BOUNDING THE j -INVARIANT OF INTEGRAL POINTS ON $X_{\text{ns}}^+(p)$

AURÉLIEN BAJOLET AND MIN SHA

(Communicated by Matthew A. Papanikolas)

ABSTRACT. For any prime $p \geq 7$, by using Baker’s method we obtain two explicit bounds in terms of p for the j -invariant of an integral point on $X_{\text{ns}}^+(p)$ which is the modular curve of level p corresponding to the normalizer of a non-split Cartan subgroup of $\text{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

1. INTRODUCTION

Let p be a prime number, $p \geq 7$. We denote by $X_{\text{ns}}^+(p)$ the modular curve of level p corresponding to the normalizer of a non-split Cartan subgroup of $\text{GL}_2(\mathbb{Z}/p\mathbb{Z})$. See, for instance, Serre [17], Section A.5 for definitions and basic properties. In particular, this curve has a canonical $\mathbb{Q}$ -model, which will be used throughout. One can similarly define $X_{\text{ns}}^+(N)$ of a composite level N , but we restrict ourselves to prime levels in this article.

We denote by j the standard j -invariant function on $X_{\text{ns}}^+(p)$. We call a rational point $P \in X_{\text{ns}}^+(p)(\mathbb{Q})$ an integral point with respect to j if $j(P) \in \mathbb{Z}$.

The modular curve $X_{\text{ns}}^+(p)$ has $(p-1)/2$ cusps, and all its cusps are conjugate over $\mathbb{Q}$. Hence, by the classical Siegel’s finiteness theorem [20], for $p \geq 7$ the curve $X_{\text{ns}}^+(p)$ can have only finitely many integral points. Moreover, as follows from [5, Proposition 5.1(a)], their size can be bounded effectively in terms of p .

In fact, under the “Runge condition” which roughly says that all the cusps are not conjugate, there is an explicit bound for the j -invariant of the integral points on arbitrary modular curves over arbitrary number fields; see [8, Theorem 1.2]. Unfortunately, the Runge condition fails for $X_{\text{ns}}^+(p)$. So we must introduce other techniques.

In this paper we use Baker’s method, more precisely Baker’s inequality in the form due to Matveev [16, Corollary 2.3], to obtain two explicit bounds in terms of p for the j -invariant of an integral point on $X_{\text{ns}}^+(p)$.

Our first main result is the following general theorem.

Theorem 1.1. *Assume that $p \geq 7$ and let $d \geq 3$ be a divisor of $(p-1)/2$. Then for any integral point P on $X_{\text{ns}}^+(p)$ we have*

$$\log |j(P)| < C(d)p^{6d+5}(\log p)^2,$$

where $C(d) = 30^{d+5} \cdot d^{-2d+4.5}$.

Received by the editors March 14, 2012 and, in revised form, August 13, 2012 and October 30, 2012.

2010 *Mathematics Subject Classification.* Primary 11G16, 11J86; Secondary 14G35, 11G50.

Key words and phrases. Modular curves, non-split Cartan, j -invariant, Baker’s method.

The second author was supported by the China Scholarship Council.

In particular, if we choose $d = \frac{p-1}{2}$ in Theorem 1.1, we obtain a bound which is explicit in p .

Theorem 1.2. *Assume that $p \geq 7$. Then for any integral point P on $X_{\text{ns}}^+(p)$ we have*

$$\log |j(P)| < 41993 \cdot 13^p \cdot p^{2p+7.5} (\log p)^2.$$

By comparing these two theorems, the bound in Theorem 1.2 can be drastically reduced if $\frac{p-1}{2}$ has a small divisor.

The interest in integral points on the modular curves corresponding to normalizers of Cartan subgroups is motivated by their relation to imaginary quadratic fields of a low class number. See Appendix A in Serre's book [17] for a nice historical account and further explanations. In particular, integral points on the curves $X_{\text{ns}}^+(24)$ and $X_{\text{ns}}^+(15)$ were studied by Heegner [12] and Siegel [21] in their classical work on the class number 1 problem. Kenku [13] determined all integral points on $X_{\text{ns}}^+(7)$, and Baran [3, 4] did this for $X_{\text{ns}}^+(9)$ and $X_{\text{ns}}^+(15)$.

A general method for computing integral points on $X_{\text{ns}}^+(p)$ is developed in [2]. Much more is known on integral and even rational points on modular curves corresponding to the normalizers of split Cartan subgroups; see [9, 10]. In particular, the authors in [9] used the bound of the j -invariant of integral points to solve Serre's uniformity problem in the split Cartan case and finally left this problem with the non-split Cartan case.

In addition, recently the second author has used a different approach by applying Baker's method to get some effective bounds for the j -invariant of integral points on arbitrary modular curves over arbitrary number fields, assuming that the number of cusps is not less than 3; see [18].

2. NOTATION AND CONVENTIONS

Throughout this paper, $\log$ stands for the principal branch of the complex logarithm.

We fix p a prime number not less than 7. Let G be the normalizer of a non-split Cartan subgroup of $\text{GL}_2(\mathbb{Z}/p\mathbb{Z})$ and $X_{\text{ns}}^+(p)$ the modular curve corresponding to G . In fact, up to conjugation, we know that

$$G = \left\{ \begin{pmatrix} \alpha & \Xi\beta \\ \beta & \alpha \end{pmatrix}, \begin{pmatrix} \alpha & \Xi\beta \\ -\beta & -\alpha \end{pmatrix} : \alpha, \beta \in \mathbb{F}_p, (\alpha, \beta) \neq (0, 0) \right\},$$

where Ξ is a quadratic non-residue modulo p . In particular, one can choose $\Xi = -1$ if $p \equiv 3 \pmod{4}$. Moreover, $|G| = 2(p^2 - 1)$ by [4, Formula (2.3)] and $\det G = \mathbb{F}_p^\times$, where $\det G$ is the image of G under the determinant map $\det : \text{GL}_2(\mathbb{Z}/p\mathbb{Z}) \rightarrow \mathbb{F}_p^\times$.

In the sequel, we fix a subgroup H of $\mathbb{F}_p^\times$ such that $-1 \in H$ and $[\mathbb{F}_p^\times : H] \geq 3$. Put $d = [\mathbb{F}_p^\times : H]$; then we have

$$d \mid \frac{p-1}{2} \quad \text{and} \quad d = [K : \mathbb{Q}],$$

where $K = \mathbb{Q}(\zeta_p)^H$ and $\zeta_p = e^{\frac{2\pi i}{p}}$. We can identify the Galois group $\text{Gal}(K/\mathbb{Q})$ with $\mathbb{F}_p^\times/H$; we also identify $\text{Gal}(\mathbb{Q}(\zeta_p)/K)$ with H . In particular, $K \subseteq \mathbb{Q}(\zeta_p)^+$, where $\mathbb{Q}(\zeta_p)^+ = \mathbb{Q}(\zeta_p + \bar{\zeta}_p)$.

Put

$$G_H = \{g \in G : \det g \in H\}.$$

Then the determinant map induces an isomorphism: $G/G_H \cong \mathbb{F}_p^\times/H$. We denote by X_H the modular curve corresponding to G_H , which is defined over K . Here X_H and $X_{\text{ns}}^+(p)$ have the same geometrically integral model, and the function field of X_H is $K(X_{\text{ns}}^+(p))$. The curve X_H also has the same cusps as $X_{\text{ns}}^+(p)$. In particular, $\text{Gal}(K(X_H)/\mathbb{Q}(X_{\text{ns}}^+(p))) \cong \text{Gal}(K/\mathbb{Q})$.

Hence, here we identify the following four groups: $\text{Gal}(K(X_H)/\mathbb{Q}(X_{\text{ns}}^+(p)))$, $\text{Gal}(K/\mathbb{Q})$, $\mathbb{F}_p^\times/H$ and G/G_H . The reader should interpret the exact meaning based on the context.

Let $\mathcal{H}$ denote the Poincaré upper half-plane: $\mathcal{H} = \{\tau \in \mathbb{C} : \text{Im}\tau > 0\}$. We put $\bar{\mathcal{H}} = \mathcal{H} \cup \mathbb{Q} \cup \{i\infty\}$. We denote by D the standard fundamental domain of $\text{SL}_2(\mathbb{Z})$. If Γ is the pullback of $G_H \cap \text{SL}_2(\mathbb{Z}/p\mathbb{Z})$ to $\text{SL}_2(\mathbb{Z})$, then the set $X_H(\mathbb{C})$ of complex points is analytically isomorphic to the quotient $\bar{\mathcal{H}}/\Gamma$, supplied with the properly defined topology and analytic structure. See any standard reference like [19] for all the missing details.

For $\mathbf{a} = (a_1, a_2) \in \mathbb{Q}^2$, we put $\ell_{\mathbf{a}} = B_2(a_1 - \lfloor a_1 \rfloor)/2$, where $B_2(T) = T^2 - T + \frac{1}{6}$ is the second Bernoulli polynomial. Obviously $|\ell_{\mathbf{a}}| \leq 1/12$; this will be used without special reference.

We put $\mathbb{A} = (p^{-1}\mathbb{Z}/\mathbb{Z})^2 \setminus \{(0, 0)\}$. In this paper, we also identify $p^{-1}\mathbb{Z}/\mathbb{Z}$ with $p^{-1}\mathbb{F}_p$. Moreover, we always choose a representative element of $\mathbf{a} = (a_1, a_2) \in (p^{-1}\mathbb{Z}/\mathbb{Z})^2$ satisfying $0 \leq a_1, a_2 < 1$. So in the sequel, for every $\mathbf{a} \in (p^{-1}\mathbb{Z}/\mathbb{Z})^2$, we have $\ell_{\mathbf{a}} = B_2(a_1)/2$.

In the sequel, we use the notation $O_1(\cdot)$. Precisely, $A = O_1(B)$ means that $|A| \leq B$.

3. PREPARATIONS

3.1. Siegel functions and modular units. Let $\mathbf{a} = (a_1, a_2) \in \mathbb{Q}^2$ be such that $\mathbf{a} \notin \mathbb{Z}^2$, and let $g_{\mathbf{a}}$ be the corresponding *Siegel function*; see [14, Section 2.1]. We have the following infinite product presentation for $g_{\mathbf{a}}$; see [8, Formula (7)]:

$$g_{\mathbf{a}}(\tau) = -q_{\tau}^{B_2(a_1)/2} e^{\pi i a_2(a_1-1)} \prod_{n=0}^{\infty} (1 - q_{\tau}^{n+a_1} e^{2\pi i a_2}) (1 - q_{\tau}^{n+1-a_1} e^{-2\pi i a_2}),$$

where $q_{\tau} = e^{2\pi i \tau}$ and $B_2(T) = T^2 - T + \frac{1}{6}$ is the second Bernoulli polynomial.

From the proof of [8, Proposition 2.3] and replacing $3|q_{\tau}|$ by $2.03|q_{\tau}|$ in [8, Formula (11)], we directly get the following lemma.

Lemma 3.1. *Let $\mathbf{a} \in \mathbb{Q}^2 \setminus \mathbb{Z}^2$. Then for $\tau \in D$, we have*

$$\log |g_{\mathbf{a}}(\tau)| = \ell_{\mathbf{a}} \log |q_{\tau}| + \log |1 - q_{\tau}^{a_1} e^{2\pi i a_2}| + \log |1 - q_{\tau}^{1-a_1} e^{-2\pi i a_2}| + O_1(2.03|q_{\tau}|).$$

Recall that by a modular unit on a modular curve we mean a rational function having poles and zeros only at the cusps.

For $\mathbf{a} \in (p^{-1}\mathbb{Z})^2 \setminus \mathbb{Z}^2$ we denote $g_{\mathbf{a}}^{12p}$ by $u_{\mathbf{a}}$, which is a modular unit on the principal modular curve $X(p)$ of level p . Moreover, we have $u_{\mathbf{a}} = u_{\mathbf{a}'}$ when $\mathbf{a} \equiv \mathbf{a}' \pmod{\mathbb{Z}^2}$. Hence, $u_{\mathbf{a}}$ is well-defined when $\mathbf{a} \in \mathbb{A}$. In addition, every $u_{\mathbf{a}}$ is integral over $\mathbb{Z}[j]$. For more details, see [8, Section 4.2].

Furthermore, the Galois action on the set $\{u_{\mathbf{a}}\}$ is compatible with the right linear action of $\text{GL}_2(\mathbb{Z}/p\mathbb{Z})$ on it. That is, for any $\sigma \in \text{Gal}(\mathbb{Q}(X(p))/\mathbb{Q}(X(1))) \cong \text{GL}_2(\mathbb{Z}/p\mathbb{Z})/\pm 1$ and any $\mathbf{a} \in \mathbb{A}$, we have

$$u_{\mathbf{a}}^{\sigma} = u_{\mathbf{a}\sigma}.$$

Here we borrow a result and its proof from [2] for the convenience of the reader.

Lemma 3.2 ([2]). *We have*

$$\prod_{\mathbf{a} \in \mathbb{A}} u_{\mathbf{a}} = p^{12p}.$$

Proof. We denote by u the left-hand side of the equality. Since the set $\mathbb{A}$ is stable with respect to $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, u is stable with respect to the Galois action over the field $\mathbb{Q}(X(1)) = \mathbb{Q}(j)$. So $u \in \mathbb{Q}(j)$. Moreover, since u is integral over $\mathbb{Z}[j]$, $u \in \mathbb{Z}[j]$. Notice that $X(1)$ has only one cusp and u has no zeros and poles outside the cusps, so u must be a constant and $u \in \mathbb{Z}$. Since

$$\sum_{(a_1, a_2) \in \mathbb{A}} B_2(a_1) = 0 \quad \text{and} \quad \sum_{(a_1, a_2) \in \mathbb{A}} a_2(1 - a_1) = \frac{p^2 - 1}{4},$$

taking $q = 0$, we have

$$u = \prod_{(a_1, a_2) \in \mathbb{A}, a_1=0} (1 - e^{2\pi i a_2})^{12p} = \prod_{1 \leq k < p} (1 - e^{2k\pi i/p})^{12p} = p^{12p}.$$

□

3.2. $X_{\mathrm{ns}}^+(p)$ and X_H . It is well-known that the curve $X_{\mathrm{ns}}^+(p)$ has $(p-1)/2$ cusps. Moreover, these cusps correspond to the orbits of the (left) action of $G \cap \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ on the set $\mathbb{F}_p^2 \setminus \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right\}$; see [7, Lemma 2.3]. By definition, these orbits are the sets $\mathcal{L}_a$, defined by $x^2 - \Xi y^2 = \pm a$, where a runs through $\mathbb{F}_p^\times / \{\pm 1\}$ and the cusp at infinity corresponds to $a = 1$.

From now on, we fix an integral point P of $X_{\mathrm{ns}}^+(p)$ and assume that $|j(P)| > 3500$. Since every integral point of $X_{\mathrm{ns}}^+(p)$ is also an integral point of X_H , P is also an integral point of X_H . Hence for our purposes, we only need to focus on the modular curve X_H .

Notice that since all the cusps have ramification index p in the natural covering $X_{\mathrm{ns}}^+(p) \rightarrow X(1)$, then so as the natural covering $X_H \rightarrow X(1)$.

We fix a uniformization $X_H(\mathbb{C}) = \mathcal{H}/\Gamma$, and let $\tau_0 \in \mathcal{H}$ be a lift of P . Pick $\sigma_c \in \mathrm{SL}_2(\mathbb{Z})$ such that $\tau = \sigma_c^{-1}(\tau_0) \in D$. As in the proof of [8, Proposition 3.1] and with the notations therein, we can choose the cusp $c = \sigma_c(i\infty)$ and construct a certain set $\Omega_c = \sigma_c(\Delta)/\Gamma$. Furthermore, for the cusp c , following [8, Section 3] let t_c be its local parameter and put $q_c = t_c^p$; then q_c and t_c are defined and analytic on Ω_c . Moreover, $q_c(P) = q_\tau$.

According to [8, Proposition 3.1], we have

$$(3.1) \quad \frac{1}{2}|j(P)| \leq |q_c(P)^{-1}| \leq \frac{3}{2}|j(P)|.$$

We will use (3.1) several times without special reference.

In the sequel we can assume that $|q_c(P)| \leq 10^{-p}$. Indeed, the inequality $|q_c(P)| > 10^{-p}$ yields a much better estimate for $\log |j(P)|$ than those given in Section 1.

3.3. Modular units on X_H . The group $\mathrm{GL}_2(\mathbb{F}_p)$ acts naturally (on the right) on the set $\mathbb{A}$. Since $G_H \subset \mathrm{GL}_2(\mathbb{F}_p)$, let us consider the natural right group action of G_H on $\mathbb{A}$. There are d orbits of this group action. These orbits are the sets $\mathcal{O}_a$, defined by $\{(x/p, y/p) : x^2 - \Xi^{-1}y^2 \in aH\}$, where a runs through $\mathbb{F}_p^\times/H$. In fact,

if $(x, y) \in \mathcal{O}_a$, then for any $g \in G_H$, noticing the two possible representations of g , it is straightforward to show that $(x, y) \cdot g \in \mathcal{O}_a$.

Based on our conventions in Section 2, we consider the natural right group action of $\text{Gal}(K/\mathbb{Q})$ on the set of orbits of the group action $\mathbb{A}/G_H$. Moreover, for any $\sigma \in \text{Gal}(K/\mathbb{Q})$ and any orbit $\mathcal{O}_a$, we have

$$\mathcal{O}_a \sigma = \mathcal{O}_{a\sigma}.$$

It is easy to see that this group action is transitive. So we obtain the following lemma.

Lemma 3.3. *We have $|\mathcal{O}_a| = (p^2 - 1)/d$.*

Let S be any subset of $\mathbb{A}$; we define

$$u_S = \prod_{\mathbf{a} \in S} u_{\mathbf{a}}.$$

Let $\mathcal{O}$ be an orbit of $\mathbb{A}/G_H$; we have

$$(3.2) \quad u_{\mathcal{O}} = \prod_{\mathbf{a} \in \mathcal{O}} u_{\mathbf{a}}.$$

By [8, Proposition 4.2 (ii)], $u_{\mathcal{O}}$ is a rational function on the modular curve X_H . Furthermore, $u_{\mathcal{O}}$ is a modular unit on X_H .

We denote by $\text{Ord}_c(u_{\mathcal{O}})$ the vanishing order of $u_{\mathcal{O}}$ at c . The following lemma is derived directly from Lemma 3.1 and [8, Proposition 4.2 (iii)].

Lemma 3.4. *We have*

$$(3.3) \quad \log |u_{\mathcal{O}}(P)| = \frac{\text{Ord}_c(u_{\mathcal{O}})}{p} \log |q_c(P)| + \log |\gamma_c| + O_1(17p^3 |q_c(P)|^{1/p}),$$

where

$$\text{Ord}_c(u_{\mathcal{O}}) = 12p^2 \sum_{\mathbf{a} \in \mathcal{O}\sigma_c} \ell_{\mathbf{a}} \quad \text{and} \quad \gamma_c = \prod_{\substack{(a_1, a_2) \in \mathcal{O}\sigma_c \\ a_1 = 0}} (1 - e^{2\pi i a_2})^{12p}.$$

Proof. Here we use the following identity:

$$u_{\mathcal{O}}(P) = u_{\mathcal{O}}(\tau_0) = u_{\mathcal{O}}(\sigma_c(\sigma_c^{-1}(\tau_0))) = u_{\mathcal{O}\sigma_c}(\tau).$$

Notice that for $|z| \leq r < 1$, we have

$$|\log |1 + z|| \leq \frac{-\log(1 - r)}{r} |z|;$$

see [8, Formula (4)]. Taking $r = 0.1$ and combining Lemma 3.1 with Lemma 3.3, we have

$$\begin{aligned} \log |u_{\mathcal{O}}(P)| &= \frac{\text{Ord}_c(u_{\mathcal{O}})}{p} \log |q_c(P)| + \log |\gamma_c| \\ &\quad + O_1 \left(26p \frac{p^2 - 1}{d} |q_c(P)|^{1/p} + 25p \frac{p^2 - 1}{d} |q_c(P)| \right). \end{aligned}$$

Then this lemma follows from $d \geq 3$. □

We want to indicate that γ_c is a real algebraic number, because if $(0, a_2) \in \mathcal{O}\sigma_c$, then we have $(0, -a_2) \in \mathcal{O}\sigma_c$, based on the fact that if $(x, y) \in \mathcal{O}$, then $(-x, -y) \in \mathcal{O}$.

Lemma 3.5. *The group generated by the principal divisor $(u_{\mathcal{O}})$, where $\mathcal{O}$ runs over the orbits of $\mathbb{A}/G_H$, is of rank $d - 1$.*

Proof. By Lemma 3.2, the rank of the free abelian group $(u_{\mathcal{O}})$ is at most $d-1$. Then the Manin-Drinfeld theorem, as stated in [14], tells us that this rank is maximal possible. $\square$

4. BAKER'S METHOD ON X_H

In this section we obtain a bound for $\log |j(P)|$, involving various parameters. Recall that P is the integral point of $X_{\text{ns}}^+(p)$ fixed in Section 3.2.

4.1. Cyclotomic units. We introduce a set of independent cyclotomic units of $\mathbb{Q}(\zeta_p)^+$ as follows:

$$\xi_{k-1} = \zeta_p^{(1-k)/2} \cdot \frac{1 - \zeta_p^k}{1 - \zeta_p} = \frac{\bar{\zeta}_p^{k/2} - \zeta_p^{k/2}}{\bar{\zeta}_p^{1/2} - \zeta_p^{1/2}}, \quad k = 2, \dots, \frac{p-1}{2};$$

for details see [23, Lemma 8.1]. In particular, $\{-1, \xi_1, \dots, \xi_{\frac{p-3}{2}}\}$ is a set of independent generators for the full group of cyclotomic units of $\mathbb{Q}(\zeta_p)^+$. Let m' be the index of $\langle \xi_1, \dots, \xi_{\frac{p-3}{2}} \rangle$ in the full unit group of $\mathbb{Q}(\zeta_p)^+$ modulo roots of unity, which is equal to the class number of $\mathbb{Q}(\zeta_p)^+$.

We put

$$\eta_k = \mathcal{N}_{\mathbb{Q}(\zeta_p)^+/K}(\xi_k) = \prod_{\sigma \in \text{Gal}(\mathbb{Q}(\zeta_p)^+/K)} \xi_k^\sigma, \quad k = 1, \dots, \frac{p-3}{2}.$$

Let m be the exponent of $\langle \eta_1, \dots, \eta_{\frac{p-3}{2}} \rangle$ in the full unit group of K modulo roots of unity. Since $[\mathbb{Q}(\zeta_p)^+ : K] = |H|/2 = \frac{p-1}{2d}$, we have

$$(4.1) \quad m \left\lfloor \frac{m'(p-1)}{2d} \right\rfloor.$$

Since m is finite and the rank of the full unit group of K is $d-1$, the group $\langle \eta_1, \dots, \eta_{\frac{p-3}{2}} \rangle$ modulo roots of unity has rank $d-1$. In particular, in the sequel we assume that $\eta_1, \dots, \eta_{d-1}$ are multiplicatively independent without loss of generality.

4.2. More about modular units on X_H . We fix an orbit $\mathcal{O}$ of the group action $\mathbb{A}/G_H$. Put $U = u_{\mathcal{O}}$, where $u_{\mathcal{O}}$ is defined in (3.2).

Based on our conventions in Section 2, for any $\sigma \in \text{Gal}(K/\mathbb{Q})$ we can define U^σ as the natural Galois action. Indeed, we can view σ as an element of $\text{Gal}(K(X_H)/\mathbb{Q}(X_{\text{ns}}^+(p)))$ and $U \in K(X_H)$. Moreover, we have $U^\sigma = u_{\mathcal{O}\sigma}$ and $U(P)^\sigma = U^\sigma(P)$.

Since the Galois group $\text{Gal}(K/\mathbb{Q})$ acts transitively on the set of orbits of $\mathbb{A}/G_H$, we can rewrite Lemma 3.2 as follows.

Lemma 4.1. *We have*

$$\prod_{\sigma \in \text{Gal}(K/\mathbb{Q})} U^\sigma = p^{12p}.$$

By Lemma 3.3 and the formula for $\text{Ord}_c u_{\mathcal{O}}$ appearing in Lemma 3.4 we obtain a bound for the vanishing order of U at c .

Lemma 4.2. *We have*

$$|\text{Ord}_c U| \leq \frac{p^2(p^2-1)}{d}.$$

For $1 - \zeta_p$, we take the $\mathbb{Q}(\zeta_p)/K$ -norm, setting $\mu = \mathcal{N}_{\mathbb{Q}(\zeta_p)/K}(1 - \zeta_p)$.

Lemma 4.3. *We have $(U(P)) = (\mu^{12p})$.*

Proof. Since P is an integral point of X_H , by [8, Proposition 4.2 (i)] and Lemma 4.1, the principal ideal $(U(P))$ is an integral ideal of the field K of the form $\mathfrak{p}^n$, where $\mathfrak{p} = (\mu)$ and n is a positive integer.

In addition, since $\mathfrak{p}$ is stable under the Galois action over $\mathbb{Q}$, we have $(U^\sigma(P)) = \mathfrak{p}^n$ for every $\sigma \in \text{Gal}(K/\mathbb{Q})$. Noticing that $\mathfrak{p}^d = (p)$, it follows from Lemma 4.1 that $n = 12p$. $\square$

So Dirichlet's unit theorem gives

$$U(P)^m = \pm \eta_0^m \eta_1^{b_1} \cdots \eta_{d-1}^{b_{d-1}},$$

where $\eta_0 = \mu^{12p}$ and $b_1, \dots, b_{d-1}$ are some rational integers.

Let

$$V = U/\eta_0;$$

then we have

$$V(P)^m = \pm \eta_1^{b_1} \cdots \eta_{d-1}^{b_{d-1}}$$

and $\text{Ord}_c V = \text{Ord}_c U$. For every $\sigma \in \text{Gal}(K/\mathbb{Q})$, we have

$$(4.2) \quad V^\sigma(P)^m = \pm (\eta_1^\sigma)^{b_1} \cdots (\eta_{d-1}^\sigma)^{b_{d-1}},$$

where $V^\sigma = U^\sigma/\eta_0^\sigma$. Furthermore, by (3.3), we have

$$(4.3) \quad \log |V^\sigma(P)| = \frac{\text{Ord}_c V^\sigma}{p} \log |q_c(P)| + \log |\Upsilon_{c,\sigma}| + O_1 \left(17p^3 |q_c(P)|^{1/p} \right),$$

where $\Upsilon_{c,\sigma} = \gamma_{c,\sigma}/\eta_0^\sigma$ and

$$\gamma_{c,\sigma} = \prod_{\substack{(a_1, a_2) \in \mathcal{O}\sigma\sigma_c \\ a_1=0}} (1 - e^{2\pi i a_2})^{12p}.$$

Notice that $\gamma_{c,\sigma} = \gamma_c$ when σ is the identity. So $\Upsilon_{c,1} = \gamma_c/\eta_0$.

Finally we put

$$B = \max\{|b_1|, \dots, |b_{d-1}|, m\}.$$

4.3. Upper bound for B. We fix an order on the elements of the Galois group by supposing

$$\text{Gal}(K/\mathbb{Q}) = \{\sigma_0 = 1, \sigma_1, \dots, \sigma_{d-1}\}.$$

Since the real algebraic numbers $\eta_1, \dots, \eta_{d-1}$ are multiplicatively independent, the $(d-1) \times (d-1)$ real matrix $A = (\log |\eta_\ell^{\sigma_k}|)_{1 \leq k, \ell \leq d-1}$ is non-singular. Let $(\alpha_{k\ell})_{1 \leq k, \ell \leq d-1}$ be the inverse matrix. Then by (4.2) we have

$$b_k = m \sum_{\ell=1}^{d-1} \alpha_{k\ell} \log |V^{\sigma_\ell}(P)|, \quad 1 \leq k \leq d-1.$$

Define the following quantities:

$$\begin{aligned}\delta_{c,k} &= \frac{m}{p} \sum_{\ell=1}^{d-1} \alpha_{k\ell} \text{Ord}_c V^{\sigma_\ell}, \\ \beta_{c,k} &= m \sum_{\ell=1}^{d-1} \alpha_{k\ell} \log |\Upsilon_{c,\sigma_\ell}|, \\ \kappa &= \max\left\{\max_k \sum_{\ell=1}^{d-1} |\alpha_{k\ell}|, 1\right\}.\end{aligned}$$

According to (4.3), we have

$$b_k = \delta_{c,k} \log |q_c(P)| + \beta_{c,k} + O_1\left(17p^3 m \kappa |q_c(P)|^{1/p}\right).$$

Let $\delta = \max_k |\delta_{c,k}|$ and $\beta = \max_k |\beta_{c,k}|$. Then we have

$$(4.4) \quad B \leq \delta \log |q_c(P)^{-1}| + \beta + 2p^3 m \kappa.$$

4.4. Preparation for Baker's inequality. We define the following function:

$$W = \begin{cases} V & \text{if } \text{Ord}_c V = 0, \\ V^{\text{Ord}_c V^\sigma} (V^\sigma)^{-\text{Ord}_c V} & \text{if } \text{Ord}_c V \neq 0, \end{cases}$$

where $\sigma \in \text{Gal}(K/\mathbb{Q})$ and $\sigma \neq 1$. So we always have $\text{Ord}_c W = 0$. Moreover, W is not a constant by Lemma 3.5. In Section 6 we will choose special U (i.e. V) and σ to deal with an exceptional case that will occur.

Define

$$\alpha_d = \begin{cases} |\Upsilon_{c,1}|^{-1} & \text{if } \text{Ord}_c V = 0, \\ \left| \frac{\Upsilon_{c,1}^{\text{Ord}_c V^\sigma}}{\Upsilon_{c,\sigma}^{\text{Ord}_c V}} \right|^{-1} & \text{if } \text{Ord}_c V \neq 0. \end{cases}$$

Then by (4.3) and Lemma 4.2 we obtain

$$(4.5) \quad \log |W(P)| = -\log \alpha_d + O_1\left(12p^7 |q_c(P)|^{1/p}\right).$$

Put

$$\Lambda = m \log |W(P)| + m \log \alpha_d.$$

If $\text{Ord}_c V = 0$, by (4.2), we have

$$\Lambda = b_1 \log |\eta_1| + \cdots + b_{d-1} \log |\eta_{d-1}| + m \log \alpha_d.$$

In this case, we put $\alpha_k = |\eta_k|$ for $1 \leq k \leq d-1$.

If $\text{Ord}_c V \neq 0$, by (4.2), we have

$$\Lambda = b_1 \log \left| \frac{\eta_1^{\text{Ord}_c V^\sigma}}{(\eta_1^\sigma)^{\text{Ord}_c V}} \right| + \cdots + b_{d-1} \log \left| \frac{\eta_{d-1}^{\text{Ord}_c V^\sigma}}{(\eta_{d-1}^\sigma)^{\text{Ord}_c V}} \right| + m \log \alpha_d.$$

In this case, we put $\alpha_k = \left| \frac{\eta_k^{\text{Ord}_c V^\sigma}}{(\eta_k^\sigma)^{\text{Ord}_c V}} \right|$ for $1 \leq k \leq d-1$.

Hence, in both of these two cases we have

$$(4.6) \quad \Lambda = b_1 \log \alpha_1 + \cdots + b_{d-1} \log \alpha_{d-1} + m \log \alpha_d.$$

Notice that all α_k , $1 \leq k \leq d$, are contained in $\mathbb{Q}(\zeta_p)^+$.

4.5. Using Baker's inequality. If $\Lambda = 0$, we can get a better bound for $\log |j(P)|$; see Section 6. So here we assume that $\Lambda \neq 0$.

Using [16, Corollary 2.3] and combining (4.4) and (4.5), we have

$$(4.7) \quad \begin{cases} |\Lambda| > \exp\left(-C_1(d)\Omega\left(\frac{p-1}{2}\right)^2(1+\log\frac{p-1}{2})(1+\log B)\right), \\ |\Lambda| \leq \lambda|q_c(P)|^{1/p} \leq \lambda \exp\left(\frac{-B+\beta+2p^3m\kappa}{\delta p}\right), \end{cases}$$

where

$$\begin{aligned} C_1(d) &= \min\left\{\frac{e}{2}d^{4.5}30^{d+3}, 2^{6d+20}\right\}, \\ A_k &\geq \max\left\{\frac{p-1}{2}h(\alpha_k), |\log \alpha_k|, 0.16\right\}, 1 \leq k \leq d, \\ \Omega &= A_1 \cdots A_d, \quad \lambda = 12p^7m, \end{aligned}$$

and $h(\cdot)$ is the usual absolute logarithmic height.

We obtain $B \leq K_1 \log B + K_2$, where

$$\begin{aligned} K_1 &= \delta p C_1(d)\Omega\left(\frac{p-1}{2}\right)^2(1+\log\frac{p-1}{2}), \\ K_2 &= \delta p C_1(d)\Omega\left(\frac{p-1}{2}\right)^2(1+\log\frac{p-1}{2}) + \beta + 2p^3m\kappa + \delta p \log \lambda. \end{aligned}$$

By [6, Lemma 2.3.3], we obtain

$$B \leq B_0 = 2(K_1 \log K_1 + K_2).$$

Then by (4.7), we have

$$|q_c(P)^{-1}| < \lambda^p \exp(pC_1(d)\Omega\left(\frac{p-1}{2}\right)^2(1+\log\frac{p-1}{2})(1+\log B_0)).$$

Finally, we have

$$(4.8) \quad \log |j(P)| < pC_1(d)\Omega\left(\frac{p-1}{2}\right)^2(1+\log\frac{p-1}{2})(1+\log B_0) + p \log \lambda + \log 2.$$

Hence, to get a bound for $\log |j(P)|$ we only need to calculate the quantities in the above inequality, and we will do this in the next section.

It is easy to see that

$$C_1(d) = \min\left\{\frac{e}{2}d^{4.5}30^{d+3}, 2^{6d+20}\right\} < 2d^{4.5}30^{d+3}.$$

5. COMPUTATIONS

5.1. Upper bound for m . Let h^+ , R^+ and D^+ be the class number, regulator and discriminant of $\mathbb{Q}(\zeta_p)^+$, respectively.

By [23, Lemma 8.1 and Theorem 8.2], we have $m' = h^+$. By [23, Proposition 2.1 and Lemma 4.19], we have $|D^+| = p^{\frac{p-3}{2}}$. Then the class number formula (see [23, page 37]) gives

$$h^+ = \left(\frac{p}{4}\right)^{\frac{p-3}{4}} \cdot \frac{1}{R^+} \prod_{\chi \neq 1} L(1, \chi).$$

Using [11, Theorem 2] to the field extension $\mathbb{Q}(\zeta_p)^+/\mathbb{Q}$, we have $R^+ > 0.32$. Applying [15, Theorem 1] to the field extension $\mathbb{Q}(\zeta_p)^+/\mathbb{Q}$ and noticing the constant

$\mu_{\mathbb{Q}}$ below formula (6) of [15], we get

$$|L(1, \chi)| < \frac{1}{2} \log p + 0.03 < \log p, \quad \text{if } \chi \neq 1.$$

Hence we have

$$h^+ < p^{\frac{p-3}{4}} (\log p)^{\frac{p-3}{2}}.$$

Finally, by (4.1) we obtain

$$(5.1) \quad m \leq \frac{h^+(p-1)}{2d} < p^{\frac{p+1}{4}} (\log p)^{\frac{p-3}{2}}.$$

In the sequel we use the following formulas. For any $n \in \mathbb{Z}$ and $a_1, \dots, a_k, \alpha \in \bar{\mathbb{Q}}$, we have

$$h(a_1 + \dots + a_k) \leq h(a_1) + \dots + h(a_k) + \log k,$$

$$h(a_1 \cdots a_k) \leq h(a_1) + \dots + h(a_k),$$

$$h(\alpha^n) = |n|h(\alpha),$$

$$h(\zeta) = 0 \quad \text{for any root of unity } \zeta \in \mathbb{C}.$$

5.2. Height of η_{k-1} for $k = 2, \dots, (p-1)/2$. Let $a \in \mathbb{F}_p^\times$ and $\sigma_a \in \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ induced by the automorphism of $\mathbb{Q}(\zeta_p) : \zeta_p \rightarrow \zeta_p^a$.

Since $\xi_{k-1}^{\sigma_a} = \frac{\bar{\zeta}_p^{ak/2} - \zeta_p^{ak/2}}{\bar{\zeta}_p^{a/2} - \zeta_p^{a/2}}$, we have $h(\xi_{k-1}^{\sigma_a}) \leq 2 \log 2$. So

$$h(\eta_{k-1}^{\sigma_a}) \leq \frac{(p-1) \log 2}{d}.$$

Notice that if $-\frac{\pi}{2} < x < \frac{\pi}{2}$, then $\frac{\sin x}{x} > \frac{2}{\pi}$. Since $\xi_{k-1}^{\sigma_a} = \frac{\sin(\pi ak/p)}{\sin(\pi a/p)}$, we have

$$|\xi_{k-1}^{\sigma_a}| \leq \frac{1}{|\sin(\pi a/p)|} \leq \frac{1}{\sin(\pi/p)} < \frac{p}{2}$$

and

$$|\xi_{k-1}^{\sigma_a}| \geq |\sin(\pi ak/p)| \geq \sin(\pi/p) > \frac{2}{p}.$$

So we have $|\log |\xi_{k-1}^{\sigma_a}|| < \log \frac{p}{2}$. Hence

$$|\log |\eta_{k-1}^{\sigma_a}|| < \frac{(p-1) \log \frac{p}{2}}{2d}.$$

Since we can view $\text{Gal}(K/\mathbb{Q})$ as a quotient group of $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, for any $\sigma \in \text{Gal}(K/\mathbb{Q})$, we have

$$(5.2) \quad h(\eta_{k-1}^\sigma) \leq \frac{(p-1) \log 2}{d} \quad \text{and} \quad |\log |\eta_{k-1}^\sigma|| < \frac{(p-1) \log \frac{p}{2}}{2d}.$$

5.3. Height of η_0 . Following the method in Section 5.2, we have $h(1 - \zeta_p^{\sigma_a}) \leq \log 2$. So

$$h(\eta_0^{\sigma_a}) \leq \frac{12p(p-1) \log 2}{d}.$$

First we have $|1 - \zeta_p^{\sigma_a}| \leq 2$. Second we have

$$|1 - \zeta_p^{\sigma_a}|^2 \geq 2 - 2 \cos \frac{\pi}{p} = 4 \left(\sin \frac{\pi}{2p} \right)^2 > \left(\frac{2}{p} \right)^2.$$

So we have $|\log |1 - \zeta_p^{\sigma_a}|| < \log \frac{p}{2}$. Hence

$$|\log |\eta_0^{\sigma_a}|| < \frac{12p(p-1) \log \frac{p}{2}}{d}.$$

Since we can view $\text{Gal}(K/\mathbb{Q})$ as a quotient group of $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, for any $\sigma \in \text{Gal}(K/\mathbb{Q})$, we obtain

$$(5.3) \quad h(\eta_0^\sigma) \leq \frac{12p(p-1) \log 2}{d} \quad \text{and} \quad |\log |\eta_0^\sigma|| < \frac{12p(p-1) \log \frac{p}{2}}{d}.$$

5.4. Height of $|\Upsilon_{c,\sigma}|$. Recall that $\Upsilon_{c,\sigma} = \gamma_{c,\sigma}/\eta_0^\sigma$, $\sigma \in \text{Gal}(K/\mathbb{Q})$ and

$$\gamma_{c,\sigma} = \prod_{\substack{(a_1, a_2) \in \mathcal{O}\sigma\sigma_c \\ a_1=0}} (1 - e^{2i\pi a_2})^{12p}.$$

Notice the description of $\mathcal{O}$ in Section 3.3; we have $|\{(a_1, a_2) \in \mathcal{O}\sigma\sigma_c : a_1 = 0\}| \leq 2|H| = \frac{2(p-1)}{d}$. Following the method in Section 5.2, we get

$$h(\gamma_{c,\sigma}) \leq \frac{24p(p-1) \log 2}{d}.$$

Since $\Upsilon_{c,\sigma} = \gamma_{c,\sigma}/\eta_0^\sigma$, we have, by (5.3),

$$h(\Upsilon_{c,\sigma}) \leq h(\gamma_{c,\sigma}) + h(\eta_0^\sigma) \leq \frac{36p(p-1) \log 2}{d}.$$

Noticing that $|\Upsilon_{c,\sigma}|^2 = \Upsilon_{c,\sigma} \bar{\Upsilon}_{c,\sigma}$, we get

$$(5.4) \quad h(|\Upsilon_{c,\sigma}|) \leq \frac{36p(p-1) \log 2}{d}.$$

Since $a_1 = 0$, we have $a_2 \in \{\frac{1}{p}, \dots, \frac{p-1}{p}\}$. First we have $|1 - e^{2i\pi a_2}| \leq 2$. Second

$$|1 - e^{2i\pi a_2}|^2 = 2(1 - \cos 2\pi a_2) \geq 2(1 - \cos \pi/p) = 4 \sin^2 \frac{\pi}{2p} \geq \frac{4}{p^2}.$$

So we have $|\log |1 - e^{2i\pi a_2}|| \leq \log \frac{p}{2}$, and then

$$|\log |\gamma_{c,\sigma}|| \leq \frac{24p(p-1) \log \frac{p}{2}}{d}.$$

Hence we have, by (5.3),

$$(5.5) \quad |\log |\Upsilon_{c,\sigma}|| \leq \frac{36p(p-1) \log \frac{p}{2}}{d}.$$

5.5. Calculation of Ω . Recall that $\Omega = A_1 \cdots A_d$, where

$$A_k \geq \max\left\{\frac{p-1}{2}h(\alpha_k), |\log \alpha_k|, 0.16\right\}, \quad 1 \leq k \leq d.$$

If $\text{Ord}_c V = 0$, then $\alpha_k = |\eta_k| = \pm \eta_k$, $1 \leq k \leq d-1$, and $\alpha_d = |\Upsilon_{c,1}|^{-1}$. Then, by (5.2), for $1 \leq k \leq d-1$, we can choose $A_k = p^2/d$. For A_d , we can choose $A_d = 36p^3/d$, by (5.4) and (5.5).

If $\text{Ord}_c V \neq 0$, then $\alpha_k = \left| \frac{\eta_k^{\text{Ord}_c V^\sigma}}{(\eta_k^c)^{\text{Ord}_c V}} \right|$, $1 \leq k \leq d-1$, and $\alpha_d = \left| \frac{\Upsilon_{c,1}^{\text{Ord}_c V^\sigma}}{\Upsilon_{c,\sigma}^{\text{Ord}_c V}} \right|^{-1}$. For $1 \leq k \leq d-1$, combining Lemma 4.2 with (5.2) we can choose $A_k = p^6/d^2$. For A_d , we can choose $A_d = 36p^7/d^2$.

Therefore, we can choose

$$(5.6) \quad \Omega = 36p^{6d+1}/d^{2d}.$$

5.6. Calculation of B_0 . For our purposes we need to calculate δ, β and κ . In fact, all we want to do is to get a bound for $|\alpha_{k\ell}|$, $1 \leq k, \ell \leq d-1$.

Let R_K be the regulator of K . By [23, Lemma 4.15], we have $|\det A| \geq mR_K$. Applying [11, Theorem 2] to the field extension $K/\mathbb{Q}$, we have $R_K > 0.32$. So we get $|\det A| > 0.32m$.

Notice that $\alpha_{k\ell} = \frac{1}{\det A} A_{\ell k}$, where $A_{\ell k}$ is the relative cofactor. The reader should not confuse the matrix A , the constants A_k introduced in Section 4.5 and the cofactors $A_{\ell k}$.

By Hadamard's inequality and (5.2), we have

$$|A_{\ell k}| \leq \left[\frac{(p-1)\sqrt{d-2} \log \frac{p}{2}}{2d} \right]^{d-2}.$$

Then we have

$$\begin{aligned} |\alpha_{k\ell}| &< \left[\frac{(p-1)\sqrt{d-2} \log \frac{p}{2}}{2d} \right]^{d-2} \cdot \frac{1}{0.32m} \\ &< (p\sqrt{p} \log p)^{\frac{p-1}{2}-2} / m \\ &= p^{\frac{3p-15}{4}} (\log p)^{\frac{p-5}{2}} / m. \end{aligned}$$

Hence, we obtain

$$\begin{aligned} \delta &< p^{\frac{3p-3}{4}} (\log p)^{\frac{p-5}{2}}, \\ \beta &< 36p^{\frac{3p-7}{4}} (\log p)^{\frac{p-3}{2}}, \\ \kappa &< p^{\frac{3p-11}{4}} (\log p)^{\frac{p-5}{2}} / m. \end{aligned}$$

Notice that $d \leq (p-1)/2$ and $p \geq 7$, so we get $C_1(d) \leq p^{p+8}$. Therefore, we have

$$K_1 < p^{5p+9} (\log p)^{p-1}, \quad K_2 < 4p^{5p+9} (\log p)^{p-1},$$

and then

$$B_0 < 16p^{5p+10} (\log p)^p, \quad 1 + \log B_0 < 8p \log p.$$

5.7. Final results. Finally, by (4.8) we get an explicit bound for $\log |j(P)|$ as follows:

$$\begin{aligned} \log |j(P)| &< 2pC_1(d) \Omega\left(\frac{p-1}{2}\right)^2 \left(1 + \log \frac{p-1}{2}\right) (1 + \log B_0) \\ &< C(d) p^{6d+5} (\log p)^2, \end{aligned}$$

where $C(d) = 30^{d+5} \cdot d^{-2d+4.5}$. Hence we obtain Theorem 1.1.

If we choose $d = (p-1)/2$, applying the bound $p-1 \geq 6p/7$ and a few numerical computations, we get Theorem 1.2.

6. THE CASE $\Lambda = 0$

In this section, we suppose that $\Lambda = 0$. Then we will obtain a better bound for $\log |j(P)|$ than Theorem 1.1.

First we assume that $\text{Ord}_c V = 0$, i.e. $\text{Ord}_c U = 0$. Then we have $|U(P)| = |\gamma_c|$. Since $U(P)$ and γ_c are real, we have $U(P)^2 = \gamma_c^2$, i.e. $U^2(P) = \gamma_c^2$.

Recall Ω_c and the q -parameter q_c mentioned in Section 3.2. Let v be an absolute value of $\mathbb{Q}(\zeta_p)$ normalized to extend a standard absolute value on $\mathbb{Q}$. For the modular function U^2 , we get the following lemma.

Lemma 6.1. *There exist an integer function $f(\cdot)$ with respect to q_c and $\lambda_1^c, \lambda_2^c, \lambda_3^c \cdots \in \mathbb{Q}(\zeta_p)$ such that the following identity holds in Ω_c :*

$$(6.1) \quad \log \frac{U^2(q_c)}{\gamma_c^2 q_c^{\frac{2\text{Ord}_c U}{p}}} = 2\pi f(q_c)i + \sum_{k=1}^{\infty} \lambda_k^c q_c^{k/p}$$

and

$$|\lambda_k^c|_v \leq \begin{cases} |k|_v^{-1} & \text{if } v \text{ is finite,} \\ 48p^2(k+p) & \text{if } v \text{ is infinite.} \end{cases}$$

In particular, for every $k \geq 1$ we have

$$h(\lambda_k^c) \leq \log(48p^3 + 48kp^2) + \log k.$$

Proof. By definition, we have

$$(6.2) \quad \frac{U^2(q_c)}{\gamma_c^2 q_c^{\frac{2\text{Ord}_c U}{p}}} = \prod_{\mathbf{a} \in \mathcal{O}_{\sigma_c}} \prod_{\substack{n=0 \\ n+a_1 \neq 0}}^{\infty} (1 - q_c^{n+a_1} e^{2\pi i a_2})^{24p} \prod_{n=0}^{\infty} (1 - q_c^{n+1-a_1} e^{-2\pi i a_2})^{24p}.$$

Since

$$\sum_{\mathbf{a} \in \mathcal{O}_{\sigma_c}} \left(\sum_{\substack{n=0 \\ n+a_1 \neq 0}}^{\infty} 24p |q_c|^{n+a_1} + \sum_{n=0}^{\infty} 24p |q_c|^{n+1-a_1} \right)$$

is convergent, it follows from [1, Chapter 5 Section 2.2 Theorem 6] that the right-hand side of (6.2) is absolutely convergent. Then we can write it as the form $\prod_{n=1}^{\infty} (1+d_n)$ such that $\prod_{n=1}^{\infty} (1+d_n)$ is absolutely convergent. Hence [1, Chapter 5, Section 2.2, Theorem 5] gives

$$\begin{aligned} & \log \frac{U^2(q_c)}{\gamma_c^2 q_c^{\frac{2\text{Ord}_c U}{p}}} \\ &= 2\pi f(q_c)i + \sum_{\mathbf{a} \in \mathcal{O}_{\sigma_c}} \left(\sum_{\substack{n=0 \\ n+a_1 \neq 0}}^{\infty} 24p \log(1 - q_c^{n+a_1} e^{2\pi i a_2}) \right. \\ & \quad \left. + \sum_{n=0}^{\infty} 24p \log(1 - q_c^{n+1-a_1} e^{-2\pi i a_2}) \right). \end{aligned}$$

Applying the Taylor expansion of the logarithm function to the right-hand side of the above formula, we get the desired identity (6.1).

For a fixed non-negative integer n (where we assume $n > 0$ if $a_1 = 0$), write

$$\log(1 - q_c^{n+a_1} e^{2\pi i a_2}) = \sum_{k=1}^{\infty} \beta_k q_c^{k/p}.$$

An immediate verification shows that

$$|\beta_k|_v \leq \begin{cases} |k|_v^{-1} & \text{if } v \text{ is finite,} \\ 1 & \text{if } v \text{ is infinite.} \end{cases}$$

The same estimates hold true for the coefficients of the q -series for

$$\log(1 - q_c^{n+1-a_1} e^{-2\pi i a_2}).$$

For each $\mathbf{a} \in \mathcal{O}_{\mathcal{S}_c}$, the number of coefficients in the q -series for $\log(1 - q_c^{n+a_1} e^{2\pi i a_2})$ which may contribute to λ_k^c (those with $0 \leq n \leq k/p$) is at most $k/p + 1$, and the same is true for the q -series for $\log(1 - q_c^{n+1-a_1} e^{-2\pi i a_2})$. The bound for $|\lambda_k^c|_v$ now follows by summation. $\square$

Corollary 6.2. *With the assumption $\text{Ord}_c U = 0$, we have $\lambda_k^c \neq 0$ for some $k \leq p^5$.*

Proof. Since $\text{Ord}_c U = 0$ and U is not a constant, there must exist some $\lambda_k^c \neq 0$. Under the assumption $\text{Ord}_c U = 0$, we have $U(c) = \gamma_c$, and then $f(q_c(c)) = 0$ by (6.1). We extend the additive valuation Ord_c from the field $K(X_H)$ to the field of formal power series $K((q_c^{1/p}))$. Then $\text{Ord}_c q_c^{1/p} = 1$ and $\text{Ord}_c (-2\pi f(q_c)i + \log(U^2/\gamma_c^2)) \leq \text{Ord}_c \log(U^2/\gamma_c^2) = \text{Ord}_c (U^2/\gamma_c^2 - 1)$. The latter quantity is bounded by the degree of $U^2/\gamma_c^2 - 1$, which is equal to the degree of U^2 .

The degree of U^2 is equal to $\sum_{c_0} |\text{Ord}_{c_0} U|$; here the sum runs through all the cusps of X_H . Then the result follows from Lemma 4.2. $\square$

Now we can get a bound for $\log |j(P)|$.

Proposition 6.3. *Under the assumptions $\Lambda = 0$ and $\text{Ord}_c U = 0$, we have*

$$\log |j(P)| \leq p^2 \log(48p^{12} + 48p^8) + p \log(96p^2(p^5 + p + 1)) + \log 2.$$

Proof. Let n be the smallest k such that $\lambda_k^c \neq 0$. Then $n \leq p^5$. We assume that $|q_c(P)| \leq 10^{-p}$, otherwise there is nothing to prove. Since $\text{Ord}_c U = 0$ and $U^2(P) = \gamma_c^2$, it follows from (6.1) that $2\pi f(q_c(P))i + \sum_{k=n}^{\infty} \lambda_k^c q_c(P)^{k/p} = 0$.

Suppose that $f(q_c(P)) = 0$. Then $|\lambda_n^c q_c(P)^{n/p}| = |\sum_{k=n+1}^{\infty} \lambda_k^c q_c(P)^{k/p}|$. On one hand, we have

$$\begin{aligned} \left| \sum_{k=n+1}^{\infty} \lambda_k^c q_c(P)^{k/p} \right| &\leq \sum_{k=n+1}^{\infty} |\lambda_k^c| |q_c(P)|^{k/p} \leq \sum_{k=n+1}^{\infty} 48p^2(k+p) |q_c(P)|^{k/p} \\ &\leq 96p^2(n+p+1) |q_c(P)|^{(n+1)/p}. \end{aligned}$$

On the other hand, using Liouville's inequality (see [22, formula (3.13)]), we get

$$|\lambda_n^c| \geq e^{-[\mathbb{Q}(\zeta_p):\mathbb{Q}]h(\lambda_n^c)} \geq (48np^3 + 48n^2p^2)^{-p+1}.$$

Then we obtain

$$\log |q_c(P)^{-1}| \leq p^2 \log(48p^{12} + 48p^8) + p \log(96p^2(p^5 + p + 1)).$$

Finally, the desired result follows from (3.1).

Suppose that $f(q_c(P)) \neq 0$. Then

$$2\pi \leq \left| \sum_{k=n}^{\infty} \lambda_k^c q_c(P)^{k/p} \right| \leq 96p^2(n+p) |q_c(P)|^{n/p}.$$

Then we get $\log |q_c(P)^{-1}| \leq p \log(96p^2(p^5 + p))$. So we have

$$\log |j(P)| \leq p \log(96p^2(p^5 + p)) + \log 2.$$

$\square$

Now we assume that $\text{Ord}_c V \neq 0$, i.e. $\text{Ord}_c U \neq 0$. By Lemma 4.1, we can choose a U such that $\text{Ord}_c U < 0$. Then we choose a σ such that $\text{Ord}_c U^\sigma > 0$. Put $n_1 = -\text{Ord}_c U$ and $n_2 = \text{Ord}_c U^\sigma$. Since $U(P)$ and γ_c are real, we have $U(P)^{2n_2} U^\sigma(P)^{2n_1} = \gamma_c^{2n_2} \gamma_{c,\sigma}^{2n_1}$, i.e. $U^{2n_2}(U^\sigma)^{2n_1}(P) = \gamma_c^{2n_2} \gamma_{c,\sigma}^{2n_1}$. Lemma 3.5 guarantees that $U^{2n_2}(U^\sigma)^{2n_1}$ is not a constant.

Applying the same method as above without difficulties, we can also get a better bound than Theorem 1.1. We omit the details here.

ACKNOWLEDGEMENTS

The authors are very grateful to their advisor, Yuri Bilu, for a careful reading and lots of stimulating suggestions and helpful discussions, especially for his key suggestion in Section 6. They are also grateful to the referee for a careful reading and very useful comments.

REFERENCES

- [1] Lars V. Ahlfors, *Complex analysis*. An introduction to the theory of analytic functions of one complex variable; International Series in Pure and Applied Mathematics, McGraw-Hill Book Co., New York, 1978. MR510197 (80c:30001)
- [2] A. Bajolet and Yu. Bilu, *Computing integral points on $X_{\text{ns}}^+(p)$* , preprint, 2012. arXiv:1212.0665
- [3] Burcu Baran, *A modular curve of level 9 and the class number one problem*, J. Number Theory **129** (2009), no. 3, 715–728, DOI 10.1016/j.jnt.2008.09.013. MR2488598 (2010f:11095)
- [4] Burcu Baran, *Normalizers of non-split Cartan subgroups, modular curves, and the class number one problem*, J. Number Theory **130** (2010), no. 12, 2753–2772, DOI 10.1016/j.jnt.2010.06.005. MR2684496 (2011i:11083)
- [5] Yuri Bilu, *Effective analysis of integral points on algebraic curves*, Israel J. Math. **90** (1995), no. 1–3, 235–252, DOI 10.1007/BF02783215. MR1336325 (96e:11082)
- [6] Yuri Bilu and Guillaume Hanrot, *Solving Thue equations of high degree*, J. Number Theory **60** (1996), no. 2, 373–392, DOI 10.1006/jnth.1996.0129. MR1412969 (97k:11040)
- [7] Yuri Bilu and Marco Illengo, *Effective Siegel’s theorem for modular curves*, Bull. Lond. Math. Soc. **43** (2011), no. 4, 673–688, DOI 10.1112/blms/bdq130. MR2820153 (2012h:11095)
- [8] Yuri Bilu and Pierre Parent, *Runge’s method and modular curves*, Int. Math. Res. Not. IMRN **9** (2011), 1997–2027, DOI 10.1093/imrn/rnq141. MR2806555 (2012m:11083)
- [9] Yuri Bilu and Pierre Parent, *Serre’s uniformity problem in the split Cartan case*, Ann. of Math. (2) **173** (2011), no. 1, 569–584, DOI 10.4007/annals.2011.173.1.13. MR2753610 (2012a:11077)
- [10] Yu. Bilu, P. Parent, and M. Rebolledo, *Rational points on $X_0^+(p^r)$* , Ann. Inst. Fourier **63** (2013), no. 3, 957–984. MR3137477
- [11] Antone Costa and Eduardo Friedman, *Ratios of regulators in totally real extensions of number fields*, J. Number Theory **37** (1991), no. 3, 288–297, DOI 10.1016/S0022-314X(05)80044-7. MR1096445 (92j:11138)
- [12] Kurt Heegner, *Diophantische Analysis und Modulfunktionen* (German), Math. Z. **56** (1952), 227–253. MR0053135 (14,725j)
- [13] M. A. Kenku, *A note on the integral points of a modular curve of level 7*, Mathematika **32** (1985), no. 1, 45–48, DOI 10.1112/S0025579300010846. MR817106 (87d:11040)
- [14] Daniel S. Kubert and Serge Lang, *Modular units*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Science], vol. 244, Springer-Verlag, New York, 1981. MR648603 (84h:12009)
- [15] Stéphane Louboutin, *Upper bounds on $|L(1, \chi)|$ and applications*, Canad. J. Math. **50** (1998), no. 4, 794–815, DOI 10.4153/CJM-1998-042-2. MR1638619 (99f:11149)
- [16] E. M. Matveev, *An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. II* (Russian, with Russian summary), Izv. Ross. Akad. Nauk Ser. Mat. **64** (2000), no. 6, 125–180, DOI 10.1070/IM2000v064n06ABEH000314; English transl., Izv. Math. **64** (2000), no. 6, 1217–1269. MR1817252 (2002e:11091)

- [17] Jean-Pierre Serre, *Lectures on the Mordell-Weil theorem*. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt. With a foreword by Brown and Serre. Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig, 1997. MR1757192 (2000m:11049)
- [18] M. Sha, *Bounding the j -invariant of integral points on modular curves*, Int. Math. Res. Notes, to appear. arXiv:1208.1337
- [19] Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*, Kanô Memorial Lectures, No. 1, Publications of the Mathematical Society of Japan, Iwanami Shoten, Publishers, Tokyo; Princeton University Press, Princeton, N.J., 1971. MR0314766 (47 #3318)
- [20] Carl Ludwig Siegel, *Über einige Anwendungen diophantischer Approximationen*, Abh. Pr. Akad. Wiss. (1929), no. 1 (=Ges. Abh. I, 209–266, Springer, 1966.) MR0197270 (33 #5441)
- [21] Carl Ludwig Siegel, *Zum Beweise des Starkeschen Satzes* (German), Invent. Math. **5** (1968), 180–191. MR0228465 (37 #4045)
- [22] Michel Waldschmidt, *Diophantine approximation on linear algebraic groups*, Transcendence properties of the exponential function in several variables. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 326, Springer-Verlag, Berlin, 2000. MR1756786 (2001c:11075)
- [23] Lawrence C. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1982. MR718674 (85g:11001)

INSTITUT DE MATHÉMATIQUES DE BORDEAUX, UNIVERSITÉ BORDEAUX 1, 33405 TALENCE CEDEX, FRANCE

E-mail address: Aurelien.Bajolet@math.u-bordeaux1.fr

INSTITUT DE MATHÉMATIQUES DE BORDEAUX, UNIVERSITÉ BORDEAUX 1, 33405 TALENCE CEDEX, FRANCE

E-mail address: shammin2010@gmail.com