JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Keisuke ARAI

On uniform lower bound of the Galois images associated to elliptic curves

Tome 20, n° 1 (2008), p. 23-43.

<http://jtnb.cedram.org/item?id=JTNB_2008__20_1_23_0>

Journal de Théorie des Nombres
de Bordeaux **20** (2008), 23-43

On uniform lower bound of the Galois images associated to elliptic curves

par Keisuke ARAI

Résumé. Soit p un nombre premier et K un corps de nombres. Soit $\rho_{E,p} : \mathrm{G}_K \longrightarrow \mathrm{Aut}(T_pE) \cong \mathrm{GL}_2(\mathbb{Z}_p)$ la représentation Galoisienne donnée par l'action du groupe de Galois sur le module de Tate p-adique d'une courbe elliptique E définie sur K. Serre a prouvé que l'image de $\rho_{E,p}$ est ouverte si E n'a pas de multiplication complexe. Pour E une courbe elliptique définie sur K et dont l'invariant j n'appartient pas à un ensemble fini exceptionnel (qui est non explicite cependant), nous donnons une minoration uniforme et explicite de la taille de l'image de $\rho_{E,p}$.

Abstract. Let p be a prime and let K be a number field. Let $\rho_{E,p} : \mathrm{G}_K \longrightarrow \mathrm{Aut}(T_pE) \cong \mathrm{GL}_2(\mathbb{Z}_p)$ be the Galois representation given by the Galois action on the p-adic Tate module of an elliptic curve E over K. Serre showed that the image of $\rho_{E,p}$ is open if E has no complex multiplication. For an elliptic curve E over K whose j-invariant does not appear in an exceptional finite set (which is non-explicit however), we give an explicit uniform lower bound of the size of the image of $\rho_{E,p}$.

1. Introduction

Let k be a field of characteristic 0, and let $\mathrm{G}_k = \mathrm{Gal}(\overline{k}/k)$ be the absolute Galois group of k where $\overline{k}$ is an algebraic closure of k. Let p be a prime number. For an elliptic curve E over k, let T_pE be the p-adic Tate module of E, and let

$$\rho_{E,p} : \mathrm{G}_k \longrightarrow \mathrm{Aut}(T_pE) \cong \mathrm{GL}_2(\mathbb{Z}_p)$$

be the p-adic representation determined by the action of G_k on T_pE. By a number field we mean a finite extension of $\mathbb{Q}$. We use the following conventions:

$$1 + p^0\mathbb{Z}_p := \mathbb{Z}_p^\times,$$
$$1 + p^0\mathrm{M}_2(\mathbb{Z}_p) := \mathrm{GL}_2(\mathbb{Z}_p),$$
$$1 + p^0\mathrm{M}_2(\mathbb{Z}/p\mathbb{Z}) := \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}).$$

Manuscrit reçu le 16 janvier 2007.

Recall a famous theorem proved by Serre (we can find a stronger form in [19, Théorème 3]):

Theorem 1.1. ([18, IV-11]) *Let K be a number field, let E be an elliptic curve over K with no complex multiplication and let p be a prime. Then the representation $\rho_{E,p}$ has an open image i.e. there exists an integer $n \geq 0$ depending on K, E and p such that*

$$\rho_{E,p}(\mathrm{G}_K) \supseteq 1 + p^n \mathrm{M}_2(\mathbb{Z}_p).$$

In this paper, we show that there exists a uniform bound of such n if we let E vary for fixed K and p.

Theorem 1.2. *Let K be a number field and let p be a prime. Then there exists an integer $n \geq 0$ depending on K and p such that for any elliptic curve E over K with no complex multiplication, we have*

$$\rho_{E,p}(\mathrm{G}_K) \supseteq 1 + p^n \mathrm{M}_2(\mathbb{Z}_p).$$

We will deduce Theorem 1.2 from the following more precise result of this paper at the end of Section 2.

Theorem 1.3. *For a prime p, there exists an integer $n \geq 0$ satisfying the following condition $(\boldsymbol{C})_p$.*
$(\boldsymbol{C})_p$: Let K be a number field. Then there exists a finite subset $\Sigma \subseteq K$ depending on p such that for any elliptic curve E over K, the condition $j(E) \notin \Sigma$ implies

$$\rho_{E,p}(\mathrm{G}_K) \supseteq (1 + p^n \mathrm{M}_2(\mathbb{Z}_p))^{\det=1}.$$

Let $n(p) \geq 0$ be the minimum integer n satisfying $(\boldsymbol{C})_p$. Then we have $n(p) = 0$ if $p \geq 23$, $n(19) = n(17) = n(13) = n(11) = 1$, $n(7) = 2$, $n(5) \leq 3$, $n(3) \leq 5$ and $n(2) \leq 11$.

Remark 1.4. *If $p \geq 23$ and*

$$\begin{cases} K \not\supseteq \text{(the quadratic subfield of } \mathbb{Q}(\zeta_p)) & \text{when } p \not\equiv \pm 3 \mod 8, \\ \text{there exists an inclusion } K \hookrightarrow \mathbb{Q}_p & \text{when } p \equiv \pm 3 \mod 8, \end{cases}$$

then the result of Theorem 1.3 follows from [3, Theorem 7; 22, Proposition 1.40, 1.43; 9, p.116-118].

If $p = 17$, 19 and $K = \mathbb{Q}$, the result of Theorem 1.3 follows from [3, Theorem 7; 8, Theorem (4.1); 9, p.116-118].

Remark 1.5. *There are many other studies of the Galois images associated to elliptic curves over number fields or rational points on modular curves in [2,4,6,7,10-17,19,21]. Several questions related to the subject of this paper are raised in [20, p.187].*

The contents of this paper are as follows:

In Section 2, we deduce Theorem 1.2 from Theorem 1.3 by studying the determinants.

In Section 3, we regard elliptic curves as rational points on modular curves, and reduce Theorem 1.3 to a genus estimate. Replacing K by its finite extension, we may assume that K contains a primitive $p^{n(p)+1}$-st root $\zeta_{p^{n(p)+1}}$ of unity. Suppose an elliptic curve E/K does not satisfy $\rho_{E,p}(\mathrm{G}_K) \supseteq (1+p^{n(p)}\mathrm{M}_2(\mathbb{Z}_p))^{\det=1}$. Then we have

$$\rho_{E,p}(\mathrm{G}_K) \mod p^{n(p)+1} \subseteq H$$

for some subgroup $H \subseteq \mathrm{SL}_2(\mathbb{Z}/p^{n(p)+1}\mathbb{Z})$ satisfying

$$H \not\supseteq (1+p^{n(p)}\mathrm{M}_2(\mathbb{Z}/p^{n(p)+1}\mathbb{Z}))^{\det=1}.$$

Thus E/K determines a rational point on the modular curve X_H corresponding to H. If the genus $g(X_H)$ of X_H is greater than or equal to 2, we conclude that X_H has only finitely many rational points by Mordell's conjecture ([3, Theorem 7]). Since there are only finitely many subgroups H as above, the number of the j-invariants of E/K not satisfying $\rho_{E,p}(\mathrm{G}_K) \supseteq (1+p^{n(p)}\mathrm{M}_2(\mathbb{Z}_p))^{\det=1}$ is finite. Thus Theorem 1.3 will follow.

In Section 4 - 7, we prove $g(X_H) \geq 2$. In section 4, we prepare for estimating $g(X_H)$. Put $G = \mathrm{SL}_2(\mathbb{Z}/p^{n(p)+1}\mathbb{Z})$, $\sigma = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $\tau = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$, $u = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. For $\alpha \in G$, let $\mathrm{Conj}(\alpha)$ be the conjugacy class containing α. If $H \ni -1$, we have the following formula ([22, Proposition 1.40]).

$$g(X_H) = 1 + \frac{1}{12}[G:H]\left(1 - 3\frac{\sharp H \cap \mathrm{Conj}(\sigma)}{\sharp \mathrm{Conj}(\sigma)} - 4\frac{\sharp H \cap \mathrm{Conj}(\tau)}{\sharp \mathrm{Conj}(\tau)} - 6\frac{\sharp \langle u \rangle \backslash G/H}{[G:H]}\right).$$

We calculate the number of elements conjugate to σ, τ, u contained in maximal subgroups of $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$.

In Section 5, we calculate the number of elements conjugate to σ, τ, u contained in $\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$, and study the fiber of the mod p^m map $\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z}) \cap \mathrm{Conj}(\alpha) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/p^m\mathbb{Z}) \cap \mathrm{Conj}(\alpha)$, where $1 \leq m \leq n$ and $\alpha = \sigma, \tau, u$. For integers $1 \leq m \leq n$, let $f_{n,m} : \mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/p^m\mathbb{Z})$ be the mod p^m map. If $m < n \leq 2m$ and $\alpha = \sigma, \tau, u$, we see that $\alpha^{-1}(f_{n,m}^{-1}(\alpha) \cap \mathrm{Conj}(\alpha))$ is a subgroup of $(1+p^m\mathrm{M}_2(\mathbb{Z}/p^n\mathbb{Z}))^{\det=1} \cong \mathrm{M}_2(\mathbb{Z}/p^{n-m}\mathbb{Z})^{\mathrm{Tr}=0}$ and is isomorphic to $(\mathbb{Z}/p^{n-m}\mathbb{Z})^2$.

In Section 6, we control the number of elements conjugate to σ, τ, u contained in H, by combining the result of Section 5 with the property $H \not\supseteq (1+p^{n(p)}\mathrm{M}_2(\mathbb{Z}/p^{n(p)+1}\mathbb{Z}))^{\det=1}$.

In Section 7, we prove $g(X_H) \geq 2$ by using the results of Section 4, 5, 6.

I would like to thank my supervisor Professor Takeshi Saito for helpful advice and warm encouragement. I would also like to thank the referee for useful comments and suggestions. This work was partly supported by 21st Century COE Program in The University of Tokyo, A Base for New Developments of Mathematics into Science and Technology.

In order to keep the paper reasonably short, many computations have been omitted. The interested reader will be able to find the details at http://arxiv.org/abs/math/0703686.

2. Deduction of Theorem 1.2

In order to deduce Theorem 1.2 from Theorem 1.3, we need some facts in group theory.

Lemma 2.1. *Let p be a prime and let H be a closed subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$. Then H contains $\mathrm{SL}_2(\mathbb{Z}_p)$ if and only if $H \bmod p^2$ contains $\mathrm{SL}_2(\mathbb{Z}/p^2\mathbb{Z})$. In particular, if a subgroup $H' \subseteq \mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$ for $n \geq 3$ maps surjectively $\bmod p^2$ onto $\mathrm{SL}_2(\mathbb{Z}/p^2\mathbb{Z})$, then $H' = \mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$.*

Assume $p \geq 5$. Then H contains $\mathrm{SL}_2(\mathbb{Z}_p)$ if and only if $H \bmod p$ contains $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. In particular, if a subgroup $H' \subseteq \mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$ for $n \geq 2$ maps surjectively $\bmod p$ onto $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, then $H' = \mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$.

Proof. See [18, IV-23]. □

Lemma 2.2. *Let $n \geq 1$ be an integer and let p be a prime. If $p = 2$, assume $n \geq 2$. Let H be a closed subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$. Then H contains $1 + p^n\mathrm{M}_2(\mathbb{Z}_p)$ (resp. $(1 + p^n\mathrm{M}_2(\mathbb{Z}_p))^{\det=1}$) if and only if $H \bmod p^{n+1}$ contains $1 + p^n\mathrm{M}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$ (resp. $(1 + p^n\mathrm{M}_2(\mathbb{Z}/p^{n+1}\mathbb{Z}))^{\det=1}$).*

Proof. It follows from the same argument as in the previous lemma ([18, IV-23]). □

Lemma 2.3. *Let $n \geq 1$ be an integer. Let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$ containing $1 + p^n\mathrm{M}_2(\mathbb{Z}_p)$ (resp. $(1 + p^n\mathrm{M}_2(\mathbb{Z}_p))^{\det=1}$), and let H' be a closed subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$ which is a subgroup of H of index 2. If $p \geq 3$, then $H' \supseteq 1 + p^n\mathrm{M}_2(\mathbb{Z}_p)$ (resp. $H' \supseteq (1 + p^n\mathrm{M}_2(\mathbb{Z}_p))^{\det=1}$); if $p = 2$ and $n \geq 2$, then $H' \supseteq 1 + 2^{n+1}\mathrm{M}_2(\mathbb{Z}_2)$ (resp. $H' \supseteq (1 + 2^{n+1}\mathrm{M}_2(\mathbb{Z}_2))^{\det=1}$).*

Lemma 2.4. *Let $n \geq 1$ be an integer and assume $p \geq 3$. Let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$. If $\det(H) = (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$, then*

$$\det|_{H\cap(1+p^n\mathrm{M}_2(\mathbb{Z}/p^{n+1}\mathbb{Z}))} : H \cap (1+p^n\mathrm{M}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})) \longrightarrow 1+p^n\mathbb{Z}/p^{n+1}\mathbb{Z}$$

is surjective.

Lemma 2.5. *Take two integers $n > r \geq 1$. If $p = 2$, assume $r \geq 2$. Let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$. If $\det(H)$ contains $1+p^r\mathbb{Z}/p^{n+1}\mathbb{Z}$ and if H contains $(1+p^{n-r}\mathrm{M}_2(\mathbb{Z}/p^{n+1}\mathbb{Z}))^{\det=1}$, then*

$$\det|_{H\cap(1+p^n\mathrm{M}_2(\mathbb{Z}/p^{n+1}\mathbb{Z}))} : H \cap (1+p^n\mathrm{M}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})) \longrightarrow 1+p^n\mathbb{Z}/p^{n+1}\mathbb{Z}$$

is surjective. In particular, H contains $1+p^n\mathrm{M}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$.

Corollary 2.6. *Let $H \subseteq \mathrm{GL}_2(\mathbb{Z}_p)$ be a closed subgroup and let $n \geq 0$, $r \geq 0$ be integers. Assume $r \geq 2$ if $p = 2$. If $H \supseteq (1+p^n\mathrm{M}_2(\mathbb{Z}_p))^{\det=1}$ and if $\det(H) \supseteq 1+p^r\mathbb{Z}_p$, then $H \supseteq 1+p^{n+r}\mathrm{M}_2(\mathbb{Z}_p)$.*

As a consequence of Theorem 1.3, we get the following.

Theorem 2.7. *Let K be a number field and let p be a prime. Let $n(p)$, Σ be as in Theorem 1.3. Suppose that the image of the p-adic cyclotomic character $\chi_p : \mathrm{G}_K \longrightarrow \mathbb{Z}_p^\times$ contains $1+p^r\mathbb{Z}_p$ with $r \geq 0$ an integer. Assume $r \geq 2$ if $p = 2$. Put*

$$n = r + n(p).$$

Then for any elliptic curve E over K, the condition $j(E) \notin \Sigma$ implies $\rho_{E,p}(\mathrm{G}_K) \supseteq 1+p^n\mathrm{M}_2(\mathbb{Z}_p)$.

Proof. It follows from Theorem 1.3 and Corollary 2.6. □

We show that there exists a lower bound of the images of $\rho_{E,p}$ if we take E's having only finitely many j-invariants.

Lemma 2.8. *Let K be a number field. Fix an element $j \in K$. Assume that an elliptic curve E over K with j-invariant j has no complex multiplication. Take a prime p. Then there exists a positive integer n depending on p and j such that for any elliptic curve E over K with j-invariant j, we have $\rho_{E,p}(\mathrm{G}_K) \supseteq 1+p^n\mathrm{M}_2(\mathbb{Z}_p)$.*

Proof. Take an E/K with j-invariant j. By Theorem 1.1, we have $\rho_{E,p}(\mathrm{G}_K) \supseteq 1+p^{n_0}\mathrm{M}_2(\mathbb{Z}_p)$ for some n_0. Let E'/K have j-invariant j. Since E has no complex multiplication, we have $j \neq 0, 1728$. Hence there exists a quadratic extension L of K satisfying $E \otimes_K L \cong E' \otimes_K L$ (see [23, p.308]). Therefore $\rho_{E,p}(\mathrm{G}_L)$ is conjugate to $\rho_{E',p}(\mathrm{G}_L)$. Since $[\rho_{E,p}(\mathrm{G}_K) : \rho_{E,p}(\mathrm{G}_L)]$ is 1 or 2, applying Lemma 2.3, we get the result. □

Theorem 1.3 and Lemma 2.8 imply Theorem 1.2.

3. Modular curves

We regard an elliptic curve with a specific Galois image as a rational point on a certain modular curve, and reduce Theorem 1.3 to a genus estimate.

Now we give a brief review of modular curves. For more details, see [1,5]. Let N be a positive integer and let k be a field of characteristic 0. For an elliptic curve E over k and an integer $N \geq 1$, let $E[N] = \mathrm{Ker}\,([N] : E \longrightarrow E)$ be the kernel of multiplication by N on E, and let $\overline{\rho}_{E,N} : \mathrm{G}_k \longrightarrow \mathrm{Aut}(E[N](\overline{k})) \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be the mod N representation determined by the action of G_k on $E[N](\overline{k})$. A level N-structure on E is an isomorphism

$$\gamma : (\mathbb{Z}/N\mathbb{Z})^2 \longrightarrow E[N].$$

Let $Y(N) \longrightarrow \mathrm{Spec}(\mathbb{Q}(\zeta_N))$ be the moduli of elliptic curves with level N-structure. We have a right action of $G = \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ on $Y(N)$ over $\mathbb{Q}(\zeta_N)$:

$$[E, \gamma] \mapsto [E, \gamma \circ h]$$

where E is an elliptic curve over k, γ a level N-structure on E and $h \in G$.

For a subgroup $H \subseteq G$, put Y_H to be the quotient $Y(N)/H$. The quotient $Y_H \longrightarrow \mathrm{Spec}(\mathbb{Q}(\zeta_N))$ is an affine smooth curve. Let E be an elliptic curve over k. Choose a basis $\langle \epsilon_1, \epsilon_2 \rangle$ of $E[N](\overline{k})$. Then the pair $(E, \langle \epsilon_1, \epsilon_2 \rangle)$ defines an element P of $Y(N)(\overline{k})$. Let $Q \in Y_H(\overline{k})$ be the image of P via the map $Y(N)(\overline{k}) \longrightarrow Y_H(\overline{k})$ induced by the natural map $Y(N) \longrightarrow Y_H$. If $\overline{\rho}_{E,N}(\mathrm{G}_k) \subseteq H$ with respect to $\langle \epsilon_1, \epsilon_2 \rangle$, then Q lies in $Y_H(k)$.

Lemma 3.1. *Let k be a field of characteristic 0. If $Y_H(k)$ is finite, then there exists a finite subset $\Sigma \subseteq k$ satisfying the following condition:*

For any elliptic curve E over k, if a conjugate of $\overline{\rho}_{E,N}(\mathrm{G}_k)$ is contained in H, then $j(E) \in \Sigma$.

Let X_H be the smooth compactification of Y_H. The following is the famous theorem known as Mordell's conjecture proved by Faltings. It shows that a curve X over a number field has only finitely many rational points if its genus $g(X)$ is greater than or equal to 2.

Theorem 3.2. *([3, Theorem 7]) Let K be a number field and let X be a proper smooth curve over K. If $g(X) \geq 2$, then $X(K)$ is finite.*

Now we compute the genus of X_H explicitly. As in Section 1, put

$$\sigma := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ \tau := \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix},\ u := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

For $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, we also use the same letter to denote the reduction of α. Put

$$g_H := 1 + \frac{1}{12}[G:H]\left(1 - 3\frac{\sharp H \cap \mathrm{Conj}(\sigma)}{\sharp \mathrm{Conj}(\sigma)} - 4\frac{\sharp H \cap \mathrm{Conj}(\tau)}{\sharp \mathrm{Conj}(\tau)} - 6\frac{\sharp \langle u \rangle \backslash G / H}{[G:H]}\right).$$

Proposition 3.3. *([22, Proposition 1.40]) Let H be a subgroup of $G = \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Assume that H contains -1. Then the genus $g(X_H)$ of the modular curve X_H is given by*

$$g(X_H) = g_H.$$

Let p be a prime and consider subgroups of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. A Borel subgroup is a subgroup which is conjugate to $\left\{\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}\right\}$; the normalizer of a split Cartan subgroup is conjugate to $\left\{\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}, \begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix}\right\}$. When $p \geq 3$, the normalizer of a non-split Cartan subgroup is conjugate to $\left\{\begin{pmatrix} x & y \\ \lambda y & x \end{pmatrix}, \begin{pmatrix} x & y \\ -\lambda y & -x \end{pmatrix} | (x,y) \in \mathbb{F}_p \times \mathbb{F}_1\right.$ where $\lambda \in \mathbb{F}_p^\times \setminus (\mathbb{F}_p^\times)^2$ is a fixed element. Assume $p \geq 5$. The quotient group $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ has a subgroup which is isomorphic to S_4; it has a subgroup which is isomorphic to A_5 if and only if $p \equiv 0, \pm 1 \mod 5$ ([19, p.281]). Take a subgroup H (of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$) whose order is prime to p. We call H an exceptional subgroup if it is the inverse image of a subgroup which is isomorphic to A_4, S_4 or A_5 by the natural surjection $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) \longrightarrow \mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$.

Proposition 3.4. *([19, p.284]) Let $p \geq 3$ be a prime and let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. If p divides the order of H, then H contains $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ or H is contained in a Borel subgroup. If p does not divide the order of H, then H is contained in the normalizer of a (split or non-split) Cartan subgroup or an exceptional subgroup.*

Put

$$\begin{aligned}
B &:= \left\{\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}\right\} \cap \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}), \\
C &:= \left\{\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}, \begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix}\right\} \cap \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}), \\
D &:= \left\{\begin{pmatrix} x & y \\ \lambda y & x \end{pmatrix}, \begin{pmatrix} x & y \\ -\lambda y & -x \end{pmatrix}\right\} \cap \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}), \\
E &:= (\text{an exceptional subgroup}) \cap \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}).
\end{aligned}$$

From now on, we use the letter E to denote this subgroup, not meaning an elliptic curve. The genera of the modular curves corresponding to B, C, D are known as follows.

Proposition 3.5. *([22, Proposition 1.40, 1.43; 9, p.117]) Let $N = p \geq 5$ be a prime. We have*

$$g_B = \frac{1}{12}(p - 6 - 3\left(\frac{-1}{p}\right) - 4\left(\frac{-3}{p}\right));$$
$$g_C = \frac{1}{24}(p^2 - 8p + 11 - 4\left(\frac{-3}{p}\right));$$
$$g_D = \frac{1}{24}(p^2 - 10p + 23 + 6\left(\frac{-1}{p}\right) + 4\left(\frac{-3}{p}\right)).$$

We have $g_B \geq 2$ if and only if $p \geq 23$; $g_C \geq 2$ if and only if $p \geq 11$; $g_D \geq 2$ if and only if $p \geq 13$.

Remark 3.6. *We can also calculate these genera by using Lemma 4.1.*

Put

$$\delta_H := 1 - 3\frac{\sharp H \cap \mathrm{Conj}(\sigma)}{\sharp \mathrm{Conj}(\sigma)} - 4\frac{\sharp H \cap \mathrm{Conj}(\tau)}{\sharp \mathrm{Conj}(\tau)} - 6\frac{\sharp \langle u \rangle \backslash G / H}{[G : H]},$$

so that

$$g_H = 1 + \frac{1}{12}[G : H]\delta_H.$$

As g_H is an integer, we have $g_H \geq 2$ if and only if $\delta_H > 0$. We have the following:

$$\begin{aligned}\frac{\sharp \langle u \rangle \backslash G / H}{[G : H]} &= \sum_{s=0}^{n-1} \frac{p-1}{p^{s+1}} \frac{\sharp H \cap \mathrm{Conj}(u^{p^s})}{\sharp \mathrm{Conj}(u^{p^s})} + \frac{1}{p^n} \\ &\leq \sum_{s=0}^{t-1} \frac{p-1}{p^{s+1}} \frac{\sharp H \cap \mathrm{Conj}(u^{p^s})}{\sharp \mathrm{Conj}(u^{p^s})} + \frac{1}{p^t}\end{aligned}$$

where $1 \leq t \leq n$.

Definition 3.7. *Let $n \geq 1$ be an integer and let $H \subseteq \mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$ be a subgroup. We call H a slim subgroup if*

$$H \not\supseteq (1 + p^{n-1}\mathrm{M}_2(\mathbb{Z}/p^n\mathbb{Z}))^{\det=1}.$$

In this definition, notice that if $n = 1$, then a slim subgroup is just a proper subgroup.

In order to prove Theorem 1.3, it suffices to estimate δ_H for any slim subgroup H.

Proposition 3.8. *If $\delta_H > 0$ for any slim subgroup $H \subseteq \mathrm{SL}_2(\mathbb{Z}/p^{n'(p)+1}\mathbb{Z})$, then Theorem 1.3 holds. Here we put $n'(p) := 0$ if $p \geq 23$, $n'(19) := n'(17) := n'(13) := n'(11) := 1$, $n'(7) := 2$, $n'(5) := 3$, $n'(3) := 5$ and $n'(2) := 10$.*

Proof. Put

$$\xi := \begin{cases} 0 & \text{if } p \geq 3, \\ 1 & \text{if } p = 2. \end{cases}$$

Let E be an elliptic curve over K satisfying

$$\rho_{E,p}(\mathrm{G}_K) \not\supseteq (1 + p^{n'(p)+\xi}\mathrm{M}_2(\mathbb{Z}_p))^{\det=1}.$$

We show that $j(E) \in K$ takes only finitely many values. Replacing K by $K(\zeta_{p^{n'(p)+1}})$, we may assume $\overline{\rho}_{E,p^{n'(p)+1}}(\mathrm{G}_K) \subseteq \mathrm{SL}_2(\mathbb{Z}/p^{n'(p)+1}\mathbb{Z})$. We may also assume that $\overline{\rho}_{E,p^{n'(p)+1}}(\mathrm{G}_K)$ is contained in a slim subgroup $H \subseteq \mathrm{SL}_2(\mathbb{Z}/p^{n'(p)+1}\mathbb{Z})$ satisfying $H \ni -1$. To see this, we consider two cases ($n'(p) = 0$ or $n'(p) \geq 1$). When $n'(p) = 0$ (equivalently $p \geq 23$), we have $\overline{\rho}_{E,p}(\mathrm{G}_K) \subsetneq \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ by Lemma 2.1, thus $\overline{\rho}_{E,p}(\mathrm{G}_K) \subseteq B, C, D, E$ by Proposition 3.4. But B, C, D, E contains -1. When $n'(p) \geq 1$, Lemma 2.3 shows $\langle \rho_{E,p}(\mathrm{G}_K), -1\rangle \not\supseteq (1+p^{n'(p)}\mathrm{M}_2(\mathbb{Z}_p))^{\det=1}$. Thus $H = \langle \rho_{E,p}(\mathrm{G}_K), -1\rangle \bmod p^{n'(p)+1}$ is a slim subgroup by Lemma 2.2. By the hypothesis and Proposition 3.3, we have $g(X_H) = g_H \geq 2$. By Theorem 3.2, we see that $X_H(K)$ is finite, hence $Y_H(K)$ is also finite. Since there are only finitely many subgroups H as above, the existence of n follows from Lemma 3.1. As $g(X_0(19)) = 1$, the integer $n(19)$ cannot be 0. We also have $g(X_0(17)) = 1$, $g(X_0(13)) = 0$, $g(X_0(11)) = 1$ and $g(X_0(7^2)) = 1$. Thus we get $n(19) = n(17) = n(13) = n(11) = 1$ and $n(7) = 2$. □

We prove $\delta_H > 0$ for any subgroup H as in Proposition 3.8. More explicitly, we prove the following theorem in Section 7.

Theorem 3.9. *1. For a subgroup $H \subseteq \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, we have $\delta_H > 0$ if one of the following conditions is satisfied.*

- *$H \subseteq B$ and $p \geq 23$*
- *$H \subseteq C$ and $p \geq 11$*
- *$H \subseteq D$ and $p \geq 13$*
- *$H \subseteq E$ and $p \geq 17$*

2. For a slim subgroup $H \subseteq \mathrm{SL}_2(\mathbb{Z}/p^2\mathbb{Z})$, we have $\delta_H > 0$ if one of the following conditions is satisfied.

- *$H \bmod p \subseteq B$ and $p \geq 11$*
- *$H \bmod p \subseteq D$ and $p \geq 11$*
- *$H \bmod p \subseteq E$ and $p \geq 11$*

3. For a slim subgroup $H \subseteq \mathrm{SL}_2(\mathbb{Z}/p^3\mathbb{Z})$, we have $\delta_H > 0$ if one of the following conditions is satisfied.

- $H \bmod p \subseteq B$ *and* $p \geq 7$
- $H \bmod p \subseteq C$ *and* $p \geq 5$
- $H \bmod p \subseteq D$ *and* $p \geq 7$
- $H \bmod p \subseteq E$ *and* $p \geq 7$

4. For a slim subgroup $H \subseteq \mathrm{SL}_2(\mathbb{Z}/5^4\mathbb{Z})$*, we have* $\delta_H > 0$ *if one of the following conditions is satisfied.*

- $H \bmod 5 \subseteq B$
- $H \bmod 5 \subseteq D$
- $H \bmod 5 \subseteq E$

5. For a slim subgroup $H \subseteq \mathrm{SL}_2(\mathbb{Z}/3^6\mathbb{Z})$*, we have* $\delta_H > 0$ *if one of the following conditions is satisfied.*

- $H \bmod 3 \subseteq B$
- $H \bmod 3 \subseteq D$
- $H \bmod 3 \subseteq E$
- $H \bmod 3 = \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$

6. For a slim subgroup $H \subseteq \mathrm{SL}_2(\mathbb{Z}/2^{10}\mathbb{Z})$*, we have* $\delta_H > 0$ *if one of the following conditions is satisfied.*

- $H \bmod 2 \subseteq$ (*subgroup of order* 3)
- $H \bmod 2 = \mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$

7. For a slim subgroup $H \subseteq \mathrm{SL}_2(\mathbb{Z}/2^{11}\mathbb{Z})$*, we have* $\delta_H > 0$ *if the following condition is satisfied.*

- $H \bmod 2 \subseteq B$

4. Calculation of conjugate elements in $\mathbf{SL_2}(\mathbb{Z}/p\mathbb{Z})$

Now we calculate the number of elements conjugate to σ, τ, u in the maximal subgroups B, C, D, E introduced in Section 3.

Lemma 4.1. *In* $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$*, the number of elements conjugate to* σ*,* τ*,* u *in* B*,* C*,* D*,* E *are as follows.*

1.

$$\sharp B \cap \mathrm{Conj}(\sigma) = \begin{cases} 0 & \text{if } p \equiv -1 \mod 4, \\ 2p & \text{if } p \equiv 1 \mod 4, \\ 1 & \text{if } p = 2. \end{cases}$$

$$\sharp B \cap \mathrm{Conj}(\tau) = \begin{cases} 0 & \text{if } p \equiv -1 \mod 3, \\ 2p & \text{if } p \equiv 1 \mod 3, \\ 1 & \text{if } p = 3. \end{cases}$$

$$\sharp B \cap \mathrm{Conj}(u) = \begin{cases} \frac{1}{2}(p-1) & \text{if } p \geq 3, \\ 1 & \text{if } p = 2. \end{cases}$$

2.

$$\sharp C \cap \mathrm{Conj}(\sigma) = \begin{cases} p-1 & \text{if } p \equiv -1 \mod 4, \\ p+1 & \text{if } p \equiv 1 \mod 4, \\ 1 & \text{if } p = 2. \end{cases}$$

$$\sharp C \cap \mathrm{Conj}(\tau) = \begin{cases} 0 & \text{if } p \not\equiv 1 \mod 3, \\ 2 & \text{if } p \equiv 1 \mod 3. \end{cases}$$

$$\sharp C \cap \mathrm{Conj}(u) = \begin{cases} 0 & \text{if } p \geq 3, \\ 1 & \text{if } p = 2. \end{cases}$$

3.

$$\sharp D \cap \mathrm{Conj}(\sigma) = \begin{cases} p+3 & \text{if } p \equiv -1 \mod 4, \\ p+1 & \text{if } p \equiv 1 \mod 4, \end{cases}$$

$$\sharp D \cap \mathrm{Conj}(\tau) = \begin{cases} 2 & \text{if } p \geq 5 \text{ and } p \equiv -1 \mod 3, \\ 0 & \text{if } p = 3 \text{ or } p \equiv 1 \mod 3. \end{cases}$$

$$\sharp D \cap \mathrm{Conj}(u) = 0 \quad \text{if } p \geq 3.$$

4.

$$\sharp E \cap \mathrm{Conj}(\sigma) \leq \begin{cases} 30 & \text{if } p \equiv \pm 1 \mod 5, \\ 18 & \text{if } p \geq 5 \text{ and } p \not\equiv \pm 1 \mod 5. \end{cases}$$

$$\sharp E \cap \mathrm{Conj}(\tau) \leq \begin{cases} 20 & \text{if } p \equiv \pm 1 \mod 5, \\ 8 & \text{if } p \geq 5 \text{ and } p \not\equiv \pm 1 \mod 5. \end{cases}$$

$$\sharp E \cap \mathrm{Conj}(u) = 0 \quad \text{if } p \geq 5.$$

5. Calculation of conjugate elements in $\mathbf{SL_2}(\mathbb{Z}/\boldsymbol{p^n}\mathbb{Z})$

We calculate the number of elements conjugate to σ, τ, u in $\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$.

Lemma 5.1. *Let $n \geq 1$ be an integer. In $\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$ we have*

$$\sharp\mathrm{Conj}(\sigma) = \begin{cases} (p-1)p^{2n-1} & \text{if } p \equiv -1 \mod 4, \\ (p+1)p^{2n-1} & \text{if } p \equiv 1 \mod 4, \\ 3 & \text{if } p = 2 \text{ and } n = 1, \\ 3 \cdot 2^{2n-3} & \text{if } p = 2 \text{ and } n \geq 2, \end{cases}$$

$$\sharp\mathrm{Conj}(\tau) = \begin{cases} (p-1)p^{2n-1} & \text{if } p \equiv -1 \mod 3, \\ (p+1)p^{2n-1} & \text{if } p \equiv 1 \mod 3, \\ 4 \cdot 3^{2n-2} & \text{if } p = 3, \end{cases}$$

$$\sharp\mathrm{Conj}(u) = \begin{cases} \frac{1}{2}(p^2-1)p^{2n-2} & \text{if } p \geq 3, \\ 3 & \text{if } p = 2 \text{ and } n = 1, \\ 6 & \text{if } p = 2 \text{ and } n = 2, \\ 3 \cdot 2^{2n-4} & \text{if } p = 2 \text{ and } n \geq 3. \end{cases}$$

Next we calculate the number of elements conjugate to u^{p^r} in $\mathrm{SL}_2(\mathbb{Z}/p^{r+n}\mathbb{Z})$.

Lemma 5.2. *Assume $r \geq 0$ and $n \geq 1$. In $\mathrm{SL}_2(\mathbb{Z}/p^{r+n}\mathbb{Z})$, we have*

$$\sharp\mathrm{Conj}(u^{p^r}) = \begin{cases} \frac{1}{2}(p^2-1)p^{2n-2} & \text{if } p \geq 3, \\ 3 & \text{if } p = 2 \text{ and } n = 1, \\ 6 & \text{if } p = 2 \text{ and } n = 2, \\ 3 \cdot 2^{2n-4} & \text{if } p = 2 \text{ and } n \geq 3. \end{cases}$$

We study the fiber of the mod p^m map

$$\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z}) \cap \mathrm{Conj}(\alpha) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/p^m\mathbb{Z}) \cap \mathrm{Conj}(\alpha),$$

where $\alpha = \sigma, \tau, u^{p^r}$.

Take two integers m, n with $1 \leq m \leq n$. As in Section 1, let

$$f_{n,m} : \mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/p^m\mathbb{Z})$$

be the mod p^m map. For $\alpha = \sigma, \tau, u^{p^r}$ $(r \geq 0)$, put

$$V_\alpha^{r+n,r+m} = \alpha^{-1}(f_{r+n,r+m}^{-1}(\alpha) \cap \mathrm{Conj}(\alpha)) \subseteq \mathrm{SL}_2(\mathbb{Z}/p^{r+n}\mathbb{Z}).$$

When $\alpha = \sigma, \tau$, we always take $r = 0$. We sometimes omit the superscripts r, n, m and simply write V_α.

Lemma 5.3. *Let $r \geq 0$, $1 \leq m < n$ be integers. Assume $n \leq 2m$. If $p \geq 3$, then each $V_\alpha^{r+n,r+m}$ $(\alpha = \sigma, \tau, u^{p^r})$ is a subgroup of*

$$(1 + p^{r+m}\mathrm{M}_2(\mathbb{Z}/p^{r+n}\mathbb{Z}))^{\det=1} \cong \mathrm{M}_2(\mathbb{Z}/p^{n-m}\mathbb{Z})^{\mathrm{Tr}=0}$$

and is isomorphic to $(\mathbb{Z}/p^{n-m}\mathbb{Z})^2$. If $p = 2$, then $V_\sigma^{n,m}$ for $m \geq 2$ (resp. $V_\tau^{n,m}$ for any m, resp. $V_{u^{p^r}}^{r+n,r+m}$ for $m \geq 3$) is a subgroup of

$$(1 + p^{r+m}\mathrm{M}_2(\mathbb{Z}/p^{r+n}\mathbb{Z}))^{\det=1} \cong \mathrm{M}_2(\mathbb{Z}/p^{n-m}\mathbb{Z})^{\mathrm{Tr}=0}$$

and is isomorphic to $(\mathbb{Z}/p^{n-m}\mathbb{Z})^2$. Explicitly:

If $p \geq 3$ or ($p = 2$ and $m \geq 2$), we have

$$\begin{aligned} V_\sigma^{n,m} &= \left\{ 1 + p^m \begin{pmatrix} a & b \\ b & -a \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z}) \right\} \\ &\cong \left\{ \begin{pmatrix} a & b \\ b & -a \end{pmatrix} \in \mathrm{M}_2(\mathbb{Z}/p^{n-m}\mathbb{Z}) \right\}; \end{aligned}$$

For any p and m, we have

$$V_\tau^{n,m} = \left\{1 + p^m \begin{pmatrix} a & b \\ b-a & -a \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})\right\}$$
$$\cong \left\{\begin{pmatrix} a & b \\ b-a & -a \end{pmatrix} \in \mathrm{M}_2(\mathbb{Z}/p^{n-m}\mathbb{Z})\right\};$$

If $p \geq 3$ or ($p = 2$ and $m \geq 3$), we have

$$V_{u^{p^r}}^{r+n,r+m} = \left\{1 + p^{r+m} \begin{pmatrix} a & b \\ 0 & -a \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/p^{r+n}\mathbb{Z})\right\}$$
$$\cong \left\{\begin{pmatrix} a & b \\ 0 & -a \end{pmatrix} \in \mathrm{M}_2(\mathbb{Z}/p^{n-m}\mathbb{Z})\right\}.$$

In particular, the inverse image of one element by the following maps consists of p^2 elements:

- $\bmod p^m : \mathrm{SL}_2(\mathbb{Z}/p^{m+1}\mathbb{Z}) \cap \mathrm{Conj}(\sigma) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/p^m\mathbb{Z}) \cap \mathrm{Conj}(\sigma)$ *if $p \geq 3$ or ($p = 2$ and $m \geq 2$),*
- $\bmod p^m : \mathrm{SL}_2(\mathbb{Z}/p^{m+1}\mathbb{Z}) \cap \mathrm{Conj}(\tau) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/p^m\mathbb{Z}) \cap \mathrm{Conj}(\tau)$ *for any p and any $m \geq 1$,*
- $\bmod p^{r+m} : \mathrm{SL}_2(\mathbb{Z}/p^{r+m+1}\mathbb{Z}) \cap \mathrm{Conj}(u^{p^r}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/p^{r+m}\mathbb{Z}) \cap \mathrm{Conj}(u^{p^r})$ *if $p \geq 3$ or ($p = 2$ and $m \geq 3$).*

Remark 5.4. *If $p = 2$, the inverse image of one element by the following maps consists of 2 elements:*

- $\bmod 2 : \mathrm{SL}_2(\mathbb{Z}/2^2\mathbb{Z}) \cap \mathrm{Conj}(\sigma) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z}) \cap \mathrm{Conj}(\sigma)$,
- $\bmod 2^{r+2} : \mathrm{SL}_2(\mathbb{Z}/2^{r+3}\mathbb{Z}) \cap \mathrm{Conj}(u^{2^r}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/2^{r+2}\mathbb{Z}) \cap \mathrm{Conj}(u^{2^r})$,
- $\bmod 2^{r+1} : \mathrm{SL}_2(\mathbb{Z}/2^{r+2}\mathbb{Z}) \cap \mathrm{Conj}(u^{2^r}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/2^{r+1}\mathbb{Z}) \cap \mathrm{Conj}(u^{2^r})$.

From now on, we always assume the hypothesis in Lemma 5.3 when we write $V_\alpha^{r+n,r+m}$ (for $\alpha = \sigma, \tau, u^{p^r}$ and their conjugates: defined below), so that $V_\alpha^{r+n,r+m}$ is a free $\mathbb{Z}/p^{n-m}\mathbb{Z}$-submodule of rank 2 of $(1 + p^{r+m}\mathrm{M}_2(\mathbb{Z}/p^{r+n}\mathbb{Z}))^{\det=1} \cong \mathrm{M}_2(\mathbb{Z}/p^{n-m}\mathbb{Z})^{\mathrm{Tr}=0}$.

Lemma 5.5. *Let $r \geq 0$, $1 \leq m < n$ be integers. Assume $n \leq 2m$. For $\alpha = \sigma$, τ, u^{p^r}, we have*

$$V_\alpha^{r+n,r+m} = \{1 + p^m(X\alpha^{-1} - \alpha^{-1}X) | X \in \mathrm{M}_2(\mathbb{Z}/p^{r+n}\mathbb{Z})\}.$$

Lemma 5.6. *Let $r \geq 0$, $1 \leq m < n$ be integers. For $\alpha = \sigma, \tau, u^{p^r}$, take an element $\alpha' \in \mathrm{Conj}(\alpha) \subseteq \mathrm{SL}_2(\mathbb{Z}/p^{r+m}\mathbb{Z})$. Suppose two elements $\alpha_1, \alpha_2 \in \mathrm{Conj}(\alpha) \subseteq \mathrm{SL}_2(\mathbb{Z}/p^{r+n}\mathbb{Z})$ satisfy $\alpha_1 \equiv \alpha_2 \equiv \alpha' \bmod p^{r+m}$. If $n \leq 2m$, then we have*

$${\alpha_1}^{-1}(f_{r+n,r+m}^{-1}(\alpha') \cap \mathrm{Conj}(\alpha)) = {\alpha_2}^{-1}(f_{r+n,r+m}^{-1}(\alpha') \cap \mathrm{Conj}(\alpha)).$$

In the above lemma, we define

$$V_{\alpha'}^{r+n,r+m} := {\alpha_1}^{-1}(f_{r+n,r+m}^{-1}(\alpha') \cap \mathrm{Conj}(\alpha)).$$

Note that we have $V_{\alpha'}^{r+n,r+m} = \{1 + p^m(X{\alpha'}^{-1} - {\alpha'}^{-1}X)\}$. For an element $g \in \mathrm{SL}_2(\mathbb{Z}/p^{r+n}\mathbb{Z})$, we have $V_{g^{-1}\alpha' g}^{r+n,r+m} = g^{-1}(V_{\alpha'}^{r+n,r+m})g$. We see that $V_{\alpha'}^{r+n,r+m}$ depends only on $\alpha' \bmod p^{r+n-m}$. Thus we can define $V_{\alpha''}^{r+n,r+m}$ for $\alpha'' \in \mathrm{Conj}(\alpha) \subseteq \mathrm{SL}_2(\mathbb{Z}/p^{r+n-m}\mathbb{Z})$.

For $\alpha = \sigma, \tau, u^{p^r}$ and their conjugates, we identify $V_{\alpha}^{r+n,r+m}$ with a free submodule of rank 2 of $\mathrm{M}_2(\mathbb{Z}/p^{n-m}\mathbb{Z})$ using the isomorphisms in Lemma 5.3.

Lemma 5.7. *Let $1 \leq m < n$ be integers. Take an element $\alpha \in \mathrm{SL}_2(\mathbb{Z}/p^m\mathbb{Z})$ which is conjugate to σ or τ. Assume $n \leq 2m$. Then $V_{\alpha}^{n,m}$ is the orthogonal complement of $\mathbb{Z}/p^{n-m}\mathbb{Z}[\alpha]$ in $\mathrm{M}_2(\mathbb{Z}/p^{n-m}\mathbb{Z})$ with respect to the pairing*

$$\mathrm{M}_2(\mathbb{Z}/p^{n-m}\mathbb{Z}) \times \mathrm{M}_2(\mathbb{Z}/p^{n-m}\mathbb{Z}) \longrightarrow \mathbb{Z}/p^{n-m}\mathbb{Z} \ : \ (A, B) \mapsto \mathrm{Tr}\,(AB).$$

Lemma 5.8. *Let $r \geq 0$, $1 \leq m < n$ be integers. Take an element $v = 1 + p^r\epsilon \in \mathrm{Conj}(u^{p^r}) \subseteq \mathrm{SL}_2(\mathbb{Z}/p^{r+m}\mathbb{Z})$. Assume $n \leq 2m$. Then $V_v^{r+n,r+m}$ is the orthogonal complement of $\mathbb{Z}/p^{n-m}\mathbb{Z}[\epsilon]$ in $\mathrm{M}_2(\mathbb{Z}/p^{n-m}\mathbb{Z})$ with respect to the pairing*

$$\mathrm{M}_2(\mathbb{Z}/p^{n-m}\mathbb{Z}) \times \mathrm{M}_2(\mathbb{Z}/p^{n-m}\mathbb{Z}) \longrightarrow \mathbb{Z}/p^{n-m}\mathbb{Z} \ : \ (A, B) \mapsto \mathrm{Tr}\,(AB).$$

Next we study the condition for the equality $V_{\alpha} = V_{\alpha'}$, where $\alpha' \in \mathrm{Conj}(\alpha)$.

Corollary 5.9. *Let $1 \leq m < n$ be integers. Take two elements $\sigma', \sigma'' \in \mathrm{Conj}(\sigma) \subseteq \mathrm{SL}_2(\mathbb{Z}/p^m\mathbb{Z})$. Assume $p \geq 3$ and $n \leq 2m$. Then $V_{\sigma'}^{n,m} = V_{\sigma''}^{n,m}$ holds if and only if $\sigma' \equiv \sigma''^{\pm 1} \bmod p^{n-m}$.*

Corollary 5.10. *Let $2 \leq m < n$ be integers. Fix an element $\sigma' \in \mathrm{Conj}(\sigma) \subseteq \mathrm{SL}_2(\mathbb{Z}/2^m\mathbb{Z})$. Assume $n \leq 2m$. Then the number of elements $\sigma'' \in \mathrm{Conj}(\sigma) \subseteq \mathrm{SL}_2(\mathbb{Z}/2^{n-m}\mathbb{Z})$ satisfying $V_{\sigma''}^{n,m} = V_{\sigma'}^{n,m}$ is*

$$\begin{cases} 1 & \text{if } n - m = 1, \\ 2 & \text{if } n - m = 2, \\ 4 & \text{if } n - m \geq 3. \end{cases}$$

Corollary 5.11. *Let $1 \leq m < n$ be integers. Take two elements $\tau', \tau'' \in \mathrm{Conj}(\tau) \subseteq \mathrm{SL}_2(\mathbb{Z}/p^m\mathbb{Z})$. Assume $p \neq 3$ and $n \leq 2m$. Suppose $m \geq 2$ if $p = 2$. Then $V_{\tau'}^{n,m} = V_{\tau''}^{n,m}$ holds if and only if $\tau' \equiv \tau''^{\pm 1} \bmod p^{n-m}$.*

Corollary 5.12. *Let $1 \leq m < n$ be integers. Fix an element $\tau' \in \mathrm{Conj}(\tau) \subseteq \mathrm{SL}_2(\mathbb{Z}/3^m\mathbb{Z})$. Assume $n \leq 2m$. Then the number of elements $\tau'' \in \mathrm{Conj}(\tau) \subseteq$*

$\mathrm{SL}_2(\mathbb{Z}/3^{n-m}\mathbb{Z})$ *satisfying* $V^{n,m}_{\tau''} = V^{n,m}_{\tau'}$ *is*

$$\begin{cases} 1 & \text{if } n-m=1, \\ 3 & \text{if } n-m \geq 2. \end{cases}$$

Corollary 5.13. *Let $r \geq 0$, $1 \leq m < n$ be integers. Take two elements $v, v' \in \mathrm{Conj}(u^{p^r}) \subseteq \mathrm{SL}_2(\mathbb{Z}/p^{r+m}\mathbb{Z})$. Assume $p \geq 3$ and $n \leq 2m$. Then $V^{r+n,r+m}_v = V^{r+n,r+m}_{v'}$ holds if and only if $v \equiv v'^{s^2} \bmod p^{r+n-m}$ where $(p,s)=1$.*

Corollary 5.14. *Let $r \geq 0$, $3 \leq m < n$ be integers. Fix an element $v \in \mathrm{Conj}(u^{2^r}) \subseteq \mathrm{SL}_2(\mathbb{Z}/2^{r+m}\mathbb{Z})$. Assume $n \leq 2m$. Then the number of elements $v' \in \mathrm{Conj}(u^{2^r}) \subseteq \mathrm{SL}_2(\mathbb{Z}/2^{r+n-m}\mathbb{Z})$ satisfying $V^{r+n,r+m}_{v'} = V^{r+n,r+m}_v$ is*

$$\begin{cases} 1 & \text{if } n-m=1, \\ 2 & \text{if } n-m=2, \\ 2^{n-m-2} & \text{if } n-m \geq 3. \end{cases}$$

6. Control of inverse images

We control the number of elements conjugate to σ, τ, u^{p^r} contained in a slim subgroup H.

Let $n \geq 1$ be an integer and let H be a subgroup of $\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$. For an integer $1 \leq s \leq n$, put

$$H_s := H \cap (1 + p^s \mathrm{M}_2(\mathbb{Z}/p^n\mathbb{Z})) = \mathrm{Ker}\,(\mathrm{mod} p^s : H \longrightarrow \mathrm{SL}_2(\mathbb{Z}/p^s\mathbb{Z})).$$

We identify H/H_s with $H \bmod p^s$. For two integers s, t with $1 \leq s \leq t \leq n$ and for $\alpha = \sigma, \tau, u^{p^r}$, let

$$f^{H,\alpha}_{t,s} : (H/H_t) \cap \mathrm{Conj}(\alpha) \longrightarrow (H/H_s) \cap \mathrm{Conj}(\alpha)$$

be the mod p^s map. Here we assume $s > r$ when $\alpha = u^{p^r}$.

Recall that a subgroup $H \subseteq \mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$ is called a slim subgroup if $H \not\supseteq (1 + p^{n-1}\mathrm{M}_2(\mathbb{Z}/p^n\mathbb{Z}))^{\det=1}$, equivalently $\sharp H_{n-1} \leq p^2$. We prepare for controlling $\sharp H \cap \mathrm{Conj}(\alpha)$ for a slim subgroup H.

Lemma 6.1. *Let $n \geq 2$ be an integer and let $H \subseteq \mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$ be a slim subgroup. Take two integers s, t with $1 \leq t < s \leq n$. Assume $t \geq 2$ if $p = 2$. Then we have $\sharp H_t/H_s \leq p^{2(s-t)}$.*

Proof. Put $G = \mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$. Take an integer i with $2 \leq i \leq n-1$. Assume $i \geq 3$ if $p = 2$. Then the p-th power map $\eta : G_{i-1}/G_i \longrightarrow G_i/G_{i+1}$ is surjective (where $G_i := G \cap (1+p^i \mathrm{M}_2(\mathbb{Z}/p^n\mathbb{Z}))$). As $\sharp G_{i-1}/G_i = \sharp G_i/G_{i+1} = p^3$, we see that η is an isomorphism. Let $\eta' : H_{i-1}/H_i \longrightarrow H_i/H_{i+1}$ be the p-th power map. The commutative diagram

$$\begin{array}{ccc} H_{i-1}/H_i & \xrightarrow{\subseteq} & G_{i-1}/G_i \\ {\scriptstyle \eta'}\downarrow & & \downarrow{\scriptstyle \eta} \\ H_i/H_{i+1} & \xrightarrow{\subseteq} & G_i/G_{i+1} \end{array}$$

shows that η' is injective. By the hypothesis $H \not\supseteq (1+p^{n-1}\mathrm{M}_2(\mathbb{Z}/p^n\mathbb{Z}))^{\det=1}$, we have $H_{n-1}/H_n \subsetneq G_{n-1}/G_n$. Hence $\sharp H_{n-1}/H_n \leq p^2$. Therefore $\sharp H_1/H_2 \leq \sharp H_2/H_3 \leq \cdots \leq \sharp H_{n-1}/H_n \leq p^2$ if $p \geq 3$, while $\sharp H_2/H_3 \leq \sharp H_3/H_4 \leq \cdots \leq \sharp H_{n-1}/H_n \leq p^2$ if $p = 2$. Consequently, we get $\sharp H_t/H_s = \prod_{i=t+1}^{s} \sharp H_{i-1}/H_i \leq p^{2(s-t)}$. □

From now to the end of this section, we use the letter α to denote any of σ, τ, u^{p^r}, where $r \geq 0$ be an integer. As usual, assume $r = 0$ if $\alpha = \sigma, \tau$.

Corollary 6.2. *Let $n \geq 2$ be an integer and let $H \subseteq \mathrm{SL}_2(\mathbb{Z}/p^{r+n}\mathbb{Z})$ be a slim subgroup. Take two integers s, t with $1 \leq t < s \leq n$. Take an element $\alpha' \in \mathrm{Conj}(\alpha) \subseteq \mathrm{SL}_2(\mathbb{Z}/p^{r+t}\mathbb{Z})$. Assume $s \leq 2t$. When $p = 2$, further assume $r + t \geq 2$. If $H/H_{r+s} \supseteq V_{\alpha'}^{r+s,r+t}$, then $H_{r+t}/H_{r+s} = V_{\alpha'}^{r+s,r+t}$.*

Lemma 6.3. *Let $n \geq 2$ be an integer and let $H \subseteq \mathrm{SL}_2(\mathbb{Z}/p^{r+n}\mathbb{Z})$ be a slim subgroup. Take three integers s, t, i satisfying $1 \leq t < s \leq n$ and $i \geq 1$. Take an element $\alpha' \in \mathrm{Conj}(\alpha) \subseteq \mathrm{SL}_2(\mathbb{Z}/p^{r+t}\mathbb{Z})$. Assume $s \leq 2t$ and $s + i \leq n$. When $p = 2$ and $\alpha = \tau$, further assume $s \leq 2t - 1$. If $H_{r+t}/H_{r+s} = V_{\alpha'}^{r+s,r+t}$, then $H_{r+t+i}/H_{r+s+i} = V_{\alpha'}^{r+s+i,r+t+i}$.*

Lemma 6.4. *Let $n \geq 2$ be an integer and let $H \subseteq \mathrm{SL}_2(\mathbb{Z}/p^{r+n}\mathbb{Z})$ be a subgroup. Take two integers t, i with $t \geq 1$, $i \geq 1$ and $t + i \leq n$. Take an element $\alpha' \in (H/H_{r+t}) \cap \mathrm{Conj}(\alpha)$. Assume $i \leq t$. If $H_{r+t}/H_{r+t+i} \neq V_{\alpha'}^{r+t+i,r+t}$, then we have $\sharp f_{r+t+i,r+t+1}((f_{r+t+i,r+t}^{H,\alpha})^{-1}(\alpha')) \leq p$.*

Proof. We show the lemma only when $r = 0$. Put

$$X := f_{t+i,t+1}((f_{t+i,t}^{H,\alpha})^{-1}(\alpha')).$$

Suppose $(f_{t+i,t}^{H,\alpha})^{-1}(\alpha') \neq \emptyset$. Take an element $\widetilde{\alpha} \in (f_{t+i,t}^{H,\alpha})^{-1}(\alpha')$. The natural surjection mod $p^{t+1} : (f_{t+i,t}^{H,\alpha})^{-1}(\alpha') \longrightarrow X$ induces the following commutative diagram :

$$\begin{array}{ccc} V_{\alpha'}^{t+i,t} \cap (H/H_{t+i}) & \xrightarrow{\mathrm{mod}p^{t+1}} & \widetilde{\alpha}^{-1}X \\ \subsetneq\big\downarrow & & \subseteq\big\downarrow \\ V_{\alpha'}^{t+i,t} & \xrightarrow{\mathrm{mod}p^{t+1}} & V_{\alpha'}^{t+1,t} \\ \cong\big\downarrow & & \cong\big\downarrow \\ (\mathbb{Z}/p^i\mathbb{Z})^{\oplus 2} & \xrightarrow{\mathrm{mod}p} & (\mathbb{Z}/p\mathbb{Z})^{\oplus 2}. \end{array}$$

All the horizontal maps in the above diagram are surjective. Since $V_{\alpha'}^{t+i,t} \cap (H/H_{t+i}) = V_{\alpha'}^{t+i,t} \cap (H_t/H_{t+i})$ is a proper subgroup of $V_{\alpha'}^{t+i,t} \cong (\mathbb{Z}/p^i\mathbb{Z})^{\oplus 2}$, we have $\sharp V_{\alpha'}^{t+i,t} \cap (H/H_{t+i}) \leq p^{2i-1}$. Since no proper subgroup of $(\mathbb{Z}/p^i\mathbb{Z})^{\oplus 2}$ maps surjectively mod$p$ onto $(\mathbb{Z}/p\mathbb{Z})^{\oplus 2}$, we get $\sharp\widetilde{\alpha}^{-1}X \leq p$. □

Corollary 6.5. *Let $n \geq 2$ be an integer and let $H \subseteq \mathrm{SL}_2(\mathbb{Z}/p^{r+n}\mathbb{Z})$ be a slim subgroup. Take two integers $i \geq 1$, $\delta \geq 0$ with $i + \delta \leq n$. Take an element $\alpha' \in (H/H_{r+i+\delta}) \cap \mathrm{Conj}(\alpha)$. Assume $2i + \delta \leq n$. When $p = 2$ and $\alpha = \tau$, further assume $\delta \geq 1$. If $H_{r+n-i}/H_{r+n} \neq V_{\alpha'}^{r+n,r+n-i}$, then we have $\sharp(f_{r+n,r+i+\delta}^{H,\alpha})^{-1}(\alpha') \leq p^{n-1-\delta}$.*

Let $n \geq 2$ be an integer and let $H \subseteq \mathrm{SL}_2(\mathbb{Z}/p^{r+n}\mathbb{Z})$ be a slim subgroup. Put

$$l := \begin{cases} \frac{n}{2} & \text{if } n \text{ is even,} \\ \frac{n-1}{2} & \text{if } n \text{ is odd.} \end{cases}$$

Define a decreasing sequence

$$Y_0 \supseteq Y_1 \supseteq \cdots \supseteq Y_i \supseteq Y_{i+1} \supseteq \cdots \supseteq Y_l$$

by

$$Y_i := \begin{cases} H \cap \mathrm{Conj}(\alpha) & \text{if } i = 0, \\ \{\alpha' \in H \cap \mathrm{Conj}(\alpha) | H_{r+n-i} = V_{\alpha'}^{r+n,r+n-i}\} & \text{if } 1 \leq i \leq l. \end{cases}$$

When $p \geq 3$, we use Y_i for $0 \leq i \leq l$; when $p = 2$, we use Y_i only for

$$\begin{cases} i = 0, 1 & \text{if } \alpha = \sigma \text{ and } 3 \leq n \leq 5, \\ 0 \leq i \leq l & \text{if } \alpha = \sigma \text{ and } n \geq 6, \\ i = 0,\ 3 \leq i \leq l & \text{if } \alpha = u^{2^r} \text{ and } n \geq 6, \end{cases}$$

so that the hypothesis in Lemma 5.3 is satisfied.

By the study above, we have the following estimate.

Proposition 6.6. *Let $n \geq 2$ be an integer and let $H \subseteq \mathrm{SL}_2(\mathbb{Z}/p^{r+n}\mathbb{Z})$ be a slim subgroup. Take an integer s satisfying $1 \leq s \leq l$. Then we have*

$$\begin{aligned}\sharp H \cap \mathrm{Conj}(\alpha) \leq{}& (p^{2(n-l)} - p^{n-1})\sharp(Y_l \bmod p^{r+l}) \\ &+ (p^2-1)p^{n-1}\sum_{i=s}^{l-1}\sharp(Y_i \bmod p^{r+i}) \\ &+ p^{n-1}\sharp(H/H_{r+s}) \cap \mathrm{Conj}(\alpha).\end{aligned}$$

We control the number of elements conjugate to σ in a slim subgroup $H \subseteq \mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$ when $p \geq 3$.

For $p \geq 3$, define a sequence $\{a(\sigma,p)_n\}_{n\geq 2}$ as follows:

$$a(\sigma,p)_n := 2p^{2(n-l)} + 2(l-1)(p^2-1)p^{n-1},$$

where $n = 2l$ or $2l+1$.

Corollary 6.7. *Let $n \geq 2$ be an integer and let $H \subseteq \mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$ be a slim subgroup. Assume $p \geq 3$. Then we have*

$$\sharp H \cap \mathrm{Conj}(\sigma) \leq a(\sigma,p)_n + p^{n-1}(\sharp(H/H_1) \cap \mathrm{Conj}(\sigma) - 2).$$

Proof. Apply Corollary 5.9 and Proposition 6.6 (put $s = 1$). □

We control the number of elements conjugate to τ in a slim subgroup $H \subseteq \mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$ when $p \geq 3$.

For $p \geq 5$, define a sequence $\{a(\tau,p)_n\}_{n\geq 2}$ by

$$a(\tau,p)_n := a(\sigma,p)_n.$$

Corollary 6.8. *Let $n \geq 2$ be an integer and let $H \subseteq \mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$ be a slim subgroup. Assume $p \geq 5$. Then we have*

$$\sharp H \cap \mathrm{Conj}(\tau) \leq a(\tau,p)_n + p^{n-1}(\sharp(H/H_1) \cap \mathrm{Conj}(\tau) - 2).$$

Define a sequence $\{a(\tau,3)_n\}_{n\geq 2}$ as follows:

$$a(\tau,3)_n := \begin{cases} 3^2 & \text{if } n = 2, \\ (4n-11)\cdot 3^n & \text{if } n = 2l \geq 4, \\ (4n-9)\cdot 3^n & \text{if } n = 2l+1. \end{cases}$$

Corollary 6.9. *Let $n \geq 2$ be an integer and let $H \subseteq \mathrm{SL}_2(\mathbb{Z}/3^n\mathbb{Z})$ be a slim subgroup. Then we have*

$$\sharp H \cap \mathrm{Conj}(\tau) \leq a(\tau,3)_n + 3^{n-1}(\sharp(H/H_1) \cap \mathrm{Conj}(\tau) - 1).$$

We control the number of elements conjugate to u^{p^r} in a slim subgroup $H \subseteq \mathrm{SL}_2(\mathbb{Z}/p^{r+n}\mathbb{Z})$.

For $p \geq 3$, define a sequence $\{a(u,p)_n\}_{n\geq 2}$ as follows:

$$a(u,p)_n := \begin{cases} \frac{1}{2}(p-1)(2\cdot p^{3l-1} - p^n) & \text{if } n = 2l, \\ \frac{1}{2}(p-1)(p^{3l+1} + p^{3l} - p^n) & \text{if } n = 2l+1. \end{cases}$$

Corollary 6.10. *Let $r \geq 0$, $n \geq 2$ be integers and let $H \subseteq \mathrm{SL}_2(\mathbb{Z}/p^{r+n}\mathbb{Z})$ be a slim subgroup. Assume $p \geq 3$. Then we have*

$$\sharp H \cap \mathrm{Conj}(u^{p^r}) \leq a(u,p)_n + p^{n-1}(\sharp(H/H_{r+1}) \cap \mathrm{Conj}(u^{p^r}) - \frac{1}{2}(p-1)).$$

Define a sequence $\{a(u,2)_n\}_{n\geq 6}$ as follows:

$$a(u,2)_n := \begin{cases} 2^{3l-1} - 2^{n+1} & \text{if } n = 2l, \\ 3 \cdot 2^{3l-1} - 2^{n+1} & \text{if } n = 2l+1. \end{cases}$$

Corollary 6.11. *Let $r \geq 0$, $n \geq 6$ be integers and let $H \subseteq \mathrm{SL}_2(\mathbb{Z}/2^{r+n}\mathbb{Z})$ be a slim subgroup. Then we have*

$$\sharp H \cap \mathrm{Conj}(u^{2^r}) \leq a(u,2)_n + 2^{n-1}(\sharp(H/H_{r+3}) \cap \mathrm{Conj}(u^{2^r}) - 2).$$

We control the number of elements conjugate to σ in a slim subgroup $H \subseteq \mathrm{SL}_2(\mathbb{Z}/2^n\mathbb{Z})$.

Define a sequence $\{a(\sigma,2)_n\}_{n\geq 3}$ as follows:

$$a(\sigma,2)_n := \begin{cases} 2^3 & \text{if } n = 3, \\ 2^5 & \text{if } n = 4, \\ 3(l-2) \cdot 2^{n+1} & \text{if } n = 2l \geq 6, \\ (3l-4) \cdot 2^{n+1} & \text{if } n = 2l+1 \geq 5. \end{cases}$$

Proposition 6.12. *Let $n \geq 3$ be an integer and let $H \subseteq \mathrm{SL}_2(\mathbb{Z}/2^n\mathbb{Z})$ be a slim subgroup. Then we have*

$$\sharp H \cap \mathrm{Conj}(\sigma) \leq a(\sigma,2)_n + 2^{n-2}(\sharp(H/H_2) \cap \mathrm{Conj}(\sigma) - 2).$$

We also use a slightly different way to control $\sharp H \cap \mathrm{Conj}(\tau)$.

We control the number of elements conjugate to τ in a slim subgroup $H \subseteq \mathrm{SL}_2(\mathbb{Z}/2^n\mathbb{Z})$.

Define a sequence $\{a(\tau,2)_n\}_{n\geq 5}$ as follows:

$$a(\tau,2)_n := \begin{cases} (3l'-5) \cdot 2^{n+1} & \text{if } n = 2l', \\ (3l'-7) \cdot 2^{n+1} & \text{if } n = 2l'-1. \end{cases}$$

Proposition 6.13. *Let $n \geq 5$ be an integer and let $H \subseteq \mathrm{SL}_2(\mathbb{Z}/2^n\mathbb{Z})$ be a slim subgroup. Then we have*

$$\sharp H \cap \mathrm{Conj}(\tau) \leq a(\tau,2)_n + 2^{n-2}(\sharp(H/H_3) \cap \mathrm{Conj}(\tau) - 8).$$

7. Proof of the main theorem

Now we prove Theorem 3.9.

Lemma 7.1. *Let $p \geq 5$ and assume a subgroup $H \subseteq \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ is contained in an exceptional subgroup E. If $p \geq 17$, then $\delta_H > 0$.*

Proof. In $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, we have $\sharp\mathrm{Conj}(\sigma) \geq (p-1)p$ and $\sharp\mathrm{Conj}(\tau) \geq (p-1)p$ by Lemma 5.1. Lemma 4.1 shows that in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ we have $\sharp E \cap \mathrm{Conj}(\sigma) \leq 30$, $\sharp E \cap \mathrm{Conj}(\tau) \leq 20$ and $\sharp E \cap \mathrm{Conj}(u) = 0$. Since $\sharp E \cap \mathrm{Conj}(u) = 0$, we have $\frac{\sharp\langle u\rangle\backslash G/H}{[G:H]} = \frac{1}{p}$. Therefore $\delta_H \geq 1 - 3\cdot\frac{30}{(p-1)p} - 4\cdot\frac{20}{(p-1)p} - 6\cdot\frac{1}{p} = \frac{p^2-7p-164}{(p-1)p} > 0$ if $p \geq 17$. □

Proposition 7.2. *Assume $p = 19$. For any slim subgroup $H \subseteq \mathrm{SL}_2(\mathbb{Z}/19^2\mathbb{Z})$ satisfying $H/H_1 \subseteq B$, we have $\delta_H > 0$.*

Proof. In $\mathrm{SL}_2(\mathbb{Z}/19^2\mathbb{Z})$, we have $\sharp\mathrm{Conj}(\tau) = 20 \cdot 19^3$ and $\sharp\mathrm{Conj}(u) = \frac{1}{2}(p^2-1)p^2$ by Lemma 5.1. Lemma 4.1 shows that in $\mathrm{SL}_2(\mathbb{Z}/19\mathbb{Z})$ we have $\sharp B \cap \mathrm{Conj}(\sigma) = 0$, $\sharp B \cap \mathrm{Conj}(\tau) = 2p = 38$ and $\sharp B \cap \mathrm{Conj}(u) = \frac{1}{2}(p-1) = 9$. By Corollary 6.8, we have $\sharp H \cap \mathrm{Conj}(\tau) \leq a(\tau,p)_2 + p(38-2) = 74\cdot 19$. Hence $\frac{\sharp H\cap\mathrm{Conj}(\tau)}{\sharp\mathrm{Conj}(\tau)} \leq \frac{74\cdot 19}{20\cdot 19^3} = \frac{37}{10\cdot 19^2}$. We have $\sharp H \cap \mathrm{Conj}(u) \leq p^2 \sharp(H/H_1) \cap \mathrm{Conj}(u)$ by Lemma 5.3. Thus $\frac{\sharp H\cap\mathrm{Conj}(u)}{\sharp\mathrm{Conj}(u)} \leq \frac{p^2\cdot\frac{1}{2}(p-1)}{\frac{1}{2}(p^2-1)p^2} = \frac{1}{p+1}$. Therefore $\frac{\sharp\langle u\rangle\backslash G/H}{[G:H]} \leq \frac{p-1}{p}\cdot\frac{1}{p+1} + \frac{1}{p} = \frac{2}{p+1} = \frac{1}{10}$. Consequently, $\delta_H \geq 1 - 3\cdot 0 - 4\cdot\frac{37}{10\cdot 19^2} - 6\cdot\frac{1}{10} = \frac{1805-74-1083}{5\cdot 19^2} > 0$, as required. □

In other cases, we can show $\delta_H > 0$ similarly.

References

[1] P. Deligne, M. Rapoport, *Les schémas de modules de courbes elliptiques*. Modular functions of one variable, II, 143–316. Lecture Notes in Math. **349**. Springer, Berlin, 1973.

[2] B. Edixhoven, *Rational torsion points on elliptic curves over number fields (after Kamienny and Mazur)*. Séminaire Bourbaki, Vol. 1993/94. Astérisque No. **227** (1995), Exp. No. 782, 4, 209–227.

[3] G. Faltings, *Finiteness theorems for abelian varieties over number fields*. Translated from the German original [Invent. Math. **73** (1983), no. 3, 349–366; ibid. **75** (1984), no. 2, 381] by Edward Shipz. Arithmetic geometry (Storrs, Conn., 1984), 9–27. Springer, New York, 1986.

[4] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*. Invent. Math. **109** (1992), no. 2, 221–229.

[5] N. Katz, B. Mazur, *Arithmetic moduli of elliptic curves*. Annals of Mathematics Studies **108**. Princeton University Press, Princeton, NJ, 1985.

[6] D.-S. Kubert, *Universal bounds on the torsion of elliptic curves*. Proc. London Math. Soc. (3) **33** (1976), no. 2, 193–237.

[7] J. Manin, *The p-torsion of elliptic curves is uniformly bounded*. Translated from the Russian original [Izv. Akad. Nauk SSSR Ser. Mat. **33** (1969), 459–465]. Mathematics of the USSR-Izvestija **3** (1969), No. 3-4, 433–438.

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

[9] B. Mazur, *Rational points on modular curves*. Modular functions of one variable V, 107–148. Lecture Notes in Math. **601**. Springer, Berlin, 1977.

[10] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*. Invent. Math. **44** (1978), no. 2, 129–162.

[11] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*. Invent. Math. **124** (1996), no. 1-3, 437–449.

[12] F. Momose, *Rational points on the modular curves $X_{\mathrm{split}}(p)$*. Compositio Math. **52** (1984), no. 1, 115–137.

[13] F. Momose, *Isogenies of prime degree over number fields*. Compositio Math. **97** (1995), no. 3, 329–348.
[14] K. Nakata, *On the* 2*-adic representation associated to an elliptic curve defined over* $\mathbb{Q}$. (Japanese), Number Theory Symposium in Kinosaki, December 1979, 221–235.
[15] P. Parent, *Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres*. J. Reine Angew. Math. **506** (1999), 85–116.
[16] P. Parent, *Towards the triviality of* $X_0^+(p^r)(\mathbb{Q})$ *for* $r > 1$. Compositio Math. **141** (2005), no. 3, 561–572.
[17] M. Rebolledo, *Module supersingulier, formule de Gross-Kudla et points rationnels de courbes modulaires*. To appear in Pacific J. Math.
[18] J.-P. Serre, *Abelian* l*-adic representations and elliptic curves*. Lecture at McGill University. W. A. Benjamin Inc., New York-Amsterdam, 1968.
[19] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*. Invent. Math. **15** (1972), no. 4, 259–331.
[20] J.-P. Serre, *Représentations* l*-adiques*. Algebraic number theory (Kyoto Internat. Sympos., Res. Inst. Math. Sci., Univ. Kyoto, Kyoto, 1976), 177–193. Japan Soc. Promotion Sci., Tokyo, 1977.
[21] J.-P. Serre, *Points rationnels des courbes modulaires* $X_0(N)$ *[d'après B. Mazur]*. Séminaire Bourbaki, 30e année (1977/78), Exp. No. 511, 89–100. Lecture Notes in Math. **710**. Springer, Berlin, 1979.
[22] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*. Princeton University Press, Princeton, NJ, 1994.
[23] J. Silverman, *The arithmetic of elliptic curves*. Graduate Texts in Mathematics **106**. Springer-Verlag, New York, 1986.

Keisuke Arai
Graduate School of Mathematical Sciences
The University of Tokyo
Tokyo 153-8914, Japan
E-mail: araik@ms.u-tokyo.ac.jp