페르마의 마지막 정리와 보형곡선

유화종

서울대학교

1 첫번째 강의: 페르마의 마지막 정리와 와일즈의 결과 소개

초록: 이번 강의에서는 다음 정리의 역사와 증명에 대해 간단하게 공부할 것이다.

Theorem 1 (Fermat's Last theorem, Wiles)**.** 임의의 자연수 $n \geq 3$에 대하여 다음의 방정식

$$x^n + y^n = z^n \quad \text{and} \quad xyz \neq 0$$

은 정수해를 갖지 않는다.

이 문제를 해결하기 위해 도입된 여러가지 현대수학들과 와일즈의 증명에 대해서 각종 유명한 정리들을 소개하고, 그들의 의미에 대해서 알아본다.

- 문제 1: 소수 p에 대하여 다음 집합의 원소의 개수를 N_p라 하자. 20이하의 소수 p에 대하여 N_p를 구하여라.
$$E = \{y^2 \equiv x^3 + x \pmod{p} : x, y \in \mathbb{Z} \quad \text{and} \quad 0 \leq x, y < p\}.$$

- 문제 2: 우선 a, b, m, n을 유리수라 하자. 좌표평면에 $y^2 = x^3 + ax + b$이 그리는 자취와 $y = mx + n$이 세개의 점 $(x_1, y_1), (x_2, y_2), (x_3, y_3)$에서 만난다고 가정하자. ($x_i = x_j$ $(i \neq j)$인 경우도 허용한다.) 이 때, x_1, x_2가 유리수이면 x_3, y_1, y_2, y_3는 모두 유리수임을 증명하여라.

- 문제 3: 체 F를 finite Galois extension field of $\mathbb{Q}$라고 하자. 또한 Extension $F/\mathbb{Q}$의 갈루아 군을 G라고하자. 우선 $f(x, y) \in \mathbb{Q}(x, y)$를 유리계수의 이 변수 다항식이라고 하자. 점 $(a, b) \in F \times F$를 $f(a, b) = 0$을 만족시키는 체 F안에 있는 방정식 $f(x, y) = 0$의 해라고 할 때, 임의의 $\sigma \in G$에 대하여 $f(\sigma(a), \sigma(b)) = 0$임을 보여라. 다시 말해서, $P = (a, b) \in F \times F$가 $f(x, y) = 0$의 해라면 $\sigma \cdot P = (\sigma(a), \sigma(b)) \in F \times F$도 역시 방정식 $f(x, y) = 0$의 해가 된다.

- 문제 4: $\mathrm{SL}_2(\mathbb{Z})$를 정수계수의 이차 정사각행렬 중 행렬식이 1인 것들이라고 하자. 다시 말해,

  $$\mathrm{SL}_2(\mathbb{Z}) := \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbb{Z}) : ad - bc = 1 \right\}.$$

  또한 $\mathbb{H} := \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$를 복소 상반평면이라고 하자. (허수부가 양수인 복소수의 집합) 이 때, $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mathrm{SL}_2(\mathbb{Z})$와 $z \in \mathbb{H}$에 대하여 다음과 같이 정의한다.

  $$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot z := \frac{az + b}{cz + d}.$$

($\mathrm{SL}_2(\mathbb{Z})$가 $\mathbb{H}$에 linear fractional transformation, or Möbius transformation, 으로 작용한다 (act)고 한다.) 이 때, 다음을 만족하는 $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$를 찾아라.

$$\gamma^k \cdot z = z \text{ for some } k \in \mathbb{N} \quad \text{and} \quad z \in \mathbb{H}.$$

(Hint: $k = 1$ 일 때 조건을 찾고 그를 이용하여 $k \geq 2$인 경우를 다뤄보아라.)

2 두번째 강의: 타원곡선과 리만곡면론

초록: 타원곡선과 리만곡면에 대해 소개하고, 복소함수론의 여러결과들을 이용하여 타원곡선과 리만곡면에 대한 여러 정리들을 소개한다. 좀더 자세히 말해서 j-invariant, Weierstrass의 결과와 Riemann-Hurwitz의 정리를 소개한다. 리만곡면 위에 정의된 meromorphic 함수와 differential forms에 대한 내용을 공부한다.

- 문제 1: $\Lambda_z = \mathbb{Z} \oplus \mathbb{Z}_z$와 $\Lambda_{z'} = \mathbb{Z} \oplus \mathbb{Z}_{z'}$이 언제 같은 lattice가 되는지 알아보아라.

- 문제 2: 자연수 $N > 1$이 주어졌다고 하자. 문제 1을 잘 해결하면 다음의 결과를 얻는다.

$$\Lambda_z \simeq \Lambda_{z'} \iff \exists \gamma \in \mathrm{SL}_2(\mathbb{Z}) \text{ such that } \gamma \cdot z = z'.$$

  이제 $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$가 존재하여 $\gamma \cdot z = z'$이라고 하자. 그러면 isomorphism $f : \Lambda_z \to \Lambda_{z'}$이 존재한다. 만일 $f(\frac{1}{N}) = \frac{1}{N}$이 성립한다면 $abcd$는 어떠한 조건을 만족해야 하는지 찾아라. 좀 더 일반적으로 만일 $f(\frac{1}{N}) = \frac{k}{N}$ for some $k \in \mathbb{Z}$ with $\gcd(k, N) = 1$이 성립한다면 어떠한 조건이 필요한지 찾아라.

- 문제 3: 임의의 유리수 $\frac{p}{q}$와 ∞에 대하여 다음의 action을 정의한다.

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot \frac{p}{q} = \frac{ap + bq}{cp + dq} \quad \text{and} \quad \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot \infty = \frac{a}{c}.$$

  여기서 $cp + dq = 0$이면 $\frac{ap+bq}{cp+dq} = \infty$를 의미한다. 이제, 임의의 유리수 x와 y에 대하여 다음을 만족시키는 행렬 $\gamma \in \mathrm{SL}_2(\mathbb{Z})$가 존재함을 보여라.

$$\gamma \cdot x = y.$$

3 세번째 강의: 보형곡선과 보형형식 소개

두 번째 강의에서 했던 내용을 바탕으로 보형곡선과 보형형식을 소개한다. 특히 다음의 군

$$\Gamma_0(N) := \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \pmod{N}\}$$

에 대하여 보형곡선 $X_0(N)$을 정의하고 cusps에 대하여 소개한다. 특정한 N에 대하여 $X_0(N)$의 cusps을 분류하고 $X_0(N)$의 종수를 계산하는 공식을 도출해본다.

- 문제 1: 서로 다른 두 소수 p, q에 대하여 $N = p^2 q$일 때, $X_0(N)$의 cusps의 개수를 구하고 그 representatives를 찾아라.

- 문제 2: Weight 2 보형형식 f for $\Gamma_0(N)$에 대하여 $f(z)dz$가 $X_0(N)$에 살고 있는 differential form이 됨을 보여라. 역으로 임의의 differential form on $X_0(N)$은 위와 같은 형태로 쓰여짐을 보여라.

각 강의에 대한 참고문헌은 다음 웹페이지에 올려두었습니다.
https://sites.google.com/site/hwajong/references