Computation of the Order of Rational Cuspidal Divisors in the Modular Jacobian $J_0(N)$

Seokjoon Cho

02/10/2025

Table of Contents

Table of Contents

Classic Theory

1. $\mathbb{H} := \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$
2. $N \geq 1$ integer, $\Gamma_0(N) := \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \mod N\}$
3. $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathbb{H}$ by $\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \dfrac{az+b}{cz+d}$.
4. The Riemann surface $Y_0(N)_{\mathbb{C}} := \Gamma_0(N)\backslash\mathbb{H}$ is in bijection with the set of isomorphism classes of the pairs

$$\left\{(E, C) : \begin{array}{l} E : \text{elliptic curve over } \mathbb{C}, \\ C : \text{cyclic subgroup} \subset E \text{ of order } N \end{array}\right\} / \sim .$$

5. Cusps: elements of $\Gamma_0(N)\backslash\mathbb{P}^1(\mathbb{Q})$
6. $X_0(N)_{\mathbb{C}}$: Compact Riemann surface obtained by adding cusps to $Y_0(N)_{\mathbb{C}}$
7. $X_0(N)_{\mathbb{C}}$ has a canonical model over $\mathbb{Q}$ denoted by $X_0(N)$, which is a smooth projective curve with the function field $\mathbb{Q}(j, j_N)$.
8. $j : \mathbb{H} \to \mathbb{C}$, the elliptic modular function, $j_N(z) := j(Nz)$.
9. In this model, the cusps are defined over cyclotomic fields and $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ permutes the cusps.

$J_0(N)$: the Jacobian variety of $X_0(N)$, which is an abelian variety over $\mathbb{Q}$. By the Mordell-Weil theorem, $J_0(N)(\mathbb{Q})$ is a finitely generated abelian group.

$$J_0(N)(\mathbb{Q}) \cong \mathbb{Z}^r \times J_0(N)(\mathbb{Q})_{\text{tors}}$$

The (Hopeless) Ultimate Goal

Compute $J_0(N)(\mathbb{Q})$ for any $N \geq 1$.

The Ultimate Goal

Compute $J_0(N)(\mathbb{Q})_{\text{tors}}$ for any $N \geq 1$.

Cuspidal divisors

1. A **divisor** on $X_0(N)$ is a formal finite $\mathbb{Z}$-linear sum of points in $X_0(N)(\bar{\mathbb{Q}})$. A **cuspidal divisor** is a divisor supported only on cusps.
2. $\mathrm{Div}(X_0(N))$: the group of divisors on $X_0(N)$
   $\mathrm{Div}^0(X_0(N))$: the subgroup of degree 0 divisors
   $\mathrm{Div}^0_{\mathrm{cusp}}(X_0(N))$: the subgroup of degree 0 cuspidal divisors
   $\mathrm{Div}^0_{\mathrm{cusp}}(X_0(N))(\mathbb{Q})$: the subgroup of degree 0 *rational* cuspidal divisors, i.e. those fixed by the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

3. $J_0(N)(\bar{\mathbb{Q}}) = \mathrm{Div}^0(X_0(N))/\mathrm{PDiv}(X_0(N))$.
4. The canonical surjection

$$\pi : \mathrm{Div}^0(X_0(N)) \to J_0(N)(\bar{\mathbb{Q}})$$

   is Galois equivariant.
5. $J_0(N)(\mathbb{Q}) = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-invariant elements of $J_0(N)(\bar{\mathbb{Q}})$.
6. The image of $\mathrm{Div}^0_{\mathrm{cusp}}(X_0(N))$ under π is called the **cuspidal subgroup** $\mathcal{C}_N$. The subgroup $\mathcal{C}_N(\mathbb{Q}) := \mathcal{C}_N \cap J_0(N)(\mathbb{Q})$ is called the **rational cuspidal subgroup**.

Theorem (Manin-Drinfeld)

For any $N \geq 1$, $\mathcal{C}_N \subseteq J_0(N)(\bar{\mathbb{Q}})_{tors}$. In particular, $\mathcal{C}_N(\mathbb{Q}) \subseteq J_0(N)(\mathbb{Q})_{tors}$.

Theorem (Ogg's conjecture, Mazur (1977))

$\mathcal{C}_p(\mathbb{Q}) = J_0(p)(\mathbb{Q})_{tors}$ for any prime number $p \geq 5$.

More precisely, Mazur showed that $J_0(p)(\mathbb{Q})_{\text{tors}}$ is generated by a single class $\pi(0 - \infty)$, which is of order $n = \mathrm{numerator}(\frac{p-1}{12})$.

Generalized Ogg's conjecture

For any $N \geq 1$, $\mathcal{C}_N(\mathbb{Q}) = J_0(N)(\mathbb{Q})_{\text{tors}}$.

The image of $\mathrm{Div}^0_{\mathrm{cusp}}(X_0(N))(\mathbb{Q})$ under $\pi : \mathrm{Div}^0(X_0(N)) \to J_0(N)(\bar{\mathbb{Q}})$ is called the **rational cuspidal divisor class group** $\mathcal{C}(N)$. Clearly we have $\mathcal{C}(N) \subseteq \mathcal{C}_N(\mathbb{Q})$.

Conjecture

For any $N \geq 1$, $\mathcal{C}(N) = \mathcal{C}_N(\mathbb{Q})$.

Goal of this presentation:

1. Find generators of $\mathcal{C}(N)$.
2. Compute their orders.

Table of Contents

Representatives of cusps

Recall that the set of cusps of $X_0(N)$ is $\Gamma_0(N)\backslash\mathbb{P}^1(\mathbb{Q})$.

Lemma

Any cusp of $X_0(N)$ is represented as a column vector $\left[\begin{smallmatrix} x \\ d \end{smallmatrix}\right] \in \mathbb{Z}^2$ with some positive divisor $d|N$, $(x, d) = 1$. Also, such two columns $\left[\begin{smallmatrix} x \\ d \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} y \\ e \end{smallmatrix}\right]$ represent the same cusp if and only if

$$d = e \text{ and } x \equiv y \mod (d, N/d).$$

A cusp represented by some $\left[\begin{smallmatrix} x \\ d \end{smallmatrix}\right]$ is called a **cusp of level** d. There are exactly $\varphi(\gcd(d, N/d))$ cusps of level d. The unique cusp of level 1 (resp. N) is usually written 0 (resp. ∞).

The Galois action on cusps

For an integer $n \geq 1$, denote μ_n the group of n-th roots of unity in $\bar{\mathbb{Q}}$, and ζ_n a primitive n-th root of unity.

Theorem

Let $\tau \in Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ be an element sending ζ_n to ζ_n^k for some $k \in (\mathbb{Z}/N\mathbb{Z})^\times$. Then $\tau([\begin{smallmatrix} x \\ d \end{smallmatrix}]) = \left[\begin{smallmatrix} k'x \\ d \end{smallmatrix}\right]$, where $k' \in \mathbb{Z}$ is chosen so that $kk' \equiv 1 \mod N$ and $(k', x) = 1$.

Corollary

1. *A cusp $[\begin{smallmatrix} x \\ d \end{smallmatrix}]$ is defined over $\mathbb{Q}(\mu_n)$, where $n = (d, N/d)$.*
2. *$Gal(\mathbb{Q}(\mu_n)/\mathbb{Q})$ acts on the set of cusps of level d simply transitively.*

Example (squarefree N)

For any divisor $d|N$, there are exactly one cusp $\left[\frac{1}{d}\right]$ of level d since $(d, N/d) = 1$. They are all $\mathbb{Q}$-rational points of $X_0(N)$.

Example ($N = p^r$)

For each $i = 1, \cdots, r-1$, there are $(p-1)p^{s-1}$ cusps of level p^i where $s = \min\{i, r-i\}$. Those cusps are $\mathbb{Q}(\mu_{p^s})$-rational.

The generators of $C(N)$

As we have seen, $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ permutes the cusps of level d, and there are $\varphi(\gcd(d, N/d))$ cusps of level d.

$$P_d := \sum_x \left[\begin{smallmatrix} x \\ d \end{smallmatrix}\right] \qquad \in \mathrm{Div}_{\mathrm{cusp}}(X_0(N))(\mathbb{Q})$$

$$C_d := \varphi(\gcd(d, N/d))P_1 - P_d \qquad \in \mathrm{Div}^0_{\mathrm{cusp}}(X_0(N))(\mathbb{Q})$$

Proposition

$$Div_{cusp}(X_0(N))(\mathbb{Q}) = \oplus_{d|N}\, \mathbb{Z} \cdot P_d$$
$$Div^0_{cusp}(X_0(N))(\mathbb{Q}) = \oplus_{d|N}\, \mathbb{Z} \cdot C_d$$

In particular, $\mathcal{C}(N)$ is generated by $\pi(C_d)$'s.

Table of Contents

Let D be a rational cuspidal divisor of degree 0. Suppose $nD \sim 0$. By definition, there is a modular function $F \in \mathbb{Q}(j, j_N)$ such that

$$\mathrm{div}(F) = nD.$$

Such F satisfies the properties (*):

1. It has no zeros and poles on $\mathbb{H}$ (i.e. it is a *modular unit*).
2. Its order at a cusp $\left[\begin{smallmatrix} x \\ d \end{smallmatrix}\right]$ only depend on the level d (i.e. it does not depend on x).

Eta quotients

Recall the Dedekind eta function:

$$\eta(z) := e^{\frac{\pi i z}{12}} \prod_{n=1}^{\infty}(1 - e^{2\pi i n z}) = q^{\frac{1}{24}} \prod_{n=1}^{\infty}(1 - q^n)$$

Define $\eta_\delta(z) := \eta(\delta z)$.

Definition

A function $g : \mathbb{H} \to \mathbb{C}$ is called an **eta quotient** of level N if it is of the form

$$g = \prod_{\delta | N} \eta_\delta^{r_\delta}$$

for some rational numbers $r_\delta \in \mathbb{Q}$.

Lemma

An eta quotient $g = \prod_{\delta | N} \eta_\delta^{r_\delta}$ *has the divisor*

$$div(g) = \sum_{d|N} \left(\sum_{\delta | N} \frac{a_N(d,\delta)}{24} \times r_\delta \right) \cdot P_d,$$

where $a_N(d,\delta)$ *is defined as* $a_N(d,\delta) := \frac{N}{(d,N/d)} \times \frac{(d,\delta)^2}{d\delta}$.

One can show that the matrix $\boxed{\Lambda(N) := \left(\frac{a_N(d,\delta)}{24}\right)_{d,\delta|N}}$ is invertible.

Theorem (Ligozat)

An eta quotient $g = \prod_{\delta | N} \eta_\delta^{r_\delta}$ of level N is a rational function on $X_0(N)$ if and only if

(0) *all r_δ are integers;*

(1) $\sum_{\delta | N} r_\delta \cdot \delta \equiv 0 \mod 24$;

(2) $\sum_{\delta | N} r_\delta \cdot (N/\delta) \equiv 0 \mod 24$;

(3) $\sum_{\delta | N} r_\delta = 0$;

(4) $\prod_{\delta | N} \delta^{r_\delta}$ *is a square of a rational number.*

Theorem

Any modular unit on $X_0(N)$ satisfying the properties (*) is of the form $\epsilon \cdot g$ for some eta quotient g of level N and some $\epsilon \in \mathbb{C}$.

Table of Contents

General strategy

Let $D = \sum_{d|N} m_d \cdot P_d$ be a cuspidal divisor of degree 0. Put $(r_\delta) := \Lambda(N)^{-1}(m_d)$.

Theorem

D is linearly equivalent to 0 if and only if the rational numbers r_δ satisfy all the properties (0) $\sim$ (4). In particular, the order of D is the smallest positive integer n such that $n \cdot (r_\delta)$ satisfy the properties (0) $\sim$ (4).

$N = p$

The order of $C_p = 0 - \infty = \left[\frac{1}{1}\right] - \left[\frac{1}{p}\right]$ is equal to $\mathrm{numerator}(\frac{p-1}{12})$.

1. $\Lambda(N) = \frac{1}{24}\begin{pmatrix} p & 1 \\ 1 & p \end{pmatrix}$, $\Lambda(N)^{-1} = \frac{24}{p^2-1}\begin{pmatrix} p & -1 \\ -1 & p \end{pmatrix}$.
2. $m_1 = 1, m_p = -1, r_1 = \frac{24}{p-1}, r_p = \frac{24}{1-p}$.
3. Checking the properties:
   - (0) $n \cdot \frac{24}{p-1} \in \mathbb{Z}$.
   - (1-3) holds for any n.
   - (4) $\prod_{\delta | N} \delta^{n r_\delta} = p^{-24n/(p-1)}$ is a square of a rational number if and only if $n \cdot \frac{12}{p-1} \in \mathbb{Z}$.

$N = pq, p \neq q$

The order of $C_p = \left[\begin{smallmatrix}1\\1\end{smallmatrix}\right] - \left[\begin{smallmatrix}1\\p\end{smallmatrix}\right]$ is $\mathrm{lcm}\left(\mathrm{num}(\frac{(p-1)(q+1)}{12}), \mathrm{num}(\frac{(p-1)(q^2-1)}{24})\right)$.

	$p = 2$	$p = 3$	$p \geq 5$
$q = 2$	X	1	
$q = 3$	1	X	$p - 1$
$q \geq 5$	$\frac{q^2-1}{24}$	$\frac{q^2-1}{12}$	$\frac{(p-1)(q^2-1)}{24}$

1. $\Lambda(N) = \frac{1}{24}\begin{pmatrix} N & q & p & 1 \\ q & N & 1 & p \\ p & 1 & N & q \\ 1 & p & q & N \end{pmatrix}$,

   $\Lambda(N)^{-1} = \frac{24}{(p^2-1)(q^2-1)}\begin{pmatrix} N & -q & -p & 1 \\ -q & N & 1 & -p \\ -p & 1 & N & -q \\ 1 & -p & -q & N \end{pmatrix}$
2. $\begin{pmatrix} r_1 & r_p & r_q & r_N \end{pmatrix} = \frac{24}{(p-1)(q^2-1)}\begin{pmatrix} q & -q & -1 & 1 \end{pmatrix}$
3. Checking the properties:
   - (0) $n \cdot \frac{24}{(p-1)(q^2-1)} \in \mathbb{Z}$.
   - (1-3) holds for any n.
   - (4) $\prod_{\delta|N} \delta^{nr_\delta} = p^\wedge(\frac{24n}{(p-1)(q+1)})$ is a square of a rational number if and only if $n \cdot \frac{12}{(p-1)(q+1)} \in \mathbb{Z}$.

The order of $C_N = \left[\begin{smallmatrix}1\\1\end{smallmatrix}\right] - \left[\begin{smallmatrix}1\\N\end{smallmatrix}\right]$ is

(i) $\dfrac{q^2-1}{8\cdot(3,q+1)}$ if $p=2$.

(ii) $\dfrac{(p^2-1)(q^2-1)}{12\cdot(p-1,q-1)\cdot(p+1,q+1)}$ if p and q are odd.

1. $\begin{pmatrix} r_1 & r_p & r_q & r_N \end{pmatrix} = \frac{24}{(p^2-1)(q^2-1)} \begin{pmatrix} N-1 & p-q & q-p & 1-N \end{pmatrix}$
2. Checking the properties:

   (0) $n \cdot \frac{24(N-1)}{(p^2-1)(q^2-1)}, n \cdot \frac{24(p-q)}{(p^2-1)(q^2-1)} \in \mathbb{Z}$.

   (1-3) holds for any n.

   (4) $n \cdot \frac{24(N-1+p-q)}{(p^2-1)(q^2-1)} \in 2\mathbb{Z}$.