FGB-P2008-01

08학번 수학과 권혁준

2008년 1월 17일

문제를 풀기전에 다음과 같은 정의를 해 두자.

$$\begin{aligned}
\mathbf{x_1} &= (x_1 \quad x_2 \quad x_3 \quad \cdots \quad x_n \quad) \\
\mathbf{x_2} &= (x_n \quad x_1 \quad x_2 \quad \cdots \quad x_{n-1}) \\
&\vdots \\
\mathbf{x_n} &= (x_2 \quad x_3 \quad x_4 \quad \cdots \quad x_1 \quad) \\
\mathbf{y_1} &= (1 \quad 0 \quad 0 \quad \cdots \quad 0) \\
\mathbf{y_2} &= (0 \quad 1 \quad 0 \quad \cdots \quad 0) \\
&\vdots \\
\mathbf{y_n} &= (0 \quad 0 \quad 0 \quad \cdots \quad 1)
\end{aligned}$$

또한 집합 S를 다음과 같이 정의하자.

$$S = \left\{ \left(\begin{array}{c} \mathbf{z_1} \\ \vdots \\ \mathbf{z_n} \end{array} \right) \middle| \forall i (\mathbf{z_i} = \mathbf{x_i} \vee \mathbf{z_i} = \mathbf{y_i}) \right\}$$

그리고 앞으로 모든 index는 $\mathbb{F}_n$의 원소를 사용하자.

먼저 다음과 같은 $Z : \wp(\mathbb{F}_n) \to S$를 생각하자.

$$Z(A) = \left(\begin{array}{c} \mathbf{z_1} \\ \vdots \\ \mathbf{z_n} \end{array} \right) (\text{if } i \in A \text{ then } \mathbf{z_i} = \mathbf{y_i}, \text{ if not } \mathbf{z_i} = \mathbf{x_i} \ )$$

그러면 Z는 전단사함수가 되므로 모든 S의 원소는 유일하게 이러한 표기가 가능함을 알 수 있다. 그러므로 $T : S \to S$를 다음과 같이 정의할 수 있다.

$$T(Z(\{b_1, b_2, \cdots, b_m\})) = Z(\{b_1 + 1, b_2 + 1, \cdots, b_n + 1\})$$

이 때

$$\begin{aligned}
T^n(Z(\{b_1, b_2, \cdots, b_m\})) &= Z(\{b_1 + n, b_2 + n, \cdots, b_n + n\}) \\
&= Z(\{b_1, b_2, \cdots, b_n\})
\end{aligned}$$

이므로 T^n는 항등함수다. (여기서 T^n은 T를 n번 합성한 함수이다.)

또한 T는 행렬의 가장 아래에 있는 row를 맨 위로 옮기는 함수와, 가장 오른쪽에 있는 column을 가장 왼쪽으로 옮기는 합성한 함수와 같다. 여기서 두 함수는

각각, n번째 행과 $n-1$번째 행을 바꾸는 함수, $n-1$번째 행과 $n-2$번째 행을 바꾸는 함수, $\cdots$, 2번째 행과 1번째 행을 바꾸는 함수들을 합성한 함수, n번째 열과 $n-1$번째 열을 바꾸는 함수, $n-1$번째 열과 $n-2$번째 열을 바꾸는 함수, $\cdots$, 2번째 열과 1번째 열을 바꾸는 함수들을 합성한 함수이다. 즉 T는 어떠한 $n-1$개의 elementary row operation과, $n-1$개의 elementary column operation을 합성한 함수와 같다. 따라서 T는 determinant값을 변화시키지 않는다.

이제 다음과 같은 S위의 relation R을 생각하자.

$$R = \{(a,b) | \exists (i \in \mathbb{N})(T^i(a) = b)\}$$

그러면 임의의 a에 대해서 $T^n(a) = a$이므로, $(a,a) \in R$이다. 또한 $(a,b) \in R$이면, $T^i(a) = b$에서 $T^{n-i}(b) = T^{i+(n-i)}(a) = a$이므로, $(b,a) \in R$이다. 그리고 $(a,b) \in R$이고, $(b,c) \in R$이면, $T^i(a) = b$, $T^j(b) = c$에서 $T^{i+j}(a) = T^j(b) = c$이므로 $(a,c) \in R$이다. 따라서 R은 equivalence relation이고, 그러므로 equivalence class들의 집합 P를 잡을 수 있다. 여기서 T는 determinant값을 변화시키지 않으므로 우리는 P의 원소 A에 대해 $D(A)$를 A의 한 원소의 determinant값이라고 정의하면 A는 공집합이 아니고, 모든 원소의 determinant값이 같으므로 D는 well-defined된다.

여기서 $T(Z(\emptyset)) = Z(\emptyset)$이고, $T(Z(\{1,2,\cdots,n\})) = Z(\{1,2,\cdots,n\})$이므로 $\{Z(\emptyset)\}$, $\{Z(\{1,2,\cdots,n\})\}$는 P의 원소가 된다. 이제 이 둘을 제외한 나머지 모든 원소의 크기는 p의 배수임을 보이자. (p는 문제에서 주어졌듯이 $n = p^r$이게 하는 소수이다.)

$A \in P$가 존재해서 $|A|$가 p와 서로소라고 하자. 그러면 한 원소 $Z(A)$를 잡을 수 있다.(여기서 A는 공집합이 아니므로 $A = \{b_1, \cdots, b_n\}$라고 하면 적어도 b_1은 존재한다.) 이 때 $T^n = I$이므로 $|A|$는 $T^k(Z(\{b_1,\cdots,b_n\})) = Z(\{b_1,\cdots,b_n\})$이게하는 최소의 k와 같다. 따라서 이것을 최소로 하는 k는 p와 서로소이다. 여기서 $(\mathrm{mod}\ p^r)$에 대한 k의 잉여역수와 합동인 자연수 k^*를 잡자. 그러면

$$\begin{aligned} T^{kk^*}(Z(\{b_1,\cdots,b_n\})) &= T(Z(\{b_1,\cdots,b_n\})) \\ &= Z(\{b_1+1,\cdots,b_n+1\}) \end{aligned}$$

따라서 $b_i \in A$이므로 $b_i + 1 \in A$ 그러므로 $b_i + 2 \in A$이고, 마찬가지 방법으로 계속하면 $A = 1, 2, \cdots, n$이게 되이서 모순이다. 그러므로 $|A|$는 p의 배수이다.

이제 $x_1, x_2, \cdots, x_n$을 변수로 하는 다음과 같은 n변수 다항식을 생각하자.

$$\det \begin{pmatrix} x_1+1 & x_2 & x_3 & \cdots & x_n \\ x_n & x_1+1 & x_2 & \cdots & x_{n-1} \\ x_{n-1} & x_n & x_1+1 & \cdots & x_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_2 & x_3 & x_4 & \cdots & x_1+1 \end{pmatrix}$$

여기서 이 다항식에 $x_1 + x_2 + \cdots + x_n = 0$이게 값을 대입했을 때 이 식의 값을 p로 나눈 나머지가 1이 됨을 보이자.

$$\begin{aligned}
& \det \begin{pmatrix} x_1+1 & x_2 & x_3 & \cdots & x_n \\ x_n & x_1+1 & x_2 & \cdots & x_{n-1} \\ x_{n-1} & x_n & x_1+1 & \cdots & x_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_2 & x_3 & x_4 & \cdots & x_1+1 \end{pmatrix} \\
= \quad & \det \begin{pmatrix} \mathbf{x_1+y_1} \\ \mathbf{x_2+y_2} \\ \mathbf{x_3+y_3} \\ \vdots \\ \mathbf{x_n+y_n} \end{pmatrix} \\
= \quad & \det \begin{pmatrix} \mathbf{x_1} \\ \mathbf{x_2+y_2} \\ \mathbf{x_3+y_3} \\ \vdots \\ \mathbf{x_n+y_n} \end{pmatrix} + \det \begin{pmatrix} \mathbf{y_1} \\ \mathbf{x_2+y_2} \\ \mathbf{x_3+y_3} \\ \vdots \\ \mathbf{x_n+y_n} \end{pmatrix} \\
= \quad & \det \begin{pmatrix} \mathbf{x_1} \\ \mathbf{x_2} \\ \mathbf{x_3+y_3} \\ \vdots \\ \mathbf{x_n+y_n} \end{pmatrix} + \det \begin{pmatrix} \mathbf{x_1} \\ \mathbf{y_2} \\ \mathbf{x_3+y_3} \\ \vdots \\ \mathbf{x_n+y_n} \end{pmatrix} + \det \begin{pmatrix} \mathbf{y_1} \\ \mathbf{x_2} \\ \mathbf{x_3+y_3} \\ \vdots \\ \mathbf{x_n+y_n} \end{pmatrix} + \det \begin{pmatrix} \mathbf{y_1} \\ \mathbf{y_2} \\ \mathbf{x_3+y_3} \\ \vdots \\ \mathbf{x_n+y_n} \end{pmatrix}
\end{aligned}$$

$$
\begin{aligned}
&\vdots \\
&= \sum_{\forall i(\mathbf{z_i}=\mathbf{x_i}\vee\mathbf{z_i}=\mathbf{y_i})} \det \begin{pmatrix} \mathbf{z_1} \\ \mathbf{z_2} \\ \mathbf{z_3} \\ \vdots \\ \mathbf{z_n} \end{pmatrix} \\
&= \sum_{M\in S} \det(M) \\
&= \sum_{A\in P} \sum_{M\in A} \det(M) \\
&= \sum_{A\in P} |A| D(A) \\
&\equiv D(\{Z(\emptyset)\}) + D(\{Z(\{1,2,\cdots,n\})\}) (\mathrm{mod}\ p) \\
&\equiv \det \begin{pmatrix} \mathbf{x_1} \\ \mathbf{x_2} \\ \mathbf{x_3} \\ \vdots \\ \mathbf{x_n} \end{pmatrix} + 1 (\mathrm{mod}\ p)
\end{aligned}
$$

여기서 $x_1, x_2, \cdots, x_n$에 $x_1 + x_2 + \cdots + x_n = 0$이게 값을 대입하면, $\mathbf{x_1} + \mathbf{x_2} + \cdots + \mathbf{x_n} = (0 \quad 0 \quad 0 \quad \cdots \quad 0)$이게 된다. 따라서 $\mathbf{x_1}, +\mathbf{x_2}, \cdots, \mathbf{x_n}$들은 일차종속이 되어서

$$
\det \begin{pmatrix} \mathbf{x_1} \\ \mathbf{x_2} \\ \mathbf{x_3} \\ \vdots \\ \mathbf{x_n} \end{pmatrix} = 0
$$

이 된다. 그러므로 주어진 다항식의 값을 p로 나누면 나머지가 1이 된다. 여기서 $x_1, x_2, x_3, \cdots, x_n$에 각각 $a_1 - 1, a_2, a_3, \cdots, a_n$을 대입하면, $(a_1 - 1) + a_2 + a_3 +$

$\cdots + a_n = 0$이므로 결국 다음과 같은 결과를 얻을 수 있다.

$$\det \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ a_n & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1} & a_n & a_1 & \cdots & a_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_2 & a_3 & a_4 & \cdots & a_1 \end{pmatrix} \equiv 1 (\mathrm{mod}\ p)$$

그런데 여기서 p가 1이 아니므로 위의 행렬식의 값은 0이 될 수 없다. 따라서

$$\begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ a_n & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1} & a_n & a_1 & \cdots & a_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_2 & a_3 & a_4 & \cdots & a_1 \end{pmatrix}$$

은 nonsingular이다.