The rational cuspidal subgroup of $J_0(p^2M)$

Myungjun Yu

(joint with Jai-Wei Guo, Yifan Yang and Hwajong Yoo)

Korea Institute for Advanced Study

mjyu@kias.re.kr

PANT - Kyoto 2021

Dec 8, 2021

Overview

1. Modular curves $X_0(N)$ and the rational cuspidal group

2. Comparison of two cuspidal subgroups

3. Explicit conditions for modular units

4. Main theorems

Modular curves $X_0(N)$ and the rational cuspidal group

Modular curves $X_0(N)$

Let N be a positive integer. Let

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

Let $\mathbb{H}$ be the upper half plane. Let

$$Y_0(N) := \Gamma_0(N) \backslash \mathbb{H}$$

Modular curves $X_0(N)$

Let N be a positive integer. Let

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

Let $\mathbb{H}$ be the upper half plane. Let

$$Y_0(N) := \Gamma_0(N) \backslash \mathbb{H}$$

There is a compactification

$$X_0(N) = Y_0(N) \cup \{\text{cusps}\},$$

which is called a modular curve of level N.

Cusps of $X_0(N)$

We have

$$\{\text{cusps}\} = \Gamma_0(N)\backslash\mathbb{P}^1(\mathbb{Q}).$$

Cusps of $X_0(N)$

We have

$$\{\text{cusps}\} = \Gamma_0(N)\backslash\mathbb{P}^1(\mathbb{Q}).$$

Cusps of $X_0(N)$

A set of (inequivalent) cusps for $\Gamma_0(N)$ is given by

$$\left\{\frac{a}{c} : c|N, (a,c) = 1, \text{ and } 1 \le a \le (c, N/c)\right\}.$$

Cusps of $X_0(N)$

We have

$$\{\text{cusps}\} = \Gamma_0(N)\backslash\mathbb{P}^1(\mathbb{Q}).$$

Cusps of $X_0(N)$

A set of (inequivalent) cusps for $\Gamma_0(N)$ is given by

$$\left\{\frac{a}{c} : c|N, (a,c) = 1, \text{ and } 1 \leq a \leq (c, N/c)\right\}.$$

Example

$$\begin{pmatrix} 1 & 0 \\ N & 1 \end{pmatrix}\infty = \frac{1}{N} \implies \frac{1}{N} \sim \infty.$$

Cusps of $X_0(N)$

We have

$$\{\text{cusps}\} = \Gamma_0(N)\backslash\mathbb{P}^1(\mathbb{Q}).$$

Cusps of $X_0(N)$

A set of (inequivalent) cusps for $\Gamma_0(N)$ is given by

$$\left\{\frac{a}{c} : c|N, (a,c) = 1, \text{ and } 1 \leq a \leq (c, N/c)\right\}.$$

Example

$$\begin{pmatrix} 1 & 0 \\ N & 1 \end{pmatrix} \infty = \frac{1}{N} \implies \frac{1}{N} \sim \infty.$$

The number of cusps of $X_0(N)$ is

$$\sum_{1 \leq c|N} \phi((c, N/c)).$$

Cusps of $X_0(N)$

1. A cusp a/c is defined over $\mathbb{Q}(\mu_d)$, where $d = (c, N/c)$ and μ_d denotes a primitive d-th root of unity.

Cusps of $X_0(N)$

1. A cusp a/c is defined over $\mathbb{Q}(\mu_d)$, where $d = (c, N/c)$ and μ_d denotes a primitive d-th root of unity.
2. If $\sigma_s \in \mathrm{Gal}(\mathbb{Q}(\mu_d)/\mathbb{Q})$ sends μ_d to μ_d^s, then

$$\sigma_s\left(\frac{a}{c}\right) = \frac{as^*}{c},$$

where s^* is such that $ss^* \equiv 1 \pmod{d}$.

Cusps of $X_0(N)$

1. A cusp a/c is defined over $\mathbb{Q}(\mu_d)$, where $d = (c, N/c)$ and μ_d denotes a primitive d-th root of unity.
2. If $\sigma_s \in \mathrm{Gal}(\mathbb{Q}(\mu_d)/\mathbb{Q})$ sends μ_d to μ_d^s, then

$$\sigma_s\left(\frac{a}{c}\right) = \frac{as^*}{c},$$

where s^* is such that $ss^* \equiv 1 \pmod{d}$.

3. Let L be the largest integer such that $L^2|N$. Then all cusps are defined over $\mathbb{Q}(\mu_L)$.

Cusps of $X_0(N)$

1. A cusp a/c is defined over $\mathbb{Q}(\mu_d)$, where $d = (c, N/c)$ and μ_d denotes a primitive d-th root of unity.
2. If $\sigma_s \in \mathrm{Gal}(\mathbb{Q}(\mu_d)/\mathbb{Q})$ sends μ_d to μ_d^s, then

$$\sigma_s\left(\frac{a}{c}\right) = \frac{as^*}{c},$$

   where s^* is such that $ss^* \equiv 1 \pmod{d}$.
3. Let L be the largest integer such that $L^2|N$. Then all cusps are defined over $\mathbb{Q}(\mu_L)$.
4. In particular, if N is square-free (or more generally, if $N = 2^r M$ with $r \leq 3$ and M odd squarefree), then all cusps are rational.

A canonical model $X_0(N)_{\mathbb{Q}}$

The modular curve $X_0(N)_{/\mathbb{C}}$ parametrizes (E, C), where E is an elliptic curve over $\mathbb{C}$ and C is a cyclic subgroup of order N in $E(\mathbb{C})$.

A canonical model $X_0(N)_{\mathbb{Q}}$

The modular curve $X_0(N)_{/\mathbb{C}}$ parametrizes (E, C), where E is an elliptic curve over $\mathbb{C}$ and C is a cyclic subgroup of order N in $E(\mathbb{C})$.

There is a canonical model $X_0(N)_{\mathbb{Q}}$ defined over the rational field $\mathbb{Q}$ such that

$$X_0(N) \cong X_0(N)_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathbb{C}.$$

A canonical model $X_0(N)_{\mathbb{Q}}$

The modular curve $X_0(N)_{/\mathbb{C}}$ parametrizes (E, C), where E is an elliptic curve over $\mathbb{C}$ and C is a cyclic subgroup of order N in $E(\mathbb{C})$.

There is a canonical model $X_0(N)_{\mathbb{Q}}$ defined over the rational field $\mathbb{Q}$ such that

$$X_0(N) \cong X_0(N)_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathbb{C}.$$

By abuse of notation, we also write $X_0(N)$ for $X_0(N)_{\mathbb{Q}}$.

The Jacobian $J_0(N)$ and the Mordell–Weil theorem

Let $J_0(N)$ denote the Jacobian of $X_0(N)$.

The Jacobian $J_0(N)$ and the Mordell–Weil theorem

Let $J_0(N)$ denote the Jacobian of $X_0(N)$.

$$J_0(N) = \mathrm{Div}^0(X_0(N))/\mathrm{PDiv}(X_0(N)),$$

which is an abelian variety define over $\mathbb{Q}$.

- $\mathrm{Div}^0(X_0(N))$: the group of degree zero divisors on $X_0(N)$.
- $\mathrm{PDiv}(X_0(N))$: the group of principal divisors.

The Jacobian $J_0(N)$ and the Mordell–Weil theorem

Let $J_0(N)$ denote the Jacobian of $X_0(N)$.

$$J_0(N) = \mathrm{Div}^0(X_0(N))/\mathrm{PDiv}(X_0(N)),$$

which is an abelian variety define over $\mathbb{Q}$.

- $\mathrm{Div}^0(X_0(N))$: the group of degree zero divisors on $X_0(N)$.
- $\mathrm{PDiv}(X_0(N))$: the group of principal divisors.

Theorem (Mordell–Weil)

The rational points $J_0(N)(\mathbb{Q})$ form a finitely generated abelian group. Therefore we have

$$J_0(N)(\mathbb{Q}) \cong \mathbb{Z}^r \oplus J_0(N)(\mathbb{Q})_{\mathrm{tor}},$$

where r is a non-negative integer and $J_0(N)(\mathbb{Q})_{\mathrm{tor}}$ is the torsion subgroup.

The rational cuspidal subgroup

The ultimate goal

We want to compute the torsion subgroup

$$J_0(N)(\mathbb{Q})_{\mathrm{tor}}.$$

The rational cuspidal subgroup

The ultimate goal

We want to compute the torsion subgroup

$$J_0(N)(\mathbb{Q})_{\mathrm{tor}}.$$

We call $D \in \mathrm{Div}^0(X_0(N))$ a (degree 0) cuspidal divisor if D is supported only on the cusps of $X_0(N)$.

The rational cuspidal subgroup

The ultimate goal

We want to compute the torsion subgroup

$$J_0(N)(\mathbb{Q})_{\mathrm{tor}}.$$

We call $D \in \mathrm{Div}^0(X_0(N))$ a (degree 0) cuspidal divisor if D is supported only on the cusps of $X_0(N)$.

- $\mathcal{C}_N$ (called the cuspidal subgroup) is the subgroup of $J_0(N)$ generated by the cuspidal divisors.
- We call $\mathcal{C}_N(\mathbb{Q}) := J_0(N)(\mathbb{Q}) \cap \mathcal{C}_N$ the rational cuspidal group.

The rational cuspidal subgroup

The ultimate goal

We want to compute the torsion subgroup

$$J_0(N)(\mathbb{Q})_{\mathrm{tor}}.$$

We call $D \in \mathrm{Div}^0(X_0(N))$ a (degree 0) cuspidal divisor if D is supported only on the cusps of $X_0(N)$.

- $\mathcal{C}_N$ (called the cuspidal subgroup) is the subgroup of $J_0(N)$ generated by the cuspidal divisors.
- We call $\mathcal{C}_N(\mathbb{Q}) := J_0(N)(\mathbb{Q}) \cap \mathcal{C}_N$ the rational cuspidal group.

Generalized Ogg conjecture

Let N be a positive integer. Then

$$\mathcal{C}_N(\mathbb{Q}) = J_0(N)(\mathbb{Q})_{\mathrm{tor}}.$$

Generalized Ogg conjecture

Generalized Ogg conjecture

Let N be a positive integer. Then

$$\mathcal{C}_N(\mathbb{Q}) = J_0(N)(\mathbb{Q})_{\mathrm{tor}}.$$

Generalized Ogg conjecture

Generalized Ogg conjecture

Let N be a positive integer. Then

$$\mathcal{C}_N(\mathbb{Q}) = J_0(N)(\mathbb{Q})_{\mathrm{tor}}.$$

Theorem (Manin–Drinfeld)

$$\mathcal{C}_N(\mathbb{Q}) \subseteq J_0(N)(\mathbb{Q})_{\mathrm{tor}}.$$

Generalized Ogg conjecture

Generalized Ogg conjecture

Let N be a positive integer. Then

$$\mathcal{C}_N(\mathbb{Q}) = J_0(N)(\mathbb{Q})_{\mathrm{tor}}.$$

Theorem (Manin–Drinfeld)

$$\mathcal{C}_N(\mathbb{Q}) \subseteq J_0(N)(\mathbb{Q})_{\mathrm{tor}}.$$

Theorem (Mazur)

If N is a prime, then

$$\langle\ [0-\infty]\ \rangle = \mathcal{C}_N(\mathbb{Q}) = J_0(N)(\mathbb{Q})_{\mathrm{tor}}.$$

Mazur's theorem above was previously referred to as the Ogg conjecture.

Mazur's torsion theorem

In the course of proving the Ogg conjecture, Mazur was able to get his celebrated torsion theorem:

Theorem (Mazur)

Let E be an elliptic curve defined over $\mathbb{Q}$. Then the torsion points $E(\mathbb{Q})_{\mathrm{tor}}$ must be (isomorphic to) one of the following:

$$\begin{array}{ll} \mathbb{Z}/N\mathbb{Z} & 1 \le N \le 10 \text{ or } N = 12 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/(2N)\mathbb{Z} & 1 \le N \le 4. \end{array}$$

Moreover, each of these groups occurs infinitely many times.

Known results for Generalized Ogg conjecture

- (Lorenzini, 1995) If $p \not\equiv 11 \pmod{12}$ is a prime and $r \geq 2$, then

$$J_0(p^r)(\mathbb{Q})_{\mathrm{tor}}^{(2p)} = \mathcal{C}_N(\mathbb{Q})^{(2p)}.$$

Known results for Generalized Ogg conjecture

- (Lorenzini, 1995) If $p \not\equiv 11 \pmod{12}$ is a prime and $r \geq 2$, then

$$J_0(p^r)(\mathbb{Q})_{\mathrm{tor}}^{(2p)} = \mathcal{C}_N(\mathbb{Q})^{(2p)}.$$

- (Ohta, 2014) If N is squarefree, then

$$J_0(N)(\mathbb{Q})_{\mathrm{tor}}^{(2n)} = \mathcal{C}_N(\mathbb{Q})^{(2n)},$$

where $n = (3, N)$.

Known results for Generalized Ogg conjecture

- (Lorenzini, 1995) If $p \not\equiv 11 \pmod{12}$ is a prime and $r \geq 2$, then

$$J_0(p^r)(\mathbb{Q})_{\mathrm{tor}}^{(2p)} = \mathcal{C}_N(\mathbb{Q})^{(2p)}.$$

- (Ohta, 2014) If N is squarefree, then

$$J_0(N)(\mathbb{Q})_{\mathrm{tor}}^{(2n)} = \mathcal{C}_N(\mathbb{Q})^{(2n)},$$

  where $n = (3, N)$.

- (Yoo, 2020) For any positive integer N, we have

$$J_0(N)(\mathbb{Q})_{\mathrm{tor}}^{(2n)} = \mathcal{C}_N(\mathbb{Q})^{(2n)},$$

  where n is the largest perfect square dividing $3N$.

Known results for Generalized Ogg conjecture

- (Lorenzini, 1995) If $p \not\equiv 11 \pmod{12}$ is a prime and $r \geq 2$, then

$$J_0(p^r)(\mathbb{Q})_{\mathrm{tor}}^{(2p)} = \mathcal{C}_N(\mathbb{Q})^{(2p)}.$$

- (Ohta, 2014) If N is squarefree, then

$$J_0(N)(\mathbb{Q})_{\mathrm{tor}}^{(2n)} = \mathcal{C}_N(\mathbb{Q})^{(2n)},$$

  where $n = (3, N)$.

- (Yoo, 2020) For any positive integer N, we have

$$J_0(N)(\mathbb{Q})_{\mathrm{tor}}^{(2n)} = \mathcal{C}_N(\mathbb{Q})^{(2n)},$$

  where n is the largest perfect square dividing $3N$.

- Some other results by Ling, Ren, Ligozat, Poulakis, Ozman–Siksek, Box, and so on.

Comparison of two cuspidal subgroups

The rational cuspidal divisor class group

Recall

- $\mathcal{C}_N$ is the subgroup of $J_0(N)$ generated by the cuspidal divisors.
- $\mathcal{C}_N(\mathbb{Q}) = J_0(N)(\mathbb{Q}) \cap \mathcal{C}_N$ is the rational cuspidal group.

The rational cuspidal divisor class group

Recall

- $\mathcal{C}_N$ is the subgroup of $J_0(N)$ generated by the cuspidal divisors.
- $\mathcal{C}_N(\mathbb{Q}) = J_0(N)(\mathbb{Q}) \cap \mathcal{C}_N$ is the rational cuspidal group.

We define a "possibly" smaller subgroup

$$\mathcal{C}(N) \subseteq \mathcal{C}_N(\mathbb{Q}),$$

which is generated by (the image of) rational cuspidal divisors.

The rational cuspidal divisor class group

Recall

- $\mathcal{C}_N$ is the subgroup of $J_0(N)$ generated by the cuspidal divisors.
- $\mathcal{C}_N(\mathbb{Q}) = J_0(N)(\mathbb{Q}) \cap \mathcal{C}_N$ is the rational cuspidal group.

We define a "possibly" smaller subgroup

$$\mathcal{C}(N) \subseteq \mathcal{C}_N(\mathbb{Q}),$$

which is generated by (the image of) rational cuspidal divisors.

We call $\mathcal{C}(N)$ the rational cuspidal divisor class group.

The rational cuspidal divisor class group

Recall

- $\mathcal{C}_N$ is the subgroup of $J_0(N)$ generated by the cuspidal divisors.
- $\mathcal{C}_N(\mathbb{Q}) = J_0(N)(\mathbb{Q}) \cap \mathcal{C}_N$ is the rational cuspidal group.

We define a "possibly" smaller subgroup

$$\mathcal{C}(N) \subseteq \mathcal{C}_N(\mathbb{Q}),$$

which is generated by (the image of) rational cuspidal divisors.

We call $\mathcal{C}(N)$ the rational cuspidal divisor class group.

$\mathcal{C}(N)$ vs $\mathcal{C}_N(\mathbb{Q})$

Let $[D]$ be the image of D in the map $\mathrm{Div}^0_{\text{cusp}}(X_0(N)) \to J_0(N)$.

- $\mathcal{C}(N) = \{[D] : D^\sigma = D \text{ for every } \sigma \in G_{\mathbb{Q}}\}$.
- $\mathcal{C}_N(\mathbb{Q}) = \{[D] : D^\sigma = D + \mathrm{div}(f_\sigma) \text{ for some } f_\sigma \text{ for every } \sigma \in G_{\mathbb{Q}}\}$.

The Ribet–Yoo conjecture

Ribet–Yoo Conjecture

For every positive integer N, we have

$$\mathcal{C}(N) = \mathcal{C}_N(\mathbb{Q}).$$

The Ribet–Yoo conjecture

Ribet–Yoo Conjecture

For every positive integer N, we have

$$\mathcal{C}(N) = \mathcal{C}_N(\mathbb{Q}).$$

Remark

1. We have

$$\mathcal{C}(N) \subseteq \mathcal{C}_N(\mathbb{Q}) \subseteq J_0(N)(\mathbb{Q})_{\mathrm{tor}}.$$

The Ribet–Yoo conjecture

Ribet–Yoo Conjecture

For every positive integer N, we have

$$\mathcal{C}(N) = \mathcal{C}_N(\mathbb{Q}).$$

Remark

1. We have
$$\mathcal{C}(N) \subseteq \mathcal{C}_N(\mathbb{Q}) \subseteq J_0(N)(\mathbb{Q})_{\mathrm{tor}}.$$

2. All known results toward the Generalized Ogg Conjecture showed the "stronger" equality
$$\mathcal{C}(N)[\ell^\infty] = J_0(N)(\mathbb{Q})_{\mathrm{tor}}[\ell^\infty].$$

The group $\mathcal{C}(N)$

The group $\mathcal{C}(N)$ is very explicit to study.

$$\mathcal{C}(N) = \left\langle \, [\sum_{\substack{(a,c)=1 \\ 0<a<c}} \frac{a}{c}\,] : c|N \, \right\rangle.$$

The group $\mathcal{C}(N)$

The group $\mathcal{C}(N)$ is very explicit to study.

$$\mathcal{C}(N) = \left\langle \, [\sum_{\substack{(a,c)=1 \\ 0<a<c}} \frac{a}{c}\,] : c|N \, \right\rangle.$$

Also the structure of $\mathcal{C}(N)$ is known by the work of Hwajong Yoo.

Theorem (Yoo, 2019)

For every prime ℓ, there are rational cuspidal divisors $Z_\ell(d)$ such that

$$\mathcal{C}(N)[\ell^\infty] \cong \bigoplus_{1<d|N} \langle [Z_\ell(d)] \rangle,$$

where the order of $[Z_\ell(d)]$ can be computed.

Known results for the Ribet–Yoo conjecture

Since we know the structure of $\mathcal{C}(N)$ well, it is desirable to prove Ribet–Yoo conjecture as it can be potentially helpful in proving the Generalized Ogg conjecture.

Known results for the Ribet–Yoo conjecture

Since we know the structure of $\mathcal{C}(N)$ well, it is desirable to prove Ribet–Yoo conjecture as it can be potentially helpful in proving the Generalized Ogg conjecture.

There are very few known cases for the Ribet–Yoo conjecture:

Known results for the Ribet–Yoo conjecture

Since we know the structure of $\mathcal{C}(N)$ well, it is desirable to prove Ribet–Yoo conjecture as it can be potentially helpful in proving the Generalized Ogg conjecture.

There are very few known cases for the Ribet–Yoo conjecture:

- Suppose that N is squarefree (or more generally, $N = 2^r M$ with $r \leq 3$ and M odd squarefree). Then

$$\mathcal{C}(N) = \mathcal{C}_N(\mathbb{Q}),$$

  for a trivial reason.

Known results for the Ribet–Yoo conjecture

Since we know the structure of $\mathcal{C}(N)$ well, it is desirable to prove Ribet–Yoo conjecture as it can be potentially helpful in proving the Generalized Ogg conjecture.

There are very few known cases for the Ribet–Yoo conjecture:

- Suppose that N is squarefree (or more generally, $N = 2^r M$ with $r \leq 3$ and M odd squarefree). Then

$$\mathcal{C}(N) = \mathcal{C}_N(\mathbb{Q}),$$

  for a trivial reason.
- (Wang–Yang, 2020) Let $N = n^2 M$ for $n|24$ and M squarefree. Then

$$\mathcal{C}(N) = \mathcal{C}_N(\mathbb{Q}).$$

The main results

Theorem (Guo–Yang–Yoo–Y. (2021))

Let p be an arbitrary prime. $N = p^2M$ or p^3M, where M is squarefree such that $(p, M) = 1$. Then

$$\mathcal{C}(N) = \mathcal{C}_N(\mathbb{Q}).$$

The main results

Theorem (Guo–Yang–Yoo–Y. (2021))

Let p be an arbitrary prime. $N = p^2M$ or p^3M, where M is squarefree such that $(p, M) = 1$. Then

$$\mathcal{C}(N) = \mathcal{C}_N(\mathbb{Q}).$$

Theorem (Yoo-Y. (2021+))

Let p, q be odd prime numbers. Let M be a squarefree integer. Let $N = p^rM$ or $N = p^rq^sM$ for non-negative integer r, s. Then

$$\mathcal{C}(N) = \mathcal{C}_N(\mathbb{Q}).$$

Explicit conditions for modular units

Motivation for explicit conditions for modular units

Our Goal

$$\mathcal{C}(N) = \mathcal{C}_N(\mathbb{Q}).$$

Motivation for explicit conditions for modular units

Our Goal

$$\mathcal{C}(N) = \mathcal{C}_N(\mathbb{Q}).$$

Let $[D] \in \mathcal{C}_N(\mathbb{Q})$. By definition, for every $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, there exists a modular unit f_σ such that

$$D^\sigma - D = \mathrm{div}(f_\sigma).$$

Motivation for explicit conditions for modular units

Our Goal

$$\mathcal{C}(N) = \mathcal{C}_N(\mathbb{Q}).$$

Let $[D] \in \mathcal{C}_N(\mathbb{Q})$. By definition, for every $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, there exists a modular unit f_σ such that

$$D^\sigma - D = \mathrm{div}(f_\sigma).$$

A modular unit on $X_0(N)$ is a meromorphic function on $X_0(N)$ whose divisor is supported only on cusps.

Motivation for explicit conditions for modular units

Our Goal

$$\mathcal{C}(N) = \mathcal{C}_N(\mathbb{Q}).$$

Let $[D] \in \mathcal{C}_N(\mathbb{Q})$. By definition, for every $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, there exists a modular unit f_σ such that

$$D^\sigma - D = \mathrm{div}(f_\sigma).$$

A modular unit on $X_0(N)$ is a meromorphic function on $X_0(N)$ whose divisor is supported only on cusps.

To derive the rationality of "D", it is helpful to have an explicit condition to be a modular unit.

Generalized Dedekind eta function (quotient)

$$E_{g,h}(\tau) := q^{B_2(g/N)/2} \prod_{n=1}^{\infty} \left(1 - \zeta_N^h q^{n-1+g/N}\right) \left(1 - \zeta_N^{-h} q^{n-g/N}\right),$$

where $q = e^{2\pi i \tau}$ and $B_2(x) = x^2 - x + 1/6$.

Generalized Dedekind eta function (quotient)

$$E_{g,h}(\tau) := q^{B_2(g/N)/2} \prod_{n=1}^{\infty} \left(1 - \zeta_N^h q^{n-1+g/N}\right) \left(1 - \zeta_N^{-h} q^{n-g/N}\right),$$

where $q = e^{2\pi i\tau}$ and $B_2(x) = x^2 - x + 1/6$.

Transformation properties of $E_{g,h}$

$$E_{g+N,h} = E_{-g,-h} = -\zeta_N^{-h} E_{g,h}, \quad E_{g,h+N} = E_{g,h}.$$

Moreover, let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Then for $c = 0$, we have

$$E_{g,h}(\tau + b) = e^{\pi i b B_2(g/N)} E_{g,bg+h}(\tau),$$

and for $c \neq 0$,

$$E_{g,h}(\gamma\tau) = \epsilon_\gamma e^{\pi i \delta} E_{ag+ch,bg+dh}(\tau),$$

for $\delta \in \mathbb{Q}$ and some root of unity ϵ_γ

Generalized Dedekind eta function (quotient)

$$E_{g,h}(\tau) := q^{B_2(g/N)/2} \prod_{n=1}^{\infty} \left(1 - \zeta_N^h q^{n-1+g/N}\right) \left(1 - \zeta_N^{-h} q^{n-g/N}\right),$$

where $q = e^{2\pi i \tau}$ and $B_2(x) = x^2 - x + 1/6$.

Transformation properties of $E_{g,h}$

$$E_{g+N,h} = E_{-g,-h} = -\zeta_N^{-h} E_{g,h}, \quad E_{g,h+N} = E_{g,h}.$$

Moreover, let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Then for $c = 0$, we have

$$E_{g,h}(\tau + b) = e^{\pi i b B_2(g/N)} E_{g,bg+h}(\tau),$$

and for $c \neq 0$,

$$E_{g,h}(\gamma\tau) = \epsilon_\gamma e^{\pi i \delta} E_{ag+ch,bg+dh}(\tau),$$

for $\delta \in \mathbb{Q}$ and some root of unity ϵ_γ

Construction of modular units

- $\mathcal{D}_N := \{m|N : m \neq N\}$.

Construction of modular units

- $\mathcal{D}_N := \{m|N : m \neq N\}$.

For each $m \in \mathcal{D}_N$, we fix a set $S_{m''} \subset \{1, \ldots, m''-1\}$ of representatives of $(\mathbb{Z}/m''\mathbb{Z})^\times/\{\pm 1\}$. For each $\alpha \in S_{m''}$, let $\delta \in \{1, \ldots, m''-1\}$ be an integer such that $\alpha\delta \equiv 1 \pmod{m''}$. If $m'' \neq 2$, we set

$$F_{m,h}(\tau) := \prod_{\alpha \in S_{m''}} E_{\alpha m\ell, \delta h N'}(N'\tau).$$

Construction of modular units

- $\mathcal{D}_N := \{m|N : m \neq N\}$.

For each $m \in \mathcal{D}_N$, we fix a set $S_{m''} \subset \{1, \ldots, m''-1\}$ of representatives of $(\mathbb{Z}/m''\mathbb{Z})^\times/\{\pm 1\}$. For each $\alpha \in S_{m''}$, let $\delta \in \{1, \ldots, m''-1\}$ be an integer such that $\alpha\delta \equiv 1 \pmod{m''}$. If $m'' \neq 2$, we set

$$F_{m,h}(\tau) := \prod_{\alpha \in S_{m''}} E_{\alpha m \ell, \delta h N'}(N'\tau).$$

Then for $\gamma \in \Gamma_0(N)$, we have

$$F_{m,h}(\gamma\tau) = \epsilon(\gamma, m, h) F_{m,h}(\tau),$$

for a $\mathrm{lcm}(2m'', 24)$-th root unity $\epsilon(\gamma, m, h)$. Therefore, $F_{m,h}$ is "almost" a modular unit on $X_0(N)$.

More notation

- $\mathcal{D}_N = \{m|N : m \neq N \text{ and } m > 0\}$.
- $m \in \mathcal{D}_N$.
- $\ell(m)$: the largest integer such that $\ell(m)^2|\frac{N}{m}$.
- $L = \ell(1)$: the largest integer such that $L^2|N$.

More notation

- $\mathcal{D}_N = \{m|N : m \neq N \text{ and } m > 0\}$.
- $m \in \mathcal{D}_N$.
- $\ell(m)$: the largest integer such that $\ell(m)^2|\frac{N}{m}$.
- $L = \ell(1)$: the largest integer such that $L^2|N$.

We have

$$F_{m,h} = \epsilon F_{m,h+\ell(m)},$$

for a root of unity ϵ.

More notation

- $\mathcal{D}_N = \{m|N : m \neq N \text{ and } m > 0\}$.
- $m \in \mathcal{D}_N$.
- $\ell(m)$: the largest integer such that $\ell(m)^2 | \frac{N}{m}$.
- $L = \ell(1)$: the largest integer such that $L^2|N$.

We have

$$F_{m,h} = \epsilon F_{m,h+\ell(m)},$$

for a root of unity ϵ.

So it suffices to consider $0 \leq h \leq \ell(m) - 1$ $(m \in \mathcal{D}_N)$ to construct a modular unit with $F_{m,h}$.

Various expressions for modular units on $X_0(N)$

Theorem

Every modular unit on $X_0(N)$ can be uniquely expressed as

$$\epsilon \prod_{m \in \mathcal{D}_N} \prod_{h=0}^{\phi(\ell(m))-1} F_{m,h}^{e_{m,h}} \quad \text{for some} \;\; e_{m,h} \in \mathbb{Z} \text{ and } \epsilon \in \mathbb{C}^{\times}.$$

Various expressions for modular units on $X_0(N)$

Theorem

Every modular unit on $X_0(N)$ can be uniquely expressed as

$$\epsilon \prod_{m \in \mathcal{D}_N} \prod_{h=0}^{\phi(\ell(m))-1} F_{m,h}^{e_{m,h}} \quad \text{for some} \quad e_{m,h} \in \mathbb{Z} \text{ and } \epsilon \in \mathbb{C}^{\times}.$$

Theorem

Every modular unit on $X_0(N)$ can be uniquely expressed as

$$\epsilon \prod_{m \in \mathcal{D}_N} \prod_{h=1}^{\phi(\ell(m))} F_{m,h}^{e_{m,h}} \quad \text{for some} \quad e_{m,h} \in \mathbb{Z} \text{ and } \epsilon \in \mathbb{C}^{\times}.$$

Sketch of proof

Let

- $\mathcal{I}_N := \{(m, h) : m \in \mathcal{D}_N \text{ and } 0 \leq h \leq \phi(\ell(m)) - 1\}$.
- $\mathcal{U}_N$ = the (multiplicative) group of modular units on $X_0(N)$.
- $\mathcal{U}_N^0$ = subgroup of $\mathcal{U}_N$, which consists of the product of $F_{m,h}$,

Sketch of proof

Let

- $\mathcal{I}_N := \{(m, h) : m \in \mathcal{D}_N \text{ and } 0 \leq h \leq \phi(\ell(m)) - 1\}$.
- $\mathcal{U}_N$ = the (multiplicative) group of modular units on $X_0(N)$.
- $\mathcal{U}_N^0$ = subgroup of $\mathcal{U}_N$, which consists of the product of $F_{m,h}$,

Sketch of proof

1. The cardinality of the set $\mathcal{I}_N$ is equal to the rank of $\mathcal{U}_N$, i.e., the number of cusps of $X_0(N)$ minus one.

Sketch of proof

Let

- $\mathcal{I}_N := \{(m,h) : m \in \mathcal{D}_N \text{ and } 0 \le h \le \phi(\ell(m)) - 1\}$.
- $\mathcal{U}_N$ = the (multiplicative) group of modular units on $X_0(N)$.
- $\mathcal{U}_N^0$ = subgroup of $\mathcal{U}_N$, which consists of the product of $F_{m,h}$,

Sketch of proof

1. The cardinality of the set $\mathcal{I}_N$ is equal to the rank of $\mathcal{U}_N$, i.e., the number of cusps of $X_0(N)$ minus one.
2. There are no multiplicative relations among $F_{m,h}$ with $(m,h) \in \mathcal{I}_N$. (related fact : $\zeta_{\ell(m)}^0, \zeta_{\ell(m)}^1, \ldots, \zeta_{\ell(m)}^{\phi(\ell(m))-1}$ are linearly independent)

Sketch of proof

Let

- $\mathcal{I}_N := \{(m,h) : m \in \mathcal{D}_N \text{ and } 0 \leq h \leq \phi(\ell(m)) - 1\}$.
- $\mathcal{U}_N$ = the (multiplicative) group of modular units on $X_0(N)$.
- $\mathcal{U}_N^0$ = subgroup of $\mathcal{U}_N$, which consists of the product of $F_{m,h}$,

Sketch of proof

1. The cardinality of the set $\mathcal{I}_N$ is equal to the rank of $\mathcal{U}_N$, i.e., the number of cusps of $X_0(N)$ minus one.
2. There are no multiplicative relations among $F_{m,h}$ with $(m,h) \in \mathcal{I}_N$. (related fact : $\zeta_{\ell(m)}^0, \zeta_{\ell(m)}^1, \ldots, \zeta_{\ell(m)}^{\phi(\ell(m))-1}$ are linearly independent)
3. $\mathcal{U}_N^0$ has the same rank as $\mathcal{U}_N$.

Sketch of proof

Let

- $\mathcal{I}_N := \{(m,h) : m \in \mathcal{D}_N \text{ and } 0 \le h \le \phi(\ell(m)) - 1\}$.
- $\mathcal{U}_N$ = the (multiplicative) group of modular units on $X_0(N)$.
- $\mathcal{U}_N^0$ = subgroup of $\mathcal{U}_N$, which consists of the product of $F_{m,h}$,

Sketch of proof

1. The cardinality of the set $\mathcal{I}_N$ is equal to the rank of $\mathcal{U}_N$, i.e., the number of cusps of $X_0(N)$ minus one.
2. There are no multiplicative relations among $F_{m,h}$ with $(m,h) \in \mathcal{I}_N$. (related fact : $\zeta_{\ell(m)}^0, \zeta_{\ell(m)}^1, \dots, \zeta_{\ell(m)}^{\phi(\ell(m))-1}$ are linearly independent)
3. $\mathcal{U}_N^0$ has the same rank as $\mathcal{U}_N$.
4. If $g \in \mathcal{U}_N$ and $g^k \in \mathcal{U}_N^0$, then $g \in \mathcal{U}_N^0$.

Criterion for a modular unit

Theorem

Let

$$f = \prod_{m|N, m\neq N} \prod_{h=0}^{\ell(m)-1} F_{m,h}^{e_{m,h}} \quad \text{for some} \quad e_{m,h} \in \mathbb{Z}.$$

Then f^L is a modular unit if the following conditions are satisfied:

1. *The order of f at ∞ is an integer.*
2. *The order of f at 0 is an integer.*
3. *The order of f at $1/N_0$ is an integer (if $N_0 := N/2 \in \mathbb{Z}$)*
4. $\sum_{m:m''=p^r} \sum_{h=0}^{\ell(m)-1} e_{m,h} \equiv 0 \pmod 2$.

Criterion for a modular unit

Corollary

Let $n = (3, L)$. *Then*

$$\prod_{m|N, m\neq N} \prod_{h=1}^{\ell(m)-1} \left(\frac{F_{m,h}}{F_{m,0}}\right)^{nLa_{m,h}} \quad \textit{for} \quad a_{m,h} \in \mathbb{Z}.$$

is a modular unit.

Criterion for a modular unit

Corollary

Let $n = (3, L)$. Then

$$\prod_{m|N, m\neq N} \prod_{h=1}^{\ell(m)-1} \left(\frac{F_{m,h}}{F_{m,0}}\right)^{nLa_{m,h}} \quad \text{for} \quad a_{m,h} \in \mathbb{Z}.$$

is a modular unit.

Lemma

Let $m \in \mathcal{D}_N$. Then for an integer h, the order of $F_{m,h}$ at a cusp $\frac{a}{c}$ of $X_0(N)$ is

$$\frac{\ell(N', c)^2}{4c(c, N/c)} \sum_{\alpha \in (\mathbb{Z}/m''\mathbb{Z})^\times} P_2\left(\frac{\alpha a'}{m''} + \frac{\delta h c'}{\ell}\right),$$

where $P_2(x) = B_2(\{x\})$ is the second Bernoulli function, $a' = \frac{N'a}{(N',c)}$ and $c' = \frac{c}{(N',c)}$.

Main theorems

The main result

Theorem (Guo–Yang–Yoo–Y. (2021))

Let p be an arbitrary prime. Let $N = p^2M$ or p^3M, where M is squarefree such that $(p, M) = 1$. Then

$$\mathcal{C}(N) = \mathcal{C}_N(\mathbb{Q}).$$

The main result

Theorem (Guo–Yang–Yoo–Y. (2021))

Let p be an arbitrary prime. Let $N = p^2M$ or p^3M, where M is squarefree such that $(p, M) = 1$. Then

$$\mathcal{C}(N) = \mathcal{C}_N(\mathbb{Q}).$$

Note the following two statements are equivalent.

1. $\mathcal{C}(N) = \mathcal{C}_N(\mathbb{Q})$.
2. $\mathcal{C}(N)[q^\infty] = \mathcal{C}_N(\mathbb{Q})[q^\infty]$ for any prime q.

The main result

Theorem (Guo–Yang–Yoo–Y. (2021))

Let p be an arbitrary prime. Let $N = p^2M$ or p^3M, where M is squarefree such that $(p, M) = 1$. Then

$$\mathcal{C}(N) = \mathcal{C}_N(\mathbb{Q}).$$

Note the following two statements are equivalent.

1. $\mathcal{C}(N) = \mathcal{C}_N(\mathbb{Q})$.
2. $\mathcal{C}(N)[q^\infty] = \mathcal{C}_N(\mathbb{Q})[q^\infty]$ for any prime q.

Let D be a cuspidal divisor of degree 0 such that $[D] \in \mathcal{C}_N(\mathbb{Q})[q^\infty]$. It is enough to show that $[D] \in \mathcal{C}(N)$, or equivalent, there exists a rational cuspidal divisor D' such that $[D] = [D']$.

Case (i): $q \nmid \phi(L)$

Suppose that $[D] \in \mathcal{C}_N(\mathbb{Q})[q^\infty]$ has order q^r in $J_0(N)$. Let

$$D' := \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\mu_L)/\mathbb{Q})} \sigma(D).$$

Then by definition, we have

$$\phi(L)[D] = [D'] \quad \text{and} \quad [D'] \in \mathcal{C}(N).$$

There exist $a, k \in \mathbb{Z}$ such that $(k, q) = 1$ and

$$[D] = (1 + aq^r)[D] = k\phi(L)[D] = k[D'].$$

Therefore it follows that

$$[D] \in \mathcal{C}(N).$$

Case (ii): $q \mid \phi(L)$

Recall that $[D] \in \mathcal{C}_N(\mathbb{Q})[q^\infty]$ has order q^r in $J_0(N)$. Then $q^r D = \mathrm{div}(f)$ for some modular unit f. Then

1. $$f = \prod_{m \in \mathcal{D}_N} \prod_{h=0}^{\phi(\ell(m))-1} F_{m,h}^{e_{m,h}} \quad \text{for some} \quad e_{m,h} \in \mathbb{Z}.$$
2. $q^r | e_{m,h}$ if $h \neq 0$.
3. The product
$$g = \prod_{m \in \mathcal{D}_N^1} \prod_{h=0}^{p-2} \left(\frac{F_{m,h}}{F_{m,0}}\right)^{npq^{-r}e_{m,h}},$$
where $n = (3, p)$, is a modular unit.

Put $D' = npD - \mathrm{div}(g)$. Then D' is a rational cuspidal divisor. It turns out that there exists k coprime to q such that

$$[D] = k[D'].$$

Forthcoming work

Theorem (Yoo–Y.2021+)

Let $N = p^r M$ or $N = p^r q^s M$, where p, q are odd primes and M is squarefree. Then

$$\mathcal{C}(N) = \mathcal{C}_N(\mathbb{Q}).$$

Forthcoming work

Theorem (Yoo–Y.2021+)

Let $N = p^r M$ or $N = p^r q^s M$, where p, q are odd primes and M is squarefree. Then

$$\mathcal{C}(N) = \mathcal{C}_N(\mathbb{Q}).$$

To use the same strategy as in the previous work, we need more explicit criterion for modular units on $X_0(N)$.

The modular unit criterion

Theorem (Yoo–Y.)

Suppose that L is odd (Recall $L = \max(n : n^2 | N)$). Let

$$f = \prod_{m|N, m\neq N} \prod_{h=0}^{\ell(m)-1} F_{m,h}^{k(m,h)} \quad \text{for} \ \ k(m,h) \in \mathbb{Z}.$$

Then f is a modular unit on $X_0(N)$ if and only if the following hold.

1. *The order of f at a cusp ∞ is an integer.*
2. *The order of f at a cusp 0 is an integer.*
3. *The order of f at a cusp $1/N_0$ is an integer.*
4. *(the mod L conditions)*

$$\sum_{m|N, m\neq N} \psi_i(m) \sum_{h=1}^{\ell(m)-1} hk(m,h) \equiv 0 \pmod{L}.$$

5. *(the mod 2 condition)* $\sum_{m:m''=p^r} \sum_{h=0}^{\ell(m)-1} k(m,h) \equiv 0 \pmod{2}$.

Conjecture A

Conjecture A

Let $[D] \in \mathcal{C}_N(\mathbb{Q})$, Suppose that the order of $[D]$ is n, so there is a modular unit

$$f = \prod_{m|N, m \neq N} \prod_{h=0}^{\phi(\ell(m))-1} F_{m,h}^{e(m,h)}$$

such that $\mathrm{div}(f) = nD$. Then $e(m,h)$ is divisible by n when $h \neq 0$.

It turns out that (when L is odd)

Conjecture A $\Longrightarrow$ Ribet–Yoo conjecture.

Conjecture A $\Longrightarrow$ Ribet–Yoo conjecture

Let $g(m,h) := \frac{1}{n}e(m,h) \in \mathbb{Z}$ if $h \neq 0$ and $g(m,0) := 0$. We define

$$G = \begin{cases} \prod_{m\in\mathcal{D}_N^1} \prod_{h=0}^{\ell(m)-1} \left(\frac{F_{m,h}}{F_{m,0}}\right)^{g(m,h)} & \text{if } 3 \nmid L \\ F_{N/3,0}^{16a} \prod_{m\in\mathcal{D}_N^1} \prod_{h=0}^{\ell(m)-1} \left(\frac{F_{m,h}}{F_{m,0}}\right)^{g(m,h)} & \text{if } 3 \mid L \end{cases}$$

One can check G is a modular unit by the previous theorem. Put $D' = D - \operatorname{div}(G)$. Then

$$nD' = \sum \operatorname{div}(F_{m,0}^{r(m)}),$$

for some $r(m) \in \mathbb{Z}$, which means D' is a rational cuspidal divisor. Therefore, $[D] = [D'] \in \mathcal{C}(N)$.

Consequence

Theorem

Conjecture A is true if $N = p^r M$ or $N = p^r q^s M$, where p, q are primes and M is squarefree.

Consequence

Theorem

Conjecture A is true if $N = p^r M$ *or* $N = p^r q^s M$*, where* p, q *are primes and* M *is squarefree.*

Corollary (Yoo–Y. 2021+)

Let p, q *are odd primes and let* M *be squarefree. Let* $N = p^r M$ *or* $N = p^r q^s M$*. Then*

$$\mathcal{C}(N) = \mathcal{C}_N(\mathbb{Q}).$$

Thank you very much for your attention!