1&1\\0&0&1\\1&0&0\end{pmatrix}$ $\begin{pmatrix}1&1&1\\0&1&0\\0&1&1\end{pmatrix}$ $\begin{pmatrix}1&1&1\\0&1&1\\0&0&1\end{pmatrix}$ $\begin{pmatrix}1&1&1\\1&0&0\\0&1&0\end{pmatrix}$ $\begin{pmatrix}1&1&1\\1&0&1\\1&1&0\end{pmatrix}$ $\begin{pmatrix}1&1&1\\1&1&0\\1&0&1\end{pmatrix}$

4. $GL(3, Z_p)$의 원소의 위수

이미 언급한 바와 같이, 라그랑주의 정리에 따르면 어떤 행렬 $A\in GL(3, Z_p)$에 대하여 항상 $A^{|GL(3, Z_p)|}=E$가 성립한다. 그러므로 A의 위수는 $|GL(3, Z_2)|$의 약수이다. 하지만 k가 커짐에 따라 가능한 위수의 최대 범위가 증가하므로 계산이 복잡해진다. 따라서 우리는 행렬의 위수를 더욱 간단하고 빠르게 구할 수 있는 방법을 모색하게 되었다.

가. 특성다항식과 행렬의 위수

우리는 앞에서 얻은 자료를 통하여, 행렬의 위수는 특성다항식 내지는 최소다항식이 결정할 것이라는 추측을 하였다. 이로써, 우리는 $A\in GL(3, Z_p)$에 대해 A의 특성다항식과 A의 최소다항식이 같을 때, 특성다항식의 위수와 행렬의 위수는 서로 같다는 성질을 발견하였다.

<Table 13> Proof of theorem 1

$A \in GL(3, Z_p)$(단, p는 소수)에 대해 A의 특성다항식과 A의 최소다항식이 같을 때, 특성다항식의 위수와 행렬의 위수는 서로 같다.

증명.
1) A의 위수를 n, A의 특성다항식 $p(x)$의 위수를 m이라 하자.
$p(x)|x^m - 1$이므로 $x^m - 1 = p(x)q(x)$를 만족하는 다항식 $q(x)$가 존재한다.
$A^m - E = p(A)q(A) = O$이므로 n은 m의 약수이다.
2) $x^n - 1 = p(x)s(x) + r(x)$라고 하자. (단, $r(x)$는 2차 이하 다항식)
$A^n - E = O$이므로
$A^n - E = p(A)s(A) + r(A)$
$= O + r(A)$
$= r(A)$이다.
따라서 $r(A) = O$이다.
최소다항식과 특성다항식이 같다는 가정에 의해 $r(x) = 0$이다.
m은 n의 약수이다.

1), 2)에 의하여 $n = m$이다.

이를 확장하여 특성다항식과 최소다항식이 서로 일치한다는 가정을 빼면, 행렬 A의 위수는 특성다항식 $p(x)$의 위수의 약수가 됨을 알 수 있다. 즉, $A \in GL(n, Z_p)$(단, p는 소수)에 대해, A의 위수를 n이라 하고 A의 특성다항식을 $p(x)$의 위수를 m이라 하면, $n|m$이다.

나. $GL(3, Z_p)$의 원소의 위수의 최댓값

또한, 우리는 사전연구로 $GL(2, Z_p)$의 원소들의 위수를 조사하던 중, 가능한 위수들이 모두 $p^2 - 1$ 이하라는 사실을 발견했다. 이에 우리는 $GL(3, Z_p)$의 원소들의 위수가 모두 $p^3 - 1$ 이하이지 않을까 추측하게 되었다. 즉, $A \in GL(3, Z_p)$의 위수는 $p^3 - 1$ 이하인 $(p^3 - 1)(p^3 - p)(p^3 - p^2)$의 약수라는 것이다.
따라서 우리는 이를 확인하기 위하여 $GL(3, Z_p)$의 원소의 위수의 종류와 수를 출력하는 프로그램을 제작하였다. 실행 결과, 이 추측은 $p = 2, 3, 5$일 때는 성립함을 확인하였다. 그러나 우리는 더욱 엄밀한 확인을 위하여 수학적인 증명을 시도하였으며, $p \geq 7$인 경우를 계산하기 위해 프로그램을 수정하던 중, 교수님의 자문을 통하여 $A \in GL(n, Z_p)$의 임의의 원소 A의 위수는 $p^n - 1$ 이하라는 결론을 얻을 수 있었다. 그 자세한 증명은 다음과 같다.

<Table 14> Proof of theorem 2

$A \in GL(n, Z_p)$의 임의의 원소 A의 위수는 $p^n - 1$ 이하인 $\prod_{k=0}^{n-1}(p^n - p^k)$의 약수이다.

증명.
행렬 $A \in GL(n, Z_p)$를 생각하자.

보조정리.
케일리-해밀턴 정리에 의하여 A의 특성다항식은 n차식이다.
그러므로 $k \geq n$이면 A^{n-1}, A^{n-2}, ... , A, E의 일차결합으로 A^k를 나타낼 수 있다.

1) $k=n$일 때.
케일리-해밀턴 정리에 의해 Z_p에 속하는 적당한 $a_{n-1}, \cdots, a_0$가 있어
$A^n + a_{n-1}A^{n-1} + \cdots + a_0E = O$이다.
그러므로 $A^n = -a_{n-1}A^{n-1} - \cdots - a_0E$이므로 성립한다.

2) $k \geq m$일 때. (단, $m > n$)
$k \geq m$일 때 성립한다고 가정하자.
$(A^n + a_{n-1}A^{n-1} + \cdots + a_0E)A^{m+1-n} = A^{m+1} + a_{n-1}A^m + \cdots + a_0A^{m+1-n} = O$
그러므로 $A^{m+1} = -a_{n-1}A^m - \cdots - a_0A^{m+1-n}$이다.
$k \geq m$일 때. 가정이 성립한다고 했으므로, $A^m, \cdots, A^{m+1-n}$은 모두 $A^{n-1}, \cdots, E$의 일차결합으로 나타낼 수 있으므로 $k=m+1$일 때도 성립한다.

그러므로 1), 2)에 의해 어떤 행렬 A에 대하여, A^k에서 $k \geq n$이면 A^{n-1}, A^{n-2}, ... , A, E의 일차결합으로 A^k를 나타낼 수 있다.

$f(x) \in Z_p[x]$에 대하여 $f(A)$는 $n-1$차 이하의 계수만 생각하면 되므로, 새로운 집합을 생각하여 $F = \{f(A) | f(x) \in Z_p[x], A \in GL(n, Z_p)\}$라 하면, $|F| = p^n$이다. 이 가운데 O이 아닌 것은 $p^n - 1$개다. 또한, 새로운 집합 $K = \{A^{p^n-1}, A^{p^n-2}, \ldots, A, E | A \in GL(n, Z_p)\}$를 생각하자. 보조정리 1에 의해 $K \subset F$이다. K의 원소들은 모두 O이 아니므로, 비둘기 집 원리에 의하여 $A^k = E$인 k를 $p^n - 1$보다 작은 범위에서 찾을 수 있다. 즉, A의 위수는 $p^n - 1$을 넘지 않는다.
따라서 Lagrange의 정리에 의하여 A의 위수는 $p^n - 1$ 이하인 $\prod_{k=0}^{n-1}(p^n - p^k)$의 약수이다.

이것은 행렬의 위수를 더 간단하고 빠르게 구할 수 있는 새로운 방법의 토대가 될 수 있으므로, 행렬의 위수에 대한 유용한 명제라 할 수 있다.

5. K_p^n의 대수적 성질 분석

만약 군 $GL(3, Z_2)$의 어떤 부분집합이 특정한 성질을 가진다면, $GL(3, Z_2)$의 원소들을 분류하여 그 특성을 조금 더 쉽게 알 수 있다. 그러므로 우리는 K_p^n의 다른 대수적 성질에 대해서도 알아보았다. 그 결과, K_p^n, K^n, K_p는 곱셈에 대해 닫혀 있지 않다는 것을 알게 되었으며, 그밖에 알게 된 이들의 대수적 성질은 다음과 같다.

<Table 15> Characteristics of K_p^n (1)

특성다항식 $p(x)$가 대칭다항식이 아닐 때 $A \in K_p^n$이면 $A^{-1} \notin K_p^n$이다. (단, 역은 성립하지 않음)

증명.
대칭다항식의 정의에 따라 $f(x)(x^{-1})^n = f(x^{-1})$이다.
어떤 행렬 A의 특성다항식을 $f(x)$라 하자. 이때 $f(A)(A^{-1})^n = O = f(A^{-1})$이다.
따라서 $f(A^{-1}) = O$이므로 A^{-1} 또한 $f(x)$를 특성다항식으로 가진다.

<Table 16> Characteristics of K_p^n (2)

임의의 $A \in K_p^n$ 에 대하여, $D^{-1}AD \in K_p^n$이다. ($D \in GL(3, Z_2)$)

증명.
(1) 위수가 동일함
m이 $1 \leqq m < n$인 정수라 하면 $(D^{-1}AD)^m = D^{-1}A^m D \neq E$
또한, $(D^{-1}AD)^n = D^{-1}A^n D = E$
그러므로 $D^{-1}AD$의 위수는 n이다. 즉, $D^{-1}AD \in K^n$이다.
(2) 특성다항식이 동일함
행렬 A가 특성다항식으로 p를 가진다면, $p(D^{-1}AD) = D^{-1}p(A)D = 0$이므로,
행렬 $D^{-1}AD$ 또한 특성다항식으로 p를 가진다. 즉, $D^{-1}AD \in K_p$이다.
$D^{-1}AD \in K^n$이고 $D^{-1}AD \in K_p$이므로 $D^{-1}AD \in K_p^n$이다.

<Table 17> Characteristics of K_p^n (3)

$A \in K^n$이면 $A^{-1} \in K^n$이다.

증명.
(1) $n = 1$인 경우 자명하다.
(2) $n \geq 2$인 경우
임의의 행렬 $A \in K^n$에 대하여 $AA^{n-1} = A^n = E$이다. 그러므로 $A^{-1} = A^{n-1}$이다.
k를 A^{-1}의 위수라고 하자. 이때 $(A^{n-1})^k = (A^{-1})^k = E$이고, $(A^{n-1})^k = A^{(n-1)k}$이다.
따라서 $n \mid (n-1)k$이어야 한다. 그런데 n과 $n-1$은 서로소이므로 $n \mid k$이다.
한편, $(A^{-1})^n = (A^{n-1})^n = (A^n)^{n-1} = E$이다.
그러므로 행렬 A^{-1}의 위수 또한 n이다. 즉, $A^{-1} \in K^n$이다.

<Table 18> Characteristics of K_p^n (4)

임의의 행렬 $A \in K^n$에 대하여 $\gcd(m, n) = 1$이면 $A^m \in K^n$이다.

증명.
k가 $1 \leq k < n$인 정수라 하자. mk는 n의 배수가 아니므로 $(A^m)^k = A^{mk} \neq E$이다.
또한, $(A^m)^n = (A^n)^m = E$이므로 A^m의 위수는 n이다. 즉, $A^m \in K^n$이다.

$p(x)$가 대칭다항식이면 K_p^n가 곱셈에 대하여 닫혀있는 것을 제외하고 군이 되기 위한 성질을 모두 만족하고, 임의의 $A \in K_p^n$ 에 대하여 $D^{-1}AD \in K_p^n$이 성립하므로 K_p^n가 정규부분군이 될 수 있지 않을까 추측을 하였으나 곱셈에 대하여 닫혀 있지 않아서 집합을 확장해 나갔다. K^n과 K_p로 집합을 확장하여 곱셈에 대하여 닫혀 있는지 확인하였으나 닫혀 있지 않았다.
그러던 중 $GL(3, Z_2)$가 단순군이라는 사실을 발견하였다. 단순군이란 자기 자신과 항등원만을 정규부분군으로 가진다는 것이다. 우리가 조사한 세 집합이 K_p^n, K^n, K_p이 군이 된다면 $D^{-1}AD \in K_p^n$이기 때문에 이들은 $GL(3, Z_2)$의 정규부분군이 되는데, 이는 이미 밝혀진 $GL(3, Z_2)$가 단순군이라는 사실에 모순이 되어 군이 될 수 없음을 추론할 수 있었다.

Ⅳ. 연구 결과

1. $GL(3, Z_2)$의 원소의 특성다항식 및 위수 결정

우리는 다항식과 행렬의 위수를 정의하였고, $GL(3, Z_2)$의 원소의 위수가 특성다항식의 위수의 약수라는 점을 이용하여 이들의 위수를 거듭제곱을 하지 않고 구하였다. 특히 위수가 3, 7인 경우는 특성다항식만으로 위수를 구분할 수 있고, 위수가 1, 2, 4인 경우는 최소다항식까지 고려하면 위수를 구별할 수 있다.
또한, 우리는 $GL(3, Z_p)$의 원소들의 위수가 모두 p^3-1 이하라는 추측을 제시하였으며, <Table 14>에서 이 추측이 참임을 확인하였다.

2. 집합 K_p^n의 대수적 성질 파악

$GL(3,Z_2)$의 부분집합인 집합 K_p^n이 군이 될 것으로 예상하여 조사한 결과 K_p^n의 각 원소의 역원은 K_p^n의 원소가 되었고, K_p^n은 각 원소의 닮음행렬을 모두 포함하는 집합이었다. 하지만 K_p^n이 곱셈에 대하여 닫혀 있지 않아 군이 되지 않았다. 그래서 집합을 확장하여 K_p와 K^n을 정의하였으며, 이 세 집합의 대수적 성질을 연구하였으나, K_p^n과 유사한 성질을 만족할 뿐이었다.

Ⅴ. 고찰

선행연구에 따르면 정수론에서 성립하는 페르마의 작은 정리와 오일러의 정리가 행렬에서도 성립한다고 한다. 이에 우리는 행렬에서도 정수론의 성질들이 적용되는지를 탐구하기 위하여 주제를 선정하던 중 행렬에 위수의 개념을 적용해보게 되었다.
우리는 행렬에서의 위수를 탐구하기 위하여 다항식의 위수를 정의하였고, 이를 바탕으로 $GL(3, Z_2)$의 원소의 위수를 구하였으며, 집합 K^n을 정의하여 그 대수적 성질을 살펴보았다.
행렬의 위수 탐색을 통하여 행렬의 연산을 간소화할 수 있고, 행렬에 이산로그를 적용하는 등, 수학 연구에 있어 더욱 다양한 시도를 할 수 있을 것으로 생각된다. 또한, $GL(3, Z_p)$의 원소의 위수에 대하여 p가 증가할수록 행렬의 수가 급격히 증가하므로, 암호학에도 응용할 수 있을 것이다.

Ⅵ. 결론

우리는 본 연구를 통해 특성다항식의 위수를 이용하면 $GL(3, Z_2)$의 원소의 위수를 구하기 쉽다는 것을 발견하였다. 즉, 특성다항식의 위수의 약수가 행렬의 위수가 되므로 특성다항식을 조사하여 행렬의 위수를 판별할 수 있다. 우리가 연구했던 $GL(3,Z_2)$에서는 위수가 3, 7인 경우 특성다항식만으로 위수를 구분할 수 있고, 위수가 1, 2, 4인 경우는 최소다항식까지 고려하면 위수를 구별할 수 있다. 따라서 행렬의 위수를 거듭제곱을 하지 않고 최소다항식과 특성다항식을 이용하여 알 수 있다.
또한, $GL(3, Z_2)$ 상에서 정의한 집합 K_p^n의 각 원소가 $p(x)$가 대칭다항식일 때에는 역원을, 그리고 닮음인 원소를 포함하여 정규부분군이 될 수 있을 것이라 추측하였으나, 닫혀 있지 않았다. 이에 군의 조건을 만족하도록 집합을 확장하여 K^n, K_p를 정의하였으나, 이들 또한 닫혀 있지 않아서 군이 되지 않음을 알 수 있었다.

우리는 이 연구에서 $GL(3, Z_p)$ 상의 $(p^3-1)(p^3-p)(p^3-p^2)$개의 원소 위수를 연구하는 것은 p^3-p^2개의 집합 K_p을 연구하는 것으로 해결할 수 있음을 밝혔다. 그리고 $GL(3, Z_p)$상의 원소의 위수의 최댓값이 p^3-1이 될 것이라는 추측이 참임이 밝혀졌기 때문에, 우리는 이를 이용하면 더욱 효율적인 방법으로 행렬의 위수를 구할 수 있을 것으로 기대한다.

Ⅶ. 참고문헌

[1] 김응태, 박승안 (2011). 현대대수학. 경문사.

[2] 사이언스올 과학백과사전. http://www.scienceall.com/특성다항식 (검색일: 2016.3.25.).

[3] 조셉 실버만 (2015). 친절한 수론 길라잡이. 경문사.

[4] 한재영, 한응섭, 김익성 (2012). 선형대수학. 경문사.

[5] 황석근 (2012). ENV 정수론. 교우미디어.

[6] Gabe Cunningham (2005). http://www-math.mit.edu/~dav/genlin.pdf (검색일: 2016.3.25.).

[7] Howard Anton (2015). 알기 쉬운 선형대수. 범한서적.