ARTICLE IN PRESS YJNTH:5985

Journal of Number Theory ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Rational torsion subgroups of modular Jacobian varieties

Yuan Ren

Sichuan Normal University, School of Mathematical Sciences, Chengdu, Sichuan, China

A R T I C L E   I N F O

Article history:
Received 29 July 2017
Received in revised form 29 January 2018
Accepted 14 February 2018
Available online xxxx
Communicated by A. Pal

Keywords:
Modular curve
Generalized Ogg's conjecture
Eisenstein ideal

A B S T R A C T

In this article, we study the $\mathbb{Q}$-rational torsion subgroups of the Jacobian varieties of modular curves. The main result is that, for any positive integer N, $J_0(N)(\mathbb{Q})_{\mathrm{tor}}[q^\infty] = 0$ if q is a prime not dividing $6 \cdot N \cdot \prod_{p|N}(p^2 - 1)$. To prove the result, we explicitly construct a collection of Eisenstein series with rational Fourier expansions, and then determine their constant terms to control the size of the rational torsion subgroups.

Contents

E-mail address: rytgyx@126.com.

https://doi.org/10.1016/j.jnt.2018.02.009
0022-314X/

Please cite this article in press as: Y. Ren, Rational torsion subgroups of modular Jacobian varieties, J. Number Theory (2018), https://doi.org/10.1016/j.jnt.2018.02.009

1. Introduction

For any positive integer N, let $X_0(N)$ be Shimura's canonical model over $\mathbb{Q}$ of the modular curve of level $\Gamma_0(N)$. Let $J_0(N)$ be the Jacobian variety of $X_0(N)$ over $\mathbb{Q}$. In this article, we study the rational torsion subgroup of $J_0(N)$. This kind of investigation began with the work of Ogg (see [5] and [6]), who conjectured that, if $N = p$ is a prime, then

$$J_0(p)(\mathbb{Q})_{\mathrm{tor}} = \langle [0] - [\infty] \rangle,$$

where $[0]$ and $[\infty]$ are the only two cusps of $X_0(p)$. This conjecture of Ogg is proved by Mazur in [4]. The basic idea is to consider the Hecke module structure of $J_0(p)(\mathbb{Q})_{\mathrm{tor}}$. The following is a brief explanation of the method of Mazur.

Let $\mathbb{T}_0(p) \subseteq \mathrm{End}_{\mathbb{Q}}(J_0(p))$ be the Hecke algebra of level $\Gamma_0(p)$ generated over $\mathbb{Z}$ by all the Hecke operator T_ℓ's, where ℓ runs over all the primes. By the Eichler–Shimura theory, we have

$$T_\ell = 1 + \ell \text{ on } J_0(p)(\mathbb{Q})_{\mathrm{tor}}$$

for any prime $\ell \neq p$. On the other hand, since there is no old form in $S_2(\Gamma_0(p), \mathbb{C})$, the newform theory implies that

$$T_p = \pm 1 \text{ on } J_0(p)(\mathbb{Q})_{\mathrm{tor}}.$$

In fact, it can be proved that $T_p = 1$ on $J_0(p)(\mathbb{Q})_{\mathrm{tor}}$, so that $J_0(p)(\mathbb{Q})_{\mathrm{tor}}$ is a $\mathbb{T}_0(p)/I_0(p)$-module with $I_0(p) := (\{T_\ell - (1+\ell)\}_{\ell \neq p}, T_p - 1)$ being the Eisenstein ideal introduced by Mazur. It is easy to see that $\langle [0] - [\infty] \rangle$ is also annihilated by $I_0(p)$. The above conjecture of Ogg then follows from ring theoretical properties of $\mathbb{T}_0(p)$ at the Eisenstein ideal $I_0(p)$. For example, it can be shown that the index of $I_0(p)$ in $\mathbb{T}_0(p)$ is prime to $6(p-1)$. Thus we find that, for any prime q not dividing $6(p-1)$, the q-part of $J_0(p)(\mathbb{Q})_{\mathrm{tor}}$ must be zero, which is in agreement with the order of the group $\langle [0] - [\infty] \rangle$.

The work of Mazur has later been generalized to some other modular Jacobian varieties. For any positive integer N, let $C_0(N)$ be the subgroup of $J_0(N)(\overline{\mathbb{Q}})$ generated by the cusps of $X_0(N)$. Let $C_0(N)(\mathbb{Q})$ be the $\mathbb{Q}$-rational subgroup of $C_0(N)$. Then, if $p \geq 5$ is a prime and $r \in \mathbb{Z}_{\geq 2}$, it is known that $J_0(p^r)(\mathbb{Q})[q^\infty] = C_0(p^r)(\mathbb{Q})[q^\infty]$ for any prime $q \nmid 6p$ (see [3]). Secondly, if N is a square-free positive integer, then it is proved by Ohta that $J_0(N)(\mathbb{Q})[q^\infty] = C_0(N)[q^\infty]$ for any prime $q \nmid 6$ (see [7]). This square-free case has also been studied and improved by Yoo (see [10] for example). Note that when N is square-free, all the cusps of $X_0(N)$ are $\mathbb{Q}$-rational and hence $C_0(N) = C_0(N)(\mathbb{Q})$. After these pioneering work, one is naturally led to the following

Conjecture 1.1 *(Generalized Ogg's conjecture). For any positive integer N, we have that*

$$J_0(N)(\mathbb{Q})_{tor} = C_0(N)(\mathbb{Q}),$$

where $C_0(N)$ is the subgroup of $J_0(N)(\overline{\mathbb{Q}})$ generated by the cusps of $X_0(N)$ and $C_0(N)(\mathbb{Q})$ is the $\mathbb{Q}$-rational subgroup of it.

In this article, we will provide, for any positive integer N, a "support" for those primes q such that the q-part of $J_0(N)(\mathbb{Q})_{\mathrm{tor}}$ is not zero. More precisely, our main result is the following

Theorem 1.2. *For any positive integer N, we have that*

$$J_0(N)(\mathbb{Q})[q^\infty] = 0$$

for any prime $q \nmid 6 \cdot N \cdot \varpi(N)$, where $\varpi(N) := \prod(p^2 - 1)$ with p runs over all prime divisors of N.

The idea of the proof for the above theorem is similar to that of Mazur, except that we have to deal with the problem caused by old forms. To this end, we will first prove the same assertion as in the above theorem with $J_0(N)$ replaced by its new-subvariety, and then use an inductive argument to yield the desired result. Note that, for any prime $p \mid N$, the action of the p-th Hecke operator on the new-part of $J_0(N)$ is basically determined by whether p^2 divides N or not. We are therefore led to first consider the situation when the level N is of the form DC, where D is a positive square-free integer and $C \mid D$ a divisor of D. In the second section, we construct a collection of rational Eisenstein series of level $\Gamma_0(DC)$ which are all eigenforms. These Eisenstein series will provide us with the Eisenstein ideals to study the rational torsion subgroups later. The rest of the second section is devoted to the determination of the constant terms of these Eisenstein series. Then, we will use these results to control the indexes of the corresponding Eisenstein ideals and complete the proof of Theorem 1.2 in the third section.

Notations. We denote by $B_2(x)$ to be the second Bernoulli polynomial. For any positive integer $N = \prod_{p|N} p^{v_p(N)}$, let $\varpi(N) := \prod_{p|N}(p^2-1)$, $\psi(N) := \prod_{p|N}(p+1)$, and $\nu(N) := \sum_{p|N} v_p(N)$. Let $\mathfrak{q}$ be the function $z \mapsto e^{2\pi i z}$ on the upper half plane used in the Fourier expansions of modular forms. For any function g on the upper half plane and any $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{R})$, we denote by $g|\gamma$ to be the function $z \mapsto \det(\gamma) \cdot g(\gamma z) \cdot (cz+d)^{-2}$.

2. Rational Eisenstein series of level $\Gamma_0(DC)$

In the following, let D be a positive square-free integer and C be a positive divisor of D. In this section, we will construct some Eisenstein series in $\mathcal{E}_2(\Gamma_0(DC), \mathbb{C})$ whose Fourier coefficients at $[\infty]$ are all rational numbers. We will show that these Eisenstein series are all eigenforms and then determine their constant terms at the cusps of $X_0(DC)$.

Please cite this article in press as: Y. Ren, Rational torsion subgroups of modular Jacobian varieties, J. Number Theory (2018), https://doi.org/10.1016/j.jnt.2018.02.009

2.1. The definition and Hecke action

Let N be a positive integer and $\mathcal{M}_2(\Gamma_0(N), \mathbb{C})$ be the space of weight two modular forms of level $\Gamma_0(N)$. Then

$$\mathcal{M}_2(\Gamma_0(N), \mathbb{C}) = S_2(\Gamma_0(N), \mathbb{C}) \oplus \mathcal{E}_2(\Gamma_0(N), \mathbb{C}),$$

where $S_2(\Gamma_0(N), \mathbb{C})$ is the sub-space of cusp forms and $\mathcal{E}_2(\Gamma_0(N), \mathbb{C})$ is the sub-space of Eisenstein series. For any prime ℓ, there is a Hecke operator $\mathcal{T}_\ell^{\Gamma_0(N)}$ acting on $\mathcal{M}_2(\Gamma_0(N), \mathbb{C})$ with respect to the above decomposition. Let $\mathcal{T}_0(N)$ be the $\mathbb{Z}$-algebra generated by the $\mathcal{T}_\ell^{\Gamma_0(N)}$ for all the primes ℓ. Denote the restriction of $\mathcal{T}_\ell^{\Gamma_0(N)}$ to $S_2(\Gamma, \mathbb{C})$ by $T_\ell^{\Gamma_0(N)}$. Then we define the Hecke algebra of level $\Gamma_0(N)$ to be the $\mathbb{Z}$-algebra generated by the $T_\ell^{\Gamma_0(N)}$ for all the primes ℓ and is denoted as $\mathbb{T}_0(N)$. Note that $\mathbb{T}_0(N)$ is a quotient ring of $\mathcal{T}_0(N)$. If $E \in \mathcal{E}_2(\Gamma_0(N), \mathbb{C})$, then we define the *Eisenstein ideal of E* as the image of $\mathrm{Ann}_{\mathcal{T}_0(N)}(E)$ in $\mathbb{T}_0(N)$, which is denoted by $I_{\Gamma_0(N)}(E)$.

Before giving the definition of the above mentioned rational Eisenstein series, we will first introduce some operators on the $\mathbb{C}$-vector space $\mathcal{M}_2$ of weight two holomorphic modular forms of all levels. Note that similar operators are also considered by Yoo in [10]. For any prime p, we denote by γ_p to be the operator on $\mathcal{M}_2$, which maps any $g \in \mathcal{M}_2$ to $g|\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$. Then we define the following two operators $[p]^\pm : \mathcal{M}_2 \to \mathcal{M}_2$ by

$$[p]^+ := 1 - \gamma_p$$
$$[p]^- := 1 - \frac{1}{p}\gamma_p$$

More precisely, for any $g \in \mathcal{M}_2$ and $z \in \mathfrak{H}$, we have

$$[p]^+(g)(z) = g(z) - p \cdot g(pz)$$
$$[p]^-(g)(z) = g(z) - g(pz)$$

It is easy to see that if p_1 and p_2 are two primes, then the four operators $[p_1]^+, [p_1]^-, [p_2]^+$ and $[p_2]^-$ are commutative with each other. This enables us to define, for any positive square-free integer M, two operators $[M]^\pm$ on $\mathcal{M}_2$ as

$$[M]^\pm := [p_1]^\pm \circ [p_2]^\pm \circ ... \circ [p_k]^\pm$$

with $M = p_1 \cdot p_2 ... \cdot p_k$ in any order.

To give the construction of our Eisenstein series, recall that there is a collection of functions $\phi_{\underline{x}}$ on the upper half plane, indexed by all row vectors $\underline{x} \in (\mathbb{Q}/\mathbb{Z})^{\oplus 2}$ with the following properties:

For any $\underline{x} \neq 0$, $\phi_{\underline{x}}$ is an Eisenstein series, and we have that

$$\phi_{\underline{x}}|\gamma = \phi_{\underline{x}\cdot\gamma} \tag{2.1}$$

for any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, with $\mathrm{SL}_2(\mathbb{Z})$ acts on the row vectors form the right in the usual way. Moreover, these functions satisfy the following *distribution law*

$$\phi_{\underline{x}} = \sum_{\underline{y}\cdot\alpha=\underline{x}} \phi_{\underline{y}}|\alpha \tag{2.2}$$

For more details about these functions, especially their Fourier expansions and the action of Hecke operators, we refer the reader to §2.4 of [9].

Definition 2.1. For any two of positive divisors M and L of D such that $M \neq 1$ and $D \mid ML \mid DC$, we define the following

$$E_{M,L} := [L]^- \circ [M]^+(-\frac{1}{2}\phi_{(0,0)})$$

which is an Eisenstein series of level $\Gamma_0(DC)$. In the following, we will denote by $\mathcal{H}(DC)$ to be the set of pairs M, L of positive divisors of D with $M \neq 1$ and $D \mid ML \mid DC$.

Example 1. When $D = p$ is a prime and $C = 1$, we have $\mathcal{H}(p) = \{(p, 1)\}$. The Eisenstein series corresponding to $(p, 1)$ is $E_{p,1} = [p]^+(-\frac{1}{2}\phi_{(0,0)})$ by definition, so it follows from the distribution law that

$$\begin{aligned} E_{p,1} &= -\frac{1}{2}\phi_{(0,0)} + \frac{1}{2}\sum_{y\in\mathbb{Z}/p\mathbb{Z}} \phi_{(0,\frac{y}{p})} \\ &= \frac{1}{2}\sum_{y\in(\mathbb{Z}/p\mathbb{Z})^\times} \phi_{(0,\frac{y}{p})}. \end{aligned}$$

By §2.4 of [9], the Fourier expansion of $E_{p,1}$ at $[\infty]$ is given as

$$\begin{aligned} E_{p,1} &= \frac{1}{2}\sum_{y\in(\mathbb{Z}/p\mathbb{Z})^\times}\left[\frac{1}{2}B_2(0) - \sum_{k=1}^{\infty} ke^{2\pi im(kz+\frac{y}{p})} + \sum_{k=1}^{\infty} ke^{2\pi im(kz-\frac{y}{p})}\right] \\ &= \frac{p-1}{24} - \sum_{n=1}^{\infty}\left[\sum_{1\leq d|n} d(\sum_{y\in(\mathbb{Z}/p\mathbb{Z})^\times} e^{2\pi i\frac{n}{d}\frac{y}{p}})\right] e^{2\pi inz} \\ &= \frac{p-1}{24} + \sum_{n=1}^{\infty}\sigma_p(n)\cdot \mathfrak{q}^n, \end{aligned}$$

where $\sigma_p(n) := \sum_{1\leq d|n, p\nmid d} d$ for any positive integer n.

Please cite this article in press as: Y. Ren, Rational torsion subgroups of modular Jacobian varieties, J. Number Theory (2018), https://doi.org/10.1016/j.jnt.2018.02.009

Proposition 2.2. *For any $(M, L) \in \mathcal{H}(DC)$, we have $a_1(E_{M,L}; [\infty]) = 1$. In other words, all these Eisenstein series are normalized.*

Proof. We first observe that, if f is any modular form of level $\Gamma_0(N)$ for some positive integer N with its Fourier expansion at $[\infty]$ being $\sum_{n=1}^{\infty} a_n \cdot \mathfrak{q}^n$, then the Fourier expansion of $f|\gamma_p$ is $\sum_{n=1}^{\infty}(\ell a_n) \cdot \mathfrak{q}^{\ell n}$ for any prime ℓ. In particular, we find that $a_1(f|\gamma_p; [\infty]) = 0$ and hence $a_1(f; [\infty]) = a_1([\ell]^{\pm}(f); [\infty])$.

For any $(M, L) \in \mathcal{H}(DC)$, we choose an arbitrary prime divisor p of M and find then by definition that

$$E_{M,L} = [L]^- \circ [\frac{M}{p}]^+(E_{p,1})$$

Since $a_1(E_{p,1}; [\infty]) = 1$ as we have seen in Example 1, it follows that $E_{M,L}$ is also normalized by the above observation. $\square$

Lemma 2.3. *For any prime p, we have that*

$$\mathcal{T}_\ell^{\Gamma_0(p)}(E_{p,1}) = \begin{cases} (1+\ell) \cdot E_{p,1}, & \text{if } \ell \neq p \\ E_{p,1}, & \text{if } \ell = p \end{cases}$$

Proof. By Proposition 2.4.7 of [9], we have

$$\mathcal{T}_\ell^{\Gamma_1(p)}(\phi_{(0,\frac{y}{p})}) = \begin{cases} \ell \cdot \phi_{(0,\frac{y}{p})} + \phi_{(0,\frac{\ell y}{p})}, & \text{if } \ell \nmid p \\ \ell \cdot \phi_{(0,\frac{y}{p})} + \phi_{(0,\frac{\ell y}{p})} - \sum_{k=0}^{\ell-1} \phi_{(0,\frac{y}{p}+\frac{k}{p})}, & \text{if } \ell = p \end{cases}$$

for any y. Since $E_{p,1} = \frac{1}{2}\sum_{y\in(\mathbb{Z}/p\mathbb{Z})^\times} \phi_{(0,\frac{y}{p})}$, it follows that

$$\begin{aligned} \mathcal{T}_\ell^{\Gamma_0(p)}(E_{p,1}) &= \mathcal{T}_\ell^{\Gamma_0(p)}\left(\frac{1}{2}\sum_{y\in(\mathbb{Z}/p\mathbb{Z})^\times} \phi_{(0,\frac{y}{p})}\right) \\ &= \frac{1}{2}\sum_{y\in(\mathbb{Z}/p\mathbb{Z})^\times}\left(\mathcal{T}_\ell^{\Gamma_1(p)}(\phi_{(0,\frac{y}{p})})\right) \\ &= (1+\ell)\cdot E_{p,1} \end{aligned}$$

for any prime $\ell \neq p$. On the other hand, if $\ell = p$, then we have that

$$\mathcal{T}_p^{\Gamma_0(p)}(E_{p,1}) = p \cdot E_{p,1} + (p-1)\cdot\phi_{(0,0)} - \sum_{y\in(\mathbb{Z}/p\mathbb{Z})^\times}\sum_{k=0}^{p-1}\phi_{(0,\frac{y}{p}+\frac{k}{p})}$$

Please cite this article in press as: Y. Ren, Rational torsion subgroups of modular Jacobian varieties, J. Number Theory (2018), https://doi.org/10.1016/j.jnt.2018.02.009

$$
\begin{aligned}
&= p \cdot E_{p,1} - (p-1) \cdot E_{p,1} \\
&= E_{p,1},
\end{aligned}
$$

which completes the proof of the lemma. □

Lemma 2.4. *For any* $1 \neq M \mid D$*, we have that*

$$
\mathcal{T}_\ell^{\Gamma_0(D)}(E_{M,D/M}) = \begin{cases} E_{M,D/M}, & \text{if } \ell \mid M \\ \ell \cdot E_{M,D/M}, & \text{if } \ell \mid D/M \\ (1+\ell) \cdot E_{M,D/M}, & \text{if } \ell \nmid D \end{cases}
$$

Proof. Let ℓ be a prime not dividing D. Choose a prime $p \mid M$. Then we find by definition that

$$
E_{M,D/M} = [\frac{D}{M}]^- \circ [\frac{M}{p}]^+(E_{p,1}).
$$

It follows that

$$
\begin{aligned}
\mathcal{T}_\ell^{\Gamma_0(D)}(E_{M,D/M}) &= [\frac{D}{M}]^- \circ [\frac{M}{p}]^+ \circ \mathcal{T}_\ell^{\Gamma_0(p)}(E_{p,1}) \\
&= (1+\ell) \cdot E_{M,D/M},
\end{aligned}
$$

which proves the third assertion.

If ℓ is a prime divisor of M, then we have that

$$
\begin{aligned}
\mathcal{T}_\ell^{\Gamma_0(D)}(E_{M,D/M}) &= \mathcal{T}_\ell^{\Gamma_0(D)}\left([\frac{D}{M}]^- \circ [\frac{M}{\ell}]^+(E_{\ell,1})\right) \\
&= [\frac{D}{M}]^- \circ [\frac{M}{\ell}]^+ \circ \mathcal{T}_\ell^{\Gamma_0(\ell)}(E_{\ell,1}) \\
&= E_{M,D/M},
\end{aligned}
$$

which proves the first assertion.

Finally, if ℓ is a prime divisor of D/M, then we have

$$
E_{M,D/M} = [\ell]^-(E_{M,D/M\ell}),
$$

and hence

$$
\begin{aligned}
\mathcal{T}_\ell^{\Gamma_0(D)}(E_{M,D/M}) &= \mathcal{T}_\ell^{\Gamma_0(\frac{D}{\ell})}(E_{M,\frac{D}{M\ell}}) - E_{M,\frac{D}{M\ell}}| \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix} \\
&\quad - \frac{1}{\ell} E_{M,\frac{D}{M\ell}}| \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix} \sum_{k=0}^{\ell-1} \begin{pmatrix} 1 & k \\ 0 & \ell \end{pmatrix}
\end{aligned}
$$

$$= \ell \cdot E_{M,\frac{D}{M\ell}} - E_{M,\frac{D}{M\ell}} | \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix}$$

$$= \ell \cdot E_{M,D/M},$$

which proves the second assertion and completes the proof. □

Proposition 2.5. *For any $(M, L) \in \mathcal{H}(DC)$, we have that*

$$\mathcal{T}_\ell^{\Gamma_0(DC)}(E_{M,L}) = \begin{cases} (1+\ell) \cdot E_{M,L}, & \text{if } \ell \nmid D \\ E_{M,L}, & \text{if } \ell \mid \frac{M}{(M,L)} \\ \ell \cdot E_{M,L}, & \text{if } \ell \mid \frac{L}{(M,L)} \\ 0, & \text{if } \ell \mid (M,L) \end{cases}$$

In particular, the Eisenstein ideal $I_{\Gamma_0(DC)}(E_{M,L})$ of $\mathbb{T}_0(DC)$ associated to $E_{M,L}$ equals to $(\{T_\ell - (1+\ell)\}_{\ell \nmid D}, \{T_\ell - 1\}_{\ell \mid \frac{M}{(M,L)}}, \{T_\ell - \ell\}_{\ell \mid \frac{L}{(M,L)}}, \{T_\ell\}_{\ell \mid (M,L)})$.

Proof. It remains to prove this theorem for those $E_{M,L}$ with $(M, L) \neq 1$. By the definition, we have that $E_{M,L} = [(M, L)]^-(E_{M,D/M})$, so if ℓ is a prime not dividing D, then

$$\begin{aligned} \mathcal{T}_\ell^{\Gamma_0(DC)}(E_{M,L}) &= \mathcal{T}_\ell^{\Gamma_0(DC)} \circ [(M,L)]^-(E_{M,D/M}) \\ &= [(M,L)]^- \circ \mathcal{T}_\ell^{\Gamma_0(\frac{DC}{(M,L)})}(E_{M,D/M}) \\ &= (1+\ell) \cdot E_{M,L}, \end{aligned}$$

where the last equality holds because $\mathcal{T}_\ell^{\Gamma_0(\frac{DC}{(M,L)})}$ and $\mathcal{T}_\ell^{\Gamma_0(\frac{D}{(M,L)})}$ are given by the same formula and we have already seen in Lemma 2.4 that $\mathcal{T}_\ell^{\Gamma_0(\frac{D}{(M,L)})}(E_{M,D/M}) = (1+\ell) \cdot E_{M,D/M}$ for any prime $\ell \nmid D$. By similar arguments as above, we can prove that $\mathcal{T}_\ell^{\Gamma_0(DC)}(E_{M,L}) = E_{M,L}$ for any prime $\ell \mid \frac{M}{(M,L)}$ and $\mathcal{T}_\ell^{\Gamma_0(DC)}(E_{M,L}) = \ell \cdot E_{M,L}$ for any prime $\ell \mid \frac{L}{(M,L)}$.

Finally, if ℓ is a prime divisor of (M, L), then $\ell^2 \mid ML \mid DC$ and we find that

$$\begin{aligned} \mathcal{T}_\ell^{\Gamma_0(DC)}(E_{M,L}) &= \mathcal{T}_\ell^{\Gamma_0(DC)} \circ [(M,L)/\ell]^- \circ [\ell]^-(E_{M,D/M}) \\ &= [(M,L)/\ell]^- \circ \mathcal{T}_\ell^{\Gamma_0(D\ell)} \circ [\ell]^-(E_{M,D/M}) \\ &= [(M,L)/\ell]^- \left[\left(E_{M,D/M} - \frac{1}{\ell} \cdot E_{M,D/M} | \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix} \right) | \sum_{k=0}^{\ell-1} \begin{pmatrix} 1 & k \\ 0 & \ell \end{pmatrix} \right] \\ &= [(M,L)/\ell]^- \left(\mathcal{T}_\ell^{\Gamma_0(D)}(E_{M,D/M}) - E_{M,D/M} \right) = 0, \end{aligned}$$

which completes the proof of the theorem. □

2.2. The constant terms

Now we turn to the calculation of the constant terms of $E_{M,L}$. Note that similar results have been obtained by Banerjee in the prime square case (see [1]). Firstly, we give some convenient representatives for the cusps of $X_0(DC)$.

Lemma 2.6. *If we take r to be a positive divisor of $\frac{D}{C}$, s,t two positive divisors of C satisfying $(s,t)=1$ and let x runs over a set of representative of $(\mathbb{Z}/t\mathbb{Z})^\times$ which are prime to D, then $\{[\frac{rs^2tx}{DC}]\}$ is a full set of representative for the cusps of $X_0(DC)$.*

Proof. It is clear that any divisor of $DC=\frac{D}{C}\cdot C^2$ is of the form rs^2t with some r,s,t as above, and we have $(rs^2t, \frac{DC}{rs^2t})=t$ for any such a divisor, so the above set has at most $\sum_{1\le d|DC}\varphi(d,\frac{DC}{d})$ elements. Thus, it is enough to prove that the above are all different cusps, since we know that the number of cusps of $S_0(DC)$ is also $\sum_{1\le d|DC}\varphi(d,\frac{DC}{d})$.

Suppose, to the contrary that we have $[\frac{r_1s_1^2t_1x_1}{DC}]=[\frac{r_2s_2^2t_2x_2}{DC}]$, then there exists some $\gamma=\begin{pmatrix}\alpha & \beta\\ DC\delta & \omega\end{pmatrix}\in\Gamma_0(DC)$ such that $\gamma(\frac{r_1s_1^2t_1x_1}{DC})=\frac{r_2s_2^2t_2x_2}{DC}$. It follows that we have

$$r_2s_2^2t_2x_2=r_1s_1^2t_1x_1\cdot\frac{\alpha x_1+\beta\frac{DC}{r_1s_1^2t_1}}{\delta r_1s_1^2t_1x_1+\omega}.$$

But as $\delta r_1s_1^2t_1x_1+\omega$ is a unit at every prime dividing $r_1s_1t_1$, we find that r_1,s_1,t_1 divides r_2,s_2,t_2 respectively, and hence $r_1=r_2, s_1=s_2$ and $t_1=t_2$ by symmetry. If we choose some u_i,v_i $(i=1,2)$ such that $\begin{pmatrix}x_i & u_i\\ \frac{DC}{rs^2t} & v_i\end{pmatrix}\in SL_2(\mathbb{Z})$, then

$$\gamma\cdot\begin{pmatrix}x_1 & u_1\\ \frac{DC}{rs^2t} & v_1\end{pmatrix}(\infty)=\begin{pmatrix}x_2 & u_2\\ \frac{DC}{rs^2t} & v_2\end{pmatrix}(\infty),$$

so that there exists some integer n such that

$$\pm\gamma\cdot\begin{pmatrix}x_1 & u_1\\ \frac{DC}{rs^2t} & v_1\end{pmatrix}=\begin{pmatrix}x_2 & u_2\\ \frac{DC}{rs^2t} & v_2\end{pmatrix}\begin{pmatrix}1 & n\\ 0 & 1\end{pmatrix},$$

which implies, after a straight forward calculation, that

$$\frac{DC}{rs^2t}v_1-\frac{DC}{rs^2t}v_2\equiv n\cdot\frac{DC}{rs^2t}\cdot\frac{DC}{rs^2t}\pmod{DC}.$$

Since $t^2\mid DC$, it follows that

$$v_1\equiv v_2\pmod{t}\Rightarrow x_1\equiv x_2\pmod{t},$$

and hence completes the proof of the lemma. $\square$

Please cite this article in press as: Y. Ren, Rational torsion subgroups of modular Jacobian varieties, J. Number Theory (2018), https://doi.org/10.1016/j.jnt.2018.02.009

By a similar argument, we can prove the following

Lemma 2.7. *Let p be a prime divisor of D and $[\frac{rs^2tx}{DC}]$ be a cusp of $X_0(DC)$, then we have that:*

(1) *If $p \mid r$, then $[\frac{rs^2tx}{DC}] = [\frac{(r/p)s^2tx}{DC/p}]$ in $X_0(DC/p)$;*
(2) *If $p \mid s$, then $[\frac{rs^2tx}{DC}] = [\frac{r(s/p)^2tx}{DC/p^2}]$ in $X_0(DC/p^2)$;*
(3) *If $p \mid t$, then $[\frac{rs^2tx}{DC}] = [\frac{rs^2(t/p)\cdot(px)}{DC/p^2}]$ in $X_0(DC/p^2)$;*
(4) *If $p \mid \frac{D}{Cr}$, then $[\frac{rs^2tx}{DC}] = [\frac{rs^2t\cdot(px)}{DC/p}]$ in $X_0(DC/p)$;*
(5) *If $p \mid \frac{C}{st}$, then $[\frac{rs^2tx}{DC}] = [\frac{rs^2t\cdot(p^2x)}{DC/p^2}]$ in $X_0(DC/p^2)$.*

Proof. The first two assertions are obvious. Since the proofs of last three assertions are similar, we will in the following only give that of (3). If $[\frac{rs^2tx}{DC}] = [\frac{r's'^2t'x'}{DC/p^2}]$ in $X_0(DC/p^2)$, then there exists some $\gamma = \begin{pmatrix} \alpha & \beta \\ \frac{DC}{p^2}\delta & \omega \end{pmatrix} \in \Gamma_0(\frac{DC}{p^2})$ sending the former point to the latter one, and we find thus

$$r's'^2t'x' = rs^2(t/p) \cdot \frac{x\alpha + \beta\frac{DC}{rs^2t}}{\delta rs^2(t/p)x + \omega p}.$$

Since $\delta rs^2(t/p)x + \omega p$ is a unit for any prime dividing $rs^2(t/p)$, it follows that $r, s, t/p$ divides r', s', t' respectively. We find thus

$$\frac{r'}{r} \cdot \frac{s'^2}{s^2} \cdot \frac{t'}{t/p} \cdot x' = \frac{x\alpha + \beta\frac{DC}{rs^2t}}{\delta rs^2(t/p)x + \omega p}.$$

If there is some prime $q \mid r's't'$ (so that $q \neq p$ as $p \nmid t'$) but not dividing rst, then $x\alpha + \beta\frac{DC}{rs^2t}$ will be a q-adic unit. But this contradicts to the above equation, so we have proved the assertion. $\square$

To determine the constant terms of $E_{M,L}$, we still need to know how the operators $[p]^{\pm}$ effect on the constant terms of a modular forms. Let $[\frac{a}{c}]$ be a cusp represented by two integers a, c with $(a, c) = 1$, and we choose some $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ so that $\gamma([\infty]) = [\frac{a}{c}]$. Let $N \in \mathbb{Z}_{\geq 1}$ and $f \in M_2(\Gamma_0(N), \mathbb{C})$. For any prime p, we have that

$$\gamma_p \cdot \gamma = \begin{cases} \begin{pmatrix} a & pb \\ c/p & d \end{pmatrix} \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}, & \text{if } p \mid c \\ \begin{pmatrix} ap & b \\ c & d/p \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}, & \text{if } p \nmid c, \end{cases}$$

where we may and will always assume $p \mid d$ if $p \nmid c$. We find then by definition that

$$a_0([p]^+(f);[\frac{a}{c}]) = \begin{cases} a_0(f;[\frac{a}{c}]) - p \cdot a_0(f;[\frac{ap}{c}]), & \text{if } p \mid c \\ a_0(f;[\frac{a}{c}]) - p^{-1} \cdot a_0(f;[\frac{ap}{c}]), & \text{if } p \nmid c, \end{cases}$$

and

$$a_0([p]^-(f);[\frac{a}{c}]) = \begin{cases} a_0(f;[\frac{a}{c}]) - a_0(f;[\frac{ap}{c}]), & \text{if } p \mid c \\ a_0(f;[\frac{a}{c}]) - p^{-2} \cdot a_0(f;[\frac{ap}{c}]), & \text{if } p \nmid c. \end{cases}$$

It follows by an easy inductive argument that, if K is a positive square-free integer, then

$$a_0([K]^+(f);[\frac{a}{c}]) = \begin{cases} \sum_{1\le\alpha|K} (-1)^{\nu(\alpha)} \cdot \alpha \cdot a_0(f;[\frac{\alpha a}{c}]), & \text{if } K \mid c \\ \sum_{1\le\alpha|K} (-1)^{\nu(\alpha)} \cdot \alpha^{-1} \cdot a_0(f;[\frac{\alpha a}{c}]), & \text{if } (K,c)=1, \end{cases} \tag{2.3}$$

and

$$a_0([K]^-(f);[\frac{a}{c}]) = \begin{cases} \sum_{1\le\alpha|K} (-1)^{\nu(\alpha)} \cdot a_0(f;[\frac{\alpha a}{c}]), & \text{if } K \mid c \\ \sum_{1\le\alpha|K} (-1)^{\nu(\alpha)} \cdot \alpha^{-2} \cdot a_0(f;[\frac{\alpha a}{c}]), & \text{if } (K,c)=1. \end{cases} \tag{2.4}$$

Lemma 2.8. *The constant terms of $E_{D,1}$ are given by*

$$a_0(E_{D,1};[\frac{rs^2tx}{DC}]) = \frac{(-1)^{\nu(\frac{D}{rs})-1}\varphi(D)}{24rs}.$$

In particular, we find that the constant terms of $E_{D,1}$ are independent of t and x.

Proof. By applying the second formula of (2.3) to the cusp $[\frac{rs^2tx}{DC}]$ with $K = rs$, we find that

$$a_0(E_{D,1};[\frac{rs^2tx}{DC}]) = \sum_{1\le\alpha|rs} (-1)^{\nu(\alpha)} \cdot \alpha^{-1} \cdot a_0(E_{D/rs,1};[\frac{rs^2t(\alpha x)}{DC}]).$$

Since $E_{D/rs,1}$ is of level $\Gamma_0(D/rs)$, it follows from (1) and (2) of Lemma 2.7 that

$$\begin{aligned} a_0(E_{D,1};[\frac{rs^2tx}{DC}]) &= \sum_{1\le\alpha|rs} (-1)^{\nu(\alpha)} \cdot \alpha^{-1} \cdot a_0(E_{D/rs,1};[\frac{t(\alpha x)}{D/rs \cdot C/s}]) \\ &= \left(\sum_{1\le\alpha|rs} (-1)^{\nu(\alpha)} \cdot \alpha^{-1}\right) \cdot a_0(E_{D/rs,1};[\infty]) \\ &= \frac{\varphi(rs)}{rs} \cdot a_0(E_{D/rs,1};[\infty]). \end{aligned}$$

Thus we only need to prove the lemma for the cusp $[\infty]$. However, if p be an arbitrary prime divisor of D, then the first formula of (2.3) shows that

$$\begin{aligned} a_0(E_{D,1};[\infty]) &= \left(\sum_{1\le\alpha|D/p}(-1)^{\nu(\alpha)}\cdot\alpha\right)\cdot a_0(E_{p,1};[\infty]) \\ &= (-1)^{\nu(\frac{D}{p})}\varphi(D/p)\cdot\frac{p-1}{24} \\ &= \frac{(-1)^{\nu(D)-1}\varphi(D)}{24} \end{aligned}$$

and our assertion follows. □

Lemma 2.9. *The constant terms of* $E_{M,D/M}$ *are given as*

$$a_0(E_{M,D/M};[\frac{rs^2tx}{DC}]) = \begin{cases} \frac{(-1)^{\nu(\frac{D}{rs})-1}\varphi(D)\cdot\psi(\frac{D}{M})}{24rs\frac{D}{M}}, & \text{if } \frac{D}{M}\mid rs \\ 0, & \text{if } \frac{D}{M}\nmid rs. \end{cases}$$

In particular, we find that the constant terms of $E_{M,D/M}$ *are independent of* t *and* x.

Proof. If $[\frac{rs^2tx}{DC}]$ is a cusp such that $\frac{D}{M}\mid rs$, then $(\frac{D}{M},\frac{DC}{rs^2t})=1$ and we find by the second formula of (2.4) and (1), (2) of Lemma 2.7 that

$$\begin{aligned} a_0(E_{M,D/M};[\frac{rs^2tx}{DC}]) &= \sum_{1\le\alpha|\frac{D}{M}}(-1)^{\nu(\alpha)}\cdot\alpha^{-2}\cdot a_0(E_{M,1};[\frac{\alpha rs^2tx}{DC}]) \\ &= \sum_{1\le\alpha|\frac{D}{M}}(-1)^{\nu(\alpha)}\cdot\alpha^{-2}\cdot a_0(E_{M,1};[\frac{r'(s')^2t(\alpha x)}{M\cdot(M,C)}]) \end{aligned}$$

with $r's'\cdot\frac{D}{M}=rs$. By Lemma 2.8, it then follows that

$$\begin{aligned} a_0(E_{M,D/M};[\frac{rs^2tx}{DC}]) &= \left(\sum_{1\le\alpha|\frac{D}{M}}(-1)^{\nu(\alpha)}\cdot\alpha^{-2}\right)\cdot\frac{(-1)^{\nu(\frac{M}{r's'})-1}\varphi(M)}{24r's'} \\ &= \frac{(-1)^{\nu(\frac{D}{rs})-1}\varphi(D)\cdot\psi(\frac{D}{M})}{24rs\frac{D}{M}}. \end{aligned}$$

However, if $\frac{D}{M}\nmid rs$, then $K:=(\frac{D}{M},\frac{DC}{rs^2t})\neq 1$ and we find by the first formula of (2.4) that

$$a_0(E_{M,D/M};[\frac{rs^2tx}{DC}]) = \sum_{1\le\alpha|K}(-1)^{\nu(\alpha)}\cdot a_0(E_{M,\frac{D}{MK}};[\frac{\alpha rs^2tx}{DC}])$$

$$= \sum_{1\le\alpha|K}(-1)^{\nu(\alpha)}\cdot a_0(E_{M,\frac{D}{MK}};[\frac{rs^2(\frac{t}{(t,\alpha)})x}{\frac{D}{\alpha}\cdot\frac{C}{(C,\alpha)}}]).$$

But as $(K,rs)=1$, Lemma 2.7 implies that $[\frac{rs^2(\frac{t}{(t,\alpha)})x}{\frac{D}{\alpha}\cdot\frac{C}{(C,\alpha)}}] = [\frac{rs^2t'x'}{\frac{D}{K}\cdot\frac{C}{(C,K)}}]$ as a cusp of $X_0(\frac{D}{K}\cdot\frac{C}{(C,K)})$ for some t' and x', so that all these $a_0(E_{M,\frac{D}{MK}};[\frac{rs^2(\frac{t}{(t,\alpha)})x}{\frac{D}{\alpha}\cdot\frac{C}{(C,\alpha)}}])$ are the same by the above result. It follows that $a_0(E_{M,D/M};[\frac{rs^2tx}{DC}])=0$ which completes the proof. □

Proposition 2.10. *For any pair of integers M and L as before, the constant terms of $E_{M,L}$ are given as*

$$a_0(E_{M,L};[\frac{rs^2tx}{DC}]) = \begin{cases} \prod_{p|(M,L,s)}(1-\frac{1}{p})\frac{(-1)^{\nu(\frac{D}{rs})-1}\varphi(D)\cdot\psi(L)}{24rsL}, & \text{if } \frac{D}{M}\mid rs \text{ and } (M,L)\mid st \\ 0, & \text{otherwise.}\end{cases}$$

Proof. We have already proved the above assertions when $(M,L)=1$ in Lemma 2.8 and Lemma 2.9, so we assume in the following that $K:=(M,L)\neq 1$. Note that we must have $K\mid C$. Now, if $[\frac{rs^2tx}{DC}]$ is a cusp such that $K\mid st$, then we can decompose $K=K_s\cdot K_t$ with $K_s:=(K,s)$ and $K_t:=(K,t)$. It then follows from the second formula of (2.4) that

$$a_0(E_{M,L};[\frac{rs^2tx}{DC}]) = \sum_{1\le\alpha_s|K_s}(-1)^{\nu(\alpha_s)}\cdot\alpha_s^{-2}\cdot a_0(E_{M,K_t\frac{D}{M}};[\frac{rs^2t(\alpha_sx)}{DC}]).$$

Since $[\frac{rs^2t(\alpha_sx)}{DC}] = [\frac{rs^2t(\alpha_sx+\frac{s}{\alpha_s}\cdot\frac{DC}{rs^2t})}{DC}]$ with $x_s:=\alpha_sx+\frac{s}{\alpha_s}\cdot\frac{DC}{rs^2t}$ prime to D, we find that

$$a_0(E_{M,L};[\frac{rs^2tx}{DC}]) = \sum_{1\le\alpha_s|K_s}(-1)^{\nu(\alpha_s)}\cdot\alpha_s^{-2}\cdot a_0(E_{M,K_t\frac{D}{M}};[\frac{rs^2tx_s}{DC}])$$

$$= \sum_{1\le\alpha_s|K_s}\sum_{1\le\alpha_t|K_t}(-1)^{\nu(\alpha_s\alpha_t)}\cdot\alpha_s^{-2}\cdot a_0(E_{M,K_t\frac{D}{M}};[\frac{r(s\alpha_t)^2(t/\alpha_t)x_s}{DC}]),$$

and hence get the assertion by a straightforward calculation using previous results. However, if $H:=\frac{(M,L)}{(M,L,st)}\neq 1$, then $H\mid\frac{DC}{rs^2t}$ and we find by the first formula of (2.4) that

$$a_0(E_{M,L};[\frac{rs^2tx}{DC}]) = \sum_{1\le\alpha|H}(-1)^{\nu(\alpha)}\cdot a_0(E_{M,L/H};[\frac{rs^2t(\alpha x)}{DC}]).$$

But it is easy to see from the above result that all these $a_0(E_{M,L/H};[\frac{rs^2t(\alpha x)}{DC}])$ are the same, so it follows that $a_0(E_{M,L};[\frac{rs^2tx}{DC}])=0$. We have thus completed the proof of the proposition. □

Please cite this article in press as: Y. Ren, Rational torsion subgroups of modular Jacobian varieties, J. Number Theory (2018), https://doi.org/10.1016/j.jnt.2018.02.009

3. Proof of the main theorem

3.1. Algebraic modular forms

Here, we briefly review the algebraic theory of modular forms. For more details, the reader is referred to [7].

The algebraic modular forms that we will mainly use in the following are those in the sense of Serre and Swinnerton-Dyer. For any positive integer N, let

$$M_2(\Gamma_0(N),\mathbb{Z}) := \{f \in M_2(\Gamma_0(N),\mathbb{C}) | f(\mathfrak{q}) \in \mathbb{Z}[[\mathfrak{q}]]\},$$
$$S_2(\Gamma_0(N),\mathbb{Z}) := \{f \in S_2(\Gamma_0(N),\mathbb{C}) | f(\mathfrak{q}) \in \mathbb{Z}[[\mathfrak{q}]]\}.$$

Then we define, for any ring R, that

$$M_2(\Gamma_0(N),R) := M_2(\Gamma_0(N),\mathbb{Z}) \otimes_{\mathbb{Z}} R,$$
$$S_2(\Gamma_0(N),R) := S_2(\Gamma_0(N),\mathbb{Z}) \otimes_{\mathbb{Z}} R.$$

These are the spaces of algebraic modular forms that are denoted as M_2^B and S_2^B respectively in [7]. On the other hand, we have also the following spaces of modular forms in the sense of Deligne–Rapoport and Katz (see Definition 1.2.5 of [7])

$$M_2^A(\Gamma_0(N),R) \supseteq S_2^A(\Gamma_0(N),R),$$

which are defined from the view of moduli. If R is any $\mathbb{Z}[1/N]$-algebra, then there are $\mathfrak{q}$-expansion preserved injections ([7], lemma 1.3.5)

$$M_2(\Gamma_0(N),R) \hookrightarrow M_2^A(\Gamma_0(N),R),\ \ S_2(\Gamma_0(N),R) \hookrightarrow S_2^A(\Gamma_0(N),R)$$

between these two kinds of modular forms. Moreover, if R is flat over $\mathbb{Z}[1/N]$, then the above injections are in fact isomorphisms ([7] (1.3.4)).

For any prime ℓ, there is a Hecke operator $T(\ell)$ acting on $M_2^A(\Gamma_0(N),R)$. If $f \in M_2^A(\Gamma_0(N),R)$ has its Fourier expansion as $\sum_{n=0}^{\infty} a_n\mathfrak{q}^n$, then (see (1.5.1) of [7])

$$T(\ell)(f) = \begin{cases} \sum_{n=0}^{\infty} a_{n\ell}\mathfrak{q}^n + \ell\cdot\sum_{n=0}^{\infty} a_n\mathfrak{q}^{n\ell}, & \text{if } \ell \nmid N \\ \sum_{n=0}^{\infty} a_{n\ell}\mathfrak{q}^n, & \text{if } \ell \mid N. \end{cases}$$

Note that $T(\ell)$ is denoted as $U(\ell)$ in the paper of Ohta. When $R = \mathbb{Z}[1/N]$, these operators coincide with the classical Hecke operators $T_\ell^{\Gamma_0(N)}$'s. It follows that these operators preserves the sub-spaces $M_2(\Gamma_0(N),R)$ and $S_2(\Gamma_0(N),R)$ for any $\mathbb{Z}[1/N]$-algebra R. We will denote $T_\ell^{\Gamma_0(N)}$ as T_ℓ for simplicity in the following and refer to them as either the classical operators or the algebraical operators if there is no risk of confusion.

3.2. New-part of modular Jacobian varieties

Let N be a positive integer. For any positive divisors $n \mid N$ and $m \mid \frac{N}{n}$, we have the following homomorphism

$$S_2(\Gamma_0(n), \mathbb{C}) \to S_2(\Gamma_0(N), \mathbb{C}),$$

which maps $f(z)$ to $f(mz)$. These maps then induce the following homomorphism

$$\prod_{n|N, n \neq N \ and \ m|\frac{N}{d}} S_2(\Gamma_0(n), \mathbb{C}) \to S_2(\Gamma_0(N), \mathbb{C}),$$

whose cokernel is isomorphic to the subspace of new forms of level $\Gamma_0(N)$. The above homomorphism induces the following morphism between abelian varieties over $\mathbb{Q}$

$$\iota_N : J_0(N) \to \prod_{n|N, n \neq N, m|\frac{N}{n}} J_0(n).$$

The *new-part* of $J_0(N)$ is then defined to be the kernel of the above morphism, so we have the following Cartesian diagram

$$\begin{tikzcd} J_0^{new}(N) \arrow[r] \arrow[d] & 0 \arrow[d] \\ J_0(N) \arrow[r] & J_0^{old}(N) \end{tikzcd}$$

where $J_0^{old}(N)$ is defined to be the image of ι_N which is a sub-abelian variety of $\prod_{n|N, n \neq N, m|\frac{N}{n}} J_0(n)$.

3.3. The proof of Theorem 1.2

For any positive integer N, we can uniquely write it as

$$N = D \cdot C \cdot C_1 \cdots C_k,$$

where $D, C, C_1, ..., C_k$ are all square-free positive integers such that $1 < C_k \mid \cdots \mid C_1 \mid C \mid D$. Thus, for any pair of integers M and L in $\mathcal{H}(DC)$, we find that the Eisenstein series $E_{M,L} \in \mathcal{E}_2(\Gamma_0(DC), \mathbb{C})$ and hence also in $\mathcal{E}_2(\Gamma_0(N), \mathbb{C})$, so we have the corresponding Eisenstein ideal $I_{\Gamma_0(N)}(E_{M,L})$ of $\mathbb{T}_0(N)$.

Lemma 3.1. *For any pair of two integers M, L in $\mathcal{H}(DC)$, there is a natural isomorphism*

$$\mathbb{T}_0(N)/I_{\Gamma_0(N)}(E_{M,L}) \simeq \mathbb{Z}/m\mathbb{Z}$$

Please cite this article in press as: Y. Ren, Rational torsion subgroups of modular Jacobian varieties, J. Number Theory (2018), https://doi.org/10.1016/j.jnt.2018.02.009

for some non-zero integer m. Moreover, if $(M, L) \neq 1$, then $q \nmid m$ for any prime $q \nmid 6 \cdot N \cdot \varpi(N)$.

Proof. We first prove that the above quotient ring is finite. Since it is obvious that the natural homomorphism $\mathbb{Z} \to \mathbb{T}_0(N)/I_{\Gamma_0(N)}(E_{M,L})$ is surjective, we only need to prove that the kernel of this homomorphism is non-zero. However, if the kernel is zero so that $\mathbb{Z} \simeq \mathbb{T}_0(N)/I_{\Gamma_0(N)}(E_{M,L})$, then the ring homomorphism $\mathbb{T} \to \mathbb{T}_0(N)/I_{\Gamma_0(N)}(E_{M,L}) \simeq \mathbb{Z} \hookrightarrow \mathbb{C}$ will give rise to a normalized cusp form whose eigenvalue is $1 + \ell$ for any $\ell \nmid D$ which this contradicts the Ramanujan bound. This proves the first statement.

Now we turn to the second assertion of the lemma. Suppose that $q \nmid 6 \cdot N \cdot \varpi(N)$ is a prime divisor of the above index m of $I_{\Gamma_0(N)}(E_{M,L})$ in $\mathbb{T}_0(N)$. Recall that there is a perfect pairing of $\mathbb{Z}$-modules (see [8])

$$\mathbb{T}_0(N) \times S_2(\Gamma_0(N), \mathbb{Z}) \to \mathbb{Z}, \ (T, f) \mapsto a_1(f|T; [\infty]).$$

Then, by base change from $\mathbb{Z}$ to $\mathbb{Z}/q\mathbb{Z}$, it follows that there is also a perfect pairing

$$\mathbb{T}_0(N)/q\mathbb{T}_0(N) \times S_2(\Gamma_0(N), \mathbb{Z}/q\mathbb{Z}) \to \mathbb{Z}/q\mathbb{Z}.$$

Since $\mathbb{T}_0(N)/(q, I_{\Gamma_0(N)}(E_{M,L}))$ is a quotient of $\mathbb{T}_0(n)/q\mathbb{T}_0(N)$, we get thus the following perfect pairing

$$\mathbb{T}_0(N)/(q, I_{\Gamma_0(N)}(E_{M,L})) \times S_2(\Gamma_0(N), \mathbb{Z}/q\mathbb{Z})[I_{\Gamma_0(N)}(E_{M,L})] \to \mathbb{Z}/q\mathbb{Z}$$

of $\mathbb{Z}/q\mathbb{Z}$-modules, which induces a canonical isomorphism

$$S_2(\Gamma_0(N), \mathbb{Z}/q\mathbb{Z})[I_{\Gamma_0(N)}(E_{M,L})] \simeq \mathbb{Z}/q\mathbb{Z}.$$

Since $a_0(E_{M,L}; [\infty]) = 0$ when $(M, L) \neq 1$, it follows that $S_2(\Gamma_0(N), \mathbb{Z}/q\mathbb{Z})[I_{\Gamma_0(N)}(E_{M,L})]$ is expanded by $E_{M,L} \pmod q$. So there exists some $g \in M_2(\Gamma_0(N), \mathbb{Z})$ such that $E_{M,L} + q \cdot g \in S_2(\Gamma_0(N), \mathbb{Z})$. Note that, as we have mentioned before, $M_2(\Gamma_0(N), \mathbb{Z}) \subseteq M_2(\Gamma_0(N), \mathbb{Z}[1/n\mathbb{Z}])$ is naturally embedded in $M_2^A(\Gamma_0(N), \mathbb{Z}[1/n\mathbb{Z}])$, g can be naturally viewed as a modular form in the sense of Katz with coefficients in $\mathbb{Z}[1/n\mathbb{Z}]$. Now since $X_0(N)$ is connected, it follows from Corollary 1.6.2 of [2] that the constant terms of g at the various cusps of $X_0(N)$ are all in $\mathbb{Z}[\frac{1}{6N}, \mu_N]$, so that

$$a_0(E_{M,L}; [c]) \in q \cdot \mathbb{Z}[\frac{1}{6N}, \mu_N] \bigcap \mathbb{Q} = q \cdot \mathbb{Z}[\frac{1}{6N}]$$

for any cusp c in $X_0(N)$, which contradicts to Proposition 2.10. This completes the proof of the lemma. □

Lemma 3.2. *For any positive integer N, we have $J_0^{new}(N)(\mathbb{Q})[q^\infty] = 0$ for any $q \nmid 6 \cdot N \cdot \varpi(N)$.*

Please cite this article in press as: Y. Ren, Rational torsion subgroups of modular Jacobian varieties, J. Number Theory (2018), https://doi.org/10.1016/j.jnt.2018.02.009

Proof. Suppose to the contrary that there is a prime $q \nmid 6 \cdot N \cdot \varpi(N)$ such that $J_0^{new}(N)(\mathbb{Q})[q^\infty] \neq 0$. There exists a non-zero point $P \in J_0^{new}(N)(\mathbb{Q})[q] \subseteq J_0(N)(\mathbb{Q})[q]$. By Eichler–Shimura theory, we have

$$T_\ell(P) = (1+\ell)P$$

for any $\ell \nmid N$. On the other hand, by the newform theory, we have

$$T_\ell(P) = \begin{cases} \delta_\ell \cdot P, & \text{if } \ell \mid \frac{D}{C} \\ 0, & \text{if } \ell \mid C, \end{cases}$$

where $\delta_\ell \in \{\pm\}$, so that

$$q \mid [\mathbb{T}_0(N) : I_P],$$

where I_P is the ideal

$$I_P := (\{T_\ell - (1+\ell)\}_{\ell \nmid N}, \{T_\ell\}_{\ell \mid C}, \{T_\ell - \delta_\ell\}_{\ell \mid \frac{D}{C}}).$$

Then, by the same argument as that in Lemma 3.1, we find that $S_2(\Gamma_0(N), \mathbb{Z}/q\mathbb{Z})[I_P] \neq 0$ and is generated by a unique normalized f_P.

Let $F_P \in S_2(\Gamma_0(N), \mathbb{Z})$ such that $F_P \equiv f_P \pmod q$. For any $\ell \mid \frac{D}{C}$, we have $F_P - \frac{\delta_\ell}{\ell} \cdot F_P$ belongs to $S_2(\Gamma_0(N\ell), \mathbb{Z}[1/N])$. Moreover, simple manipulation on Fourier expansions shows that

$$\begin{aligned} T_\ell(F_P - \frac{\delta_\ell}{\ell} \cdot F_P) &= T_\ell(F_P) - \delta_\ell \cdot F_P \\ &\equiv \delta_\ell \cdot f_P - \delta \cdot f_P = 0 \pmod q. \end{aligned}$$

Thus, by raising the levels in such a way, we will finally get a normalized $\Theta \in S_2(\Gamma_0(ND/C), \mathbb{Z}[1/N])$, and hence, by reduction, a normalized $\theta \in S_2(\Gamma_0(ND/C), \mathbb{Z}/q\mathbb{Z})$ which spans

$$S_2(\Gamma_0(ND/C), \mathbb{Z}/q\mathbb{Z})[I_{\Gamma_0(ND/C)}(E_{D,D})].$$

It then follows that $q \mid [\mathbb{T}_0(ND/C) : I_{\Gamma_0(ND/C)}(E_{D,D})]$, which contradicts to Lemma 3.1 and hence completes the proof. $\square$

Proof of Theorem 1.2. We prove the theorem by induction on $\nu(N)$. When $\nu(N) = 1$ so that N is a prime, the claim follows from the theorems of Ogg and Mazur. In general, if q is a prime such that $q \mid 6 \cdot N \cdot \varpi(N)$, then we also have $q \nmid 6 \cdot n \cdot \varpi(n)$ for any $n \mid N$. Thus, by the induction hypothesis, a point $P \in J_0(N)(\mathbb{Q})[q^\infty]$ must be mapped by ι_N to zero of $J_0^{old}(N)$, because $\nu(n) < \nu(N)$ for any $n \mid N$ and $n \neq N$. It follows that $P \in J_0^{new}(N)(\mathbb{Q})[q^\infty]$ and is hence zero by Lemma 3.2. This completes the proof of our theorem. $\square$

References

[1] D. Banerjee, A note on the Eisenstein elements of prime square level, Proc. Amer. Math. Soc. 142 (11) (2014) 3675–3686.
[2] N. Katz, P-adic properties of modular schemes and modular forms, in: Lecture Notes in Mathematics, vol. 350, 1973, pp. 69–190.
[3] S. Ling, On the Q-rational cuspidal subgroup and the component group of $J_0(p^r)$, Israel J. Math. 99 (1) (1997) 29–54.
[4] B. Mazur, Modular curves and the Eisenstein ideal, Publ. Math. Inst. Hautes Études Sci. 47 (1) (1977) 33–186.
[5] A. Ogg, Rational points on certain elliptic modular curves, Proc. Sympos. Pure Math. 24 (1973) 221–231.
[6] A. Ogg, Diophantine equations and modular forms, Bull. Amer. Math. Soc. 81 (1975) 14–27.
[7] M. Ohta, Eisenstein ideals and the rational torsion subgroups of modular Jacobian varieties II, Tokyo J. Math. 37 (2) (2014).
[8] K. Ribet, Mod p Hecke operators and congruences between modular forms, Invent. Math. 71 (1) (1983) 193–205.
[9] G. Stevens, Arithmetic of Modular Curves, Progress in Mathematics, vol. 20, Birkhäuser, 1982.
[10] H. Yoo, The index of an Eisenstein ideal and multiplicity one, Math. Z. 282 (3–4) (2016) 1097–1116.

Please cite this article in press as: Y. Ren, Rational torsion subgroups of modular Jacobian varieties, J. Number Theory (2018), https://doi.org/10.1016/j.jnt.2018.02.009