Math 6170 C, Lecture on May 18 , 2020

Yongchang Zhu

Plan

(1) XI (Knapp). Eichler-Shimura Theory (continued)

(2) Famous Conjectures about Elliptic Curves

(3) Final Exam

XI. Eichler-Shimura Theory (continued).

Let $\mathcal{H}^* = \mathcal{H} \sqcup \mathbb{Q} \sqcup \{\infty\}$.

$$X_0(N) = \Gamma_0(N) \backslash \mathcal{H}^*$$

is a compact Riemann surface therefore a projective algebraic curve over $\mathbb{C}$.

Proposition 11.6 The space of holomorphic differentials on $X_0(N)$ is canonically isomorphic to $S_2(\Gamma_0(N))$.

Since $X_0(1) \cong \mathbb{P}^1$, the function field of $X_0(1)$ is isomorphic to $\mathbb{C}(t)$.
The function field of $X_0(1)$ is $\mathbb{C}(j)$
where

$$j(\tau) = 1728 g_2(\tau)^3 / \Delta(\tau)$$

It has q-expansion

$$j = q^{-1} + 744 + \sum_{n=1}^{\infty} c_n q^n,$$

All the coefficients are in $\mathbb{Z}_{>0}$.

Theorem 11.33. The function field of $X_0(N)$ is $\mathbb{C}(j, j_N)$.

Where $j_N(\tau) = j(N\tau)$. The minimal polynomial of j_N over $\mathbb{C}(j(\tau))$ is

$$\Phi_N(X) = \Pi_{i=1}^{k_N}(X - j \circ \alpha_i)$$

where α_i $(i = 1, \ldots, k_N)$ are given by

$$SL(2,\mathbb{Z}) \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} SL(2,\mathbb{Z}) = \sqcup_{i=1}^{k_N} SL(2,\mathbb{Z})\alpha_i$$

Because $\mathbb{Q}(j, j_N) \cap \bar{\mathbb{Q}} = \mathbb{Q}$, so $X_0(N)$ has a model over $\mathbb{Q}$.

Theorem. Let $f(\tau) = \sum_{n=1}^{\infty} c_n e^{2\pi i n\tau}$ be a new form in $S_2(\Gamma_0(N))$ with $c_1 = 1$ and $c_n \in \mathbb{Z}$, then there exists an elliptic curve E such that

$$L(E, s) = L(f, s) = \sum_{n=1}^{\infty} \frac{c_n}{n^s}.$$

E is a quotient of the Jacobian variety $J(X_0(N))$ by a codimension one subvariety.

The Hecke algebra of $\Gamma_0(N)$ acts on $J(X_0(N))$ as endomorphisms of abelian variety and this action plays a key role in the construction.

The function j also appears in finite group theory and conformal field theory in a surprising way.

A finite group G is called a simple group if it has only two normal subgroups $\{e\}$ and G itself.

Classification of finite simple groups:

(1). Cyclic groups of prime order.

(2). Alternating groups A_n ($n \geq 5$).

(3) (generic type) Lie type.
Examples: $SL(n, F_q)/Z$, where F_q is a finite field of order q, Z is the center.
In general $G(F_q)/Z$, where G is a simple algebraic group over F_q, Z is the center.

(4) 26 exceptional finite simple groups: sporadic groups.

The largest (in terms of order) sporadic group is the so called the Monster M. The order of M is

$$2^{46} \cdot 3^{20} \cdot 5^{9} \cdot 7^{6} \cdot 11^{2} \cdot 13^{3} \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$$

which has more than 50 decimal digits.

The Monster group can be characterized as the symmetry group of a very special vertex operator algebras (some structure appeared first in mathematical physics) so called the Moonshine module V.

$$V = V_0 \oplus V_1 \oplus V_2 \oplus \dots$$

The graded dimension

$$Ch\, V = q^{-1} \sum_{n=0}^{\infty} \dim V_n\, q^n$$

is equal to $j(\tau) - 744$.

Its relation with the theory of elliptic curves is not explored.

Some Famous Conjectures.

Taniyama-Shimura-Weil Conjecture.
Every elliptic curves over $\mathbb{Q}$ can be constructed from a normalized new form in $S_2(\Gamma_0(N))$ with $\mathbb{Z}$-coefficients.

Wiles proved the conjecture in 1995 for semi-stable elliptic curves.

Diamond, Conrad, Taylor and Breuil proved the remaining cases based on Wiles' work.

To state ABC Conjecture, we need to define the radical of a positive integer.
Let n be a positive integer, the radical of n is defined as

$$\mathrm{rad}(n) = \Pi_{p:\mathrm{primes}\, p|n} p$$

Examples. $\mathrm{rad}(100) = 2 \cdot 5 = 10$

$\mathrm{rad}(2020) = 2 \cdot 5 \cdot 101 = 1010$
Because $2020 = 2^2 \cdot 5 \cdot 101$.

ABC Conjecture. For every $r > 1$, and positive integers A, B, C such that

$$A + B = C,\ \gcd(A, B, C) = 1$$

Then

$$C \leq \delta \operatorname{rac}(ABC)^r$$

for some scalar δ depending only on r.

Szpiro conjecture. Given $\epsilon > 0$, there exists a constant $C(\epsilon)$ such that for any elliptic curve E defined over $\mathbb{Q}$ with minimal discriminant Δ and conductor N, we have

$$|\Delta| \leq C(\epsilon)\, N^{6+\epsilon}.$$

A quick way to define the conductor is to use modularity result: assume E corresponds to a new form $f \in S_2(\Gamma_0(N))$, its conductor is N.

Modified Szpiro conjecture. Given $\epsilon > 0$, there exists a constant $C(\epsilon)$ such that for any elliptic curve E over $\mathbb{Q}$ with invariants c_4, c_6 (in the minimal model) and conductor N, we have

$$\max(|c_4|^3, |c_6|^2) \leq C(\epsilon)\, N^{6+\epsilon}$$

It is knows that the modified Szpiro conjecture implies ABC conjecture.

In 2012, Shinichi Mochizuki claimed a proof of Szpiro's conjecture. But the proof has not been accepted by number theory community.

Birch and Swinnerton-Dyer conjecture. The rank of $E(\mathbb{Q})$ is equal to the order of vanishing of $L(s, E)$ at $s = 1$.

Final Exam.

Problem 1. Let p be an odd prime with $p \equiv 2 \mod 3$. Let $B \in \mathbb{Z}$ is relatively prime to p.
(1). Prove that E given by the equation

$$y^2 = x^3 + B$$

is an elliptic curve over finite field $\mathbb{Z}/p\mathbb{Z}$.
(2). Prove that $|E(\mathbb{Z}/p\mathbb{Z})| = p + 1$.
(3). Find the zeta function of E.
(4). Find $|E(k_{p^n})|$, where k_{p^n} is the finite finite field with p^n elements.

Hint: (1) An equation $y^2 = x^3 + Ax + B$ over a field K defines an elliptic curve iff $x^3 + Ax + B = 0$ has no multiple roots in $\bar{K}$ iff $4A^3 + 27B^2 \neq 0$.

(2) Give $y \in \mathbb{Z}/p\mathbb{Z}$, prove that there is unique $x \in \mathbb{Z}/p\mathbb{Z}$ such that (x, y) is a solution.

(3) (4) Use results in [S] Chapter V, $Z(E, T) = \frac{1 - aT + pT^2}{(1-T)(1-pT)}$ Factorize

$$1 - aT + pT^2 = (1 - \alpha T)(1 - \beta T)$$

Then

$$|E(k_{p^n})| = 1 - \alpha^n - \beta^n + p^n$$

Problem 2.

Let $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$, $\mathcal{M}(\Lambda)$ be the space of elliptic functions $f(z)$ with period lattice Λ. For each positive integer n, $f \in \mathcal{M}(\Lambda)$, we define

$$(T_n f)(z) = \sum_{j,k=0}^{n-1} f(\frac{z}{n} + \frac{j}{n}\tau + \frac{k}{n})$$

(1) Prove that $T_n f$ is an elliptic functions with period lattice Λ. So we have a linear operator $T_n : \mathcal{M}(\Lambda) \to \mathcal{M}(\Lambda)$.
(2) Prove that $T_m T_n = T_{mn}$.
(3). Let $\wp(z, \tau)$ be the Weierstrass function for Λ, i.e.,

$$\wp(z, \tau) = \frac{1}{z^2} + \sum_{\omega \in \Lambda - \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

Prove that

$$T_n \wp(z, \tau) - n^2 \wp(z, \tau) = \sum_{0 \le j,k \le n-1, \text{not both } 0} \wp(\frac{j}{n}\tau + \frac{k}{n}, \tau)$$

Hint: Prove that

$$\sum_{0 \leq j,k \leq n-1, \text{not both } 0} \wp(\frac{j}{n}\tau + \frac{k}{n}, \tau) = 0$$

is a modular form of weight 2 for $SL(2, \mathbb{Z})$. Then apply Corollary 8.7 in [K].

Problem 3. The height of a point $P \in \mathbb{P}^1(\mathbb{Q})$ is defined as follows: write $P = [m, n]$ so that $gcd(m, n) = 1$,

$$H_{\mathbb{Q}}(P) = \max(|m|, |n|).$$

The height zeta function of $\mathbb{P}^1(\mathbb{Q})$ is defined as

$$Z_H(s) = \sum_{P \in \mathbb{P}^1(\mathbb{Q})} \frac{1}{H_{\mathbb{Q}}(P)^s}.$$

Prove that $Z_H(s)$ converges on $\operatorname{re} s > 2$ and is equal to

$$4\frac{\zeta(s-1)}{\zeta(s)}$$

where $\zeta(s)$ is the Riemann zeta function.

hint: To a Dirichlet series $\sum_{n=1}^{\infty} c_n n^s$ converges on $\mathrm{re}\, s > r$, try to prove $\sum_{n=1}^{\infty} |c_n| n^{\mathrm{re}\, s} < \infty$ for $\mathrm{re}\, s > r$, compare it with Riemann zeta function.

If a Dirichlet series $\sum_{n=1}^{\infty} c_n n^s$ is multiplicative, i.e., $c_{mn} = c_m c_n$ for $gcd(m, n) = 1$, then it has an Euler product

$$\Pi_{p:\mathrm{primes}}(1 + \frac{c_p}{p^s} + \frac{c_{p^2}}{p^{2s}} + \dots)$$

Problem 4. Let E be a unique elliptic curve E over $\mathbb{C}$ such that $\mathrm{End}(E) \neq \mathbb{Z}$, prove that $j(E)$ is an algebraic number.

hint: use $E = \mathbb{C}/\Lambda$ for some lattice $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$. then every $f \in \mathrm{End}(E)$ is given by a complex number α such that $\alpha\Lambda \subset \Lambda$.

Two elliptic curves are isomorphic iff $j(E_1) = j(E_2)$. For $E = \mathbb{C}/\mathbb{Z} + \mathbb{Z}\tau$, $j(E) = j(\tau)$.

End