J. Math. Soc. Japan
Vol. 66, No. 4 (2014) pp. 1249–1301
doi: 10.2969/jmsj/06641249

The $\mathbb{Q}$-rational cuspidal group of $J_1(2p)$

By Toshikazu Takagi

(Received May 14, 2012)
(Revised Nov. 13, 2012)

Abstract. Let p be a prime not equal to 2 or 3. In this paper we study the $\mathbb{Q}$-rational cuspidal group $\mathcal{C}_{\mathbb{Q}}$ of the jacobian $J_1(2p)$ of the modular curve $X_1(2p)$. We prove that the group $\mathcal{C}_{\mathbb{Q}}$ is generated by the $\mathbb{Q}$-rational cusps. We determine the order of $\mathcal{C}_{\mathbb{Q}}$, and give numerical tables for all $p \leq 127$. These tables give also other cuspidal class numbers for the modular curves $X_1(2p)$ and $X_1(p)$. We give a basis of the group of the principal divisors supported on the $\mathbb{Q}$-rational cusps, and using this we determine the explicit structure of $\mathcal{C}_{\mathbb{Q}}$ for all $p \leq 127$. We determine the structure of the Sylow p-subgroup of $\mathcal{C}_{\mathbb{Q}}$, and the explicit structure for all $p \leq 4001$.

1. Introduction.

1.1. The $\mathbb{Q}$-rational cuspidal group.

Let X be a modular curve defined over $\mathbb{Q}$ of genus greater than 0, and let J_X be its jacobian defined over $\mathbb{Q}$. Let us assume that the cusp P_∞ on X represented by the infinity is rational over $\mathbb{Q}$. Let $i_\infty : P \mapsto [P - P_\infty]$ be the cuspidal embedding of X into J_X sending a point P to the divisor class of $P - P_\infty$. When P is a cusp of X, the point $i_\infty(P)$ is a torsion point of J_X (Manin [**11**], Drinfeld [**4**]). Let $T(J_X)_{\mathbb{Q}}$ be the group of all $\mathbb{Q}$-rational torsion points of J_X. Let $\mathcal{C}(J_X)$ be the subgroup of J_X generated by all cusps of X, and let $\mathcal{C}(J_X)_{\mathbb{Q}}$ be the subgroup of $\mathcal{C}(J_X)$ consisting of all $\mathbb{Q}$-rational points of $\mathcal{C}(J_X)$. Then we have $\mathcal{C}(J_X)_{\mathbb{Q}} \subset T(J_X)_{\mathbb{Q}}$. We call $\mathcal{C}(J_X)_{\mathbb{Q}}$ the $\mathbb{Q}$-*rational cuspidal group* of J_X.

The group $T(J_X)_{\mathbb{Q}}$ is a very important object in the arithmetic theory of the modular jacobian. But its study requires deep knowledge of the arithmetic algebraic geometry. On the other hand, for some modular curves, the group $\mathcal{C}(J_X)_{\mathbb{Q}}$ can be studied without the knowledge of the arithmetic algebraic geometry. Moreover, in some cases it is verified that $\mathcal{C}(J_X)_{\mathbb{Q}} = T(J_X)_{\mathbb{Q}}$, and also conjectured that the equality holds generally. The purpose of the present paper is to study the group $\mathcal{C}(J_X)_{\mathbb{Q}}$ and its subgroups in the case of $X = X_1(2p)$. First we recall some known results.

Let $X = X_0(n)$ ($n \in \mathbb{N}$). Then $X_0(n)$ has a $\mathbb{Q}$-rational model with P_∞ a $\mathbb{Q}$-rational point. If n is square-free, then all cusps on $X_0(n)$ are $\mathbb{Q}$-rational. Therefore, the group $\mathcal{C}(J_X)_{\mathbb{Q}}$ coincides with $\mathcal{C}(J_X)$, and its order is known (cf. Ogg [**13**] for the case where n is a prime, Takagi [**20**] for the case where n is arbitrary). In particular, when n is a prime, Ogg [**14**] conjectured and Mazur [**12**] proved that $\mathcal{C}(J_X)_{\mathbb{Q}} = T(J_X)_{\mathbb{Q}}$. When $n = pq$ with p, q distinct primes, Chua and Ling [**2**] determined the structure of the

2010 *Mathematics Subject Classification.* Primary 11G18; Secondary 11F03, 14G05, 14G35, 14H40.
Key Words and Phrases. modular curve, Jacobian variety, rational point, torsion subgroup, cuspidal class number, modular unit.

group $\mathcal{C}(J_X)_{\mathbb{Q}}$. For the twelve values $n = 11, 14, 15, 17, 19, 20, 21, 24, 27, 32, 36, 49$ with the genus of X one, Ogg [**13**] determined the structure of the group $\mathcal{C}(J_X)_{\mathbb{Q}}$ and verified that $\mathcal{C}(J_X)_{\mathbb{Q}} = T(J_X)_{\mathbb{Q}}$ and it is generated by the $\mathbb{Q}$-rational cusps. When $n = 5^3$, Poulakis [**16**] proved that $\mathcal{C}(J_X)_{\mathbb{Q}} = T(J_X)_{\mathbb{Q}}$ and it is a cyclic group of order 25. When $n = p^r$ with p a prime such that $p \geq 5$ and $p \not\equiv 11 \pmod{12}$, Lorenzini [**10**] proved that the prime-to-$2p$ parts of the groups $\mathcal{C}(J_X)_{\mathbb{Q}}$ and $T(J_X)_{\mathbb{Q}}$ coincide, and determined its structure. Also Ling [**9**], in the case where $n = p^r$ with $p \geq 3$ a prime, determined the structure of the group $\mathcal{C}(J_X)_{\mathbb{Q}}$, and proved that the prime-to-$6p$ (respectively prime-to-$2p$) parts of the groups $\mathcal{C}(J_X)_{\mathbb{Q}}$ and $T(J_X)_{\mathbb{Q}}$ coincide if $p \geq 5$ (respectively $p \geq 5$ and $r = 2$).

Let $X = X_1(n)$ ($n \in \mathbb{N}$). Then $X_1(n)$ has a $\mathbb{Q}$-rational model with P_∞ a $\mathbb{Q}$-rational point. When $n = p \neq 2, 3$ is a prime, Conrad, Edixhoven and Stein [**3**, Conjecture 6.2.2.] conjectured that the group $T(J_X)_{\mathbb{Q}}$ is generated by the ∞-cusps of $X_1(p)$, and verified it for all primes $p \leq 157$ except for $p = 29$, 97, 101, 109, and 113. (A cusp on $X_1(n)$ is called an ∞-cusp if it lies over the cusp ∞ of the curve $X_0(n)$. All ∞-cusps are $\mathbb{Q}$-rational points.) This conjecture is stronger than the statement $\mathcal{C}(J_X)_{\mathbb{Q}} = T(J_X)_{\mathbb{Q}}$. Recently, Ohta [**15**] proved that the conjecture of Conrad, Edixhoven and Stein is true up to 2-torsion. For the values $n = 13, 16, 18$ with the genus of X two, Ogg [**13**] determined the structure of the group $\mathcal{C}(J_X)_{\mathbb{Q}}$ and verified that $\mathcal{C}(J_X)_{\mathbb{Q}} = T(J_X)_{\mathbb{Q}}$ and it is generated by the $\mathbb{Q}$-rational cusps.

Generally, let Γ be a subgroup of $\mathrm{SL}_2(\mathbb{Z})/\{\pm 1_2\}$ with $\Gamma_0(n)/\{\pm 1_2\} \supset \Gamma \supset \pm\Gamma_1(n)/\{\pm 1_2\}$. Let $X = X_\Gamma$ be the modular curve corresponding to Γ. The curve X_Γ has a $\mathbb{Q}$-rational model with P_∞ a $\mathbb{Q}$-rational point. The group $\mathcal{C}(J_X)_{\mathbb{Q}}$ contains several subgroups. We denote by $\mathcal{C}(J_X)_\infty$, $\mathcal{C}(J_X)_1$, or $\mathcal{C}(J_X)_2$ the subgroup of $\mathcal{C}(J_X)_{\mathbb{Q}}$ generated by all ∞-cusps, the subgroup of $\mathcal{C}(J_X)_{\mathbb{Q}}$ generated by all $\mathbb{Q}$-rational cusps, or the subgroup of $\mathcal{C}(J_X)_{\mathbb{Q}}$ generated by all cuspidal divisors defined over $\mathbb{Q}$, respectively. (Similarly to the case of $X_1(n)$, a cusp on X_Γ is called an ∞-cusp if it lies over the cusp ∞ of the curve $X_0(n)$, and all ∞-cusps are $\mathbb{Q}$-rational.) Then we have $\mathcal{C}(J_X)_\infty \subset \mathcal{C}(J_X)_1 \subset \mathcal{C}(J_X)_2 \subset \mathcal{C}(J_X)_{\mathbb{Q}} \subset T(J_X)_{\mathbb{Q}}$.

The conjecture of Conrad, Edixhoven and Stein claims that $\mathcal{C}(J_X)_\infty = T(J_X)_{\mathbb{Q}}$ for $X = X_1(p)$ with p a prime. If it is true, then we have $\mathcal{C}(J_X)_\infty = \mathcal{C}(J_X)_1 = \mathcal{C}(J_X)_2 = \mathcal{C}(J_X)_{\mathbb{Q}} = T(J_X)_{\mathbb{Q}}$ for $X = X_1(p)$. (We can prove the first three equalities. For this, see Subsection 1.3 below.) When $X = X_1(n)$, the group $\mathcal{C}(J_X)_\infty$ is studied by several authors. The order of $\mathcal{C}(J_X)_\infty$ was determined first by Klimek [**6**] (the case where $n = p$ is a prime), next by Kubert and Lang [**8**] (the case where n is a power of a prime $p \neq 2, 3$), and last by Yu [**24**] (the case where n is arbitrary). (In fact, they considered the subgroup $\mathcal{C}(J_X)_0$ of $\mathcal{C}(J_X)$ supported on the 0-cusps. But it is isomorphic to $\mathcal{C}(J_X)_\infty$.) Concerning the structure of $\mathcal{C}(J_X)_\infty$, Yang [**23**] constructs an explicit basis for the group of modular units on $X_1(n)$ with n arbitrary whose divisors are supported on ∞-cusps.

However, in general, on the contrary to the case $X = X_1(p)$, the group $\mathcal{C}(J_X)_\infty$ does not coincide with $\mathcal{C}(J_X)_{\mathbb{Q}}$. Chen [**1**] considers the curve $X = X_\Gamma$ with Γ satisfying $\Gamma_0(p)/\{\pm 1_2\} \supsetneqq \Gamma \supsetneqq \pm\Gamma_1(p)/\{\pm 1_2\}$, constructs an explicit basis for the group of modular units whose divisors are supported on the divisors defined over $\mathbb{Q}$, determines the order of $\mathcal{C}(J_X)_2$, and shows that $\mathcal{C}(J_X)_\infty \subsetneqq \mathcal{C}(J_X)_2$. In this case the $\mathbb{Q}$-rational cusps are

∞-cusps, therefore, we have $\mathcal{C}(J_X)_\infty = \mathcal{C}(J_X)_1$. In [**1**] a numerical table is given. On the other hand, Conrad, Edixhoven and Stein [**3**, Table 2–3.] also give some numerical tables on the bound of the order of $T(J_X)_\mathbb{Q}$. Comparing these tables, we can verify that in several groups Γ with $\Gamma_0(p)/\{\pm 1_2\} \supsetneqq \Gamma \supsetneqq \pm\Gamma_1(p)/\{\pm 1_2\}$ the order of $\mathcal{C}(J_X)_2$ and the bound of the order of $T(J_X)_\mathbb{Q}$ coincide, which implies that in those cases we have $\mathcal{C}(J_X)_2 = \mathcal{C}(J_X)_\mathbb{Q} = T(J_X)_\mathbb{Q}$.

1.2. Main results.

In the present paper we consider the modular curve $X = X_1(2p)$ with $p \neq 2, 3$ a prime. In view of the results above, we might expect that $\mathcal{C}(J_X)_\mathbb{Q} = T(J_X)_\mathbb{Q}$. In fact there is an example of the equality. Let $X = X_1(14)$. The curve $X_1(14)$ is an elliptic curve. We can prove that the group $\mathcal{C}(J_X)_\mathbb{Q}$ is of order 6 (cf. Table 4). On the other hand the group $T(J_X)_\mathbb{Q}$ is also a group of order 6. This follows from a deep result of [**12**] that the only rational points of $X_1(14)$ are the rational cusps whose number is 6. Therefore, in this case we have $\mathcal{C}(J_X)_\mathbb{Q} = T(J_X)_\mathbb{Q}$. But the study of $T(J_X)_\mathbb{Q}$ is very hard. Our objects of the study are the group $\mathcal{C}(J_X)_\mathbb{Q}$ and its subgroups $\mathcal{C}(J_X)_\infty$, $\mathcal{C}(J_X)_1$, and $\mathcal{C}(J_X)_2$.

In Takagi [**21**] we determined the cuspidal class number of the modular curve $X_1(2p)$. The arguments of this paper is a continuation of [**21**]. For simplicity we denote the group $\mathcal{C}(J_X)_\mathbb{Q}$ by $\mathcal{C}_\mathbb{Q}$. Also we denote simply by $\mathcal{C}_\infty$, $\mathcal{C}_1$, and $\mathcal{C}_2$ the groups $\mathcal{C}(J_X)_\infty$, $\mathcal{C}(J_X)_1$, and $\mathcal{C}(J_X)_2$, respectively. Note that in Introduction of [**21**] we denoted the group $\mathcal{C}(J_X)_2$ by $C_\mathbb{Q}$.

In the following we state our main results. Concerning the relation between the groups $\mathcal{C}_\infty$, $\mathcal{C}_1$, $\mathcal{C}_2$ and $\mathcal{C}_\mathbb{Q}$, we have the following.

THEOREM 1.1. *Let p be a prime ≥ 7, and let $X = X_1(2p)$. Let $\mathcal{C}_\infty$, $\mathcal{C}_1$, $\mathcal{C}_2$ and $\mathcal{C}_\mathbb{Q}$ be as above. Then we have $\mathcal{C}_\infty \subsetneqq \mathcal{C}_1 = \mathcal{C}_2 = \mathcal{C}_\mathbb{Q}$.*

The condition $p \geq 7$ simply means that the genus of $X_1(2p)$ is not 0. The equalities $\mathcal{C}_1 = \mathcal{C}_2 = \mathcal{C}_\mathbb{Q}$ are given by Theorems 3.7 and 4.11. The inequality $\mathcal{C}_\infty \subsetneqq \mathcal{C}_1$ follows from the comparison of the orders of $\mathcal{C}_\infty$ and $\mathcal{C}_1$ as stated below.

The equality $\mathcal{C}_2 = \mathcal{C}_\mathbb{Q}$ can be restated in the language of homological algebra. Let I_P be the group of principal divisors of all modular units on $X_1(2p)$. Since the cusps of $X_1(2p)$ are rational over the field $k_{2p} = \mathbb{Q}(\zeta_{2p})$ with $\zeta_{2p} = \exp[2\pi i/2p]$, the group I_P is a G-module where $G = \mathrm{Gal}(k_{2p}/\mathbb{Q})$. Let $H^n(G, I_P)$ (respectively $H_n(G, I_P)$) be the n-th cohomology group (respectively homology group). Then we have the following (cf. Theorem 4.13).

THEOREM 1.2. *For all $n \geq 1$, we have $H^{2n-1}(G, I_P) = H_{2n}(G, I_P) = 0$.*

Let

$$a = \frac{p^2 - 1}{24}, \tag{1.1}$$

$$A = \frac{1}{p} \prod_{\psi} (4 - \psi(2)), \tag{1.2}$$

$$B = p\prod_{\psi}\left(\frac{1}{4}B_{2,\psi}\right), \tag{1.3}$$

where ψ runs over all even, primitive Dirichlet characters modulo p, and $B_{2,\psi}$ denotes the generalized Bernoulli number defined by

$$B_{2,\psi} = p\sum_{a=1}^{p-1}\psi(a)\left\{\left(\frac{a}{p}\right)^2 - \frac{a}{p} + \frac{1}{6}\right\}. \tag{1.4}$$

Then a, A and B are positive integers.

THEOREM 1.3. *The order $h_{\mathbb{Q}}$ of $\mathcal{C}_{\mathbb{Q}}$ is given by $h_{\mathbb{Q}} = aAB^2$.*

This is given by Theorem 5.3. The order $h_1^{\infty}(2p)$ of $\mathcal{C}_{\infty}$ is known to be equal to AB (cf. [**24**]). Hence we have $\mathcal{C}_{\infty} \subsetneqq \mathcal{C}_1$ because $aB \neq 1$ (cf. Tables 1 and 3).

The orders of several cuspidal groups of the modular curves $X_1(2p)$ and $X_1(p)$ can be expressed by the integers a, A, B. In fact, let $h_1(2p)$ be the full cuspidal class number of $X_1(2p)$ (cf. [**21**]), $h_1(p)$ the full cuspidal class number of $X_1(p)$ (cf. Takagi [**19**]), and $h_1^{\infty}(p)$ the order of the subgroup of the cuspidal divisor class group of $X_1(p)$ which is generated by the ∞-cusps (cf. [**8**, Chapter 6, Theorem 3.4]). Then we have $h_1(2p) = aA^2B^4$, $h_1(p) = B^2$ and $h_1^{\infty}(p) = B$. For the convenience of readers, instead of a numerical table only for $h_{\mathbb{Q}}$, we give numerical tables for a, A, and B with $7 \leq p \leq 127$ separately (cf. Tables 1–3).

For the study of the group structure of $\mathcal{C}_{\mathbb{Q}} = \mathcal{C}_1$, we give an explicit basis of the group of the principal divisors which are supported on the $\mathbb{Q}$-rational cusps. But, since it is complicated to state it in this Introduction, we refer the reader to Theorem 6.2. The determination of the explicit group structure for each prime p amounts to computing the Smith normal form of the matrix representing the divisors in the basis. A list of the explicit structures for the primes $7 \leq p \leq 127$ is given in Table 4.

Lastly, we determine the structure of the Sylow p-subgroup $\mathcal{C}_{\mathbb{Q},p}$ of $\mathcal{C}_{\mathbb{Q}}$. In order to state the result, we define an integer $W(q)$ for any prime q. Let n be an integer ≥ 0 satisfying

$$2^{q^n-1} \equiv 1 \pmod{q^{n+1}}, \tag{1.5}$$

which holds for any q if $n = 0$. Then there exists the maximal one of all such n, which we denote by $W(q)$ (cf. Proposition 7.12). A prime q is called a *Wieferich prime* if the congruence (1.5) with $n = 1$ holds. Then a prime q is a Wieferich prime if and only if $W(q) \geq 1$ (cf. Proposition 7.12). Although the number of Wieferich primes is believed to be infinite, the only ones that have been discovered so far are 1093 and 3511. Knauer and Richstein [**7**] reported that there are no other Wieferich primes less than $1.25 \cdot 10^{15}$. Let $q \neq 2, 3$ be a prime, and a be an integer with $1 \leq a \leq (q-3)/2$. We define an integer $B(q, 2a)$ for all pairs of q and a as follows. Let $n \geq 1$ be an integer satisfying

$$B_{(2a-2)q^{n-1}+2} \equiv 0 \pmod{q^n\mathbb{Z}_q}, \tag{1.6}$$

where $B_{(2a-2)q^{n-1}+2}$ denotes the Bernoulli number. If there is no such integer n, then put $B(q,2a)=0$. If there exists at least one, then it can be proved that there exists the maximal one of all such n, which we denote by $B(q,2a)$ (cf. Proposition 7.17). A pair $(q,2a)$ is called an *irregular pair* if the congruence (1.6) with $n=1$ holds. Then a pair $(q,2a)$ is an irregular pair if and only if $B(q,2a)\geq 1$ (cf. Proposition 7.17).

The group $\mathcal{C}_{\mathbb{Q},p}$ contains two subgroups denoted by $\mathcal{C}_{\mathbb{Q},p}(k,+)$ and $\mathcal{C}_{\mathbb{Q},p}(k,-)$ corresponding to each integer k with $1\leq k\leq (p-3)/2$. For the precise definition of these subgroups, see Section 7.3. Then we have the decomposition

$$\mathcal{C}_{\mathbb{Q},p}=\bigoplus_{k=1}^{(p-3)/2}\mathcal{C}_{\mathbb{Q},p}(k,+)\oplus\bigoplus_{k=1}^{(p-3)/2}\mathcal{C}_{\mathbb{Q},p}(k,-) \tag{1.7}$$

(cf. (7.26)). Let δ be the order of 2 in the group $(\mathbb{Z}/p\mathbb{Z})^{\times}$. Then the group structure of each subgroup is given as follows (cf. Theorems 7.24 and 7.25).

THEOREM 1.4. *Let k and δ be as above.*

(1) *If $k=1$, then $\mathcal{C}_{\mathbb{Q},p}(1,+)=0$.*
(2) *If $2\leq k\leq (1/2)(p-3)$, then*

$$\mathcal{C}_{\mathbb{Q},p}(k,+)\cong\begin{cases}\mathbb{Z}/p^{B(p,p+1-2k)+W(p)+1}\mathbb{Z} & \begin{cases}\text{if } \delta \text{ is even and } k=1+(\delta/2)l\\ \text{with } l \text{ an odd integer,}\end{cases}\\ \mathbb{Z}/p^{B(p,p+1-2k)}\mathbb{Z} & \text{otherwise.}\end{cases}$$

THEOREM 1.5. *Let k and δ be as above.*

(1) *If $k=1$, then $\mathcal{C}_{\mathbb{Q},p}(1,-)\cong\mathbb{Z}/p^{W(p)}\mathbb{Z}$.*
(2) *If $2\leq k\leq (1/2)(p-3)$, then*

$$\mathcal{C}_{\mathbb{Q},p}(k,-)\cong\begin{cases}\mathbb{Z}/p^{B(p,p+1-2k)+W(p)+1}\mathbb{Z} & \text{if } k\equiv 1 \pmod{\delta},\\ \mathbb{Z}/p^{B(p,p+1-2k)}\mathbb{Z} & \text{otherwise.}\end{cases}$$

In particular, when p is regular and not a Wieferich prime, we have the following (cf. Corollary 7.26). The notation $[x]$ ($x\in\mathbb{R}$) denotes the greatest integer that is less than or equal to x.

THEOREM 1.6. *Let $p\neq 2,3$ be a regular prime and not a Wieferich prime. Let $f_1=[(1/2\delta)(p-5)]$ and $f_2=[(1/2\delta)(p-5)+1/2]$. Then*

$$\mathcal{C}_{\mathbb{Q},p}\cong\begin{cases}(\mathbb{Z}/p\mathbb{Z})^{f_1} & \text{if } \delta \text{ is odd,}\\ (\mathbb{Z}/p\mathbb{Z})^{f_1+f_2} & \text{if } \delta \text{ is even.}\end{cases}$$

When p is irregular or a Wieferich prime with $p\leq 4001$, we have the following results. The reason why we consider the primes with $p\leq 4001$ is that we want to use the table given in Washington [**22**, Section 2 of Tables] where all irregular pairs $(p,2a)$

with $p \leq 4001$ are given. About the only known Wieferich primes 1093 and 3511, the prime 1093 is regular and the prime 3511 is irregular. When p is irregular, we can verify that $B(p, 2a) = 1$ for all irregular pairs $(p, 2a)$ with $p \leq 4001$ (cf. Example 7.20). We denote by $I(p)$ the number of the integers a such that $(p, 2a)$ is an irregular pair, which is called the *index of irregularity* of p. Then we have the following (cf. Examples 7.27, 7.28, 7.29).

EXAMPLE 1.7. Let p be an irregular prime such that $p \leq 4001$ and $p \neq 3511$. Let $f_1 = [(1/2\delta)(p-5)]$ and $f_2 = [(1/2\delta)(p-5) + 1/2]$. Then

$$\mathcal{C}_{\mathbb{Q},p} \cong \begin{cases} (\mathbb{Z}/p\mathbb{Z})^{f_1+2I(p)} & \text{if } \delta \text{ is odd,} \\ (\mathbb{Z}/p\mathbb{Z})^{f_1+f_2+2I(p)} & \text{if } \delta \text{ is even.} \end{cases}$$

EXAMPLE 1.8. (1) Let $p = 1093$, which is the only known regular Wieferich prime. Then

$$\mathcal{C}_{\mathbb{Q},p} \cong (\mathbb{Z}/1093\mathbb{Z}) \oplus (\mathbb{Z}/1093^2\mathbb{Z})^2.$$

(2) Let $p = 3511$, which is the only known irregular Wieferich prime. Then

$$\mathcal{C}_{\mathbb{Q},p} \cong (\mathbb{Z}/3511\mathbb{Z})^5.$$

The explicit structures of $\mathcal{C}_{\mathbb{Q},p}$ for all primes p with $7 \leq p \leq 4001$ are listed in Table 5.

1.3. The case $X = X_1(p)$.

For the curve $X = X_1(p)$, we can prove that $\mathcal{C}(J_X)_\infty = \mathcal{C}(J_X)_1 = \mathcal{C}(J_X)_2 = \mathcal{C}(J_X)_{\mathbb{Q}}$, though their proofs are not given in this paper. The proofs of $\mathcal{C}(J_X)_1 = \mathcal{C}(J_X)_2 = \mathcal{C}(J_X)_{\mathbb{Q}}$ are similar to and simpler than those of the corresponding equalities in Theorem 1.1 given in Sections 3 and 4 if we use the arguments in [**19**]. For the curve $X_1(p)$, a cusp is $\mathbb{Q}$-rational if and only if it is an ∞-cusp, therefore, we have $\mathcal{C}(J_X)_\infty = \mathcal{C}(J_X)_1$. Of course, if the conjecture of Conrad, Edixhoven and Stein referred to above is true, these equalities follow immediately.

1.4. The contents of each section.

The present paper is organized as follows. In Section 2, we define a $\mathbb{Q}$-rational model $X_1(2p)_{\mathbb{Q}}$ of $X_1(2p)$, study the Galois action on the cusps of $X_1(2p)_{\mathbb{Q}}$, and define the three subgroups $\mathcal{C}_1$, $\mathcal{C}_2$ and $\mathcal{C}_{\mathbb{Q}}$ of the $\mathbb{Q}$-rational torsion group of $J_1(2p)_{\mathbb{Q}}$. In Section 3 we prove $\mathcal{C}_1 = \mathcal{C}_2$. In Section 4 we prove $\mathcal{C}_2 = \mathcal{C}_{\mathbb{Q}}$. In Section 5 we determine the order of the $\mathbb{Q}$-rational cuspidal group $\mathcal{C}_{\mathbb{Q}}$. In Section 6 we give a $\mathbb{Z}$-basis of the group of the principal divisors supported on the $\mathbb{Q}$-rational cusps so that we can determine the structure of $\mathcal{C}_{\mathbb{Q}}$ explicitly for a given value of p. In Section 7 we determine the structure of the Sylow p-subgroup $\mathcal{C}_{\mathbb{Q},p}$ of $\mathcal{C}_{\mathbb{Q}}$. In Section 8 we give a few tables of computational results.

In the present paper we denote by $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, 1_2, $\mathbb{Z}_p$, $\mathbb{Q}_p$ the set of natural numbers, the ring of rational integers, the field of rational numbers, the field of real numbers, the field of complex numbers, the two-by-two identity matrix, the ring of p-

adic integers, the field of p-adic numbers, respectively.

2. The $\mathbb{Q}$-rational cuspidal group $\mathcal{C}_\mathbb{Q}$ of $J_1(2p)_\mathbb{Q}$.

Let p be a prime $\neq 2, 3$. In this section we define a $\mathbb{Q}$-rational model $X_1(2p)_\mathbb{Q}$ of $X_1(2p)$, study the Galois action on the cusps of $X_1(2p)_\mathbb{Q}$, and define the three subgroups $\mathcal{C}_1$, $\mathcal{C}_2$ and $\mathcal{C}_\mathbb{Q}$ of the $\mathbb{Q}$-rational torsion group of $J_1(2p)_\mathbb{Q}$. Our object of the study is the group $\mathcal{C}_\mathbb{Q}$, the $\mathbb{Q}$-rational cuspidal group of $J_1(2p)_\mathbb{Q}$, which is isomorphic to a subgroup of the cuspidal divisor class group of $X_1(2p)$.

2.1. A $\mathbb{Q}$-rational model $X_1(N)_\mathbb{Q}$ of $X_1(N)$.

Let Γ be a Fuchsian group of the first kind. We denote by X_Γ the complete non-singular curve associated with the quotient $\Gamma\backslash\mathfrak{H}$, where the symbol $\mathfrak{H}$ denotes the upper half plane.

Let N be a positive integer. Let $\Gamma(N)$ be the principal congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ consisting of all matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ $(\in \mathrm{SL}_2(\mathbb{Z}))$ with $a-1 \equiv d-1 \equiv b \equiv c \equiv 0 \pmod N$. When $\Gamma = \Gamma(N)$, we denote the curve X_Γ by $X(N)$. Let $\Gamma_1(N)$ be the subgroup of $\mathrm{SL}_2(\mathbb{Z})$ consisting of all matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ $(\in \mathrm{SL}_2(\mathbb{Z}))$ with $a-1 \equiv d-1 \equiv c \equiv 0 \pmod N$. When $\Gamma = \Gamma_1(N)$, we denote the curve X_Γ by $X_1(N)$.

We define a $\mathbb{Q}$-rational model $X_1(N)_\mathbb{Q}$ of $X_1(N)$ as follows (cf. Shimura [**18**, Chapter 6]).

Let $\mathfrak{F}_N$ (respectively $\mathfrak{F}_1$) denote the field of all automorphic functions with respect to the group $\Gamma(N)$ (respectively $\mathrm{SL}_2(\mathbb{Z})$) such that their Fourier coefficients belong to the cyclotomic field $k_N = \mathbb{Q}(e^{2\pi i/N})$ (respectively $\mathbb{Q}$). Then it is known that the field $\mathfrak{F}_N$ is a Galois extension of $\mathfrak{F}_1$, and its Galois group is isomorphic to the group $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\}$.

Let $G_1(N)$ be the subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\}$ consisting of elements of the form $\pm\left(\begin{smallmatrix} 1 & b \\ 0 & d \end{smallmatrix}\right)$ with b, d arbitrary. Let $\mathfrak{F}_1(N)$ be the subfield of $\mathfrak{F}_N$ corresponding to the subgroup $G_1(N)$. Then the field $\mathfrak{F}_1(N)$ consists of all automorphic functions with respect to the group $\Gamma_1(N)$ such that their Fourier coefficients belong to $\mathbb{Q}$. It is known that the field $\mathbb{Q}$ is algebraically closed in $\mathfrak{F}_1(N)$ and the field $\mathbb{C}\mathfrak{F}_1(N)$ is the field of all automorphic functions with respect to $\Gamma_1(N)$. Hence the filed $\mathfrak{F}_1(N)$ defines a $\mathbb{Q}$-rational model $X_1(N)_\mathbb{Q}$ of $X_1(N)$. We shall consider this model.

2.2. A parametrization of the cusps on $X_1(M)$ with M square-free.

Here we give a parametrization of the cusps on $X_1(N)$ by an abelian group when N is square-free.

Let $M \neq 1$ be a square-free integer, and put $N = M$. In order to parametrize the cusps on $X_1(M)$, we recall the results in [**21**, Section 2].

Let T be the set of all positive divisors of M. We regard it as a group with the product defined by $r \circ s = rs/(r,s)^2$ where (r,s) denotes the greatest common divisor of r and s $(r, s \in T)$. Let $\mathcal{O}$ be the order defined by $\mathcal{O} = \sum_{r\in T} \mathbb{Z}\sqrt{r}$. We denote by $G(\sqrt{M})$ the subgroup of $SL_2(\mathcal{O})$ consisting of all elements α of the form

$$\alpha = \begin{pmatrix} a\sqrt{r} & b\sqrt{r^*} \\ c\sqrt{r^*} & d\sqrt{r} \end{pmatrix}, \tag{2.1}$$

where a, b, c, $d \in \mathbb{Z}$, $r \in T$ and $r^* = M/r$. We call r the *type* of α, and denote it by $t(\alpha)$. Let I be the ideal of $\mathcal{O}$ defined by $I = \sqrt{M}\mathcal{O}$. We denote by $\Gamma(I)$ the subgroup of $G(\sqrt{M})$ consisting of all elements α satisfying $\alpha \equiv 1_2 \pmod{I}$, and call it a *principal congruence subgroup* of $G(\sqrt{M})$. When $\Gamma = \Gamma(I)$, we denote the curve X_Γ by X_I. Since we have

$$\Gamma(I) = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{M} \end{pmatrix}^{-1} \Gamma_1(M) \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{M} \end{pmatrix}, \tag{2.2}$$

the curve $X_1(M)$ is isomorphic to the curve X_I.

Let $\mathfrak{F}_I^{(M)}$ (respectively $\mathfrak{F}_1^{(M)}$) denote the field of all automorphic functions with respect to the group $\Gamma(I)$ (respectively $G(\sqrt{M})$) such that their Fourier coefficients belong to the cyclotomic field k_M (respectively $\mathbb{Q}$). Let $\mathcal{G}_I$ denote the subgroup of $GL_2(\mathcal{O}/I)$ consisting of all elements α which can be represented by a matrix A ($\in M_2(\mathcal{O})$) of the form

$$A = \begin{pmatrix} a\sqrt{r} & b\sqrt{r^*} \\ c\sqrt{r^*} & d\sqrt{r} \end{pmatrix}, \tag{2.3}$$

where a, b, c, $d \in \mathbb{Z}$, $r \in T$ and $r^* = M/r$. It is known that the field $\mathfrak{F}_I^{(M)}$ is a Galois extension of $\mathfrak{F}_1^{(M)}$, and its Galois group is isomorphic to the group $\mathcal{G}_I(\pm) \overset{\text{def}}{=} \mathcal{G}_I/\{\pm 1_2\}$ ([**19**, Section 1 (1.15)]). Let α be an element of $\mathcal{G}_I$ or $\mathcal{G}_I(\pm)$. We denote by $\sigma(\alpha)$ the element of the Galois group $\mathrm{Gal}(\mathfrak{F}_I^{(M)}/\mathfrak{F}_1^{(M)})$ corresponding to α. Let α be represented by the matrix A in (2.3). Then the element r of T is determined only by α. We call r the *type* of α, and denote it by $t(\alpha)$.

Let $\mathcal{P}_\infty$ denote the prime divisor of $\mathfrak{F}_I^{(M)}$ defined by the q-expansion. Let $\mathcal{P}$ be a prime divisor of $\mathfrak{F}_I^{(M)}$, and $\nu_\mathcal{P}$ the valuation of $\mathcal{P}$. For any element σ of $\mathrm{Gal}(\mathfrak{F}_I^{(M)}/\mathfrak{F}_1^{(M)})$, we define the prime divisor $\mathcal{P}^\sigma$ by $\nu_{\mathcal{P}^\sigma}(h^\sigma) = \nu_\mathcal{P}(h)$ ($h \in \mathfrak{F}_I^{(M)}$), which defines a right action of the group $\mathrm{Gal}(\mathfrak{F}_I^{(M)}/\mathfrak{F}_1^{(M)})$. The conjugates $\mathcal{P}_\infty^\sigma$ are of degree one, and can be identified with the cusps on the curve X_I. If $\alpha \in \mathcal{G}_I$ is represented by a matrix $A \in G(\sqrt{M})$, the prime divisor $\mathcal{P}_\infty^{\sigma(\alpha)}$ corresponds to the cusp on X_I represented by $A^{-1}(\infty)$. The conjugates $\mathcal{P}_\infty^\sigma$ are called the *cuspidal prime divisors*.

Let C_I be the subgroup of $\mathcal{G}_I$ consisting of all elements α which can be represented by a matrix A ($\in M_2(\mathcal{O})$) of the form

$$A = \begin{pmatrix} a\sqrt{r} & b\sqrt{r^*} \\ b\sqrt{r^*} & a\sqrt{r} \end{pmatrix} \tag{2.4}$$

with a, $b \in \mathbb{Z}$, $r \in T$ and $(ar, br^*, M) = 1$. It is an abelian subgroup of $\mathcal{G}_I$, and called a *Cartan group*.

Every cuspidal prime divisor can be expressed as $\mathcal{P}_\infty^{\sigma(\alpha)}$ with a unique element $\alpha \in C_I(\pm) \overset{\text{def}}{=} C_I/\{\pm 1_2\}$. Thus the set of cusps on the curve X_I can be parametrized by

the abelian group $C_I(\pm)$ using the bijective mapping $\alpha \mapsto \mathcal{P}_\infty^{\sigma(\alpha)}$. This gives also the parametrization of the cusps on the curve $X_1(M)$.

2.3. The Galois action on the cusps of $X_1(M)_{\mathbb{Q}}$.

Let M and I be the same as in the subsection 2.2. We define a $\mathbb{Q}$-rational model of the curve X_I as follows (cf. [**19**, Section 1]).

Let H_I be the subgroup of $\mathcal{G}_I$ consisting of the elements of the form $\left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right)$ with d arbitrary. Let $\mathfrak{F}_{I,\mathbb{Q}}^{(M)}$ be the subfield of $\mathfrak{F}_I^{(M)}$ corresponding to the subgroup H_I. Then the field $\mathfrak{F}_{I,\mathbb{Q}}^{(M)}$ consists of all automorphic functions with respect to the group $\Gamma(I)$ such that their Fourier coefficients belong to $\mathbb{Q}$. It is known that the field $\mathbb{Q}$ is algebraically closed in $\mathfrak{F}_{I,\mathbb{Q}}^{(M)}$ and the field $\mathbb{C}\mathfrak{F}_{I,\mathbb{Q}}^{(M)}$ is the field of all automorphic functions with respect to $\Gamma(I)$. Hence the field $\mathfrak{F}_{I,\mathbb{Q}}^{(M)}$ defines a $\mathbb{Q}$-rational model $X_{I,\mathbb{Q}}$ of X_I.

The mapping $f(\tau) \mapsto f(\tau/\sqrt{M})$ defines an isomorphism of the function field $\mathfrak{F}_1(M)$ onto the function field $\mathfrak{F}_{I,\mathbb{Q}}^{(M)}$. Hence the curve $X_1(M)_{\mathbb{Q}}$ is isomorphic over $\mathbb{Q}$ to the curve $X_{I,\mathbb{Q}}$. We shall consider the cusps of $X_{I,\mathbb{Q}}$ instead of $X_1(M)_{\mathbb{Q}}$.

Since the cuspidal prime divisors of $\mathfrak{F}_I^{(M)}$ are of degree one, the cusps of $X_{I,\mathbb{Q}}$ are rational over k_M. We consider the action of the Galois group $\mathrm{Gal}(k_M/\mathbb{Q})$ on the cusps of $X_{I,\mathbb{Q}}$. Let d be an integer satisfying $(d, M) = 1$, and let $\sigma_d \in \mathrm{Gal}(k_M/\mathbb{Q})$ be the element defined by

$$\sigma_d : \zeta_M \mapsto \zeta_M^d \tag{2.5}$$

where $\zeta_M = \exp[2\pi i/M]$. Let P be a cusp of $X_{I,\mathbb{Q}}$, and let P^{σ_d} be the image of P by the action of σ_d. Let f be an element of $\mathfrak{F}_{I,\mathbb{Q}}^{(M)}$ which is defined at P. Then the value $f(P)$ of f at P belongs to k_M. The image P^{σ_d} satisfies by definition

$$f(P^{\sigma_d}) = f(P)^{\sigma_d}. \tag{2.6}$$

PROPOSITION 2.1. *Let d and σ_d be as above. Let γ_d be the element of $\mathcal{G}_I$ represented by the matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right)$. Let P be a cusp of $X_{I,\mathbb{Q}}$, and let $\mathcal{P}$ be the cuspidal prime divisor of $\mathfrak{F}_I^{(M)}$ corresponding to P. Then the cuspidal prime divisor of $\mathfrak{F}_I^{(M)}$ corresponding to the conjugate cusp P^{σ_d} is $\mathcal{P}^{\sigma(\gamma_d)}$.*

PROOF. Let f be an element of $\mathfrak{F}_{I,\mathbb{Q}}^{(M)}$ which is defined at P. Let $\mathfrak{m}_{\mathcal{P}}$ be the maximal ideal of the valuation ring of $\mathcal{P}$. Then we have

$$f \equiv f(P) \ (\mathrm{mod}\, \mathfrak{m}_{\mathcal{P}}).$$

Hence $f^{\sigma(\gamma_d)} \equiv f(P)^{\sigma(\gamma_d)} \ (\mathrm{mod}(\mathfrak{m}_{\mathcal{P}})^{\sigma(\gamma_d)})$. Since $f \in \mathfrak{F}_{I,\mathbb{Q}}^{(M)}$, we have $f^{\sigma(\gamma_d)} = f$. Also we have $f(P)^{\sigma(\gamma_d)} = f(P)^{\sigma_d} = f(P^{\sigma_d})$ and $(\mathfrak{m}_{\mathcal{P}})^{\sigma(\gamma_d)} = \mathfrak{m}_{\mathcal{P}^{\sigma(\gamma_d)}}$. Hence

$$f \equiv f(P^{\sigma_d}) \ (\mathrm{mod}\, \mathfrak{m}_{\mathcal{P}^{\sigma(\gamma_d)}}).$$

This proves that the cusp P^{σ_d} corresponds to the cuspidal prime divisor $\mathcal{P}^{\sigma(\gamma_d)}$. □

We can describe the action of $\mathrm{Gal}(k_M/\mathbb{Q})$ on the cusps by the use of the parametrization by the Cartan group.

PROPOSITION 2.2. *Let d, σ_d and γ_d be as in Proposition* 2.1. *Let d_1 be an integer satisfying $dd_1 \equiv 1 \pmod{M}$. Let P be a cusp of $X_{I,\mathbb{Q}}$ corresponding to a cuspidal prime divisor $\mathcal{P}_\infty^{\sigma(\alpha^{-1})}$ of $\mathfrak{F}_I^{(M)}$, where α is an element of C_I represented by a matrix $\left(\begin{smallmatrix} a\sqrt{r} & b\sqrt{r^*} \\ b\sqrt{r^*} & a\sqrt{r} \end{smallmatrix}\right)$ (cf.* (2.4)). *Then the cusp P^{σ_d} corresponds to the cuspidal prime divisor $\mathcal{P}_\infty^{\sigma(\alpha_1^{-1})}$ of $\mathfrak{F}_I^{(M)}$, where α_1 is the element of C_I represented by the matrix $\left(\begin{smallmatrix} a\sqrt{r} & bd_1\sqrt{r^*} \\ bd_1\sqrt{r^*} & a\sqrt{r} \end{smallmatrix}\right)$.*

PROOF. By Proposition 2.1, the cusp P^{σ_d} corresponds to the cuspidal prime divisor $\mathcal{P}_\infty^{\sigma(\alpha^{-1})\sigma(\gamma_d)} = \mathcal{P}_\infty^{\sigma(\alpha^{-1}\gamma_d)}$. Let $\mathcal{P}_\infty^{\sigma(\alpha^{-1}\gamma_d)} = \mathcal{P}_\infty^{\sigma(\alpha_1^{-1})}$ with an element $\alpha_1 \in C_I(\pm)$. Then we have $\mathcal{P}_\infty^{\sigma(\alpha^{-1}\gamma_d\alpha_1)} = \mathcal{P}_\infty$, whence $\alpha^{-1}\gamma_d\alpha_1 \in \pm H_I$ (cf. [**21**, Section 2.6]). This implies that

$$\alpha^{-1}\gamma_d\alpha_1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \equiv \pm \begin{pmatrix} 1 \\ 0 \end{pmatrix} \pmod{I},$$

which gives

$$\alpha_1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \equiv \pm \begin{pmatrix} a\sqrt{r} \\ bd_1\sqrt{r^*} \end{pmatrix} \pmod{I}.$$

This proves the proposition. □

We determine the $\mathbb{Q}$-rational cusps of $X_{I,\mathbb{Q}}$.

THEOREM 2.3. *Let P be a cusp of $X_{I,\mathbb{Q}}$ corresponding to a cuspidal prime divisor $\mathcal{P}_\infty^{\sigma(\alpha^{-1})}$ of $\mathfrak{F}_I^{(M)}$ with α an element of C_I of type r. Then P is $\mathbb{Q}$-rational if and only if one of the following* (1)–(4) *holds*:

(1) $r = 1$; (2) $r = 2$ *and* M *is even*; (3) $r = 3$ *and* $M = 3, 6$; (4) $r = 6$ *and* $M = 6$.

PROOF. Let d, σ_d and d_1 be as in Proposition 2.2. Then, by the proposition, $P^{\sigma_d} = P$ if and only if

$$\begin{pmatrix} a\sqrt{r} \\ b\sqrt{r^*} \end{pmatrix} \equiv \pm \begin{pmatrix} a\sqrt{r} \\ bd_1\sqrt{r^*} \end{pmatrix} \pmod{I},$$

which is equivalent to that the following (i) or (ii) holds:

(i) $b \equiv bd_1 \pmod{r}$,
(ii) $a \equiv -a \pmod{r^*}$, $b \equiv -bd_1 \pmod{r}$.

Since $(ar, br^*, M) = 1$, we have $(a, r^*) = (b, r) = 1$. It is easy to see that the condition (i) is equivalent to $d_1 \equiv 1 \pmod{r}$, and (ii) is equivalent to that $2 \equiv 0 \pmod{r^*}$

and $d_1 \equiv -1 \pmod r$. If (i) or (ii) holds for any d_1 with $(d_1, M) = 1$, then $d_1 \equiv \pm 1 \pmod r$, i.e., $(\mathbb{Z}/r\mathbb{Z})^\times = 1$ or $\{\pm 1\}$. This implies that $r = 1, 2, 3, 6$. If $r = 1$, then (i) holds for any d_1 with $(d_1, M) = 1$. If $r = 2$, then M must be even. In this case, for any d_1 with $(d_1, M) = 1$, we have $d_1 \equiv 1 \pmod r$, hence (i) holds. If $r = 3$, then M must be a multiple of 3. For any d_1 with $(d_1, M) = 1$, we have $d_1 \equiv 1 \pmod r$ or $d_1 \equiv -1 \pmod r$. If $d_1 \equiv 1 \pmod r$, then (i) holds. If $d_1 \equiv -1 \pmod r$, then (i) does not hold, hence we must have $2 \equiv 0 \pmod{r^*}$, whence $r^* = 1, 2$. This implies that M is 3 or 6. If $r = 6$, then M must be a multiple of 6. For any d_1 with $(d_1, M) = 1$, we have $d_1 \equiv 1 \pmod r$ or $d_1 \equiv -1 \pmod r$. If $d_1 \equiv 1 \pmod r$, then (i) holds. If $d_1 \equiv -1 \pmod r$, then (i) does not hold, hence we must have $2 \equiv 0 \pmod{r^*}$, whence $r^* = 1$. This implies $M = 6$. Thus the proof is completed. □

2.4. The cuspidal divisor class group of $X_1(2p)$.

Let p be a prime $\neq 2, 3$. Henceforth, we assume that

$$M = 2p. \tag{2.7}$$

Let $\mathcal{D}$ be the free abelian group generated by the cuspidal prime divisors of $\mathfrak{F}_I$, and $\mathcal{D}_0$ the subgroup of $\mathcal{D}$ consisting of all elements of degree 0. Let $R = \mathbb{Z}[C_I(\pm)]$ be the group ring of $C_I(\pm)$, and R_0 the additive subgroup of R consisting of all elements of degree 0. Let

$$\varphi : \mathcal{D} \cong R \tag{2.8}$$

be the isomorphism defined by the mapping $\mathcal{P}_\infty^{\sigma(\alpha)} \mapsto \alpha$.

Let $\mathcal{F}$ or $\mathcal{F}_\mathbb{C}$ be the group of all modular units in $\mathfrak{F}_I^{(M)}$ or $\mathbb{C}\mathfrak{F}_I^{(M)}$ respectively. Since $\mathcal{F}_\mathbb{C} = \mathbb{C}^\times \mathcal{F}$ ([**21**, Corollary 3.1]), the divisor group $\operatorname{div}(\mathcal{F})$ can be identified with the divisor group $\operatorname{div}(\mathcal{F}_\mathbb{C})$. We call the factor group

$$\mathcal{C} = \mathcal{D}_0 / \operatorname{div}(\mathcal{F}) \tag{2.9}$$

the *cuspidal divisor class group* of the curve X_I and the order of $\mathcal{C}$ the *cuspidal class number* of X_I or of $X_1(2p)$.

We denote by I_P the image $\varphi(\operatorname{div}(\mathcal{F}))$ of the principal divisors $\operatorname{div}(\mathcal{F})$. Then it is an additive subgroup of R_0, and moreover an ideal of R (cf. [**21**, Remark 5.1]).

Put $\mathcal{D}_\mathbb{Q} = \mathcal{D} \otimes \mathbb{Q}$ and $R_\mathbb{Q} = R \otimes \mathbb{Q}$. Then we have an isomorphism $\mathcal{D}_\mathbb{Q} \cong R_\mathbb{Q}$ the extension of φ, which we also denote by φ. In order to describe the group I_P, we define two elements θ_2 and θ_p of $R_\mathbb{Q}$ as follows (cf. [**21**, (2.42), Proposition 3.1]):

$$\theta_2 = \frac{1}{24}\Big\{ -\sum_{t(\alpha)=1} p \cdot \alpha^{-1} + \sum_{t(\alpha)=2} p \cdot \alpha^{-1} - \sum_{t(\alpha)=p} \alpha^{-1} + \sum_{t(\alpha)=2p} \alpha^{-1} \Big\}, \tag{2.10}$$

$$\theta_p = \sum_{t(\alpha)=1} pB_2\left(\left\langle \frac{a}{p}\right\rangle\right)\cdot\alpha^{-1} + \sum_{t(\alpha)=2}\frac{p}{2}B_2\left(\left\langle\frac{2a}{p}\right\rangle\right)\cdot\alpha^{-1}$$
$$+\frac{1}{6}\sum_{t(\alpha)=p}\alpha^{-1}+\frac{1}{12}\sum_{t(\alpha)=2p}\alpha^{-1}, \tag{2.11}$$

where in each summation the element α runs over the group $C_I(\pm)$ with the described type, and in (2.11) we assume that α is represented by a matrix $\left(\begin{smallmatrix} a & 0\\ 0 & a\end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} a\sqrt{2} & \sqrt{p}\\ \sqrt{p} & a\sqrt{2}\end{smallmatrix}\right)$ $(a\in\mathbb{Z})$ according as $t(\alpha)=1$ or 2 respectively.

Let α be any element of $C_I(\pm)$ of type r. Let $a(\alpha)$ and $b(\alpha)$ be integers such that α can be represented by the matrix

$$\begin{pmatrix} a(\alpha)\sqrt{r} & b(\alpha)\sqrt{r^*}\\ b(\alpha)\sqrt{r^*} & a(\alpha)\sqrt{r}\end{pmatrix}. \tag{2.12}$$

Although such integers $a(\alpha)$ and $b(\alpha)$ are not unique, the residue classes $a(\alpha)\pmod{r^*}$ and $b(\alpha)\pmod{r}$ are uniquely determined up to the multiplication by ±1. In particular, the element α determines the residue class $a(\alpha)^2\pmod{p}$ (respectively $b(\alpha)^2\pmod{p}$) uniquely when $r=1,2$ (respectively $r=p,\,2p$).

We have the following theorem (cf. [**21**, Theorem 5.1]). In the theorem we denote by $C_I^{(r)}(\pm)$ $(r\in T)$ the subset of $C_I(\pm)$ consisting of the elements of type r, and by $C_I^{(r,s)}(\pm)$ $(r,s\in T,\ r\neq s)$ the subset of $C_I(\pm)$ consisting of the elements of type r or s.

THEOREM 2.4. *Let $\varphi:\mathcal{D}\cong R$ be the isomorphism* (2.8). *Let* $\mathrm{div}(\mathcal{F})$ *be the group of the principal divisors of the modular units in $\mathfrak{F}_I$. Then the image $I_P=\varphi(\mathrm{div}(\mathcal{F}))$ coincides with the subgroup of $R_{\mathbb{Q}}$ consisting of all elements $2k\theta_2+\{\sum_{\alpha\in C_I(\pm)}m(\alpha)\alpha\}\theta_p$, where k and $m(\alpha)$ are integers such that the following congruences* (i)–(iv) *hold*:

(i) $k+\sum_{\alpha\in C_I(\pm)}t(\alpha)m(\alpha)\equiv 0\pmod{12}$,
(ii) $\sum_{\alpha\in C_I^{(1,2)}(\pm)}m(\alpha)+p\sum_{\alpha\in C_I^{(p,2p)}(\pm)}m(\alpha)\equiv 0\pmod{4}$,
(iii) $\sum_{\alpha\in C_I^{(1)}(\pm)}a(\alpha)^2m(\alpha)+2\sum_{\alpha\in C_I^{(2)}(\pm)}a(\alpha)^2m(\alpha)\equiv 0\pmod{p}$,
(iv) $\sum_{\alpha\in C_I^{(2p)}(\pm)}b(\alpha)^2m(\alpha)+2\sum_{\alpha\in C_I^{(p)}(\pm)}b(\alpha)^2m(\alpha)\equiv 0\pmod{p}$.

REMARK 2.5. Since $\varphi(\mathrm{div}(\mathcal{F}))$ is contained in R_0, this theorem implies that the elements of the form $2k\theta_2+\{\sum_{\alpha\in C_I(\pm)}m(\alpha)\alpha\}\theta_p$ satisfying the congruences (i)–(iv) are contained in R_0, in other words their coefficients are integers. In the statement of [**21**, Theorem 5.1] the group $R_{\mathbb{Q}}$ is replaced by R_0, but we can use $R_{\mathbb{Q}}$ by its proof.

2.5. The $\mathbb{Q}$-rational divisors on $X_1(2p)_{\mathbb{Q}}$.

Let $\mathcal{D}_g$ be the free abelian group generated by the cusps of the curve $X_{I,\mathbb{Q}}$, and let $\mathcal{D}_{g,0}$ be the subgroup of $\mathcal{D}_g$ consisting of all elements of degree 0. We call the elements of $\mathcal{D}_g$ the *cuspidal divisors* on $X_{I,\mathbb{Q}}$. We identify the cusps of the curve $X_{I,\mathbb{Q}}$ with the cuspidal prime divisors of $\mathfrak{F}_I^{(2p)}$, and denote by the same symbol φ the isomorphism of $\mathcal{D}_g$ to R which corresponds to the isomorphism (2.8):

$$\varphi : \mathcal{D}_g \cong R. \tag{2.13}$$

PROPOSITION 2.6. *Let d and σ_d be as in Proposition* 2.1 *with $M = 2p$. We denote by $\langle d\rangle$ the element of $C_I(\pm)$ represented by the matrix $\left(\begin{smallmatrix} d & 0 \\ 0 & d \end{smallmatrix}\right)$. Let P be a cusp of $X_{I,\mathbb{Q}}$ with $\varphi(P) = \alpha$ $(\in C_I(\pm))$. Let r be the type of α. Then $\varphi(P^{\sigma_d}) = \alpha$ or $\alpha\langle d\rangle$ according as $r = 1, 2$ or $p, 2p$ respectively.*

PROOF. The case $r = 1, 2$ follows from Theorem 2.3. Assume $r = p, 2p$. The cusp P corresponds to the cuspidal prime divisor $\mathcal{P}_\infty^{\sigma(\beta^{-1})}$ with $\beta = \alpha^{-1}$. Let β be represented by a matrix $\left(\begin{smallmatrix} a\sqrt{r} & b\sqrt{r^*} \\ b\sqrt{r^*} & a\sqrt{r} \end{smallmatrix}\right)$. Let d_1 be an integer with $dd_1 \equiv 1 \pmod{2p}$. Then, by Proposition 2.2, the cusp P^{σ_d} corresponds to $\mathcal{P}_\infty^{\sigma(\beta_1^{-1})}$, where β_1 is represented by the matrix $\left(\begin{smallmatrix} a\sqrt{r} & bd_1\sqrt{r^*} \\ bd_1\sqrt{r^*} & a\sqrt{r} \end{smallmatrix}\right)$. Since $r = p, 2p$ and $d_1 \equiv 1 \pmod 2$, we have $ad_1\sqrt{r} \equiv a\sqrt{r} \pmod I$. This implies $\beta_1 = \beta\langle d_1\rangle$, therefore $\varphi(P^{\sigma_d}) = \alpha\langle d\rangle$. □

Let d and σ_d be as in Proposition 2.6. Let $D = \sum_P m(P)P$ be an element of $\mathcal{D}_g$ with P the cusps of $X_{I,\mathbb{Q}}$ and $m(P) \in \mathbb{Z}$. The action of σ_d on D is defined by $D^{\sigma_d} = \sum_P m(P)P^{\sigma_d}$. We say that D is $\mathbb{Q}$-rational if $D^{\sigma_d} = D$ for any d.

Let $\xi = \sum_{\alpha\in C_I(\pm)} m(\alpha)\alpha$ be an element of R with $m(\alpha) \in \mathbb{Z}$. We define the action of σ_d on ξ by $\xi^{\sigma_d} = \sum_{\alpha\in C_I(\pm)} m(\alpha)\alpha^{\sigma_d}$, where

$$\alpha^{\sigma_d} = \begin{cases} \alpha & \text{if } t(\alpha) = 1, 2, \\ \alpha\langle d\rangle & \text{if } t(\alpha) = p, 2p. \end{cases} \tag{2.14}$$

COROLLARY 2.7. *Let D be an element of $\mathcal{D}_g$. Then D is $\mathbb{Q}$-rational if and only if $\varphi(D) \in \sum_{\alpha\in C_I^{(1,2)}(\pm)} \mathbb{Z}\alpha + \mathbb{Z}\sum_{\alpha\in C_I^{(p)}(\pm)} \alpha + \mathbb{Z}\sum_{\alpha\in C_I^{(2p)}(\pm)} \alpha$.*

PROOF. This follows immediately from Proposition 2.6. □

2.6. The cuspidal group of $J_1(2p)_\mathbb{Q}$ and its subgroups $\mathcal{C}_1$, $\mathcal{C}_2$ and $\mathcal{C}_\mathbb{Q}$.

Let $\mathcal{C} \cong R_0/I_P$ be the isomorphism induced by (2.8). We define three subgroups $\mathcal{C}_1$, $\mathcal{C}_2$ and $\mathcal{C}_\mathbb{Q}$ of $\mathcal{C}$ using this isomorphism as follows.

Put $R^{(1,2)} = \mathbb{Z}[C_I^{(1,2)}(\pm)]$ and $R_0^{(1,2)} = R^{(1,2)} \cap R_0$. The group $\mathcal{C}_1$ is the subgroup of $\mathcal{C}$ defined by

$$\mathcal{C}_1 \cong R_0^{(1,2)}/\big(I_P \cap R^{(1,2)}\big). \tag{2.15}$$

By Theorem 2.3 this is the subgroup generated by the $\mathbb{Q}$-rational cusps.

For $r = p, 2p$, put

$$\mu^{(r)} = \sum_{\alpha\in C_I^{(r)}(\pm)} \alpha. \tag{2.16}$$

Let $R_0^\mathbb{Q} = R^\mathbb{Q} \cap R_0$, where

$$R^{\mathbb{Q}} = R^{(1,2)} + \mathbb{Z}\mu^{(p)} + \mathbb{Z}\mu^{(2p)}. \tag{2.17}$$

Then the group $\mathcal{C}_2$ is the subgroup of $\mathcal{C}$ defined by

$$\mathcal{C}_2 \cong R_0^{\mathbb{Q}}/\big(I_P \cap R^{\mathbb{Q}}\big). \tag{2.18}$$

By Corollary 2.7 this is the subgroup generated by the $\mathbb{Q}$-rational cuspidal divisors.

Let d be an integer prime to $2p$ that generates the cyclic group $(\mathbb{Z}/2p\mathbb{Z})^\times/\{\pm 1\}$. Let $\sigma = \sigma_d$ be the automorphism of k_{2p} defined by (2.5). Let η be an element of R. We define the action of σ on the divisor class $\eta + I_P$ by

$$(\eta + I_P)^\sigma = \eta^\sigma + I_P, \tag{2.19}$$

which is well defined because $I_P^\sigma = I_P$. We say that a divisor class $\eta + I_P$ is $\mathbb{Q}$-rational if and only if $\eta^\sigma + I_P = \eta + I_P$. It is equivalent to that $\eta^\sigma - \eta$ belongs to I_P. Let R^* be the subgroup of R consisting of the elements η such that $\eta^\sigma - \eta \in I_P$, and put $R_0^* = R^* \cap R_0$. It is obvious that $I_P \subset R_0^*$. Then the group $\mathcal{C}_{\mathbb{Q}}$ is the subgroup of $\mathcal{C}$ defined by

$$\mathcal{C}_{\mathbb{Q}} \cong R_0^*/I_P. \tag{2.20}$$

This is the subgroup generated by the $\mathbb{Q}$-rational divisor classes. Since $R^{\mathbb{Q}} \subset R^*$ by (2.14), we have

$$\mathcal{C}_1 \subset \mathcal{C}_2 \subset \mathcal{C}_{\mathbb{Q}}. \tag{2.21}$$

Let g be the genus of $X_1(2p)$. Then we have $g = (1/8)\{(p-4)^2 - 1\}$, hence $g = 0$ or > 0 according as $p = 5$ or $p \geq 7$ respectively. Let $p \geq 7$. Let $J_1(2p)_{\mathbb{Q}}$ (respectively $J_{I,\mathbb{Q}}$) be the Jacobian of $X_1(2p)_{\mathbb{Q}}$ (respectively $X_{I,\mathbb{Q}}$) defined over $\mathbb{Q}$. Then the Jacobians $J_1(2p)_{\mathbb{Q}}$ and $J_{I,\mathbb{Q}}$ are isomorphic over $\mathbb{Q}$.

Let P_∞ be the cusp on $X_1(2p)_{\mathbb{Q}}$ (respectively $X_{I,\mathbb{Q}}$) represented by the infinity. By Theorem 2.3, the cusp P_∞ is $\mathbb{Q}$-rational. Let $i_\infty : P \mapsto [P - P_\infty]$ be the cuspidal embedding of $X_1(2p)_{\mathbb{Q}}$ (respectively $X_{I,\mathbb{Q}}$) into $J_1(2p)_{\mathbb{Q}}$ (respectively $J_{I,\mathbb{Q}}$) sending a point P to the divisor class of $P - P_\infty$. Let D be a divisor supported on cusps. Then $i_\infty(D)$ is a torsion point on $J_1(2p)_{\mathbb{Q}}$ (respectively $J_{I,\mathbb{Q}}$).

The cuspidal embedding i_∞ induces an isomorphism of the cuspidal divisor class group $\mathcal{C}$ onto the subgroup of the torsion group of $J_1(2p)_{\mathbb{Q}}$ (respectively $J_{I,\mathbb{Q}}$) generated by the images of the cusps of $X_1(2p)_{\mathbb{Q}}$ (respectively $X_{I,\mathbb{Q}}$), which we call the *cuspidal group* of $J_1(2p)_{\mathbb{Q}}$ (respectively $J_{I,\mathbb{Q}}$) and denote by $i_\infty(\mathcal{C})$. The cuspidal groups of $J_1(2p)_{\mathbb{Q}}$ and $J_{I,\mathbb{Q}}$ are isomorphic. Let D be a divisor supported on cusps. Then $i_\infty(D)$ is $\mathbb{Q}$-rational if and only if the divisor class of D is $\mathbb{Q}$-rational.

The images of the three subgroups $\mathcal{C}_1$, $\mathcal{C}_2$ and $\mathcal{C}_{\mathbb{Q}}$ are the following.

(1) The group $i_\infty(\mathcal{C}_1)$ is the subgroup of $i_\infty(\mathcal{C})$ generated by the images of the $\mathbb{Q}$-rational cusps.
(2) The group $i_\infty(\mathcal{C}_2)$ is the subgroup of $i_\infty(\mathcal{C})$ generated by the images of the $\mathbb{Q}$-rational

cuspidal divisors.

(3) The group $i_\infty(\mathcal{C}_\mathbb{Q})$ is the subgroup of $i_\infty(\mathcal{C})$ generated by the $\mathbb{Q}$-rational points of $i_\infty(\mathcal{C})$, which we call the $\mathbb{Q}$-*rational cuspidal group*.

For simplicity we omit the notation i_∞, and consider the groups $\mathcal{C}$, $\mathcal{C}_1$, $\mathcal{C}_2$ and $\mathcal{C}_\mathbb{Q}$ as the subgroups of the Jacobian $J_{I,\mathbb{Q}}$ (or $J_1(2p)_\mathbb{Q}$) if $p \geq 7$.

In the following two sections, we prove $\mathcal{C}_1 = \mathcal{C}_2 = \mathcal{C}_\mathbb{Q}$.

3. The proof of $\mathcal{C}_1 = \mathcal{C}_2$.

Let p be a prime $\neq 2, 3$. In this section we prove $\mathcal{C}_1 = \mathcal{C}_2$.

3.1. The group $I_P \cap R^\mathbb{Q}$ of the $\mathbb{Q}$-rational principal divisors.

Put $R_\mathbb{C} = R \otimes \mathbb{C}$. For any element $\xi = \sum_{\alpha \in C_I(\pm)} m(\alpha)\alpha \in R_\mathbb{C}$ $(m(\alpha) \in \mathbb{C})$ we denote by $\xi^{(r)}$ $(r \in T)$ the element of $R_\mathbb{C}$ defined by

$$\xi^{(r)} = \sum_{\alpha \in C_I^{(r)}(\pm)} m(\alpha)\alpha, \tag{3.1}$$

and by $\xi^{(r,s)}$ $(r \neq s \in T)$ the element $\xi^{(r)} + \xi^{(s)}$. We denote by μ the element of R defined by

$$\mu = \sum_{\alpha \in C_I(\pm)} \alpha. \tag{3.2}$$

Then the notation $\mu^{(r)}$ in (2.16) coincides with that defined by (3.1). Let us recall the definitions of $\mathcal{C}_1$ and $\mathcal{C}_2$ ((2.15), (2.18)):

$$\mathcal{C}_1 \cong R_0^{(1,2)}/\big(I_P \cap R^{(1,2)}\big), \tag{3.3}$$

$$\mathcal{C}_2 \cong R_0^\mathbb{Q}/\big(I_P \cap R^\mathbb{Q}\big). \tag{3.4}$$

In this subsection we study the group $I_P \cap R^\mathbb{Q}$ which is the $\mathbb{Q}$-rational principal divisors supported on the cusps.

For any $r \in T$, we denote by $[r]$ the element of $C_I^{(r)}(\pm)$ represented by the matrix $\begin{pmatrix} \sqrt{r} & \sqrt{r^*} \\ \sqrt{r^*} & \sqrt{r} \end{pmatrix}$ (cf. [**21**, (2.45)]). Let ψ be any character of the group $C_I^{(1)}(\pm)$. We put

$$e_\psi^{\langle 1 \rangle} = \frac{1}{\big|C_I^{(1)}(\pm)\big|} \sum_{\alpha \in C_I^{(1)}(\pm)} \psi(\alpha)\alpha^{-1}. \tag{3.5}$$

For an element $\xi = \sum_{\alpha \in C_I(\pm)} m(\alpha)\alpha$ of $R_\mathbb{C}$, we denote by $\xi_\psi^{(r)}$ the number defined by

$$\xi_\psi^{(r)} = \sum_{\alpha \in C_I^{(1)}(\pm)} m(\alpha[r])\psi(\alpha). \tag{3.6}$$

Since $\xi^{(r)} = \{\sum_{\alpha\in C_I^{(1)}(\pm)} m(\alpha[r])\alpha\}[r]$, we have

$$\xi^{(r)} = \left\{\sum_{\psi} \xi_\psi^{(r)} e_\psi^{\langle 1\rangle}\right\}[r], \tag{3.7}$$

where ψ runs over all characters of the group $C_I^{(1)}(\pm)$.

Let us denote by the same symbol ψ the character of $(\mathbb{Z}/p\mathbb{Z})^\times$ induced by the character ψ of the group $C_I^{(1)}(\pm)$ (cf. [**21**, (5.8)]). We denote by $B(\psi)$ the number defined by

$$B(\psi) = p\sum_{a=1}^{p-1} \psi(a) B_2\left(\frac{a}{p}\right). \tag{3.8}$$

If ψ is non-trivial, then $B(\psi)$ coincides with the usual generalized Bernoulli number $B_{2,\psi}$.

By (3.7) and the definition (2.11) of θ_p, we have

$$\theta_p = \sum_{\psi}\left(\frac{1}{2}B(\bar\psi)\right)e_\psi^{\langle 1\rangle} + \sum_{\psi}\left(\frac{1}{4}B(\bar\psi)\right)e_\psi^{\langle 1\rangle}[2] + \frac{p-1}{12}e_1^{\langle 1\rangle}[p] + \frac{p-1}{24}e_1^{\langle 1\rangle}[2p], \tag{3.9}$$

where $\bar\psi$ denotes the complex conjugate of ψ.

Put $R_{\mathbb{C}}^{\mathbb{Q}} = R^{\mathbb{Q}} \otimes \mathbb{C}$. Then

$$R_{\mathbb{C}}^{\mathbb{Q}} = \mathbb{C}\big[C_I^{(1,2)}(\pm)\big] + \mathbb{C}\mu^{(p)} + \mathbb{C}\mu^{(2p)}. \tag{3.10}$$

LEMMA 3.1. *Let $\xi \in R_{\mathbb{C}}$ with $\xi\theta_p \in R_{\mathbb{C}}^{\mathbb{Q}}$. Then, for any character $\psi \neq 1$ of $C_I^{(1)}(\pm)$, we have $\xi_\psi^{(p)} = \xi_\psi^{(2p)} = 0$.*

PROOF. We have

$$(\xi\theta_p)^{(2p)} = \xi^{(1)}\theta_p^{(2p)} + \xi^{(2)}\theta_p^{(p)} + \xi^{(p)}\theta_p^{(2)} + \xi^{(2p)}\theta_p^{(1)}.$$

Since $[2][p] = \langle p+2\rangle[2p]$ and $\langle p+2\rangle e_\psi^{\langle 1\rangle} = \psi(2)e_\psi^{\langle 1\rangle}$, we have

$$\begin{aligned}\xi^{(p)}\theta_p^{(2)} &= \left\{\sum_{\psi}\xi_\psi^{(p)}e_\psi^{\langle 1\rangle}\right\}[p]\cdot\left\{\sum_{\psi}\left(\frac{1}{4}B(\bar\psi)\right)e_\psi^{\langle 1\rangle}\right\}[2]\\ &= \left\{\sum_{\psi}\left(\psi(2)\xi_\psi^{(p)}\cdot\frac{1}{4}B(\bar\psi)\right)e_\psi^{\langle 1\rangle}\right\}[2p].\end{aligned}$$

Also we have

$$\xi^{(2p)}\theta_p^{(1)} = \Big\{\sum_{\psi}\xi_{\psi}^{(2p)}e_{\psi}^{\langle 1\rangle}\Big\}[2p]\cdot\Big\{\sum_{\psi}\Big(\frac{1}{2}B(\bar{\psi})\Big)e_{\psi}^{\langle 1\rangle}\Big\}$$
$$= \Big\{\sum_{\psi}\Big(\xi_{\psi}^{(2p)}\cdot\frac{1}{2}B(\bar{\psi})\Big)e_{\psi}^{\langle 1\rangle}\Big\}[2p],$$

hence

$$\xi^{(p)}\theta_p^{(2)} + \xi^{(2p)}\theta_p^{(1)} = \Big\{\sum_{\psi}\Big(\big(\psi(2)\xi_{\psi}^{(p)} + 2\xi_{\psi}^{(2p)}\big)\cdot\frac{1}{4}B(\bar{\psi})\Big)e_{\psi}^{\langle 1\rangle}\Big\}[2p]. \tag{3.11}$$

Since $\xi\theta_p \in R_{\mathbb{C}}^{\mathbb{Q}}$, we have $(\xi\theta_p)^{(2p)} \in \mathbb{C}\mu^{(2p)}$. By (3.9) we have $\xi^{(1)}\theta_p^{(2p)} + \xi^{(2)}\theta_p^{(p)} \in \mathbb{C}\mu^{(2p)}$. Hence we have $\xi^{(p)}\theta_p^{(2)} + \xi^{(2p)}\theta_p^{(1)} \in \mathbb{C}\mu^{(2p)}$, which implies that the coefficients of $e_{\psi}^{\langle 1\rangle}$ with $\psi \neq 1$ in (3.11) are 0. Since $B(\bar{\psi}) = B_{2,\bar{\psi}} \neq 0$ for any $\psi \neq 1$, we have

$$\psi(2)\xi_{\psi}^{(p)} + 2\xi_{\psi}^{(2p)} = 0. \tag{3.12}$$

We have

$$(\xi\theta_p)^{(p)} = \xi^{(1)}\theta_p^{(p)} + \xi^{(2)}\theta_p^{(2p)} + \xi^{(p)}\theta_p^{(1)} + \xi^{(2p)}\theta_p^{(2)}.$$

In the exactly same manner, considering this equation, we have

$$2\xi_{\psi}^{(p)} + \xi_{\psi}^{(2p)} = 0. \tag{3.13}$$

By (3.12) and (3.13) we have $\xi_{\psi}^{(p)} = \xi_{\psi}^{(2p)} = 0$. □

Lemma 3.2. *Let $\xi \in R$ with $\xi\theta_p \in R_{\mathbb{C}}^{\mathbb{Q}}$. Then there exists an element $\eta \in R^{(1,2)}$ such that $\xi\theta_p = \eta\theta_p$ and $\xi - \eta \in \mathbb{Z}(\mu^{(1)} + \mu^{(p)}) + \mathbb{Z}(\mu^{(2)} + \mu^{(2p)})$.*

Proof. By Lemma 3.1 we have $\xi_{\psi}^{(p)} = \xi_{\psi}^{(2p)} = 0$ for all $\psi \neq 1$. This implies that, by (3.7), $\xi^{(p)} = \xi_1^{(p)}e_1^{\langle 1\rangle}[p] \in \mathbb{C}\mu^{(p)}$ and $\xi^{(2p)} = \xi_1^{(2p)}e_1^{\langle 1\rangle}[2p] \in \mathbb{C}\mu^{(2p)}$. Since $\xi \in R$, we have $\xi^{(p)} = m\mu^{(p)}$ and $\xi^{(2p)} = n\mu^{(2p)}$ with $m, n \in \mathbb{Z}$. By [**21**, Proposition 3.2], we have $(\mu^{(1)} + \mu^{(p)})\theta_p = 0$ and $(\mu^{(2)} + \mu^{(2p)})\theta_p = 0$, whence $\mu^{(p)}\theta_p = -\mu^{(1)}\theta_p$ and $\mu^{(2p)}\theta_p = -\mu^{(2)}\theta_p$. Therefore, we have

$$\xi\theta_p = \big(\xi^{(1)} + \xi^{(2)} + m\mu^{(p)} + n\mu^{(2p)}\big)\theta_p$$
$$= \big\{\big(\xi^{(1)} - m\mu^{(1)}\big) + \big(\xi^{(2)} - n\mu^{(2)}\big)\big\}\theta_p.$$

Put $\eta = (\xi^{(1)} - m\mu^{(1)}) + (\xi^{(2)} - n\mu^{(2)})$. Then we have $\eta \in R^{(1,2)}$, $\xi\theta_p = \eta\theta_p$ and $\xi - \eta \in \mathbb{Z}(\mu^{(1)} + \mu^{(p)}) + \mathbb{Z}(\mu^{(2)} + \mu^{(2p)})$, which completes the proof. □

Let I_{12} be the subgroup of R consisting of all elements $\sum_{\alpha\in C_I(\pm)} m(\alpha)\alpha$ of R with

$m(\alpha) \in \mathbb{Z}$ such that the integers $m(\alpha)$ satisfy the following condition (i*) and the conditions (ii)–(iv) of Theorem 2.4 (cf. [**21**, (5.5)]):

$$\text{(i*)} \qquad \sum_{\alpha \in C_I(\pm)} t(\alpha) m(\alpha) \equiv 0 \pmod{12}. \tag{3.14}$$

LEMMA 3.3. *The elements $\mu^{(1)} + \mu^{(p)}$ and $\mu^{(2)} + \mu^{(2p)}$ belong to I_{12}.*

PROOF. This can be verified directly. □

The following theorem describes the $\mathbb{Q}$-rational principal divisors supported on the cusps.

THEOREM 3.4. *The group $I_P \cap R^{\mathbb{Q}}$ consists of all elements of the form $2k\theta_2 + \xi\theta_p \in R_{\mathbb{C}}$ where $k \in \mathbb{Z}$ and $\xi = \sum_{\alpha \in C_I^{(1,2)}(\pm)} m(\alpha)\alpha \in R^{(1,2)}$ with $m(\alpha) \in \mathbb{Z}$ such that the following congruences* (i)–(iii) *hold*:

(i) $k + \sum_{\alpha \in C_I^{(1)}(\pm)} m(\alpha) + 2 \sum_{\alpha \in C_I^{(2)}(\pm)} m(\alpha) \equiv 0 \pmod{12}$,
(ii) $\sum_{\alpha \in C_I^{(1,2)}(\pm)} m(\alpha) \equiv 0 \pmod{4}$,
(iii) $\sum_{\alpha \in C_I^{(1)}(\pm)} a(\alpha)^2 m(\alpha) + 2 \sum_{\alpha \in C_I^{(2)}(\pm)} a(\alpha)^2 m(\alpha) \equiv 0 \pmod{p}$.

PROOF. Let $\eta = 2k\theta_2 + \xi'\theta_p$ be any element of $I_P \cap R^{\mathbb{Q}}$, where $\xi' = \sum_{\alpha \in C_I(\pm)} m'(\alpha)\alpha \in R$, and k and $m'(\alpha)$ are integers satisfying the conditions (i)–(iv) of Theorem 2.4. Since $2k\theta_2 \in R_{\mathbb{C}}^{\mathbb{Q}}$, we have $\xi'\theta_p \in R_{\mathbb{C}}^{\mathbb{Q}}$. By Lemma 3.2, there exists an element $\xi \in R^{(1,2)}$ such that $\xi'\theta_p = \xi\theta_p$ and $\xi' - \xi \in \mathbb{Z}(\mu^{(1)} + \mu^{(p)}) + \mathbb{Z}(\mu^{(2)} + \mu^{(2p)})$. Write $\xi = \sum_{\alpha \in C_I^{(1,2)}(\pm)} m(\alpha)\alpha$ with $m(\alpha) \in \mathbb{Z}$. By Lemma 3.3, the integers k and $m(\alpha)$ also satisfy the conditions (i)–(iv) of Theorem 2.4. This proves that any element of $I_P \cap R^{\mathbb{Q}}$ can be written in the form stated above.

Conversely, let $\eta = 2k\theta_2 + \xi\theta_p$ be any element of $R_{\mathbb{C}}$ with $k \in \mathbb{Z}$, $\xi = \sum_{\alpha \in C_I^{(1,2)}(\pm)} m(\alpha)\alpha \in R^{(1,2)}$ and $m(\alpha) \in \mathbb{Z}$ such that k and $m(\alpha)$ satisfy the conditions (i)–(iii) stated above. By Theorem 2.4, we have $\eta \in I_P$. Since $\xi^{(p)} = \xi^{(2p)} = 0$, we have

$$(\xi\theta_p)^{(p)} = \xi^{(1)}\theta_p^{(p)} + \xi^{(2)}\theta_p^{(2p)} \in \mathbb{C}\mu^{(p)},$$
$$(\xi\theta_p)^{(2p)} = \xi^{(1)}\theta_p^{(2p)} + \xi^{(2)}\theta_p^{(p)} \in \mathbb{C}\mu^{(2p)}.$$

Combining these with $2k\theta_2 \in R_{\mathbb{C}}^{\mathbb{Q}}$, we have $\eta^{(p)} \in \mathbb{C}\mu^{(p)}$ and $\eta^{(2p)} \in \mathbb{C}\mu^{(2p)}$. Therefore we have $\eta \in R_{\mathbb{C}}^{\mathbb{Q}}$. Since $\eta \in I_P \subset R$, we have $\eta \in R^{\mathbb{Q}}$. This proves $\eta \in I_P \cap R^{\mathbb{Q}}$. Thus the proof is completed. □

Let $\eta = 2k\theta_2 + \xi\theta_p$ be an element of $I_P \cap R^{\mathbb{Q}}$ with $k \in \mathbb{Z}$ and $\xi \in R^{(1,2)}$. Then k and ξ are uniquely determined by η. More generally we have the following.

PROPOSITION 3.5. *Let $\eta = 2k\theta_2 + \xi\theta_p$ be an element of $R_{\mathbb{C}}$ such that $k \in \mathbb{Z}$ and $\xi \in R^{(1,2)}$. Then k and ξ are uniquely determined by η.*

PROOF. It is proved in [**21**, Proof of Proposition 5.3] that k is determined uniquely by η. Let $\xi_1\theta_p = \xi_2\theta_p$ with $\xi_i \in R^{(1,2)}$ $(i = 1, 2)$. Then $(\xi_1 - \xi_2)\theta_p = 0$. By [**21**, Corollary 5.1] the e_χ-components of θ_p are non-zero for all $\chi \neq \chi_{(0)}, \chi_{(2)}$. This implies that $\xi_1 - \xi_2 \in \mathbb{C}e_{\chi_{(0)}} + \mathbb{C}e_{\chi_{(2)}}$. Since $\xi_1 - \xi_2 \in R$, by [**21**, Lemma 5.1], we have $\xi_1 - \xi_2 = m(\mu^{(1)} + \mu^{(p)}) + n(\mu^{(2)} + \mu^{(2p)})$ with $m, n \in \mathbb{Z}$. Since $\xi_1 - \xi_2 \in R^{(1,2)}$, we have $m = n = 0$. Therefore, $\xi_1 = \xi_2$. This completes the proof. □

3.2. Proof of $\mathcal{C}_1 = \mathcal{C}_2$.

First we prove that there exist special elements η_1 and η_2 of $I_P \cap R^{\mathbb{Q}}$ satisfying (i) $\eta_1^{(p)} = \mu^{(p)}$, $\eta_1^{(2p)} = 0$ and (ii) $\eta_2^{(p)} = 0$, $\eta_2^{(2p)} = \mu^{(2p)}$. Let $\eta = 2k\theta_2 + \xi\theta_p$ be an element of $I_P \cap R^{\mathbb{Q}}$, where $k = k(\eta) \in \mathbb{Z}$ and $\xi = \xi(\eta) = \sum_{\alpha \in C_I^{(1,2)}(\pm)} m(\alpha)\alpha \in R^{(1,2)}$ with $m(\alpha) \in \mathbb{Z}$ such that the conditions (i)–(iii) of Theorem 3.4 hold. Then we have

$$\eta^{(p)} = 2k\theta_2^{(p)} + \xi^{(1)}\theta_p^{(p)} + \xi^{(2)}\theta_p^{(2p)} = A(\eta)\mu^{(p)}, \tag{3.15}$$

$$\eta^{(2p)} = 2k\theta_2^{(2p)} + \xi^{(1)}\theta_p^{(2p)} + \xi^{(2)}\theta_p^{(p)} = B(\eta)\mu^{(2p)}, \tag{3.16}$$

where

$$A(\eta) = -\frac{k}{12} + \frac{1}{6}\deg\xi^{(1)} + \frac{1}{12}\deg\xi^{(2)}, \tag{3.17}$$

$$B(\eta) = \frac{k}{12} + \frac{1}{12}\deg\xi^{(1)} + \frac{1}{6}\deg\xi^{(2)}. \tag{3.18}$$

By the Lagrange's four-square theorem, the prime p can be expressed as a sum of at most four integer squares:

$$p = a_1^2 + \cdots + a_l^2,\ 2 \le l \le 4,\ a_i \in \mathbb{N}\ (1 \le i \le l). \tag{3.19}$$

PROPOSITION 3.6. *There exists an element $\eta_1 \in I_P \cap R^{\mathbb{Q}}$ such that $A(\eta_1) = 1$ and $B(\eta_1) = 0$, and also an element $\eta_2 \in I_P \cap R^{\mathbb{Q}}$ such that $A(\eta_2) = 0$ and $B(\eta_2) = 1$.*

PROOF. Let l and a_i be as in (3.19). First, assume that $l = 2$ or 4. Let α_i $(1 \le i \le l)$ be the element of $C_I^{(1)}(\pm)$ represented by the matrix $\left(\begin{smallmatrix} a_i & 0 \\ 0 & a_i \end{smallmatrix}\right)$. Put $\eta_1 = -8\theta_2 + \xi_1\theta_p$ where $k(\eta_1) = -4$ and $\xi(\eta_1) = \xi_1 = (4/l)(\alpha_1 + \cdots + \alpha_l)$ $(\in R^{(1,2)})$. It is easy to see that this element η_1 satisfies the conditions (i)–(iii) of Theorem 3.4, and $A(\eta_1) = 1$, $B(\eta_1) = 0$. Put $\eta_2 = \eta_1[2]$. Since $\theta_2[2] = -\theta_2$, we have $\eta_2 = 8\theta_2 + \xi_2\theta_p$ where $k(\eta_2) = 4$ and $\xi(\eta_2) = \xi_2 = \xi_1[2]$ $(\in R^{(1,2)})$. It is easy to see that this element η_2 satisfies the conditions (i)–(iii) of Theorem 3.4, and $A(\eta_2) = 0$, $B(\eta_2) = 1$. This proves the case $l = 2$ or 4.

Next, assume that $l = 3$. Let a_i be as in (3.19). Since $a_1^2 + a_2^2 + a_3^2 \equiv 0 \pmod p$ and $a_i \not\equiv 0 \pmod p$ for all i, there exist integers x and y such that $1 + x^2 + y^2 \equiv 0 \pmod p$, $x \not\equiv 0 \pmod p$ and $y \not\equiv 0 \pmod p$. Let α_0 be the element of $C_I^{(1)}(\pm)$ represented by the matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Let α_1 and α_2 be the elements of $C_I^{(2)}(\pm)$ represented by the matrices $\left(\begin{smallmatrix} x\sqrt{2} & \sqrt{p} \\ \sqrt{p} & x\sqrt{2} \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} y\sqrt{2} & \sqrt{p} \\ \sqrt{p} & y\sqrt{2} \end{smallmatrix}\right)$ respectively. Put $\eta_1 = -12\theta_2 + \xi_1\theta_p$ where $k(\eta_1) = -6$ and

$\xi(\eta_1) = \xi_1 = 2\alpha_0 + \alpha_1 + \alpha_2$ $(\in R^{(1,2)})$. Then it is easy to see that this element η_1 satisfies the conditions (i)–(iii) of Theorem 3.4, and $A(\eta_1) = 1$, $B(\eta_1) = 0$. Put $\eta_2 = \eta_1[2]$. We have $\eta_2 = 12\theta_2 + \xi_2\theta_p$ where $k(\eta_2) = 6$ and $\xi(\eta_2) = \xi_2 = \xi_1[2]$ $(\in R^{(1,2)})$. It is easy to see that this element η_2 satisfies the conditions (i)–(iii) of Theorem 3.4, and $A(\eta_2) = 0$, $B(\eta_2) = 1$. This proves the case $l = 3$. □

Now we have the following

THEOREM 3.7. $\mathcal{C}_1 = \mathcal{C}_2$.

PROOF. By the isomorphisms (3.3) and (3.4) it is sufficient to prove that the homomorphism $\phi : R_0^{(1,2)}/(I_P \cap R^{(1,2)}) \to R_0^{\mathbb{Q}}/(I_P \cap R^{\mathbb{Q}})$ induced by the inclusion map $R_0^{(1,2)} \to R_0^{\mathbb{Q}}$ is an isomorphism. Since ϕ is injective, it is sufficient to show that ϕ is surjective. Let ξ be any element of $R_0^{\mathbb{Q}}$. Then $\xi^{(p,2p)} \in \mathbb{Z}\mu^{(p)} + \mathbb{Z}\mu^{(2p)}$. By Proposition 3.6, there exists an element $\eta \in I_P \cap R^{\mathbb{Q}}$ such that $\xi^{(p,2p)} = \eta^{(p,2p)}$. Put $\xi_1 = \xi - \eta$. Then $\xi_1 \in R_0^{(1,2)}$ and $\xi + I_P \cap R^{\mathbb{Q}} = \phi(\xi_1 + I_P \cap R^{(1,2)})$. This proves the theorem. □

4. The proof of $\mathcal{C}_2 = \mathcal{C}_{\mathbb{Q}}$.

Let p be a prime $\neq 2, 3$. In this section we prove $\mathcal{C}_2 = \mathcal{C}_{\mathbb{Q}}$.

Let d be an integer such that $(d, 2p) = 1$ and it generates the cyclic group $(\mathbb{Z}/2p\mathbb{Z})^\times/\{\pm 1\}$. In this section we fix such an integer d. Let $\sigma = \sigma_d$ be the automorphism of k_{2p} defined by (2.5).

4.1. The group I_P^N.

Let R^* and R_0^* be the subgroups of R defined in subsection 2.6, i.e., R^* is the group consisting of the elements η such that $\eta^\sigma - \eta \in I_P$, and $R_0^* = R^* \cap R_0$. By (2.20) we have

$$\mathcal{C}_{\mathbb{Q}} \cong R_0^*/I_P. \tag{4.1}$$

LEMMA 4.1. *Let ξ be an element of R. Then $\xi = \eta^\sigma - \eta$ with some $\eta \in R$ if and only if $\xi \in R^{(p,2p)}$ and $\deg \xi^{(p)} = \deg \xi^{(2p)} = 0$.*

PROOF. Assume that $\xi = \eta^\sigma - \eta$ with $\eta \in R$. Then by (2.14) we have $\xi = \eta^{(p,2p)}(\langle d\rangle - 1) \in R^{(p,2p)}$, $\xi^{(p)} = \eta^{(p)}(\langle d\rangle - 1)$ and $\xi^{(2p)} = \eta^{(2p)}(\langle d\rangle - 1)$, which implies that $\deg \xi^{(p)} = \deg \xi^{(2p)} = 0$. This proves the only if part. Conversely, assume that $\xi \in R^{(p,2p)}$ and $\deg \xi^{(p)} = \deg \xi^{(2p)} = 0$. Since $\langle d\rangle$ generate $C_I^{(1)}(\pm)$, we can write $\xi = \sum_{i=0}^{l-1} m_i \langle d\rangle^i[p] + \sum_{i=0}^{l-1} n_i \langle d\rangle^i[2p]$ with $l = (p-1)/2$ and $m_i, n_i \in \mathbb{Z}$. Since $\deg \xi^{(p)} = \deg \xi^{(2p)} = 0$, we have

$$\xi = \sum_{i=1}^{l-1} m_i(\langle d\rangle^i - 1)[p] + \sum_{i=1}^{l-1} n_i(\langle d\rangle^i - 1)[2p] = \eta(\langle d\rangle - 1),$$

where

$$\eta = \sum_{i=1}^{l-1} m_i(\langle d\rangle^{i-1} + \cdots + 1)[p] + \sum_{i=1}^{l-1} n_i(\langle d\rangle^{i-1} + \cdots + 1)[2p] \in R^{(p,2p)}.$$

This implies that $\xi = \eta^\sigma - \eta$, which proves the if part, and the proof is completed. □

Put

$$I_P^N = \{\xi \in I_P \mid \xi = \eta^\sigma - \eta \text{ with some } \eta \in R\}. \tag{4.2}$$

By Lemma 4.1, that $\xi \in I_P^N$ is equivalent to that $\xi \in I_P \cap R^{(p,2p)}$ with $\deg \xi^{(p)} = \deg \xi^{(2p)} = 0$. Write $\xi = \xi_0[p]$ with an element ξ_0. Then, the property of ξ is equivalent to that $\xi_0 \in I_P \cap R^{(1,2)}$ with $\deg \xi_0^{(1)} = \deg \xi_0^{(2)} = 0$ because I_P is an ideal of R (cf. [**21**, Remark 5.1]). Hence we have

$$I_P^N = \left\{\xi \in I_P \cap R^{(1,2)} \mid \deg \xi^{(1)} = \deg \xi^{(2)} = 0\right\}[p]. \tag{4.3}$$

4.2. The study of $I_P \cap R^{(1,2)}$.

Taking account of (4.3) we study here the group $I_P \cap R^{(1,2)}$, which is the group of the principal divisors supported on the $\mathbb{Q}$-rational cusps.

LEMMA 4.2. *Let $\eta = 2k\theta_2 + \xi\theta_p$ be an element of $I_P \cap R^{\mathbb{Q}}$ with $k \in \mathbb{Z}$ and $\xi \in R^{(1,2)}$ satisfying the conditions* (i)–(iii) *of Theorem* 3.4. *Then we have $\eta \in R^{(1,2)}$ if and only if $\deg \xi^{(1)} = -\deg \xi^{(2)} = k$.*

PROOF. By (3.15) and (3.16), we have $\eta \in R^{(1,2)}$ if and only if $A(\eta) = B(\eta) = 0$, which is equivalent to $\deg \xi^{(1)} = -\deg \xi^{(2)} = k$. □

Let θ be the element of $R_{\mathbb{Q}}$ defined by

$$\theta = \theta_2^{(1,2)} + \theta_p^{(1,2)}. \tag{4.4}$$

The following theorem describes the group of the principal divisors supported on the $\mathbb{Q}$-rational cusps.

THEOREM 4.3. *The group $I_P \cap R^{(1,2)}$ consists of all elements of the form $\xi\theta \in R_{\mathbb{C}}$ where $\xi = \sum_\alpha m(\alpha)\alpha \in R^{(1,2)}$ $(m(\alpha) \in \mathbb{Z})$ such that $\deg(\xi) = 0$ and the integers $m(\alpha)$ satisfy the congruence*

$$\sum_{\alpha \in C_I^{(1)}(\pm)} a(\alpha)^2 m(\alpha) + 2 \sum_{\alpha \in C_I^{(2)}(\pm)} a(\alpha)^2 m(\alpha) \equiv 0 \pmod{p}.$$

PROOF. Let $\eta = 2k\theta_2 + \xi\theta_p$ be an element of $I_P \cap R^{(1,2)}$ with $k \in \mathbb{Z}$ and $\xi \in R^{(1,2)}$ satisfying the conditions (i)–(iii) of Theorem 3.4. We have $\eta = \eta^{(1,2)} = 2k\theta_2^{(1,2)} + \xi\theta_p^{(1,2)}$. By (2.10), we have $\theta_2^{(1,2)} = \theta_2^{(1)} - \theta_2^{(1)}[2] = \theta_2^{(1)}(1 - [2])$. By Lemma 4.2, we have $\xi^{(1)}\theta_2^{(1)} = (\deg \xi^{(1)})\theta_2^{(1)} = k\theta_2^{(1)}$ and $\xi^{(2)}\theta_2^{(1)} = (\deg \xi^{(2)})\theta_2^{(1)}[2] = -k\theta_2^{(1)}[2]$. Hence we

have

$$\begin{aligned}\xi\theta_2^{(1,2)} &= \xi\theta_2^{(1)}(1-[2]) = \bigl(\xi^{(1)}\theta_2^{(1)} + \xi^{(2)}\theta_2^{(1)}\bigr)(1-[2])\\ &= k\theta_2^{(1)}(1-[2])^2 = 2k\theta_2^{(1)}(1-[2]) = 2k\theta_2^{(1,2)}.\end{aligned}$$

Here we used the equality $\theta_2^{(1)}[2]^2 = \theta_2^{(1)}$. Thus we have $\eta = 2k\theta_2^{(1,2)} + \xi\theta_p^{(1,2)} = \xi\theta_2^{(1,2)} + \xi\theta_p^{(1,2)} = \xi\theta$. Since $\deg\xi = \deg\xi^{(1)} + \deg\xi^{(2)} = k - k = 0$, the element η has the desired form.

Conversely, let $\eta = \xi\theta$, where $\xi = \sum_\alpha m(\alpha)\alpha \in R^{(1,2)}$ with $\deg(\xi) = 0$ and the integers $m(\alpha)$ satisfy the given congruence. Put $k = \deg\xi^{(1)}$ ($\in \mathbb{Z}$). It is easy to see that the integers k and $m(\alpha)$ satisfy the congruences (i)–(iii) of Theorem 3.4. Therefore, the element $\eta_1 = 2k\theta_2 + \xi\theta_p$ belongs to $I_P \cap R^{\mathbb{Q}}$ by Theorem 3.4. Since $\deg\xi^{(1)} = -\deg\xi^{(2)} = k$, the element $\eta_1 = 2k\theta_2 + \xi\theta_p$ belongs to $R^{(1,2)}$ by Lemma 4.2. The argument above shows that $\eta_1 = \xi\theta = \eta$. This completes the proof. □

Let $\eta = \xi\theta$ be an element of $I_P \cap R^{(1,2)}$ with $\xi \in R^{(1,2)}$. Then ξ is uniquely determined by η. In fact we have the following.

PROPOSITION 4.4. *The element θ is invertible in the algebra $R_{\mathbb{C}}^{(1,2)} = R^{(1,2)} \otimes \mathbb{C}$.*

PROOF. Let χ be any character of $C_I^{(1,2)}(\pm)$, and put

$$e_\chi^{\langle 1,2\rangle} = \frac{1}{|C_I^{(1,2)}(\pm)|} \sum_{\alpha \in C_I^{(1,2)}(\pm)} \chi(\alpha)\alpha^{-1}.$$

Let ψ_χ denote the character of $(\mathbb{Z}/p\mathbb{Z})^\times$ induced by χ (cf. [**21**, (5.8)]). Let χ_0 be the character of $C_I^{(1,2)}(\pm)$ which is trivial on $C_I^{(1)}(\pm)$ and satisfies $\chi_0([2]) = -1$. Then we have

$$\theta e_\chi^{\langle 1,2\rangle} = \begin{cases} \left(\dfrac{1}{4}B_{2,\overline{\psi_\chi}}\right)(2+\chi([2]))e_\chi^{\langle 1,2\rangle} & \text{if } \chi \mid C_I^{(1)}(\pm) \neq 1,\\ -\dfrac{1}{24}(p^2-1)e_\chi^{\langle 1,2\rangle} & \text{if } \chi = \chi_0,\\ -\dfrac{1}{8}(p^2-1)e_\chi^{\langle 1,2\rangle} & \text{if } \chi = 1. \end{cases} \tag{4.5}$$

Since $\theta e_\chi^{\langle 1,2\rangle} \neq 0$ for all χ, the element θ is invertible. □

4.3. A basis of I_P^N over $\mathbb{Z}$.

Here we give a basis of the group I_P^N over $\mathbb{Z}$.

Let $J_{0,0}$ be the subgroup of $R^{(1,2)}$ consisting of the elements ξ satisfying $\deg\xi^{(1)} = \deg\xi^{(2)} = 0$ and the congruence of Theorem 4.3.

LEMMA 4.5. *We have $I_P^N = J_{0,0}\theta[p]$.*

PROOF. Let $\xi \in R_{\mathbb{C}}^{(1,2)}$ and put $\xi_1 = \xi\theta$. Then we have

$$\deg \xi_1^{(1)} = \deg \xi^{(1)} \deg \theta^{(1)} + \deg \xi^{(2)} \deg \theta^{(2)}, \tag{4.6}$$

$$\deg \xi_1^{(2)} = \deg \xi^{(1)} \deg \theta^{(2)} + \deg \xi^{(2)} \deg \theta^{(1)}. \tag{4.7}$$

Assume that $\xi \in J_{0,0}$, and put $\xi_1 = \xi\theta$. Since $\deg \xi^{(1)} = \deg \xi^{(2)} = 0$, we have $\deg \xi_1^{(1)} = \deg \xi_1^{(2)} = 0$ by (4.6) and (4.7). Also, since $\deg \xi = \deg \xi^{(1)} + \deg \xi^{(2)} = 0$, we have $\xi_1 \in I_P \cap R^{(1,2)}$ by Theorem 4.3. This implies that $J_{0,0}\theta[p] \subset I_P^N$ by (4.3).

Conversely, Let $\eta = \xi_1[p]$ be any element of I_P^N, where $\xi_1 \in I_P \cap R^{(1,2)}$ and $\deg \xi_1^{(1)} = \deg \xi_1^{(2)} = 0$. By Theorem 4.3, we can write $\xi_1 = \xi\theta$ with an element $\xi \in R^{(1,2)}$ satisfying $\deg \xi = 0$ and the congruence of the theorem. We have $\deg \xi^{(1)} + \deg \xi^{(2)} = \deg \xi = 0$. Since $\deg \xi^{(2)} = -\deg \xi^{(1)}$, we have $\deg \xi^{(1)}(\deg \theta^{(1)} - \deg \theta^{(2)}) = 0$ by (4.6). Since $\deg \theta^{(1)} - \deg \theta^{(2)} = -(1/24)(p^2 - 1) \neq 0$, we have $\deg \xi^{(1)} = 0$, hence $\deg \xi^{(2)} = 0$. This implies $\xi \in J_{0,0}$, thus we have $I_P^N \subset J_{0,0}\theta[p]$. This completes the proof. □

We define the elements ξ_i $(0 \leq i \leq l-3)$ and λ_i $(i = 1, 2)$ of $R_0^{(1,2)}$ as follows with $l = (1/2)(p-1)$:

$$\xi_i = \langle d \rangle^i \big(\langle d \rangle - d^2\big)(\langle d \rangle - 1), \tag{4.8}$$

$$\lambda_1 = p(\langle d \rangle - 1), \quad \lambda_2 = (2 - [2])(\langle d \rangle - 1). \tag{4.9}$$

PROPOSITION 4.6. *Let ξ_i $(0 \leq i \leq l-3)$ and λ_i $(i = 1, 2)$ be as above. Then the set*

$$\big\{\xi_i \ (0 \leq i \leq l-3),\ \xi_i[2] \ (0 \leq i \leq l-3),\ \lambda_1,\ \lambda_2\big\}$$

is a basis of the group $J_{0,0}$ over $\mathbb{Z}$. (When $p = 5$, the elements ξ_i and $\xi_i[2]$ do not exist.)

PROOF. Let ξ be any one of the elements ξ_i, $\xi_i[2]$ and λ_i. Then it is easily verified that $\deg \xi^{(1)} = \deg \xi^{(2)} = 0$ and the congruence of Theorem 4.3, hence ξ is contained in $J_{0,0}$. Let $J_{0,0}^*$ be the subgroup of $J_{0,0}$ generated by the elements ξ_i, $\xi_i[2]$ and λ_i over $\mathbb{Z}$. Since the rank of $J_{0,0}$ over $\mathbb{Z}$ is $2(l-1)$ which is equal to the number of the elements above, it is sufficient to prove that $J_{0,0} = J_{0,0}^*$. Let ξ be any element of $J_{0,0}$. Since $\langle d \rangle$ generates $C_I^{(1)}(\pm)$ and $\deg \xi^{(1)} = \deg \xi^{(2)} = 0$, we can write

$$\xi = \sum_{i=1}^{l-1} m_i\big(\langle d \rangle^i - 1\big) + \sum_{i=1}^{l-1} n_i\big(\langle d \rangle^i - 1\big)[2]$$

with m_i, $n_i \in \mathbb{Z}$. Since $\langle d \rangle^i - 1 = (\langle d \rangle^{i-1} + \cdots + 1)(\langle d \rangle - 1)$, we have

$$\xi \in \sum_{k=0}^{l-2} \mathbb{Z}\langle d \rangle^k(\langle d \rangle - 1) + \sum_{k=0}^{l-2} \mathbb{Z}\langle d \rangle^k(\langle d \rangle - 1)[2]. \tag{4.10}$$

Since $\xi_i \in J^*_{0,0}$, we have $\langle d\rangle^{i+1}(\langle d\rangle - 1) \equiv d^2\langle d\rangle^i(\langle d\rangle - 1) \pmod{J^*_{0,0}}$ for $i = 0, \dots, l-3$, hence

$$\langle d\rangle^k(\langle d\rangle - 1) \equiv d^2\langle d\rangle^{k-1}(\langle d\rangle - 1) \equiv \cdots \equiv d^{2k}(\langle d\rangle - 1) \pmod{J^*_{0,0}}$$

for $k = 0, \dots, l-2$. Combining this with (4.10) we have

$$\xi \in \mathbb{Z}(\langle d\rangle - 1) + \mathbb{Z}(\langle d\rangle - 1)[2] + J^*_{0,0}. \tag{4.11}$$

By (4.11) we can write $\xi = \xi^* + \xi^{**}$, where $\xi^* = m(\langle d\rangle - 1) + n(\langle d\rangle - 1)[2]$ with $m,\ n \in \mathbb{Z}$ and ξ^{**} is an element of $J^*_{0,0}$. Since $\xi \in J_{0,0}$, we have $\xi^* \in J_{0,0}$. Since $\xi^* = -m + m\langle d\rangle - n[2] + n\langle d\rangle[2]$ satisfies the congruence of Theorem 4.3, we have

$$1 \cdot (-m) + d^2 \cdot m + 2\{1 \cdot (-n) + d^2 \cdot n\} \equiv 0 \pmod{p},$$

whence $(m + 2n)(d^2 - 1) \equiv 0 \pmod{p}$. If $p \geq 7$, then $d^2 - 1 \not\equiv 0 \pmod{p}$ because $l \geq 3$. If $p = 5$, then $d^2 \equiv -1 \pmod 5$, whence $d^2 - 1 \not\equiv 0 \pmod{p}$. We have therefore for any p $(\neq 2, 3)$ $m + 2n \equiv 0 \pmod{p}$. Put $m + 2n = ps$ with $s \in \mathbb{Z}$. Substituting $-2n + ps$ for m we have

$$\begin{aligned}\xi^* &= ps(\langle d\rangle - 1) - n(2 - [2])(\langle d\rangle - 1)\\ &= s\lambda_1 - n\lambda_2,\end{aligned}$$

therefore $\xi^* \in J^*_{0,0}$. This proves $\xi = \xi^* + \xi^{**} \in J^*_{0,0}$, which completes the proof. □

By Lemma 4.5 and Proposition 4.6 we have the following.

PROPOSITION 4.7. *Let l, ξ_i, λ_1 and λ_2 be the same as in Proposition* 4.6. *Then the set*

$$\big\{\xi_i[p]\theta\ (0 \leq i \leq l-3),\ \xi_i[2][p]\theta\ (0 \leq i \leq l-3),\ \lambda_1[p]\theta,\ \lambda_2[p]\theta\big\}$$

is a basis of the group I_P^N over $\mathbb{Z}$.

4.4. Proof of $\mathcal{C}_2 = \mathcal{C}_{\mathbb{Q}}$.

First we define a subgroup I_P^D of I_P^N by

$$I_P^D = \big\{\xi \in I_P \mid \xi = \eta^\sigma - \eta \text{ with some } \eta \in I_P\big\}, \tag{4.12}$$

and prove $I_P^D = I_P^N$.

LEMMA 4.8. *Let $\eta = \eta_0\theta_p$ with $\eta_0 \in R$. Then $\eta^\sigma - \eta = \eta_0^{(p,2p)}(\langle d\rangle - 1)\theta$.*

PROOF. By Proposition 2.6, we have $\eta^\sigma - \eta = \eta^{(p,2p)}(\langle d\rangle - 1)$. Since

$$\begin{aligned}\eta^{(p,2p)} &= \eta_0^{(p,2p)}\theta_p^{(1,2)} + \eta_0^{(1,2)}\theta_p^{(p,2p)} \\ &= \eta_0^{(p,2p)}\theta - \eta_0^{(p,2p)}\theta_2^{(1,2)} + \eta_0^{(1,2)}\theta_p^{(p,2p)}\end{aligned}$$

and $\theta_2^{(1,2)}(\langle d\rangle - 1) = \theta_p^{(p,2p)}(\langle d\rangle - 1) = 0$, we have $\eta^{(p,2p)}(\langle d\rangle - 1) = \eta_0^{(p,2p)}(\langle d\rangle - 1)\theta$. This proves the lemma. □

PROPOSITION 4.9. (1) *Put $\eta_0 = \langle d\rangle^i(\langle d\rangle - d^2)(-p + [p])$ and $\eta = \eta_0\theta_p$ with $i \geq 0$, $\in \mathbb{Z}$. Then we have $\eta \in I_P$, and $\eta^\sigma - \eta = \langle d\rangle^i(\langle d\rangle - d^2)(\langle d\rangle - 1)[p]\theta$.*

(2) *Put $\eta_0 = \langle d\rangle^i(\langle d\rangle - d^2)(-p + [p])[2]$ and $\eta = \eta_0\theta_p$ with $i \geq 0$, $\in \mathbb{Z}$. Then we have $\eta \in I_P$, and $\eta^\sigma - \eta = \langle d\rangle^i(\langle d\rangle - d^2)(\langle d\rangle - 1)[2][p]\theta$.*

(3) *Put $\eta_0 = p(-p+[p])$ and $\eta = \eta_0\theta_p$. Then we have $\eta \in I_P$, and $\eta^\sigma - \eta = p(\langle d\rangle - 1)[p]\theta$.*

(4) *Put $\eta_0 = (2 - [2])(-p + [p])$ and $\eta = \eta_0\theta_p$. Then we have $\eta \in I_P$, and $\eta^\sigma - \eta = (2 - [2])(\langle d\rangle - 1)[p]\theta$.*

PROOF. In every case of (1)–(4) we can prove that the element η_0 belongs to I_{12} (cf. (3.14)). In fact, for each η_0 of (1)–(4), the value of the term on the left-hand side of (3.14) is 0, and the value of the term on the left-hand side of (ii) of Theorem 2.4 is also 0. It is also easy to verify that each η_0 of (1)–(4) satisfies the congruences (iii) and (iv) of Theorem 2.4. For example, take the element η_0 of (2). Put $\alpha = \langle d\rangle^i[2][p]$. Then we have $b(\alpha)^2 \equiv (2+p)^2d^{2i} \pmod p$. The term on the left-hand side of (iv) is congruent to $(2+p)^2d^{2i}\cdot d^2 + (2+p)^2d^{2i+2}\cdot(-1)$ modulo p, whence η_0 satisfies the congruence (iv). Since $\eta_0 \in I_{12}$, we have $\eta \in I_P$ by Theorem 2.4. The equality for $\eta^\sigma - \eta$ follows from Lemma 4.8. □

PROPOSITION 4.10. $I_P^N = I_P^D$.

PROOF. Since $I_P^D \subset I_P^N$, it is sufficient to prove $I_P^N \subset I_P^D$. In order to prove $I_P^N \subset I_P^D$ it is sufficient to show that each element of a basis of I_P^N over $\mathbb{Z}$ is contained in I_P^D. By Proposition 4.7 the elements $\xi_i[p]\theta$ $(0 \leq i \leq l-3)$, $\xi_i[2][p]\theta$ $(0 \leq i \leq l-3)$, $\lambda_1[p]\theta$ and $\lambda_2[p]\theta$ constitute a basis. The inclusions $\xi_i[p]\theta \in I_P^D$, $\xi_i[2][p]\theta \in I_P^D$, $\lambda_1[p]\theta \in I_P^D$ and $\lambda_2[p]\theta \in I_P^D$ follow directly from (1), (2), (3) and (4) of Proposition 4.9 respectively. This proves the proposition. □

Now we have the following

THEOREM 4.11. $\mathcal{C}_2 = \mathcal{C}_\mathbb{Q}$.

PROOF. By the isomorphisms (3.4) and (4.1) it is sufficient to prove that the homomorphism $\phi : R_0^\mathbb{Q}/(I_P \cap R^\mathbb{Q}) \to R_0^*/I_P$ induced by the inclusion map $R_0^\mathbb{Q} \to R_0^*$ is an isomorphism. Since ϕ is injective, it is sufficient to prove that ϕ is surjective. Let η be any element of R_0^*. Then $\eta^\sigma - \eta \in I_P$, hence $\eta^\sigma - \eta \in I_P^N$. Since $I_P^N = I_P^D$ by Proposition 4.10, there exists an element $\xi \in I_P$ such that $\eta^\sigma - \eta = \xi^\sigma - \xi$. Hence we have $(\eta - \xi)^\sigma = \eta - \xi$. This implies that $\eta - \xi \in R_0^\mathbb{Q}$. Put $\eta_1 = \eta - \xi$. Then we have $\eta + I_P = \phi(\eta_1 + I_P \cap R^\mathbb{Q}) \in \mathrm{Im}(\phi)$. This proves the theorem. □

By Theorems 3.7 and 4.11 we have $\mathcal{C}_1 = \mathcal{C}_\mathbb{Q}$. If $p \geq 7$, then the genus of $X_1(2p)$ is

not 0, and we have the following.

THEOREM 4.12. *Let p be a prime ≥ 7. Then the genus of $X_1(2p)$ is not 0, and the $\mathbb{Q}$-rational cuspidal group of $J_1(2p)$ is generated by the $\mathbb{Q}$-rational cusps.*

Put $G = \mathrm{Gal}(k_{2p}/\mathbb{Q})$. The group I_P is a G-module. Let $H^n(G, I_P)$ (respectively $H_n(G, I_P)$) be the n-th cohomology group (respectively homology group). Then Proposition 4.10 is equivalent to the following theorem.

THEOREM 4.13. *For all $n \geq 1$, we have $H^{2n-1}(G, I_P) = H_{2n}(G, I_P) = 0$.*

PROOF. Put $l = (1/2)(p-1)$. Let $N : I_P \to I_P$ be the homomorphism defined by $N(\xi) = \sum_{i=0}^{l-1} \xi^{\sigma^i}$. Let $D : I_P \to I_P$ be the homomorphism defined by $D(\xi) = \xi^\sigma - \xi$. Since G is a finite cyclic group, we have $H^{2n-1}(G, I_P) = H_{2n}(G, I_P) = \ker(N)/\mathrm{Im}(D)$ (cf. Rotman [**17**, Theorems 9.27 and 9.48]). Since $N(\xi) = l\xi^{(1,2)} + (\deg \xi^{(p)})\mu^{(p)} + (\deg \xi^{(2p)})\mu^{(2p)}$, we have $N(\xi) = 0$ if and only if $\xi^{(1,2)} = 0$ and $\deg \xi^{(p)} = \deg \xi^{(2p)} = 0$. Hence we have $\ker(N) = I_P^N$ by (4.3). Also we have $\mathrm{Im}(D) = I_P^D$ by (4.12). Since $I_P^N = I_P^D$ by Proposition 4.10, we have the proof. □

5. The class number formula for $\mathcal{C}_\mathbb{Q}$.

Let p be a prime $\neq 2, 3$. In this section we determine the order of the $\mathbb{Q}$-rational cuspidal group $\mathcal{C}_\mathbb{Q}$.

By Theorems 3.7 and 4.11, the group $\mathcal{C}_\mathbb{Q}$ coincides with $\mathcal{C}_1$, where $\mathcal{C}_1 \cong R_0^{(1,2)}/I_P^{(1,2)}$ with $I_P^{(1,2)} = I_P \cap R^{(1,2)}$ (2.15). Let J_0 be the subgroup of $R_0^{(1,2)}$ consisting of all elements ξ satisfying the congruence of Theorem 4.3. Then by the theorem we have $I_P^{(1,2)} = J_0\theta$, therefore we have

$$\mathcal{C}_\mathbb{Q} \cong R_0^{(1,2)}/J_0\theta. \tag{5.1}$$

Let $h_\mathbb{Q}$ be the order of $\mathcal{C}_\mathbb{Q}$.

Let A and B be two lattices of $R_{0,\mathbb{Q}}^{(1,2)} = R_0^{(1,2)} \otimes \mathbb{Q}$, and let C be a lattice contained in $A \cap B$. Then the quotient $[A : C]/[B : C]$ does not depend on the choice of C. We denote this number by $[A : B]$. It satisfies the usual multiplicative property, namely $[A : B] = [A : D][D : B]$. In particular, we have $[R_0^{(1,2)} : J_0\theta] = [R_0^{(1,2)} : R_0^{(1,2)}\theta][R_0^{(1,2)}\theta : J_0\theta]$. Since θ is invertible by Proposition 4.4, we have $[R_0^{(1,2)}\theta : J_0\theta] = [R_0^{(1,2)} : J_0]$. Hence we have

$$h_\mathbb{Q} = \left[R_0^{(1,2)} : R_0^{(1,2)}\theta\right]\left[R_0^{(1,2)} : J_0\right]. \tag{5.2}$$

PROPOSITION 5.1. $\left[R_0^{(1,2)} : J_0\right] = p$.

PROOF. Let ξ be an element of $R_0^{(1,2)}$. Let $\phi(\xi)$ be the element of $\mathbb{Z}/p\mathbb{Z}$ defined by the term on the left-hand side of Theorem 4.3. Then ϕ is a homomorphism of $R_0^{(1,2)}$ to $\mathbb{Z}/p\mathbb{Z}$, and its kernel is J_0. Put $\xi = -1 + [2]$. Then we have $\xi \in R_0^{(1,2)}$ and $\phi(\xi) \equiv 1$

$(\mathrm{mod}\, p)$. This proves that ϕ is surjective, whence the proof is completed. □

PROPOSITION 5.2. $\left[R_0^{(1,2)} : R_0^{(1,2)}\theta\right] = ((p^2-1)/24)\prod_{\psi\neq 1}\{(4-\psi(2))((1/4)B_{2,\psi})^2\}$, *where ψ runs over all non-trivial, even characters of $(\mathbb{Z}/p\mathbb{Z})^\times$.*

PROOF. Let $f : R_{0,\mathbb{Q}}^{(1,2)} \to R_{0,\mathbb{Q}}^{(1,2)}$ be the linear transformation on the vector space $R_{0,\mathbb{Q}}^{(1,2)}$ over $\mathbb{Q}$ defined by the multiplication by θ. Then we have $[R_0^{(1,2)} : R_0^{(1,2)}\theta] = |\det(f)|$ by the theory of elementary divisors and the definition of $[R_0^{(1,2)} : R_0^{(1,2)}\theta]$. Let χ be any character of $C_I^{(1,2)}(\pm)$, and let χ_0, $e_\chi^{\langle 1,2\rangle}$, ψ_χ be the same as in the proof of Proposition 4.4. Since the elements $e_\chi^{\langle 1,2\rangle}$ with χ non-trivial constitute a basis of $R_{0,\mathbb{C}}^{(1,2)} = R_{0,\mathbb{Q}}^{(1,2)} \otimes \mathbb{C}$ over $\mathbb{C}$, we have $\det(f) = \prod_{\chi\neq 1}\chi(\theta)$, where χ runs over all non-trivial characters of $C_I^{(1,2)}(\pm)$ and $\chi(\theta)$ is the number defined by $\theta e_\chi^{\langle 1,2\rangle} = \chi(\theta)e_\chi^{\langle 1,2\rangle}$. By (4.5), we have

$$\chi(\theta) = \begin{cases} \left(\dfrac{1}{4}B_{2,\overline{\psi_\chi}}\right)(2+\chi([2])) & \text{if } \chi \mid C_I^{(1)}(\pm) \neq 1, \\ -\dfrac{1}{24}(p^2-1) & \text{if } \chi = \chi_0, \end{cases} \tag{5.3}$$

therefore

$$|\det(f)| = \frac{1}{24}(p^2-1)\left|\prod_{\chi\neq 1,\,\chi_0}\left\{\left(\frac{1}{4}B_{2,\overline{\psi_\chi}}\right)(2+\chi([2]))\right\}\right|. \tag{5.4}$$

Let ψ be a non-trivial, even character of $(\mathbb{Z}/p\mathbb{Z})^\times$. Then the set of characters χ of $C_I^{(1,2)}(\pm)$ with $\psi_\chi = \psi$ consists of two elements. Let χ be anyone of them. Then the other is $\chi\chi_0$. We prove that

$$\prod_{\chi:\psi_\chi=\psi}(2+\chi([2])) = 4-\psi(2). \tag{5.5}$$

In fact, since $(\chi\chi_0)([2]) = \chi_0([2])\chi([2]) = -\chi([2])$, the left-hand side of (5.5) is equal to $4-\chi([2]^2)$. By the definition of $[2]$ the element $[2]^2$ is an element of $C_I^{(1)}(\pm)$ represented by the matrix $(2+p)1_2$. Hence we have $\chi([2]^2) = \psi(2)$, which proves (5.5). Since we have

$$\begin{aligned}\prod_{\chi\neq 1,\,\chi_0}\left\{\left(\frac{1}{4}B_{2,\overline{\psi_\chi}}\right)(2+\chi([2]))\right\} &= \prod_{\psi\neq 1}\prod_{\chi:\psi_\chi=\psi}\left\{\left(\frac{1}{4}B_{2,\overline{\psi_\chi}}\right)(2+\chi([2]))\right\} \\ &= \prod_{\psi\neq 1}\left\{(4-\psi(2))\left(\frac{1}{4}B_{2,\overline{\psi}}\right)^2\right\}\end{aligned} \tag{5.6}$$

by (5.5) and the value of the right-hand side of (5.6) is a positive real number, combining the equality (5.4) with $[R_0^{(1,2)} : R_0^{(1,2)}\theta] = |\det(f)|$, we have the proof. □

By (5.2) and Propositions 5.1 and 5.2, we have the following

THEOREM 5.3. *Let p be a prime ≥ 5. Let $h_{\mathbb{Q}}$ be the order of $\mathcal{C}_{\mathbb{Q}}$. Then we have*

$$h_{\mathbb{Q}} = \frac{p^2-1}{24} p \prod_{\psi} \left\{ (4-\psi(2)) \left(\frac{1}{4} B_{2,\psi} \right)^2 \right\},$$

where ψ runs over all even, primitive Dirichlet characters modulo p.

REMARK 5.4. When $p \geq 7$, this gives the order of the $\mathbb{Q}$-rational cuspidal group of $J_1(2p)$.

6. A basis of the modular units with divisors supported on $\mathbb{Q}$-rational cusps.

Let p be a prime $\neq 2, 3$. As stated at the beginning of Section 5, the $\mathbb{Q}$-rational cuspidal group $\mathcal{C}_{\mathbb{Q}}$ is isomorphic to $R_0^{(1,2)}/I_P^{(1,2)}$, and $I_P^{(1,2)} = J_0\theta$ where J_0 is the subgroup of $R_0^{(1,2)}$ consisting of the elements ξ satisfying the congruence of Theorem 4.3. In this section we give a $\mathbb{Z}$-basis of $I_P^{(1,2)}$ so that we can determine the structure of $\mathcal{C}_{\mathbb{Q}}$ explicitly for a given value of p.

Let d be the same as in Section 4, i.e., an integer such that $(d, 2p) = 1$ and it generates the cyclic group $(\mathbb{Z}/2p\mathbb{Z})^\times/\{\pm 1\}$. Let ξ_i $(0 \leq i \leq l-3)$ be the elements defined in (4.8). We define the elements ξ_{l-2} and η_j $(0 \leq j \leq l-1)$ of $R_0^{(1,2)}$ as follows:

$$\xi_{l-2} = (\langle d \rangle - 1) + (d^2-1)(1-[2]), \tag{6.1}$$

$$\eta_j = \langle d \rangle^j (\langle d \rangle - d^2)(1-[2]) \ (0 \leq j \leq l-2), \quad \eta_{l-1} = p(1-[2]). \tag{6.2}$$

PROPOSITION 6.1. *Let ξ_i $(0 \leq i \leq l-2)$ and η_j $(0 \leq j \leq l-1)$ be as above. Then the set*

$$\{\xi_i \ (0 \leq i \leq l-2), \ \eta_j \ (0 \leq j \leq l-1)\}$$

is a basis of the group J_0 over $\mathbb{Z}$.

PROOF. It is easy to verify that these elements satisfy the congruence of Theorem 4.3, hence they are contained in J_0. Let J_0^* denote the subgroup of J_0 generated by these elements. Since the rank of J_0 is $2l-1$ which is equal to the number of the elements above, it is sufficient to prove that $J_0 = J_0^*$. Let ξ be any element of J_0. Since $\langle d \rangle$ generates $C_I^{(1)}(\pm)$ and $\deg \xi = 0$, we can write

$$\xi = \sum_{i=1}^{l-1} m_i \big(\langle d \rangle^i - 1 \big) + \sum_{i=0}^{l-1} n_i \big(\langle d \rangle^i [2] - 1 \big)$$

with m_i, $n_i \in \mathbb{Z}$. Since

$$\langle d\rangle^i[2]-1=\big(\langle d\rangle^i-1\big)-\langle d\rangle^i(1-[2])$$

and $\langle d\rangle^i-1=(\langle d\rangle^{i-1}+\cdots+1)(\langle d\rangle-1)$ $(i\geq 1)$, we have

$$\xi\in\sum_{k=0}^{l-2}\mathbb{Z}\langle d\rangle^k(\langle d\rangle-1)+\sum_{k=0}^{l-1}\mathbb{Z}\langle d\rangle^k(1-[2]). \tag{6.3}$$

Since $\xi_i\in J_0^*$, we have $\langle d\rangle^{i+1}(\langle d\rangle-1)\equiv d^2\langle d\rangle^i(\langle d\rangle-1) \pmod{J_0^*}$ for $i=0,\dots,l-3$, hence

$$\langle d\rangle^k(\langle d\rangle-1)\equiv d^2\langle d\rangle^{k-1}(\langle d\rangle-1)\equiv\cdots\equiv d^{2k}(\langle d\rangle-1) \pmod{J_0^*} \tag{6.4}$$

for $k=0,\dots,l-2$. Also since $\eta_j\in J_0^*$, we have $\langle d\rangle^{j+1}(1-[2])\equiv d^2\langle d\rangle^j(1-[2]) \pmod{J_0^*}$ for $j=0,\dots,l-2$, hence

$$\langle d\rangle^k(1-[2])\equiv d^2\langle d\rangle^{k-1}(1-[2])\equiv\cdots\equiv d^{2k}(1-[2]) \pmod{J_0^*} \tag{6.5}$$

for $k=0,\dots,l-1$. Combining (6.4) and (6.5) with (6.3), we have

$$\xi\in\mathbb{Z}(\langle d\rangle-1)+\mathbb{Z}(1-[2])+J_0^*. \tag{6.6}$$

By (6.6) we can write $\xi=\xi^*+\xi^{**}$, where $\xi^*=m(\langle d\rangle-1)+n(1-[2])$ with $m,n\in\mathbb{Z}$ and ξ^{**} is an element of J_0^*. Since $\xi\in J_0$, we have $\xi^*\in J_0$. Since $\xi^*=(-m+n)+m\langle d\rangle-n[2]$ satisfies the congruence of Theorem 4.3, we have

$$1\cdot(-m+n)+d^2\cdot m+2\cdot 1\cdot(-n)\equiv 0 \pmod p,$$

whence $n\equiv m(d^2-1) \pmod p$. Put $n=m(d^2-1)+ps$ with $s\in\mathbb{Z}$. Then we have

$$\begin{aligned}\xi^*&=m\big\{(\langle d\rangle-1)+(d^2-1)(1-[2])\big\}+s\cdot p(1-[2])\\&=m\xi_{l-2}+s\eta_{l-1},\end{aligned}$$

therefore $\xi^*\in J_0^*$. This proves $\xi=\xi^*+\xi^{**}\in J_0^*$, which completes the proof. □

Since $I_P^{(1,2)}=J_0\theta$ and θ is invertible, we have the following

THEOREM 6.2. *Let ξ_i $(0\leq i\leq l-2)$ and η_j $(0\leq j\leq l-1)$ be the same as in Proposition* 6.1. *Then the set*

$$\{\xi_i\theta\ (0\leq i\leq l-2),\ \eta_j\theta\ (0\leq j\leq l-1)\}$$

is a basis of the group $I_P^{(1,2)}$ over $\mathbb{Z}$.

7. The Sylow p-subgroup of $\mathcal{C}_{\mathbb{Q}}$.

Let p be a prime $\neq 2, 3$. In this section we determine the structure of the Sylow p-subgroup $\mathcal{C}_{\mathbb{Q},p}$ of $\mathcal{C}_{\mathbb{Q}}$.

7.1. The χ-eigen components.

As stated at the beginning of Section 5, the $\mathbb{Q}$-rational cuspidal group $\mathcal{C}_{\mathbb{Q}}$ is isomorphic to $R_0^{(1,2)}/I_P^{(1,2)}$, and $I_P^{(1,2)} = J_0\theta$ where J_0 is the subgroup of $R_0^{(1,2)}$ consisting of the elements ξ satisfying the congruence of Theorem 4.3:

$$\mathcal{C}_{\mathbb{Q}} \cong R_0^{(1,2)}/J_0\theta. \tag{7.1}$$

Since the Sylow p-subgroup $\mathcal{C}_{\mathbb{Q},p}$ of $\mathcal{C}_{\mathbb{Q}}$ is isomorphic to $\mathcal{C}_{\mathbb{Q}} \otimes \mathbb{Z}_p$, we have

$$\mathcal{C}_{\mathbb{Q},p} \cong \big(R_0^{(1,2)} \otimes \mathbb{Z}_p\big)/(J_0\theta \otimes \mathbb{Z}_p). \tag{7.2}$$

Let α be any element of $C_I^{(1,2)}(\pm)$. Then $\alpha^2 \in C_I^{(1)}(\pm) \cong (\mathbb{Z}/p\mathbb{Z})^\times/\{\pm 1\}$, therefore $\alpha^{p-1} = 1$. Let χ be any character of $C_I^{(1,2)}(\pm)$. Then $\chi(\alpha)$ is a $(p-1)$st root of 1. Since $\mathbb{Z}_p^\times$ contains all $(p-1)$st roots of 1, we can embed the group of $(p-1)$st roots of 1 in $\mathbb{C}$ into $\mathbb{Z}_p^\times$. We fix such an embedding and consider χ as a homomorphism into $\mathbb{Z}_p^\times$. Then $\chi(\alpha) \in \mathbb{Z}_p^\times$ for all $\alpha \in C_I^{(1,2)}(\pm)$.

Let $e_\chi^{\langle 1,2\rangle}$ be the element defined in the proof of Proposition 4.4:

$$e_\chi^{\langle 1,2\rangle} = \frac{1}{|C_I^{(1,2)}(\pm)|} \sum_{\alpha \in C_I^{(1,2)}(\pm)} \chi(\alpha)\alpha^{-1}. \tag{7.3}$$

Since $|C_I^{(1,2)}(\pm)| = p - 1 \in \mathbb{Z}_p^\times$, we have $e_\chi^{\langle 1,2\rangle} \in \mathbb{Z}_p[C_I^{(1,2)}(\pm)] = R^{(1,2)} \otimes \mathbb{Z}_p$. Let $\xi = \sum_{\alpha \in C_I^{(1,2)}(\pm)} z(\alpha)\alpha$ $(z(\alpha) \in \mathbb{Z}_p)$ be an element of $R^{(1,2)} \otimes \mathbb{Z}_p$. Put

$$\chi(\xi) = \sum_{\alpha \in C_I^{(1,2)}(\pm)} z(\alpha)\chi(\alpha). \tag{7.4}$$

Then we have

$$\xi e_\chi^{\langle 1,2\rangle} = \chi(\xi) e_\chi^{\langle 1,2\rangle}. \tag{7.5}$$

As is well-known, we have $1 = \sum_\chi e_\chi^{\langle 1,2\rangle}$ and the elements $e_\chi^{\langle 1,2\rangle}$ satisfy the orthogonality relation. Combining these facts with (7.5) we have the direct sum decomposition

$$R_0^{(1,2)} \otimes \mathbb{Z}_p = \bigoplus_{\chi \neq 1} \mathbb{Z}_p e_\chi^{\langle 1,2\rangle}. \tag{7.6}$$

In the following we identify the group $\mathcal{C}_{\mathbb{Q},p}$ with the group $(R_0^{(1,2)} \otimes \mathbb{Z}_p)/(J_0\theta \otimes$

$\mathbb{Z}_p$) through the isomorphism (7.2). Since I_P is an ideal of R, the additive subgroup $I_P^{(1,2)} \otimes \mathbb{Z}_p = J_0\theta \otimes \mathbb{Z}_p$ is also an ideal of $R^{(1,2)} \otimes \mathbb{Z}_p$. Therefore, the group $\mathcal{C}_{\mathbb{Q},p}$ is an $(R^{(1,2)} \otimes \mathbb{Z}_p)$-module. Put

$$\mathcal{C}_{\mathbb{Q},p}(\chi) = \big\{m \in \mathcal{C}_{\mathbb{Q},p} \mid \alpha m = \chi(\alpha)m \text{ for all } \alpha \in C_I^{(1,2)}(\pm)\big\}. \tag{7.7}$$

We call the subgroup $\mathcal{C}_{\mathbb{Q},p}(\chi)$ of $\mathcal{C}_{\mathbb{Q},p}$ the *χ-eigen component* of $\mathcal{C}_{\mathbb{Q},p}$.

PROPOSITION 7.1. (1) $\mathcal{C}_{\mathbb{Q},p} = \bigoplus_{\chi\neq 1} \mathcal{C}_{\mathbb{Q},p}(\chi)$.
(2) $\mathcal{C}_{\mathbb{Q},p}(\chi) \cong \mathbb{Z}_p e_\chi^{\langle 1,2\rangle} / \big(\mathbb{Z}_p e_\chi^{\langle 1,2\rangle} \cap (J_0\theta \otimes \mathbb{Z}_p)\big)$ *or* $= 0$ *according as* $\chi \neq 1$ *or* $= 1$.

PROOF. Since $1 = \sum_\chi e_\chi^{\langle 1,2\rangle}$ and $e_\chi^{\langle 1,2\rangle}$ are orthogonal idempotents, we have the ring decomposition $R^{(1,2)} \otimes \mathbb{Z}_p = \bigoplus_\chi e_\chi^{\langle 1,2\rangle}(R^{(1,2)} \otimes \mathbb{Z}_p)$, hence as an $(R^{(1,2)} \otimes \mathbb{Z}_p)$-module we have

$$\mathcal{C}_{\mathbb{Q},p} = \bigoplus_\chi e_\chi^{\langle 1,2\rangle} \mathcal{C}_{\mathbb{Q},p}.$$

If $m \in \mathcal{C}_{\mathbb{Q},p}(\chi)$, then $e_{\chi_1}^{\langle 1,2\rangle} m = m$ or 0 according as $\chi_1 = \chi$ or not, hence we have $e_\chi^{\langle 1,2\rangle} \mathcal{C}_{\mathbb{Q},p} = \mathcal{C}_{\mathbb{Q},p}(\chi)$. For the trivial character we have $\mathcal{C}_{\mathbb{Q},p}(1) = 0$ by (7.6). This proves (1). (2) follows from (7.6) and $\mathcal{C}_{\mathbb{Q},p}(\chi) = e_\chi^{\langle 1,2\rangle} \mathcal{C}_{\mathbb{Q},p}$. □

Since $\theta \in \mathbb{Q}[C_I^{(1,2)}(\pm)]$, we can regard the element θ as an element of $\mathbb{Q}_p[C_I^{(1,2)}(\pm)]$. Also we regard $\mathbb{Z}_p[C_I^{(1,2)}(\pm)]$ as a subgroup of $\mathbb{Q}_p[C_I^{(1,2)}(\pm)]$. Then we have

$$J_0\theta \otimes \mathbb{Z}_p = (J_0 \otimes \mathbb{Z}_p)\theta \subset \mathbb{Z}_p\big[C_I^{(1,2)}(\pm)\big]. \tag{7.8}$$

Though $\theta \notin \mathbb{Z}_p[C_I^{(1,2)}(\pm)]$, the value $\chi(\theta) \in \mathbb{Q}_p$ can be defined exactly in the same manner as (7.4). Then we have $\theta e_\chi^{\langle 1,2\rangle} = \chi(\theta) e_\chi^{\langle 1,2\rangle}$ exactly in the same manner as (7.5).

PROPOSITION 7.2. *Let χ be a non-trivial character of $C_I^{(1,2)}(\pm)$. Let $\chi(\theta)$ be as above. Then we have $\mathbb{Z}_p e_\chi^{\langle 1,2\rangle} \cap (J_0\theta \otimes \mathbb{Z}_p) = \chi(J_0 \otimes \mathbb{Z}_p)\chi(\theta) e_\chi^{\langle 1,2\rangle}$.*

PROOF. We prove the inclusion $\subset$. Let η be any element of $\mathbb{Z}_p e_\chi^{\langle 1,2\rangle} \cap (J_0\theta \otimes \mathbb{Z}_p)$. Then we have $\eta = z e_\chi^{\langle 1,2\rangle} = \xi\theta$ with $z \in \mathbb{Z}_p$ and $\xi \in J_0 \otimes \mathbb{Z}_p$ by (7.8). Hence $\eta = (z e_\chi^{\langle 1,2\rangle}) e_\chi^{\langle 1,2\rangle} = (\xi\theta) e_\chi^{\langle 1,2\rangle} = \chi(\xi)\chi(\theta) e_\chi^{\langle 1,2\rangle}$. This prove the inclusion.

Next we prove the reverse inclusion $\supset$. Let η be any element of $\chi(J_0 \otimes \mathbb{Z}_p)\chi(\theta) e_\chi^{\langle 1,2\rangle}$. Then we have $\eta = \chi(\xi)\chi(\theta) e_\chi^{\langle 1,2\rangle}$ with $\xi \in J_0 \otimes \mathbb{Z}_p$. Put $\eta_1 = \xi\theta e_\chi^{\langle 1,2\rangle}$. Since $J_0\theta \otimes \mathbb{Z}_p$ is an ideal of $\mathbb{Z}_p[C_I^{(1,2)}(\pm)]$, we have $\eta_1 \in J_0\theta \otimes \mathbb{Z}_p$. On the other hand, we have $\eta_1 = \xi\theta e_\chi^{\langle 1,2\rangle} = \chi(\xi)\chi(\theta) e_\chi^{\langle 1,2\rangle} = \eta$, whence $\eta \in \mathbb{Z}_p e_\chi^{\langle 1,2\rangle} \cap (J_0\theta \otimes \mathbb{Z}_p)$. This proves the reverse inclusion. Thus the proof is completed. □

By Propositions 7.1 and 7.2, for any character $\chi \neq 1$, we have

$$\mathcal{C}_{\mathbb{Q},p}(\chi) \cong \mathbb{Z}_p/(\chi(J_0 \otimes \mathbb{Z}_p)\chi(\theta)). \tag{7.9}$$

7.2. The group $\chi(J_0 \otimes \mathbb{Z}_p)$.

Here we study the subgroup $\chi(J_0 \otimes \mathbb{Z}_p)$ of $\mathbb{Z}_p$, which is an ideal of $\mathbb{Z}_p$.

Let $\bar{J}_0$ denote the subgroup of $R^{(1,2)} \otimes \mathbb{Z}_p$ consisting of all elements $\xi = \sum_{\alpha \in C_I^{(1,2)}(\pm)} z(\alpha)\alpha$ $(z(\alpha) \in \mathbb{Z}_p)$ such that $\deg(\xi) = 0$ and the coefficients $z(\alpha)$ satisfy the congruence

$$\sum_{\alpha \in C_I^{(1)}(\pm)} a(\alpha)^2 z(\alpha) + 2 \sum_{\alpha \in C_I^{(2)}(\pm)} a(\alpha)^2 z(\alpha) \equiv 0 \pmod{p}. \tag{7.10}$$

PROPOSITION 7.3. $\bar{J}_0 = J_0 \otimes \mathbb{Z}_p$.

PROOF. It is easy to verify that $J_0 \otimes \mathbb{Z}_p$ is contained in $\bar{J}_0$. We prove the reverse inclusion. Let $\xi = \sum_{\alpha \in C_I^{(1,2)}(\pm)} z(\alpha)\alpha$ $(z(\alpha) \in \mathbb{Z}_p)$ be any element of $\bar{J}_0$. Since $\deg(\xi) = 0$, we can write $\xi = \sum_{\alpha \in C_I^{(1,2)}(\pm)} z(\alpha)(\alpha - 1)$. For each $\alpha \in C_I^{(1,2)}(\pm)$, let $m(\alpha) \in \mathbb{Z}$ and $z'(\alpha) \in \mathbb{Z}_p$ be chosen as $z(\alpha) = m(\alpha) + pz'(\alpha)$. Then by (7.10) the integers $m(\alpha)$ satisfy the congruence of Theorem 4.3. Since $\deg(\xi) = 0$, we have $0 = \sum_{\alpha \in C_I^{(1,2)}(\pm)} m(\alpha) + p\sum_{\alpha \in C_I^{(1,2)}(\pm)} z'(\alpha)$, hence

$$\sum_{\alpha \in C_I^{(1,2)}(\pm)} m(\alpha) \equiv 0 \pmod{p}. \tag{7.11}$$

Put

$$\xi_0 = \sum_{\alpha \in C_I^{(1,2)}(\pm)} m(\alpha)\alpha - \Bigg(\sum_{\alpha \in C_I^{(1,2)}(\pm)} m(\alpha) \Bigg) \cdot 1 = \sum_{\alpha \in C_I^{(1,2)}(\pm)} m(\alpha)(\alpha - 1). \tag{7.12}$$

Since the element $\big(\sum_{\alpha \in C_I^{(1,2)}(\pm)} m(\alpha)\big) \cdot 1$ satisfies the congruence of Theorem 4.3 by (7.11), the element ξ_0 also satisfies the congruence of Theorem 4.3. By this and the equality $\deg(\xi_0) = 0$, we have $\xi_0 \in J_0$. Now we have

$$\xi = \xi_0 + \sum_{\alpha \in C_I^{(1,2)}(\pm)} z'(\alpha) \cdot p(\alpha - 1). \tag{7.13}$$

Since $p(\alpha - 1) \in J_0$, the equality (7.13) implies $\xi \in J_0 \otimes \mathbb{Z}_p$. This completes the proof. □

Let $\xi = \sum_{\alpha \in C_I^{(1,2)}(\pm)} z(\alpha)\alpha$ $(z(\alpha) \in \mathbb{Z}_p)$ be any element of $R^{(1,2)} \otimes \mathbb{Z}_p$. Then $\deg(\xi) = 0$ if and only if ξ is of the form $\sum_{\alpha \neq 1,\, \in C_I^{(1,2)}(\pm)} z(\alpha)(\alpha - 1)$, so that ξ is determined by the elements $z(\alpha)$ with $\alpha \neq 1$, $\in C_I^{(1,2)}(\pm)$. Moreover, by Proposition 7.3, we have $\xi \in J_0 \otimes \mathbb{Z}_p$ if and only if these elements $z(\alpha)$ $(\alpha \neq 1, \in C_I^{(1,2)}(\pm))$ satisfy the congruence

$$\sum_{\alpha\neq 1,\,\in C_I^{(1)}(\pm)} (a(\alpha)^2-1)z(\alpha) + \sum_{\alpha\in C_I^{(2)}(\pm)} (2a(\alpha)^2-1)z(\alpha) \equiv 0 \pmod p. \tag{7.14}$$

Put $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Let V be the vector space over $\mathbb{F}_p$ of all $\mathbb{F}_p$-valued functions on the set $C_I^{(1,2)}(\pm)\setminus\{1\}$. For two elements f, g of V, we define the inner product (f,g) by

$$(f,g) = \sum_{\alpha\in C_I^{(1,2)}(\pm)-\{1\}} f(\alpha)g(\alpha). \tag{7.15}$$

For any element $\xi = \sum_{\alpha\neq 1,\,\in C_I^{(1,2)}(\pm)} z(\alpha)(\alpha-1)$ of $J_0\otimes\mathbb{Z}_p$, we define a function $f_\xi\in V$ by

$$f_\xi(\alpha) = z(\alpha) \pmod p \text{ for all } \alpha\in C_I^{(1,2)}(\pm)\setminus\{1\}, \tag{7.16}$$

and denote by X the subspace of V consisting of all functions f_ξ with $\xi\in J_0\otimes\mathbb{Z}_p$. We define a function $f_a\in V$ by

$$f_a(\alpha) = \begin{cases} (a(\alpha)^2-1) \pmod p & \text{if } \alpha\in C_I^{(1)}(\pm)\setminus\{1\},\\ (2a(\alpha)^2-1) \pmod p & \text{if } \alpha\in C_I^{(2)}(\pm). \end{cases} \tag{7.17}$$

The function f_a is not 0 because $f_a([2]) = 1$. We denote by Y the one-dimensional subspace $\mathbb{F}_p f_a$ of V.

A function $f\in V$ belongs to X if and only if it satisfies the condition (7.14) with $z(\alpha) \pmod p = f(\alpha)$, which is equivalent to $(f,f_a)=0$. Therefore, the space X is the orthogonal complement of the space Y.

Let χ be a character of $C_I^{(1,2)}(\pm)$. We define a function $f_\chi\in V$ by

$$f_\chi(\alpha) = (\chi(\alpha)-1) \pmod p \text{ for all } \alpha\in C_I^{(1,2)}(\pm)\setminus\{1\}. \tag{7.18}$$

Let $\xi = \sum_{\alpha\neq 1,\,\in C_I^{(1,2)}(\pm)} z(\alpha)(\alpha-1)$ be an element of $J_0\otimes\mathbb{Z}_p$. Then by the definition (7.4) of $\chi(\xi)$ we have

$$\chi(\xi) \pmod p = (f_\chi, f_\xi). \tag{7.19}$$

Let q be any prime. Let $\omega_q : (\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{Z}_q^\times$ be the Teichmüller character with respect to q, i.e., ω_q is the unique homomorphism of $(\mathbb{Z}/q\mathbb{Z})^\times$ to $\mathbb{Z}_q^\times$ such that its values are $(q-1)$st roots of 1 and it satisfies

$$\omega_q\,(a \bmod q) \equiv a \pmod q \tag{7.20}$$

for all $a\in\mathbb{Z}$ with $(a,q)=1$. It is also well-known that the following holds:

$$\omega_q\,(a \bmod q) \equiv a^{q^n} \pmod{q^{n+1}} \tag{7.21}$$

for all $a \in \mathbb{Z}$ with $(a,q)=1$ and $n \geq 0, \in \mathbb{Z}$.

Put $\omega = \omega_p$. As is well-known $\omega(-1) = -1$, hence ω^2 is a character of $(\mathbb{Z}/p\mathbb{Z})^\times/\{\pm 1\}$. Since the group $C_I^{(1)}(\pm)$ can be identified with $(\mathbb{Z}/p\mathbb{Z})^\times/\{\pm 1\}$, we regard ω^2 as a character of $C_I^{(1)}(\pm)$.

Let χ be a character of $C_I^{(1,2)}(\pm)$ such that its restriction to $C_I^{(1)}(\pm)$ coincides with ω^2. Since $[2]^2$ is an element of $C_I^{(1)}(\pm)$ represented by the matrix $\left(\begin{smallmatrix} 2+p & 0 \\ 0 & 2+p \end{smallmatrix}\right)$, we have $\chi^2([2]) = \chi([2]^2) = \omega^2(2+p) = \omega^2(2)$, whence $\chi([2]) = \pm\omega(2)$. We denote by χ_ω the character of $C_I^{(1,2)}(\pm)$ defined by the following equalities:

$$\chi_\omega \mid C_I^{(1)}(\pm) = \omega^2 \text{ and } \chi_\omega([2]) = \omega(2). \tag{7.22}$$

LEMMA 7.4. *The function f_{χ_ω} coincides with the function f_a.*

PROOF. If $\alpha \in C_I^{(1)}(\pm) \setminus \{1\}$, then $f_{\chi_\omega}(\alpha) = (\chi_\omega(\alpha) - 1) \pmod p = (\omega^2(\alpha) - 1) \pmod p = (\omega^2(a(\alpha) \bmod p) - 1) \pmod p$. By (7.20) we have $\omega(a(\alpha) \bmod p) \equiv a(\alpha) \pmod p$. Hence $f_{\chi_\omega}(\alpha) = (a(\alpha)^2 - 1) \pmod p = f_a(\alpha)$. If $\alpha \in C_I^{(2)}(\pm)$, then α is represented by the matrix $\langle a(\alpha)\rangle[2]$ where $\langle a(\alpha)\rangle = \left(\begin{smallmatrix} a(\alpha) & 0 \\ 0 & a(\alpha) \end{smallmatrix}\right)$. Hence we have $f_{\chi_\omega}(\alpha) = (\chi_\omega(\langle a(\alpha)\rangle[2]) - 1) \pmod p = (\chi_\omega(\langle a(\alpha)\rangle)\chi_\omega([2]) - 1) \pmod p = (\omega^2(a(\alpha) \bmod p)\omega(2) - 1) \pmod p$. Since $\omega(2) \equiv 2 \pmod p$ by (7.20), we have $f_{\chi_\omega}(\alpha) = (2a(\alpha)^2 - 1) \pmod p = f_a(\alpha)$. This completes the proof. □

LEMMA 7.5. *Let χ_i $(i = 1, 2)$ be two characters of $C_I^{(1,2)}(\pm)$. If $f_{\chi_1} = f_{\chi_2}$, then $\chi_1 = \chi_2$. In particular, if $\chi \neq 1$, then $f_\chi \neq 0$.*

PROOF. If $f_{\chi_1} = f_{\chi_2}$, then $\chi_1(\alpha) \equiv \chi_1(\alpha) \pmod p$ for all $\alpha \in C_I^{(1,2)}(\pm)$, hence $(\chi_1\chi_2^{-1})(\alpha) \equiv 1 \pmod p$ for all $\alpha \in C_I^{(1,2)}(\pm)$. Since the $(p-1)$st roots of 1 are the representatives of $\mathbb{Z}_p^\times/(1+p\mathbb{Z}_p)$, we have $\chi_1\chi_2^{-1} = 1$, i.e., $\chi_1 = \chi_2$. In particular, since $f_1 = 0$, if $\chi \neq 1$, then $f_\chi \neq f_1 (= 0)$. This completes the proof. □

Now we can determine the ideal $\chi(J_0 \otimes \mathbb{Z}_p)$.

PROPOSITION 7.6. *Let χ be a non-trivial character of $C_I^{(1,2)}(\pm)$. Then the ideal $\chi(J_0 \otimes \mathbb{Z}_p)$ of $\mathbb{Z}_p$ is $p\mathbb{Z}_p$ or $\mathbb{Z}_p$ according as $\chi = \chi_\omega$ or $\neq \chi_\omega$ respectively.*

PROOF. Assume that $\chi(J_0 \otimes \mathbb{Z}_p) \subset p\mathbb{Z}_p$. Then $\chi(\xi) \pmod p = 0$ for all $\xi \in J_0 \otimes \mathbb{Z}_p$. By (7.19) we have $(f_\chi, f) = 0$ for all $f \in X$, hence f_χ belongs to the orthogonal complement of X. On the other hand X is the orthogonal complement of the space $Y = \mathbb{F}_p f_a$. Therefore f_χ is an element of $\mathbb{F}_p f_a$, i.e., there exists an element $c \in \mathbb{F}_p$ such that $f_\chi = cf_a$. Considering the values at $[2]$, we have $f_\chi([2]) = cf_a([2])$, i.e., $(\chi([2]) - 1) \pmod p = c(2-1)$, hence $\chi([2]) \pmod p = c + 1$. Again considering the values at $[2]^2$, we have $f_\chi([2]^2) = cf_a([2]^2)$, i.e., $(\chi([2]^2) - 1) \pmod p = c((2+p)^2 - 1) \pmod p$, hence $\chi([2]^2) \pmod p = 3c + 1$. Since $\chi([2]^2) \pmod p = (\chi([2]) \pmod p))^2$, we have $3c + 1 = (c+1)^2$, i.e., $c(c-1) = 0$, hence $c = 0$ or 1. If $c = 0$, then $f_\chi = 0$. Since χ is non-trivial, this is a contradiction by Lemma 7.5. Therefore we have $c = 1$, i.e., $f_\chi = f_a$. By Lemma 7.4 we have $f_a = f_{\chi_\omega}$, hence $f_\chi = f_{\chi_\omega}$, which implies that $\chi = \chi_\omega$

by Lemma 7.5. This proves that if $\chi \neq \chi_\omega$ then $\chi(J_0 \otimes \mathbb{Z}_p) = \mathbb{Z}_p$. Let $\chi = \chi_\omega$. Since $\chi_\omega(\xi) \pmod p = (f_{\chi_\omega}, f_\xi) = (f_a, f_\xi) = 0$ for all $\xi \in J_0 \otimes \mathbb{Z}_p$, we have $\chi_\omega(J_0 \otimes \mathbb{Z}_p) \subset p\mathbb{Z}_p$. Put $\xi = p([2]-1) \in J_0 \otimes \mathbb{Z}_p$. Then $\chi_\omega(\xi) = p(\chi_\omega([2]) - 1) = p(\omega(2) - 1)$. By (7.20) we have $\omega(2) - 1 \equiv 1 \pmod p$, i.e., $\omega(2) - 1 \in \mathbb{Z}_p^\times$, which implies that $\chi_\omega(J_0 \otimes \mathbb{Z}_p) = p\mathbb{Z}_p$. This completes the proof. □

7.3. The number $\chi(\theta)$.

Here we study the number $\chi(\theta)$.

Let χ be a non-trivial character of $C_I^{(1,2)}(\pm)$. Let ψ_χ be the character of $(\mathbb{Z}/p\mathbb{Z})^\times$ associated with χ as defined in the proof of Proposition 4.4. Let χ_0 be the character of $C_I^{(1,2)}(\pm)$ which is trivial on $C_I^{(1)}(\pm)$ and satisfies $\chi_0([2]) = -1$. Then by (4.5) we have

$$\chi(\theta) = \begin{cases} \left(\dfrac{1}{4} B_{2,\,\psi_\chi^{-1}}\right)(2 + \chi([2])) & \text{if } \chi \mid C_I^{(1)}(\pm) \neq 1, \\ -\dfrac{1}{24}(p^2 - 1) & \text{if } \chi = \chi_0. \end{cases} \tag{7.23}$$

Proposition 7.7. *Let χ_0 be as above. Then $\mathcal{C}_{\mathbb{Q},p}(\chi_0) = 0$.*

Proof. By (7.9) we have $\mathcal{C}_{\mathbb{Q},p}(\chi_0) \cong \mathbb{Z}_p/(\chi_0(J_0 \otimes \mathbb{Z}_p)\chi_0(\theta))$. Since $\chi_0(J_0 \otimes \mathbb{Z}_p) = \mathbb{Z}_p$ by Proposition 7.6 and $\chi_0(\theta) \in \mathbb{Z}_p^\times$ by (7.23), we have the proof. □

By Proposition 7.7, in order to study the χ-eigen component, it is sufficient to consider the case where the restriction of χ to $C_I^{(1)}(\pm)$ is non-trivial. Let χ be a character of $C_I^{(1,2)}(\pm)$ such that $\chi \mid C_I^{(1)}(\pm) \neq 1$. Since any character of $(\mathbb{Z}/p\mathbb{Z})^\times$ into $\mathbb{Z}_p^\times$ can be expressed as a power of ω, we can write

$$\chi \mid C_I^{(1)}(\pm) = \omega^{2k} \text{ with } 1 \leq k \leq \frac{1}{2}(p-3)\ (k \in \mathbb{Z}). \tag{7.24}$$

Since $\chi([2])^2 = \chi([2]^2) = \omega^{2k}([2]^2) = \omega^{2k}(2)$, we have

$$\chi([2]) = \pm\omega(2)^k. \tag{7.25}$$

We denote by $\chi_{k,+}$ (respectively $\chi_{k,-}$) the character χ which satisfies the condition (7.24) and $\chi([2]) = \omega(2)^k$ (respectively $\chi([2]) = -\omega(2)^k$). Also we denote by $\mathcal{C}_{\mathbb{Q},p}(k,+)$ (respectively $\mathcal{C}_{\mathbb{Q},p}(k,-)$) the eigen component $\mathcal{C}_{\mathbb{Q},p}(\chi_{k,+})$ (respectively $\mathcal{C}_{\mathbb{Q},p}(\chi_{k,-})$). Then we have

$$\mathcal{C}_{\mathbb{Q},p} = \bigoplus_{k=1}^{(p-3)/2} \mathcal{C}_{\mathbb{Q},p}(k,+) \oplus \bigoplus_{k=1}^{(p-3)/2} \mathcal{C}_{\mathbb{Q},p}(k,-). \tag{7.26}$$

7.3.1. The study of $2 + \chi([2])$.

Here we study the number $2 + \chi([2])$. Let δ be the order of 2 in the group $(\mathbb{Z}/p\mathbb{Z})^\times$.

Lemma 7.8. *Let q be any prime. Let a and x be integers. Let n be a non-negative*

integer. Then if $x \equiv a \pmod q$*, then* $x^{q^n} \equiv a^{q^n} \pmod{q^{n+1}}$.

PROOF. Cf. Ireland and Rosen [**5**, Chapter 4, Lemma 3]. □

LEMMA 7.9. *Let* $\chi = \chi_{k,+}$*. Then we have* $2 + \chi([2]) \in p\mathbb{Z}_p$ *if and only if* δ *is even and* $k = 1 + \delta_1 l$ *with* $\delta_1 = \delta/2$ *and* l *an odd integer.*

PROOF. Assume that δ is even and $k = 1 + \delta_1 l$ with $\delta_1 = \delta/2$ and l a positive, odd integer. Then $2^{\delta_1} \equiv -1 \pmod p$. Since $\omega(2)^k \equiv 2^k = 2^{1+\delta_1 l} \pmod p$ by (7.20), we have $2 + \chi([2]) = 2 + \omega(2)^k \equiv 2(1 + 2^{\delta_1 l}) \equiv 2\{1 + (-1)^l\} \pmod p$. Since l is odd, we have $2 + \chi([2]) \equiv 0 \pmod p$. This proves the if part.

Conversely, assume that $2 + \chi([2]) = 2 + \omega(2)^k \equiv 0 \pmod p$. Then, by (7.20), we have $2 + 2^k \equiv 2(1 + 2^{k-1}) \equiv 0 \pmod p$, i.e., $2^{k-1} \equiv -1 \pmod p$. Since $2^{2(k-1)} \equiv 1 \pmod p$, we have $2(k-1) \equiv 0 \pmod \delta$. If δ is odd, then $k - 1 \equiv 0 \pmod \delta$, hence we have $2^{k-1} \equiv 1 \pmod p$. This contradicts the congruence $2^{k-1} \equiv -1 \pmod p$, therefore δ is even. Put $\delta = 2\delta_1$. Since $2(k-1) \equiv 0 \pmod{2\delta_1}$, we have $k - 1 \equiv 0 \pmod{\delta_1}$. Put $k = 1 + \delta_1 l$ with $l \geq 0, \in \mathbb{Z}$. Then $2^{k-1} \equiv 2^{\delta_1 l} \equiv (2^{\delta_1})^l \pmod p$. Since $2^{\delta_1} \equiv -1 \pmod p$, we have $-1 \equiv (-1)^l \pmod p$. This implies that l is odd, and the only-if part is proved. □

LEMMA 7.10. *Let* $\chi = \chi_{k,-}$*. Then we have* $2 + \chi([2]) \in p\mathbb{Z}_p$ *if and only if* $k \equiv 1 \pmod \delta$.

PROOF. Since $\omega(2)^k \equiv 2^k \pmod p$ by (7.20), we have $2 + \chi([2]) = 2 - \omega(2)^k \equiv 2 - 2^k \equiv 2(1 - 2^{k-1}) \pmod p$. Therefore, $2 + \chi([2]) \equiv 0 \pmod p$ if and only if $2^{k-1} \equiv 1 \pmod p$. Since this is equivalent to $k \equiv 1 \pmod \delta$, we have the proof. □

As mentioned in Introduction, a prime q is called a *Wieferich prime* if it satisfies

$$2^{q-1} \equiv 1 \pmod{q^2}. \tag{7.27}$$

Although the number of Wieferich primes is believed to be infinite, the only ones that have been discovered so far are 1093 and 3511. Knauer and Richstein [**7**] reported that there are no other Wieferich primes less than $1.25 \cdot 10^{15}$.

DEFINITION 7.11. Let q be a prime. If there exists the greatest integer $n \geq 0$ that satisfies

$$2^{q^n - 1} \equiv 1 \pmod{q^{n+1}}, \tag{7.28}$$

then we denote it by $W(q)$.

PROPOSITION 7.12. *Let* q *be a prime. Then we have the following.*

(1) *The integer* $W(q)$ *exists.*
(2) *If* n *is an integer satisfying* $0 \leq n \leq W(q)$*, then* $2^{q^n - 1} \equiv 1 \pmod{q^{n+1}}$.
(3) *The prime* q *is a Wieferich prime if and only if* $W(q) \geq 1$.

PROOF. (1) There exists at least one integer $n \geq 0$ which satisfies (7.28) because it holds with $n = 0$. Assume that there is an infinite sequence of integers $0 \leq n_1 < n_2 < \cdots < n_k < \cdots$ such that all n_k satisfy the congruence (7.28). Then $2^{q^{n_k}} \equiv 2 \pmod{q^{n_k+1}}$ for all n_k. Let ω_q be the Teichmüller character with respect to q. Since we have $\omega_q(2) = \lim_{k\to\infty} 2^{q^{n_k}}$ by (7.21), the validity of the congruence for all n_k implies $\omega_q(2) = 2$. Since $\omega_q(2)$ is a $(q-1)$st root of 1, we have $2^{q-1} = 1$, which is a contradiction. Therefore, there exists the greatest integer $n \geq 0$. This proves (1).

(2) It is sufficient to prove that the congruence $2^{q^{n+1}-1} \equiv 1 \pmod{q^{n+2}}$ implies the congruence $2^{q^n-1} \equiv 1 \pmod{q^{n+1}}$ for $n \geq 0$. If $q = 2$, then $2^{q^{n+1}-1} \not\equiv 1 \pmod{q^{n+2}}$ for any $n \geq 0$. Therefore we can assume that $q \neq 2$. Since $2^q \equiv 2 \pmod{q}$, we have $2^{q^{n+1}} \equiv 2^{q^n} \pmod{q^{n+1}}$ by Lemma 7.8. Since $q \neq 2$, we have $2^{q^{n+1}-1} \equiv 2^{q^n-1} \pmod{q^{n+1}}$. Combining this with the assumption $2^{q^{n+1}-1} \equiv 1 \pmod{q^{n+2}}$, we have $2^{q^n-1} \equiv 1 \pmod{q^{n+1}}$. This proves (2).

(3) This follows from (2) immediately. □

Now we determine the p-order of $2 + \chi([2])$.

PROPOSITION 7.13. *Let $\chi = \chi_{k,+}$ $(1 \leq k \leq (1/2)(p-3))$. Let δ and $W(p)$ be as above. Then we have the following.*

(1) *If δ is even and $k = 1 + \delta_1 l$ with $\delta_1 = \delta/2$ and l an odd integer, then $2 + \chi([2]) \in p^{W(p)+1}\mathbb{Z}_p^\times$.*
(2) *Otherwise, $2 + \chi([2]) \in \mathbb{Z}_p^\times$.*

PROOF. (2) follows from Lemma 7.9. We prove (1). By (7.21), $2 + \chi([2]) = 2 + \omega(2)^k \equiv 2 + 2^{kp^n} \equiv 2(1 + 2^{p^n-1} \cdot 2^{\delta_1 l p^n}) \pmod{p^{n+1}}$ for any $n \geq 0$, $\in \mathbb{Z}$. Since $2^{\delta_1} \equiv -1 \pmod{p}$, we have $2^{\delta_1 p^n} \equiv (-1)^{p^n} \equiv -1 \pmod{p^{n+1}}$ by Lemma 7.8. Hence, since l is odd, we have $2^{\delta_1 l p^n} \equiv -1 \pmod{p^{n+1}}$, therefore $2 + \chi([2]) \equiv 2(1 - 2^{p^n-1}) \pmod{p^{n+1}}$. This implies that $2 + \chi([2]) \equiv 0 \pmod{p^{n+1}}$ or $\not\equiv 0 \pmod{p^{n+1}}$ according as $n \leq W(p)$ or $> W(p)$, which completes the proof. □

PROPOSITION 7.14. *Let $\chi = \chi_{k,-}$ $(1 \leq k \leq (1/2)(p-3))$. Let δ and $W(p)$ be as above. Then we have the following.*

(1) *If $k \equiv 1 \pmod{\delta}$, then $2 + \chi([2]) \in p^{W(p)+1}\mathbb{Z}_p^\times$.*
(2) *Otherwise, $2 + \chi([2]) \in \mathbb{Z}_p^\times$.*

PROOF. (2) follows from Lemma 7.10. We prove (1). By the assumption we write $k = 1 + \delta l$ with $l \in \mathbb{Z}$. Then, by (7.21), $2 + \chi([2]) = 2 - \omega(2)^k \equiv 2 - 2^{kp^n} \equiv 2(1 - 2^{p^n-1} \cdot 2^{\delta l p^n}) \pmod{p^{n+1}}$. Since $2^\delta \equiv 1 \pmod{p}$, we have $2^{\delta p^n} \equiv 1 \pmod{p^{n+1}}$ by Lemma 7.8, hence $2^{\delta l p^n} \equiv 1 \pmod{p^{n+1}}$. Thus we have $2 + \chi([2]) \equiv 2(1 - 2^{p^n-1}) \pmod{p^{n+1}}$. This implies that $2 + \chi([2]) \equiv 0 \pmod{p^{n+1}}$ or $\not\equiv 0 \pmod{p^{n+1}}$ according as $n \leq W(p)$ or $> W(p)$, which completes the proof. □

7.3.2. Properties of generalized Bernoulli numbers.

Let μ be an even Dirichlet character of conductor p with values in $\mathbb{Z}_p^\times$. Here we summarize some properties of the generalized Bernoulli numbers $B_{2,\mu}$.

PROPOSITION 7.15. *Let $\mu = \omega^{2a}$ $(1 \leq a \leq (p-3)/2,\ a \in \mathbb{Z})$. Then we have the following.*

(1) *If $a = (p-3)/2$, then*

$$B_{2,\mu} \in -\frac{1}{p} + \mathbb{Z}_p.$$

(2) *If $1 \leq a \leq (p-5)/2$, then $B_{2,\mu} \in \mathbb{Z}_p$, and for any $l \geq 0$, $\in \mathbb{Z}$, we have*

$$B_{2,\mu} \equiv \frac{1}{ap^l+1} B_{2ap^l+2} \pmod{p^{l+1}\mathbb{Z}_p}.$$

PROOF. (1) Since $\omega^{2a} = \omega^{-2}$, this is the case $n = 2$ of Washington [**22**, Exercise 7.6 (d)]. (2) In [**22**, Exercise 7.5] we replace the notation a by l, and put $m = 2$, $n = 2ap^l + 2$ and $\chi = \omega^n$. Since $n \equiv 2a + 2 \not\equiv 0 \pmod{p-1}$, we have $\chi \neq 1$. Also since $m \equiv n \pmod{p^l}$, we have, by this exercise, the congruence

$$\bigl(1 - (\chi\omega^{-m})(p) \cdot p^{m-1}\bigr) \frac{B_{m,\,\chi\omega^{-m}}}{m} \equiv \bigl(1 - (\chi\omega^{-n})(p) \cdot p^{n-1}\bigr) \frac{B_{n,\,\chi\omega^{-n}}}{n} \pmod{p^{l+1}}.$$

Since $\chi\omega^{-m} = \omega^{2ap^l} = \omega^{2a} \neq 1$, we have $(\chi\omega^{-m})(p) = 0$. Since $\chi\omega^{-n} = 1$, we have $(\chi\omega^{-n})(p) = 1$, and $1 - (\chi\omega^{-n})(p) \cdot p^{n-1} = 1 - p^{n-1}$. Since $n - 1 = 2ap^l + 1 > (1+1)^l \geq l + 1$, we have $1 - p^{n-1} \equiv 1 \pmod{p^{l+1}}$. Thus we have

$$\frac{B_{2,\mu}}{2} \equiv \frac{B_{n,1}}{n} = \frac{1}{2ap^l+2} B_{2ap^l+2} \pmod{p^{l+1}\mathbb{Z}_p},$$

which proves (2). □

7.3.3. The study of $B_{2,\psi_\chi^{-1}}$.

Here we study the number $B_{2,\psi_\chi^{-1}}$.

DEFINITION 7.16. Let q be a prime $\neq 2, 3$. Let a be an integer with $1 \leq a \leq (q-3)/2$. If there exists the greatest integer $n \geq 1$ that satisfies

$$B_{(2a-2)q^{n-1}+2} \equiv 0 \pmod{q^n\mathbb{Z}_q}, \tag{7.29}$$

then we denote it by $B(q, 2a)$. If there are no integers n which satisfy the congruence above, then put $B(q, 2a) = 0$.

Let q be a prime $\neq 2, 3$. If $B_{2a} \equiv 0 \pmod{q\mathbb{Z}_q}$ for $0 < 2a < q - 1$, then the pair $(q, 2a)$ is called an *irregular pair*. The congruence (7.29) with $a = 1$ does not hold for any $n \geq 1$ because $B_2 = 1/6$. Hence we have $B(q, 2) = 0$ for any $q \neq 2, 3$.

PROPOSITION 7.17. *Let q be a prime $\neq 2, 3$. Let a be an integer with $1 \leq a \leq (q-3)/2$.*

(1) *The integer $B(q,2a)$ exists.*
(2) *If $B(q,2a) \geq 1$ and n is an integer satisfying $1 \leq n \leq B(q,2a)$, then $B_{(2a-2)q^{n-1}+2} \equiv 0 \pmod{q^n\mathbb{Z}_q}$.*
(3) *The pair $(q,2a)$ is an irregular pair if and only if $B(q,2a) \geq 1$.*

PROOF. (1) Assume that the integer $B(q,2a)$ does not exist. Then $a \neq 1$, i.e., $a \geq 2$, and there is an infinite sequence of integers $1 \leq n_1 < n_2 < \cdots < n_k < \cdots$ such that all n_k satisfy the congruence (7.29) with $n = n_k$. Let $\mu = \omega_q^{2a-2}$. Then by (2) of Proposition 7.15, we have

$$B_{2,\mu} \equiv \frac{1}{(a-1)q^{n_k-1}+1} B_{(2a-2)q^{n_k-1}+2} \equiv 0 \pmod{q^{n_k}\mathbb{Z}_q}$$

for all n_k, which implies that $B_{2,\mu} = 0$. Since $B_{2,\mu} \neq 0$ as is well-known, this is a contradiction. Therefore, the number of the integers $n \geq 1$ that satisfy (7.29) is finite. This proves (1).

(2) It is sufficient to prove that the congruence $B_{(2a-2)q^l+2} \equiv 0 \pmod{q^{l+1}\mathbb{Z}_q}$ implies the congruence $B_{(2a-2)q^{l-1}+2} \equiv 0 \pmod{q^l\mathbb{Z}_q}$ for $l \geq 1$. Put $m = (2a-2)q^{l-1}+2$ and $n = (2a-2)q^l+2$. Since $m \not\equiv 0 \pmod{q-1}$ and $m \equiv n \pmod{(q-1)q^{l-1}}$, by the Kummer congruences [**5**, Chapter 15, Theorem 5] we have

$$(1-q^{m-1})\frac{B_m}{m} \equiv (1-q^{n-1})\frac{B_n}{n} \pmod{q^l\mathbb{Z}_q}.$$

Combining this with $B_n = B_{(2a-2)q^l+2} \equiv 0 \pmod{q^{l+1}\mathbb{Z}_q}$, we have $B_m = B_{(2a-2)q^{l-1}+2} \equiv 0 \pmod{q^l\mathbb{Z}_q}$. This proves (2).

(3) This follows from (2). □

Now we consider the case $q = p$.

PROPOSITION 7.18. *Let $\mu = \omega^{2a}$ $(1 \leq a \leq (p-5)/2,\ a \in \mathbb{Z})$. Then $B_{2,\mu} \in p^{B(p,2a+2)}\mathbb{Z}_p^\times$.*

PROOF. Assume that $B(p,2a+2) = 0$. Then $(p,2a+2)$ is not an irregular pair, i.e., $B_{2a+2} \not\equiv 0 \pmod{p\mathbb{Z}_p}$. By (2) of Proposition 7.15 we have $B_{2,\mu} \equiv (1/(a+1))B_{2a+2} \pmod{p\mathbb{Z}_p}$. This implies that $B_{2,\mu} \not\equiv 0 \pmod{p\mathbb{Z}_p}$, i.e., $B_{2,\mu} \in \mathbb{Z}_p^\times$. Next, assume that $B(p,2a+2) \geq 1$. By (2) of Proposition 7.15 we have $B_{2,\mu} \equiv (1/(ap^{l-1}+1))B_{2ap^{l-1}+2} \pmod{p^l\mathbb{Z}_p}$ for $l \geq 1$. This implies that $B_{2,\mu} \equiv 0 \pmod{p^l\mathbb{Z}_p}$ or $\not\equiv 0 \pmod{p^l\mathbb{Z}_p}$ according as $l \leq B(p,2a+2)$ or $> B(p,2a+2)$, which proves $B_{2,\mu} \in p^{B(p,2a+2)}\mathbb{Z}_p^\times$. This completes the proof. □

The following proposition determines the p-order of $B_{2,\psi_\chi^{-1}}$.

PROPOSITION 7.19. *Let $\chi = \chi_{k,+}$ or $\chi_{k,-}$ $(1 \leq k \leq (1/2)(p-3))$. Then we have the following.*

(1) *If $k = 1$, then $B_{2,\psi_\chi^{-1}} \in -(1/p) + \mathbb{Z}_p$.*

(2) *If* $2 \le k \le (1/2)(p-3)$, *then* $B_{2,\psi_\chi^{-1}} \in p^{B(p,p+1-2k)}\mathbb{Z}_p^\times$.

PROOF. Since $\psi_\chi^{-1} = \omega^{-2k} = \omega^{p-1-2k}$, put $2a = p-1-2k$. Then $1 \le a \le (1/2)(p-3)$, and $a = (1/2)(p-3)$ if and only if $k = 1$. (1) follows from (1) of Proposition 7.15. (2) follows from Proposition 7.18 because $2a+2 = p+1-2k$. This completes the proof. □

7.3.4. The determination of $B(p,2a)$ for all irregular pairs $(p,2a)$ with $p \le 4001$.

In [**22**, Section 2 of Tables] all irregular pairs $(p,2a)$ with $p \le 4001$ are given. We can determine the values of $B(p,2a)$ for all of them by a method explained in this subsubsection. The result is the following.

EXAMPLE 7.20. For all irregular pairs $(p,2a)$ with $p \le 4001$, we have $B(p,2a) = 1$.

In the following we explain the method of computation. Let m and n be positive integers. We define $S_m(n)$ by

$$S_m(n) = \sum_{k=0}^{n-1} k^m. \tag{7.30}$$

Then we have the following well-known equality (cf. [**5**, Theorem 1 in Chapter 15]):

$$(m+1)S_m(n) = \sum_{k=0}^{m} \binom{m+1}{k} B_k n^{m+1-k}. \tag{7.31}$$

PROPOSITION 7.21. *Let* p *be a prime* $\ne 2,3$. *Let* $r \ge 1$ *be an integer satisfying* $2r \not\equiv 0 \pmod{p-1}$. *Let* $l \ge 0$ *be an integer. Put* $m = 2rp^l + 2$. *Then*

$$pB_m \equiv S_m(p) \pmod{p^{l+3}\mathbb{Z}_p}.$$

PROOF. If we put $n = p$ in the equality (7.31) and divide it by $m+1$, we have

$$pB_m = S_m(p) - \sum_{k=0}^{m-1} \frac{1}{m+1}\binom{m+1}{k} B_k p^{m+1-k}.$$

Since m is even with $m \ge 4$, the integer $m-1$ is odd with $m-1 \ge 3$, whence $B_{m-1} = 0$. Since

$$\frac{1}{m+1}\binom{m+1}{k} B_k p^{m+1-k} = \frac{1}{m+1}\binom{m+1}{h} B_{m+1-h} p^h$$

with $h = m+1-k$, put

$$D_h = \frac{1}{m+1}\binom{m+1}{h} B_{m+1-h} p^h.$$

Then we have $pB_m = S_m(p) - D$, where $D = \sum_{h=3}^{m+1} D_h$.

As to the term D_3 we have

$$D_3 = \frac{m(m-1)}{6} p^3 B_{m-2}. \tag{7.32}$$

Since $m - 2 = 2rp^l \equiv 2r \not\equiv 0 \pmod{p-1}$, we have $B_{m-2} \in (m-2)\mathbb{Z}_p$ by a result of Adams [**5**, Proposition 15.2.4], whence $B_{m-2} \in p^l\mathbb{Z}_p$. Since $p \neq 2, 3$, we have

$$D_3 \in p^{l+3}\mathbb{Z}_p \tag{7.33}$$

by (7.32).

As to the terms D_h with $h \geq 4$ we have

$$D_h = (m-2)\frac{p^{h-1}}{h(h-1)(h-2)(h-3)} m(m-1)\binom{m-3}{h-4} pB_{m+1-h}. \tag{7.34}$$

We prove that

$$\frac{p^{h-1}}{h(h-1)(h-2)(h-3)} \in p^3\mathbb{Z}_p. \tag{7.35}$$

In fact, if the integers $h - i$ $(0 \leq i \leq 3)$ are all prime to p, then (7.35) holds because $h - 1 \geq 3$. Let one of the integers $h - i$ $(0 \leq i \leq 3)$ be a multiple of p. Since $p \geq 5$, only one of them is divisible by p and the others are prime to p. Let $h - i = p^e q$ where e and q are positive integers and $(q, p) = 1$. Then the p-order of the number of (7.35) is $(h-1) - e$, for which we have

$$\begin{aligned}(h-1) - e &= p^e q + i - 1 - e \geq (1+4)^e - 1 - e \\ &\geq 1 + 4e - 1 - e = 3e \geq 3.\end{aligned}$$

This proves (7.35). Since $m - 2 \in p^l\mathbb{Z}$ and $pB_{m+1-h} \in \mathbb{Z}_p$, combining these with (7.35), we have

$$D_h \in p^{l+3}\mathbb{Z}_p \tag{7.36}$$

by (7.34).

By (7.33) and (7.36) we have $D \in p^{l+3}\mathbb{Z}_p$. This completes the proof. □

Though it is difficult to determine the value of $B(p, 2a)$ by its definition, the following proposition gives a useful method. Since $B(p, 2) = 0$, it is sufficient to consider the case $a \geq 2$.

PROPOSITION 7.22. *Let a be an integer with $2 \leq a \leq (p-3)/2$, and assume that the pair $(p, 2a)$ is an irregular pair. Let $l \geq 0$ be an integer. Let $m_l = (2a-2)p^l + 2$. Then we have the following.*

(1) *If* $S_{m_l}(p) \equiv 0 \pmod{p^{l+2}}$, *then* $B(p,2a) \geq l+1$.
(2) *If* $S_{m_l}(p) \not\equiv 0 \pmod{p^{l+2}}$, *then* $B(p,2a) \leq l$.
(3) *If* $S_{m_l}(p) \equiv 0 \pmod{p^{l+2}}$ *and* $S_{m_{l+1}}(p) \not\equiv 0 \pmod{p^{l+3}}$, *then* $B(p,2a) = l+1$.

PROOF. Since $2a-2 \not\equiv 0 \pmod{p-1}$, by Proposition 7.21, we have $B_{m_l} \equiv 0 \pmod{p^{l+1}\mathbb{Z}_p}$ or $\not\equiv 0 \pmod{p^{l+1}\mathbb{Z}_p}$ according as $S_{m_l}(p) \equiv 0 \pmod{p^{l+2}}$ or $\not\equiv 0 \pmod{p^{l+2}}$ respectively. By Definition 7.16 and Proposition 7.17, these hold according as $B(p,2a) \geq l+1$ or $\leq l$. Thus we have (1) and (2). (3) follows from (1) and (2). □

COROLLARY 7.23. *Let* a *be an integer with* $2 \leq a \leq (p-3)/2$, *and assume that the pair* $(p,2a)$ *is an irregular pair. Let* $m_1 = (2a-2)p+2$. *If* $S_{m_1}(p) \not\equiv 0 \pmod{p^3}$, *then* $B(p,2a) = 1$.

PROOF. Let $m_0 = (2a-2)p^0+2 = 2a$. Then by Proposition 7.21 we have $S_{m_0}(p) \equiv pB_{2a} \pmod{p^3\mathbb{Z}_p}$. Since $(p,2a)$ is an irregular pair, we have $B_{2a} \equiv 0 \pmod{p\mathbb{Z}_p}$, whence $S_{m_0}(p) \equiv 0 \pmod{p^2\mathbb{Z}_p}$. Combining this and the assumption $S_{m_1}(p) \not\equiv 0 \pmod{p^3}$ with (3) of Proposition 7.22, we have the proof. □

We computed the residue of $S_{m_1}(p)$ modulo p^3 for all irregular pairs $(p,2a)$ with $p \leq 4001$, and verified that all of them satisfy that $S_{m_1}(p) \not\equiv 0 \pmod{p^3}$. Hence, by Corollary 7.23, we obtain the result stated in Example 7.20.

7.4. The determination of the Sylow p-subgroup.

Here we determine the structure of the Sylow p-subgroup $\mathcal{C}_{\mathbb{Q},p}$ of $\mathcal{C}_{\mathbb{Q}}$. In view of the decomposition (7.26), it is sufficient to determine the structures of $\mathcal{C}_{\mathbb{Q},p}(k,+)$ and $\mathcal{C}_{\mathbb{Q},p}(k,-)$. As before, let δ be the order of 2 in the group $(\mathbb{Z}/p\mathbb{Z})^\times$. For the notation $W(p)$ (respectively $B(p,2a)$), see Definition 7.11 (respectively Definition 7.16). Then we have the following theorems.

THEOREM 7.24. *Let* k *be an integer with* $1 \leq k \leq (1/2)(p-3)$. *Then the structure of the group* $\mathcal{C}_{\mathbb{Q},p}(k,+)$ *is given as follows.*

(1) *If* $k=1$, *then* $\mathcal{C}_{\mathbb{Q},p}(1,+) = 0$.
(2) *If* $2 \leq k \leq (1/2)(p-3)$, *then*

$$\mathcal{C}_{\mathbb{Q},p}(k,+) \cong \begin{cases} \mathbb{Z}/p^{B(p,p+1-2k)+W(p)+1}\mathbb{Z} & \begin{cases}\text{if } \delta \text{ is even and } k = 1+(\delta/2)l \\ \text{with } l \text{ an odd integer,}\end{cases} \\ \mathbb{Z}/p^{B(p,p+1-2k)}\mathbb{Z} & \text{otherwise.} \end{cases}$$

PROOF. By (7.9) and (7.23), we have

$$\mathcal{C}_{\mathbb{Q},p}(k,+) \cong \mathbb{Z}_p/\big(\chi_{k,+}(J_0 \otimes \mathbb{Z}_p)(2+\chi_{k,+}([2]))B_{2,\psi_{\chi_{k,+}}^{-1}}\big).$$

Since $\chi_\omega = \chi_{1,+}$, by Proposition 7.6, we have $\chi_{k,+}(J_0 \otimes \mathbb{Z}_p) = p\mathbb{Z}_p$ or $\mathbb{Z}_p$ according as $k=1$ or $\neq 1$ respectively. By Proposition 7.13, $2+\chi_{1,+}([2]) \in \mathbb{Z}_p^\times$, and by (1) of Proposition 7.19, $B_{2,\psi_\chi^{-1}} \in -(1/p)+\mathbb{Z}_p$ with $\chi = \chi_{1,+}$. These results imply that

$\chi_{1,+}(J_0 \otimes \mathbb{Z}_p)(2 + \chi_{1,+}([2]))B_{2,\psi_\chi^{-1}} = \mathbb{Z}_p$ with $\chi = \chi_{1,+}$. This proves (1). Let $k \neq 1$. Since $\chi_{k,+}(J_0 \otimes \mathbb{Z}_p) = \mathbb{Z}_p$, the statement (2) follows immediately from Propositions 7.13 and 7.19. □

THEOREM 7.25. *Let k be an integer with $1 \leq k \leq (1/2)(p-3)$. Then the structure of the group $\mathcal{C}_{\mathbb{Q},p}(k,-)$ is given as follows.*

(1) *If $k = 1$, then $\mathcal{C}_{\mathbb{Q},p}(1,-) \cong \mathbb{Z}/p^{W(p)}\mathbb{Z}$.*
(2) *If $2 \leq k \leq (1/2)(p-3)$, then*

$$\mathcal{C}_{\mathbb{Q},p}(k,-) \cong \begin{cases} \mathbb{Z}/p^{B(p,p+1-2k)+W(p)+1}\mathbb{Z} & \text{if } k \equiv 1 \pmod{\delta}, \\ \mathbb{Z}/p^{B(p,p+1-2k)}\mathbb{Z} & \text{otherwise.} \end{cases}$$

PROOF. Since $\chi_{k,-} \neq \chi_\omega (= \chi_{1,+})$, we have $\chi_{k,-}(J_0 \otimes \mathbb{Z}_p) = \mathbb{Z}_p$ by Proposition 7.6. Hence, by (7.9) and (7.23), we have

$$\mathcal{C}_{\mathbb{Q},p}(k,-) \cong \mathbb{Z}_p/\big((2 + \chi_{k,-}([2]))B_{2,\psi_{\chi_{k,-}}^{-1}}\big)\mathbb{Z}_p.$$

By Proposition 7.14, $2+\chi_{1,-}([2]) \in p^{W(p)+1}\mathbb{Z}_p^\times$, and by (1) of Proposition 7.19, $B_{2,\psi_\chi^{-1}} \in -1/p + \mathbb{Z}_p$ with $\chi = \chi_{1,-}$. Hence we have $((2 + \chi_{1,-}([2]))B_{2,\psi_\chi^{-1}})\mathbb{Z}_p = p^{W(p)}\mathbb{Z}_p$ with $\chi = \chi_{1,-}$. This proves (1). Let $k \neq 1$. Then the statement (2) follows immediately from Propositions 7.14 and 7.19. □

When p is regular and is not a Wieferich prime, the Sylow p-subgroup can be completely determined as follows. In the following corollary, we denote by $[x]$ ($x \in \mathbb{R}$) the greatest integer that is less than or equal to x.

COROLLARY 7.26. *Let $p \neq 2, 3$ be a regular prime and not a Wieferich prime. Let $f_1 = [(1/2\delta)(p-5)]$ and $f_2 = [(1/2\delta)(p-5) + 1/2]$. Then*

$$\mathcal{C}_{\mathbb{Q},p} \cong \begin{cases} (\mathbb{Z}/p\mathbb{Z})^{f_1} & \text{if } \delta \text{ is odd,} \\ (\mathbb{Z}/p\mathbb{Z})^{f_1+f_2} & \text{if } \delta \text{ is even.} \end{cases}$$

PROOF. Let $1 \leq k \leq (1/2)(p-3)$. By the assumption we have $W(p) = B(p, p+1-2k) = 0$. Hence, by Theorems 7.24 and 7.25, we have

$$\mathcal{C}_{\mathbb{Q},p}(k,+) \cong \begin{cases} \mathbb{Z}/p\mathbb{Z} & \text{if } \delta \text{ is even and } k = 1 + (\delta/2)l \text{ with } l \text{ an odd integer,} \\ 0 & \text{otherwise,} \end{cases}$$

and

$$\mathcal{C}_{\mathbb{Q},p}(k,-) \cong \begin{cases} \mathbb{Z}/p\mathbb{Z} & \text{if } k \equiv 1 \pmod{\delta} \text{ and } k \geq 2, \\ 0 & \text{otherwise.} \end{cases}$$

Let f_1 be the number of k with $\mathcal{C}_{\mathbb{Q},p}(k,-) \cong \mathbb{Z}/p\mathbb{Z}$. Since in that case $k = 1 + n\delta$ with $n \in \mathbb{N}$ and $k \leq (1/2)(p-3)$, we have $1 \leq n \leq (1/2\delta)(p-5)$, therefore $f_1 = [(1/2\delta)(p-5)]$. If δ is odd, we have $\mathcal{C}_{\mathbb{Q},p}(k,+) = 0$ for all k. This proves the case of odd δ. Let δ be even. Let f_2 be the number of k with $\mathcal{C}_{\mathbb{Q},p}(k,+) \cong \mathbb{Z}/p\mathbb{Z}$. In that case we have $k = 1 + (\delta/2)l$, $l = 2m-1$ with $m \in \mathbb{N}$ and $k \leq (1/2)(p-3)$. Hence we have $1 \leq m \leq (1/2\delta)(p-5)+1/2$, therefore $f_2 = [(1/2\delta)(p-5) + 1/2]$. This proves the case of even δ. □

In the following examples we consider the irregular primes or the Wieferich primes with $p \leq 4001$. In [**22**, Section 2 of Tables] all irregular pairs $(p, 2a)$ with $p \leq 4001$ are given. The only known Wieferich primes are 1093 and 3511. The prime 1093 is regular and the prime 3511 is irregular. First we consider the irregular primes such that $p \leq 4001$ and $p \neq 3511$. For any irregular prime q, the number of the integers a such that $(q, 2a)$ is an irregular pair is called the *index of irregularity* of q. We denote it by $I(q)$.

EXAMPLE 7.27. Let p be an irregular prime such that $p \leq 4001$ and $p \neq 3511$. Let $f_1 = [(1/2\delta)(p-5)]$ and $f_2 = [(1/2\delta)(p-5) + 1/2]$. Then

$$\mathcal{C}_{\mathbb{Q},p} \cong \begin{cases} (\mathbb{Z}/p\mathbb{Z})^{f_1+2I(p)} & \text{if } \delta \text{ is odd,} \\ (\mathbb{Z}/p\mathbb{Z})^{f_1+f_2+2I(p)} & \text{if } \delta \text{ is even.} \end{cases}$$

PROOF. Let $(p, 2a)$ be an irregular pair. Let $k_a = (p+1)/2 - a$. Then $2 \leq k_a \leq (p-3)/2$. We can verify, for all irregular pairs $(p, 2a)$ such that $p \leq 4001$ and not a Wieferich prime, that $k_a \not\equiv 1 \pmod{\delta}$, and also $k_a \not\equiv 1 \pmod{\delta/2}$ if δ is even. This implies that if $k \equiv 1 \pmod{\delta}$, or if $k \equiv 1 \pmod{\delta/2}$ when δ is even, then $k \neq k_a$ for any irregular pair $(p, 2a)$, hence $B(p,\, p+1-2k) = 0$. Since p is not a Wieferich prime, we have $W(p) = 0$. Also, by Example 7.20, we have $B(p,\, p+1-2k_a) = B(p, 2a) = 1$. Therefore, by Theorems 7.24 and 7.25, we have, for each k with $1 \leq k \leq (1/2)(p-3)$,

$$\mathcal{C}_{\mathbb{Q},p}(k,+) \cong \begin{cases} \mathbb{Z}/p\mathbb{Z} & \begin{cases} \text{if (i) } \delta \text{ is even and } k = 1 + (\delta/2)l \text{ with } l \text{ an odd integer,} \\ \text{or (ii) } k = k_a \text{ for some irregular pair } (p, 2a), \end{cases} \\ 0 & \text{otherwise,} \end{cases}$$

and

$$\mathcal{C}_{\mathbb{Q},p}(k,-) \cong \begin{cases} \mathbb{Z}/p\mathbb{Z} & \begin{cases} \text{if (i) } k \equiv 1 \pmod{\delta} \text{ and } k \geq 2, \\ \text{or (ii) } k = k_a \text{ for some irregular pair } (p, 2a), \end{cases} \\ 0 & \text{otherwise.} \end{cases}$$

Let g_1 be the number of k with $\mathcal{C}_{\mathbb{Q},p}(k,-) \cong \mathbb{Z}/p\mathbb{Z}$. Let f_1 be the number of k with $k \equiv 1 \pmod{\delta}$ and $k \geq 2$. Then $f_1 = [(1/2\delta)(p-5)]$ as is shown in the proof of Corollary 7.26, and $g_1 = f_1 + I(p)$. Let g_2 be the number of k with $\mathcal{C}_{\mathbb{Q},p}(k,+) \cong \mathbb{Z}/p\mathbb{Z}$. If δ is odd, then $g_2 = I(p)$. Hence $\mathcal{C}_{\mathbb{Q},p} \cong (\mathbb{Z}/p\mathbb{Z})^{g_1+g_2} = (\mathbb{Z}/p\mathbb{Z})^{f_1+2I(p)}$. This proves the case of odd δ. Let δ be even. Let f_2 be the number of k such that $k = 1 + (\delta/2)l$ with l an odd integer. Then $f_2 = [(1/2\delta)(p-5) + 1/2]$ as is shown in the proof of Corollary 7.26, and

$g_2 = f_2 + I(p)$. Hence $\mathcal{C}_{\mathbb{Q},p} \cong (\mathbb{Z}/p\mathbb{Z})^{g_1+g_2} = (\mathbb{Z}/p\mathbb{Z})^{f_1+f_2+2I(p)}$. This proves the case of even δ. □

Next we consider the only known Wieferich primes.

EXAMPLE 7.28. Let $p = 1093$, which is the only known regular Wieferich prime. Then

$$\mathcal{C}_{\mathbb{Q},p} \cong (\mathbb{Z}/1093\mathbb{Z}) \oplus (\mathbb{Z}/1093^2\mathbb{Z})^2.$$

PROOF. We have $\delta = 364$, and $W(1093) = 1$ because $2^{p^2-1} \equiv 581\,794\,064 \not\equiv 1 \pmod{p^3}$. Let $1 \le k \le (1/2)(p-3) = 545$. Since p is regular, we have $B(p, p+1-2k) = 0$. Hence, by Theorems 7.24 and 7.25, we have

$$\mathcal{C}_{\mathbb{Q},p}(k,+) \cong \begin{cases} \mathbb{Z}/p^2\mathbb{Z} & \text{if } k = 1 + 182l \text{ with } l \text{ an odd integer,} \\ 0 & \text{otherwise,} \end{cases}$$

and

$$\mathcal{C}_{\mathbb{Q},p}(k,-) \cong \begin{cases} \mathbb{Z}/p\mathbb{Z} & \text{if } k = 1, \\ \mathbb{Z}/p^2\mathbb{Z} & \text{if } k \equiv 1 \pmod{364} \text{ and } k \ge 2, \\ 0 & \text{otherwise.} \end{cases}$$

If $1 \le k \le 545$ and $k = 1 + 182l$ with l an odd integer, then $k = 183$. Hence, $\mathcal{C}_{\mathbb{Q},p}(k,+) \cong \mathbb{Z}/p^2\mathbb{Z}$ or 0 according as $k = 183$ or not, respectively. If $2 \le k \le 545$ and $k \equiv 1 \pmod{364}$, then $k = 365$. Hence, $\mathcal{C}_{\mathbb{Q},p}(k,-) \cong \mathbb{Z}/p\mathbb{Z}$, $\mathbb{Z}/p^2\mathbb{Z}$, 0 according as $k = 1$, 365, otherwise, respectively. □

EXAMPLE 7.29. Let $p = 3511$, which is the only known irregular Wieferich prime. Then

$$\mathcal{C}_{\mathbb{Q},p} \cong (\mathbb{Z}/3511\mathbb{Z})^5.$$

PROOF. We have $\delta = 1755$, and $W(3511) = 1$ because $2^{p^2-1} \equiv 628\,683\,172 \not\equiv 1 \pmod{p^3}$. Let $1 \le k \le (1/2)(p-3) = 1754$. By Theorems 7.24 and 7.25, we have

$$\mathcal{C}_{\mathbb{Q},p}(k,+) \cong \begin{cases} 0 & \text{if } k = 1, \\ \mathbb{Z}/p^{B(p,p+1-2k)}\mathbb{Z} & \text{otherwise,} \end{cases}$$

and

$$\mathcal{C}_{\mathbb{Q},p}(k,-) \cong \begin{cases} \mathbb{Z}/p\mathbb{Z} & \text{if } k = 1, \\ \mathbb{Z}/p^{B(p,p+1-2k)+2}\mathbb{Z} & \text{if } k \equiv 1 \pmod{1755} \text{ and } k \ge 2, \\ \mathbb{Z}/p^{B(p,p+1-2k)}\mathbb{Z} & \text{otherwise.} \end{cases}$$

The irregular pairs $(p, 2a)$ are $(3511, 1416)$ and $(3511, 1724)$, hence $a = 708,\ 862$. Put $k_a = (p+1)/2 - a$. Then $k_a = 1048,\ 894$ according as $a = 708,\ 862$ respectively. By Example 7.20, we have $B(p, p+1-2k) = 1 (= B(p, 2a))$ or 0 according as $k = k_a$ for some a or not, respectively. Hence, $B(p, p+1-2k) = 1$ for $k = 1048, 894$, and $= 0$ for other values of k. Thus, we have $\mathcal{C}_{\mathbb{Q},p}(k, +) \cong \mathbb{Z}/3511\mathbb{Z}$ for $k = 894, 1048$, and $\mathcal{C}_{\mathbb{Q},p}(k, -) \cong \mathbb{Z}/3511\mathbb{Z}$ for $k = 1, 894, 1048$. For other values of k, we have $\mathcal{C}_{\mathbb{Q},p}(k, +) = \mathcal{C}_{\mathbb{Q},p}(k, -) = 0$. □

8. Numerical results.

Let p be a prime $\neq 2, 3$. In this section we give several tables of computational results.

8.1. Several cuspidal class numbers of $X_1(2p)$ and $X_1(p)$.

Let

$$a = \frac{p^2 - 1}{24}, \tag{8.1}$$

$$A = \frac{1}{p} \prod_{\psi} (4 - \psi(2)), \tag{8.2}$$

$$B = p \prod_{\psi} \left(\frac{1}{4} B_{2,\psi} \right), \tag{8.3}$$

where ψ runs over all even, primitive Dirichlet characters modulo p. Then a, A and B are positive integers.

We consider here several cuspidal class numbers of the modular curves $X_1(2p)$ and $X_1(p)$.

We denote the order $h_{\mathbb{Q}}$ of $\mathcal{C}_{\mathbb{Q}}$ by $h_1^{\mathbb{Q}}(2p)$. Then, by Theorem 5.3, we have

$$h_1^{\mathbb{Q}}(2p) = aAB^2. \tag{8.4}$$

Let $h_1(2p)$ be the full cuspidal class number of $X_1(2p)$. Then, by [**21**, Theorem 5.2], we have

$$h_1(2p) = aA^2B^4. \tag{8.5}$$

Let $h_1(p)$ be the full cuspidal class number of $X_1(p)$. Let $h_1^{\infty}(2p)$ (respectively $h_1^{\infty}(p)$) be the order of the subgroup of the cuspidal divisor class group of $X_1(2p)$ (respectively $X_1(p)$) which is generated by the ∞-cusps. (A cusp on $X_1(n)$ with $n \in \mathbb{N}$ is called an ∞-cusp if it lies over the cusp ∞ of $X_0(n)$.) The formula for $h_1(p)$ is given by [**19**, Theorem 4.1]. The formula for $h_1^{\infty}(p)$ is given by [**8**, Theorem 3.4 in Chapter 6]. The formula for $h_1^{\infty}(2p)$ is given by [**24**]. Then we have

$$h_1^{\infty}(2p) = AB, \tag{8.6}$$

$$h_1(p) = B^2, \tag{8.7}$$

$$h_1^{\infty}(p) = B. \tag{8.8}$$

8.2. Tables.

In Tables 1–3 we list the values a, A and B for all primes p with $7 \le p \le 127$. Note that if $p = 5$, then the genus of $X_1(10)$ is 0, and $a = A = B = 1$. In Table 4 we give the structure of the $\mathbb{Q}$-rational cuspidal group $\mathcal{C}_{\mathbb{Q}} = \mathcal{C}_1(2p)_{\mathbb{Q}}$ of $J_1(2p)_{\mathbb{Q}}$ for all primes p with $7 \le p \le 127$. There the notation $[n_1, n_2, \ldots]$ denotes the group $(\mathbb{Z}/n_1\mathbb{Z}) \oplus (\mathbb{Z}/n_2\mathbb{Z}) \oplus \cdots$. In Table 5 we give the structure of the Sylow p-subgroup $\mathcal{C}_{\mathbb{Q},p} = \mathcal{C}_1(2p)_{\mathbb{Q},p}$ of the $\mathbb{Q}$-rational cuspidal group $\mathcal{C}_1(2p)_{\mathbb{Q}}$ for all primes p with $7 \le p \le 4001$. In that table, if $p \ne 1093$, then the number e indicates that $\mathcal{C}_1(2p)_{\mathbb{Q},p} \cong (\mathbb{Z}/p\mathbb{Z})^e$, and if $p = 1093$, then the numbers $e = 1, 2$ indicates that $\mathcal{C}_1(2p)_{\mathbb{Q},p} \cong (\mathbb{Z}/p\mathbb{Z}) \oplus (\mathbb{Z}/p^2\mathbb{Z})^2$.

Table 1. The value of $a = (p^2 - 1)/24$.

p	a	p	a	p	a	p	a
7	2	31	$2^3 \cdot 5$	61	$5 \cdot 31$	97	$2^3 \cdot 7^2$
11	5	37	$3 \cdot 19$	67	$11 \cdot 17$	101	$5^2 \cdot 17$
13	7	41	$2 \cdot 5 \cdot 7$	71	$2 \cdot 3 \cdot 5 \cdot 7$	103	$2 \cdot 13 \cdot 17$
17	$2^2 \cdot 3$	43	$7 \cdot 11$	73	$2 \cdot 3 \cdot 37$	107	$3^2 \cdot 53$
19	$3 \cdot 5$	47	$2^2 \cdot 23$	79	$2^2 \cdot 5 \cdot 13$	109	$3^2 \cdot 5 \cdot 11$
23	$2 \cdot 11$	53	$3^2 \cdot 13$	83	$7 \cdot 41$	113	$2^2 \cdot 7 \cdot 19$
29	$5 \cdot 7$	59	$5 \cdot 29$	89	$2 \cdot 3 \cdot 5 \cdot 11$	127	$2^5 \cdot 3 \cdot 7$

Table 2. The value of A.

p	A	p	A
7	3	61	$3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 31 \cdot 41 \cdot 151 \cdot 331 \cdot 1321$
11	31	67	$3 \cdot 7 \cdot 23 \cdot 89 \cdot 683 \cdot 20\,857 \cdot 599\,479$
13	$3 \cdot 5 \cdot 7$	71	$11 \cdot 31 \cdot 43 \cdot 127 \cdot 281 \cdot 86\,171 \cdot 122\,921$
17	$3 \cdot 5^2 \cdot 17$	73	$3^{11} \cdot 7^4 \cdot 19^4 \cdot 73^3$
19	$3^2 \cdot 7 \cdot 73$	79	$3 \cdot 7 \cdot 2731 \cdot 8191 \cdot 121\,369 \cdot 22\,366\,891$
23	$89 \cdot 683$	83	$13\,367 \cdot 164\,511\,353 \cdot 8831\,418\,697$
29	$5 \cdot 43 \cdot 113 \cdot 127$	89	$3^3 \cdot 23^4 \cdot 89^3 \cdot 683^4$
31	$3^2 \cdot 11^3 \cdot 31^2$	97	$3^3 \cdot 5^2 \cdot 7^2 \cdot 13^2 \cdot 17^2 \cdot 97 \cdot 241^2 \cdot 257^2 \cdot 673^2$
37	$3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 19 \cdot 73 \cdot 109$	101	$5^3 \cdot 11 \cdot 31 \cdot 41 \cdot 251 \cdot 601 \cdot 1801 \cdot 4051 \cdot 8101 \cdot 268\,501$
41	$3 \cdot 5^4 \cdot 11^2 \cdot 31^2 \cdot 41$	103	$3 \cdot 7 \cdot 307 \cdot 2143 \cdot 2857 \cdot 6529 \cdot 11\,119 \cdot 43\,691 \cdot 131\,071$
43	$3^2 \cdot 43^2 \cdot 127^3$	107	$6361 \cdot 69\,431 \cdot 20\,394\,401 \cdot 28\,059\,810\,762\,433$
47	$178\,481 \cdot 2796\,203$	109	$3^8 \cdot 5^3 \cdot 7^3 \cdot 13^3 \cdot 19^3 \cdot 37^3 \cdot 73^3 \cdot 109^2$
53	$5 \cdot 157 \cdot 1613 \cdot 2731 \cdot 8191$	113	$3^3 \cdot 5^4 \cdot 29^4 \cdot 43^4 \cdot 113^3 \cdot 127^4$
59	$233 \cdot 1103 \cdot 2089 \cdot 3033\,169$	127	$3^8 \cdot 43^9 \cdot 127^8$

Table 3. The value of B

p	B
7	1
11	5
13	19
17	$2^3 \cdot 73$
19	$3^2 \cdot 487$
23	$11 \cdot 37\,181$
29	$2^6 \cdot 3 \cdot 7 \cdot 43 \cdot 17\,837$
31	$2^2 \cdot 5^2 \cdot 7 \cdot 11 \cdot 2302\,381$
37	$3^2 \cdot 5 \cdot 7 \cdot 19 \cdot 37 \cdot 73 \cdot 577 \cdot 17\,209$
41	$2^4 \cdot 5 \cdot 13 \cdot 31^2 \cdot 431 \cdot 250\,183\,721$
43	$2^2 \cdot 7 \cdot 19 \cdot 29 \cdot 463 \cdot 1051 \cdot 416\,532\,733$
47	$23 \cdot 139 \cdot 82\,397\,087 \cdot 12\,451\,196\,833$
53	$7 \cdot 13 \cdot 85\,411 \cdot 96\,331 \cdot 379\,549 \cdot 641\,949\,283$
59	$29 \cdot 59 \cdot 9988\,553\,613\,691\,393\,812\,358\,794\,271$
61	$5 \cdot 7^2 \cdot 11^2 \cdot 19 \cdot 31 \cdot 2081 \cdot 2801 \cdot 40\,231 \cdot 411\,241 \cdot 514\,216\,621$
67	$11 \cdot 67 \cdot 193 \cdot 661^2 \cdot 2861 \cdot 8009 \cdot 11\,287 \cdot 9383\,200\,455\,691\,459$
71	$5 \cdot 7 \cdot 31 \cdot 113 \cdot 211 \cdot 281 \cdot 701^2 \cdot 12\,713 \cdot 13\,070\,849\,919\,225\,655\,729\,061$
73	$2^3 \cdot 3^2 \cdot 11 \cdot 79 \cdot 89 \cdot 241 \cdot 23\,917 \cdot 3341\,773 \cdot 11\,596\,933 \cdot 31\,964\,959\,893\,317\,833$
79	$13 \cdot 157 \cdot 199 \cdot 521^2 \cdot 1249 \cdot 4447 \cdot 1130\,429 \cdot 323\,623 \cdot 68\,438\,648\,614\,508\,149\,381$
83	$41 \cdot 17\,210\,653 \cdot 151\,251\,379 \cdot 18\,934\,761\,332\,741 \cdot 48\,833\,370\,476\,331\,324\,749\,419$
89	$2^3 \cdot 5 \cdot 11 \cdot 13 \cdot 37 \cdot 397 \cdot 4027 \cdot 262\,504\,573 \cdot 15\,354\,699\,728\,897 \cdot 49\,135\,060\,828\,995\,551\,670\,374\,357$
97	$2^4 \cdot 5^2 \cdot 7^2 \cdot 17 \cdot 149 \cdot 241 \cdot 367 \cdot 421 \cdot 2753 \cdot 147\,689 \cdot 651\,997 \cdot 21\,205\,889 \cdot 41\,481\,169 \cdot 5429\,704\,177 \cdot 2758\,053\,952\,369$
101	$5^2 \cdot 19 \cdot 101 \cdot 1201 \cdot 52\,951 \cdot 54\,371 \cdot 599\,491 \cdot 1493\,651 \cdot 12\,355\,051 \cdot 709\,068\,505\,801 \cdot 58\,884\,077\,243\,434\,864\,347\,851$
103	$7^2 \cdot 13 \cdot 17^2 \cdot 103 \cdot 613 \cdot 100\,458\,793\,666\,879 \cdot 123\,953\,701\,101\,455\,911\,613 \cdot 60\,417\,254\,667\,158\,883\,466\,061\,055\,469$
107	$53 \cdot 304\,009 \cdot 1598\,587 \cdot 7762\,787\,405\,087\,851 \cdot 1827\,219\,997\,313\,025\,527 \cdot 340\,411\,510\,885\,100\,431\,606\,787\,699\,221$
109	$2^4 \cdot 3^9 \cdot 37^2 \cdot 103 \cdot 127^2 \cdot 3187 \cdot 22\,483 \cdot 129\,763 \cdot 2230\,759 \cdot 144\,218\,626\,120\,352\,809 \cdot 7225\,241\,488\,211\,218\,811\,391\,927\,451$
113	$2^{20} \cdot 3^2 \cdot 5 \cdot 7 \cdot 13^2 \cdot 41 \cdot 1597 \cdot 2689 \cdot 5419 \cdot 7393 \cdot 33\,181 \cdot 47\,609 \cdot 83\,685\,281 \cdot 1338\,273\,009\,109 \cdot 3747\,533\,743\,340\,403\,014\,797\,054\,313$
127	$2^8 \cdot 3^2 \cdot 7^2 \cdot 19^3 \cdot 113 \cdot 181 \cdot 197 \cdot 1303 \cdot 2647 \cdot 8461 \cdot 36\,037 \cdot 62\,497 \cdot 310\,631\,203 \cdot 10\,360\,369\,321 \cdot 404\,502\,990\,175\,243 \cdot 1383\,982\,596\,554\,597\,891\,267\,948\,732\,467$

Table 4. The structure of the group $\mathcal{C}_1(2p)_{\mathbb{Q}}$.

p	$\mathcal{C}_1(2p)_{\mathbb{Q}}$
7	[6]
11	[5, 775]
13	[133, 1995]
17	[8760, 595 680]
19	[9, 4383, 33 595 695]
23	[408 991, 546 949 390 174]
29	[4, 4, 4, 172, 322 136 220, 32 360 838 252 540]
31	[2, 110, 110, 164 873 503 410, 36 272 170 750 200]
37	[19, 87 381, 160 516 686 697 605, 3411 782 175 757 594 275]
41	[155, 775, 5927 283 967 445 469 200, 10 206 782 991 941 097 962 400]
43	[2, 254, 25 615 681 147 891 287 499 998, 1972 407 448 387 629 137 499 846]
47	[3279 937 688 802 933 030 787, 150 596 232 943 748 173 091 148 093 312 463 772]
53	[182 427 302 879 183 759 829 891 277, 604 558 524 480 886 037 852 237 469 814 929 069 041 745]
59	[17 090 415 233 025 974 812 945 896 997 681, 4035 404 732 342 277 108 170 716 765 844 763 161 918 273 801 455]
61	[11, 2387, 11 935, 56 225 660 010 204 969 117 708 316 979 075, 41 551 702 665 883 717 153 363 255 281 876 574 280 013 975]
67	[661, 661, 228 166 524 544 404 715 482 454 653 548 693 117, 15 663 080 867 536 742 150 839 527 629 458 568 154 286 994 804 349 521 577]
71	[701, 6106 411, 846 772 703 911 192 558 471 548 563 811 885 556 615, 113 145 744 367 708 244 484 094 396 172 159 112 123 891 138 288 052 908 150]
73	[2, 18, 18, 7182, 524 286, 289 531 651 675 514 560 686 218 323 729 279 418 167 306 307 934, 10 712 671 111 994 038 745 390 077 977 983 338 472 190 333 393 558]
79	[521, 521, 29 427 100 164 209 457 485 089 447 933 533 181 481 550 301 759, 9756 906 232 145 215 045 426 321 958 474 091 161 603 333 533 130 029 106 098 424 849 722 260]
83	[98 686 349 372 029 170 201 616 572 533 501 298 687 049 100 544 333 193, 550 046 338 223 536 944 537 177 801 039 598 479 975 252 869 789 692 614 645 701 297 283 093 053 307 377]
89	[2, 2, 2, 94 254, 41 943 030, 70 265 056 281 482 671 660 937 420 666 518 844 451 392 907 429 147 495 037 877 039 790, 772 915 619 096 309 388 270 311 627 331 707 288 965 321 981 720 622 445 416 647 437 690]
97	[7, 35, 35, 143 395, 143 395, 1244 192 473 582 723 094 429 387 076 766 808 629 065 856 227 229 359 353 230 662 320 127 421 680, 20 275 360 549 504 055 546 821 291 802 991 913 419 257 193 078 929 640 020 246 873 168 796 463 697 280]
101	[25, 383 117 416 917 938 352 821 669 377 816 486 750 985 276 713 608 300 916 153 150 414 182 182 375, 1089 927 841 549 376 523 065 381 215 693 745 802 372 768 032 196 246 699 028 918 876 820 398 242 643 144 597 836 660 823 482 589 375]

p	$\mathcal{C}_1(2p)_{\mathbb{Q}}$
103	[17, 221, 514 392 345 891 589 895 637 048 628 820 472 810 730 201 209 034 367 243 706 045 518 045 882 353, 286 995 107 375 502 283 436 235 629 741 272 483 303 400 322 442 880 784 642 402 227 938 248 338 023 704 082 167 228 437 263 282 542 534]
107	[124 368 774 979 658 821 687 008 991 761 829 524 338 976 491 262 179 565 361 941 056 699 780 117 649 583, 14 993 542 105 818 702 095 231 514 512 965 884 941 527 289 785 953 606 709 533 622 214 968 128 417 472 411 947 197 406 991 349 579 948 549 843 373]
109	[333, 333, 999, 7612 380, 2882 435 299 380, 2098 254 297 692 675 704 196 841 472 130 099 322 860 334 318 873 515 928 004 254 333 139 440 932 364 772 140, 23 080 797 274 619 432 746 165 256 193 431 092 551 463 677 507 608 675 208 046 797 664 533 850 256 012 493 540]
113	[4, 4, 4, 16, 16, 16, 80, 80, 494 111 280, 55 834 574 640, 5483 524 885 024 393 161 762 841 970 809 345 247 950 732 845 933 100 542 058 585 370 932 546 237 525 349 573 520, 2187 926 429 124 732 871 543 373 946 352 928 753 932 342 405 527 307 116 281 375 563 002 085 948 772 614 479 834 480]
127	[2, 2, 2, 2, 2, 2, 2, 2, 258, 32 766, 32 766, 32 766, 32 766, 4357 878, 4357 878, 355 545 311 789 286 764 686 582 131 743 881 757 199 809 814 062 904 079 693 483 879 940 487 081 326 438 386 594 437 423 721 679 286, 39 821 074 920 400 117 644 897 198 755 314 756 806 378 699 175 045 256 925 670 194 553 334 553 108 561 099 298 576 991 456 828 080 032]

Table 5. The structure of the Sylow p-subgroup of $\mathcal{C}_1(2p)_{\mathbb{Q}}$.

p	e	p	e	p	e	p	e	p	e	p	e	p	e
7	0	191	0	421	2	661	0	941	0	1217	13	1493	0
11	0	193	1	431	4	673	17	947	0	1223	0	1499	2
13	0	197	0	433	7	677	2	953	15	1229	2	1511	0
17	1	199	0	439	2	683	32	967	0	1231	0	1523	2
19	0	211	0	443	0	691	6	971	6	1237	2	1531	0
23	0	223	2	449	1	701	0	977	1	1249	7	1543	0
29	0	227	0	457	5	709	0	983	0	1259	0	1549	0
31	2	229	2	461	2	719	0	991	0	1277	0	1553	7
37	2	233	5	463	2	727	4	997	2	1279	2	1559	2
41	1	239	0	467	4	733	2	1009	1	1283	2	1567	0
43	2	241	9	479	0	739	2	1013	10	1289	3	1571	0
47	0	251	4	487	0	743	0	1019	0	1291	4	1579	2
53	0	257	17	491	6	751	2	1021	2	1297	5	1583	0
59	2	263	2	499	2	757	2	1031	0	1301	2	1597	4
61	0	269	0	503	0	761	3	1033	3	1303	0	1601	3
67	2	271	2	509	0	769	1	1039	0	1307	4	1607	0
71	0	277	2	521	1	773	2	1049	3	1319	2	1609	5
73	3	281	3	523	2	787	0	1051	2	1321	21	1613	32
79	0	283	4	541	2	797	2	1061	2	1327	4	1619	2
83	0	293	2	547	4	809	5	1063	0	1361	1	1621	2
89	3	307	4	557	2	811	4	1069	2	1367	2	1627	2
97	1	311	2	563	0	821	2	1087	0	1373	0	1637	2
101	2	313	1	569	1	823	0	1091	2	1381	2	1657	17
103	2	317	0	571	4	827	2	1093	1, 2	1399	2	1663	4
107	0	331	10	577	5	829	0	1097	3	1409	3	1667	0
109	2	337	7	587	4	839	2	1103	18	1423	2	1669	4
113	3	347	2	593	5	853	0	1109	0	1427	0	1693	0
127	8	349	0	599	0	857	1	1117	2	1429	18	1697	1
131	2	353	7	601	11	859	0	1123	0	1433	3	1699	2
137	1	359	0	607	2	863	0	1129	3	1439	2	1709	6
139	0	367	0	613	2	877	2	1151	6	1447	0	1721	5
149	2	373	0	617	9	881	9	1153	5	1451	0	1723	2
151	4	379	4	619	2	883	0	1163	6	1453	0	1733	4
157	6	383	0	631	10	887	2	1171	0	1459	2	1741	0
163	0	389	2	641	9	907	0	1181	4	1471	2	1747	0
167	0	397	8	643	2	911	4	1187	0	1481	3	1753	13
173	0	401	3	647	6	919	2	1193	5	1483	2	1759	2
179	0	409	3	653	2	929	5	1201	5	1487	0	1777	25
181	0	419	0	659	2	937	3	1213	0	1489	1	1783	0

p	e	p	e	p	e	p	e	p	e	p	e	p	e
1787	2	2099	2	2399	0	2719	0	3049	5	3389	6	3701	0
1789	6	2111	2	2411	6	2729	1	3061	16	3391	18	3709	0
1801	35	2113	47	2417	1	2731	104	3067	0	3407	4	3719	0
1811	10	2129	3	2423	4	2741	0	3079	0	3413	0	3727	0
1823	0	2131	0	2437	0	2749	2	3083	2	3433	3	3733	0
1831	4	2137	3	2441	7	2753	3	3089	5	3449	3	3739	6
1847	6	2141	0	2447	0	2767	4	3109	6	3457	5	3761	19
1861	0	2143	22	2459	0	2777	3	3119	2	3461	0	3767	0
1867	0	2153	2	2467	0	2789	4	3121	19	3463	2	3769	1
1871	2	2161	1	2473	3	2791	4	3137	3	3467	0	3779	2
1873	1	2179	2	2477	0	2797	0	3163	2	3469	2	3793	1
1877	2	2203	2	2503	2	2801	1	3167	0	3491	2	3797	2
1879	2	2207	0	2521	1	2803	0	3169	1	3499	0	3803	0
1889	5	2213	2	2531	0	2819	0	3181	4	3511	5	3821	6
1901	2	2221	0	2539	0	2833	25	3187	0	3517	4	3823	2
1907	0	2237	0	2543	2	2837	0	3191	28	3527	0	3833	9
1913	3	2239	2	2549	0	2843	0	3203	2	3529	5	3847	0
1931	0	2243	0	2551	0	2851	0	3209	1	3533	4	3851	4
1933	6	2251	2	2557	2	2857	29	3217	3	3539	4	3853	2
1949	0	2267	2	2579	2	2861	2	3221	6	3541	14	3863	0
1951	2	2269	0	2591	4	2879	0	3229	4	3547	0	3877	0
1973	0	2273	7	2593	15	2887	0	3251	4	3557	0	3881	13
1979	2	2281	11	2609	1	2897	1	3253	0	3559	4	3889	5
1987	2	2287	2	2617	1	2903	0	3257	5	3571	0	3907	0
1993	3	2293	2	2621	2	2909	4	3259	2	3581	2	3911	0
1997	4	2297	1	2633	2	2917	2	3271	2	3583	2	3917	2
1999	2	2309	4	2647	3	2927	2	3299	0	3593	5	3919	0
2003	10	2311	0	2657	17	2939	6	3301	4	3607	4	3923	0
2011	4	2333	0	2659	0	2953	5	3307	0	3613	2	3929	1
2017	7	2339	0	2663	2	2957	4	3313	5	3617	5	3931	0
2027	0	2341	2	2671	6	2963	0	3319	0	3623	0	3943	8
2029	0	2347	2	2677	0	2969	3	3323	2	3631	4	3947	0
2039	2	2351	24	2683	0	2971	26	3329	3	3637	4	3967	2
2053	2	2357	2	2687	16	2999	2	3331	14	3643	0	3989	2
2063	0	2371	4	2689	13	3001	1	3343	2	3659	0	4001	5
2069	0	2377	3	2693	0	3011	2	3347	0	3671	2		
2081	1	2381	6	2699	0	3019	0	3359	0	3673	3		
2083	0	2383	6	2707	0	3023	2	3361	19	3677	2		
2087	4	2389	2	2711	0	3037	0	3371	0	3691	0		
2089	35	2393	3	2713	1	3041	1	3373	2	3697	3		

References

[1] Y.-H. Chen, Cuspidal $\mathbb{Q}$-rational torsion subgroup of $J(\Gamma)$ of level P, Taiwanese J. Math., **15** (2011), 1305–1323.

[2] S.-K. Chua and S. Ling, On the rational cuspidal subgroup and the rational torsion points of $J_0(pq)$, Proc. Amer. Math. Soc., **125** (1997), 2255–2263.

[3] B. Conrad, B. Edixhoven and W. Stein, $J_1(p)$ has connected fibers, Doc. Math., **8** (2003), 331–408.

[4] V. G. Drinfel'd, Two theorems on modular curves, Funct. Anal. Appl., **7** (1973), 155–156.

[5] K. F. Ireland and M. I. Rosen, A Classical Introduction to Modern Number Theory, Grad. Texts in Math., **84**, Springer-Verlag, New York, 1982.

[6] P. E. Klimek, Modular functions for $\Gamma_1(n)$, Ph. D. thesis, University of California, Berkeley, 1975.

[7] J. Knauer and J. Richstein, The continuing search for Wieferich primes, Math. Comp., **74** (2005), 1559–1563.

[8] D. S. Kubert and S. Lang, Modular Units, Grundlehren Math. Wiss., **244**, Springer-Verlag, Berlin, 1981.

[9] S. Ling, On the **Q**-rational cuspidal subgroup and the component group of $J_0(p^r)$, Israel J. Math., **99** (1997), 29–54.

[10] D. J. Lorenzini, Torsion points on the modular Jacobian $J_0(N)$, Compositio Math., **96** (1995), 149–172.

[11] J. I. Manin, Parabolic points and zeta functions of modular curves, Izv. Akad. Nauk SSSR Ser. Mat., **36** (1972), 19–66.

[12] B. Mazur, Modular curves and the Eisenstein ideal, Inst. Hautes Études Sci. Publ. Math., **47** (1977), 33–186.

[13] A. P. Ogg, Rational points on certain elliptic modular curves, In: Analytic Number Theory, St. Louis, 1972, (ed. H. G. Diamond), Proc. Sympos. Pure Math., **24**, Amer. Math. Soc., Providence, RI, 1973, pp. 221–231.

[14] A. P. Ogg, Diophantine equations and modular forms, Bull. Amer. Math. Soc., **81** (1975), 14–27.

[15] M. Ohta, Eisenstein ideals and the rational torsion subgroups of modular Jacobian varieties, J. Math. Soc. Japan, **65** (2013), 733–772.

[16] D. Poulakis, La courbe modulaire $X_0(125)$ et sa jacobienne, J. Number Theory, **25** (1987), 112–131.

[17] J. J. Rotman, An Introduction to Homological Algebra. 2nd ed., Universitext, Springer-Verlag, 2009.

[18] G. Shimura, Introduction to the Arithmetic Theory of Automorphic Functions, Publications of the Mathematical Society of Japan, **11**, Iwanami Shoten, Publishers, Tokyo, 1971.

[19] T. Takagi, Cuspidal class number formula for the modular curves $X_1(p)$, J. Algebra, **151** (1992), 348–374.

[20] T. Takagi, The cuspidal class number formula for the modular curves $X_0(M)$ with M square-free, J. Algebra, **193** (1997), 180–213.

[21] T. Takagi, The cuspidal class number formula for the modular curves $X_1(2p)$, J. Math. Soc. Japan, **64** (2012), 23–85.

[22] L. C. Washington, Introduction to Cyclotomic Fields, Grad. Texts in Math., **83**, Springer-Verlag, New York, 1982.

[23] Y. Yang, Modular units and cuspidal divisor class groups of $X_1(N)$, J. Algebra, **322** (2009), 514–553.

[24] J. Yu, A cuspidal class number formula for the modular curves $X_1(N)$, Math. Ann., **252** (1980), 197–216.

Toshikazu TAKAGI

Faculty of Arts and Sciences at Fujiyoshida
Showa University
Fujiyoshida
Yamanashi 403-0005, Japan
E-mail: takagi@cas.showa-u.ac.jp