Functiones et Approximatio
49.2 (2013), 321–330
doi: 10.7169/facm/2013.49.2.10

LOCAL DIOPHANTINE PROPERTIES OF SHIMURA CURVES AND THE $\bar{\mathbb{F}}_p$-GONALITY

Chuangxun Cheng

Abstract: In this paper, we study the local points of small degrees on Shimura curves $X_0^D(N)$ over a totally real field F. We then study the $\bar{\mathbb{F}}_p-$gonality for these Shimura curves in the case $F = \mathbb{Q}$.

Keywords: Shimura curve, gonality.

1. Introduction

In [5], the authors studied the local Diophantine properties of Shimura curves. In [10], the authors generalized the results in [5] and constructed Shimura curves which violates Hasse principle. In [3], the author constructed infinitely many Shimura curves which violates Hasse principle. One of the key ingredients in [3] is a careful study of local points on Shimura curves. All these papers focus on the Shimura curves over $\mathbb{Q}$. In this paper, we study the local points of small degrees on Shimura curves $X_0^D(N)$ over a totally real field F. We show that most of the results in section 3 of [3] still hold in totally real field case.

We also study the $\bar{\mathbb{F}}_p-$gonality of $X_0^D(N)$ in the case $F = \mathbb{Q}$ and give lower bound for this invariant. The reason we assume that $F = \mathbb{Q}$ is because, over a totally real field F, $X_0^D(N)$ is not geometrically integral in general and the $\bar{\mathbb{F}}_p-$gonality is not defined. One of the important tools we use is the inequality in Theorem 3.1, which is proved in [8].

1.1. Curve $X_0^D(N)$

Let F be a totally real field of degree d. We fix an embedding $\tau_1 : F \hookrightarrow \mathbb{R}$. Let S_D be a finite set of finite primes of F such that

$$|S_D| \equiv d - 1 \pmod 2.$$

2010 Mathematics Subject Classification: primary: 11G20

We also denote S_D the product of primes in this set. Let D be a quaternion algebra over F which is ramified at places $S_D \cup \{v|\infty : v \neq \tau_1\}$. D is unique up to isomorphism. We exclude the case $D = M_2(\mathbb{Q})$ in this paper.

Fix $\mathcal{O}_D$ a maximal order of D. If v is a finite prime of F such that $v \nmid S_D$, we fix an isomorphism $D \otimes F_v \cong M_2(F_v)$, under which we have $(\mathcal{O}_D \otimes \mathcal{O}_{F_v})^\times = GL_2(\mathcal{O}_{F_v})$. Let $\mathcal{O}_F$ be the ring of integers of F. Let N be a squarefree idea of $\mathcal{O}_F$ such that $(N, S_D) = 1$. Let $\Gamma_0^D(N)$ be an open compact subgroup of $(D \otimes \mathbb{A}_F^\infty)^\times$ defined as follows,

$$\Gamma_0^D(N)_v = \begin{cases} (\mathcal{O}_D \otimes \mathcal{O}_{F_v})^\times & \text{if } v \nmid N \\ \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathcal{O}_{F_v}) : v \mid c\} & \text{if } v \mid N \end{cases}$$

The curve $X_0^D(N)$ is the Shimura curve attached to D and $\Gamma_0^D(N)$. It is a compact smooth algebraic curve over F with $\mathbb{C}-$points

$$X_0^D(N)(\mathbb{C}) \cong D^\times \backslash (\mathbb{C} - \mathbb{R}) \times (D \otimes \mathbb{A}_F^\infty)^\times / \Gamma_0^D(N).$$

1.2. m-invariant

Let $X_{/K}$ be a variety over a field K. Following [3], define the *m − invariant* $m(X) = m(X_{/K})$ to be the minimum degree of a finite field extension L/K such that $X(L) \neq \emptyset$.

If K is a number field. Write Ω_K for the set of all places of K. For each $v \in \Omega_K$, we put

$$m_v(X) := m(X_{/K_v})$$

and

$$m_{loc}(X) = \mathrm{lcm}_{v \in \Omega_K} m_v(X).$$

As remarked in Remark 2.1 of [3], $m_v(X) = 1$ for all but finitely many v, therefore, $m_{loc}(X)$ is well defined.

One of the main results of this paper is the following theorem, which generalizes Theorem 8(b) of [3].

Theorem 1.1. *For our curve $X_0^D(N)_{/F}$, we have $m_{loc}(X_0^D(N)) \mid 12$.*

1.3. Gonality

The *K − gonality* of a geometrically integral curve $C_{/K}$, denoted $\gamma_K(C)$, is the least positive integer n for which there exists a degree n dominant rational map $C \to \mathbf{P}^1_K$. If L/K is a field extension, we define also the $L-$gonality $\gamma_L(C)$ of C as the gonality of $C_L := C \times_K L$. See appendix of [8] for some general facts about gonality.

If $C_{/K}$ has gonality γ, where K is a field with finitely many elements. Then there exists a degree γ dominant rational map $C \to \mathbf{P}^1_K$. Therefore we have the obvious inequality

$$|C(K)| \leqslant \gamma |\mathbf{P}^1(K)| = \gamma(|K| + 1).$$

So $\gamma \geqslant \frac{|C(K)|}{|K|+1}$. With this easy estimate and Theorem 3.1, we give a lower bound for $\gamma_{\bar{\mathbb{F}}_p}(X_0^D(N))$ in the case $F = \mathbb{Q}$, by some counting arguments. See the corollaries in section 3 for details. In particular, we have the following result.

Theorem 1.2. *Fix prime number p. If N is squarefree, then $\gamma_{\bar{\mathbb{F}}_p}(X_0^D(N)) \to \infty$ as $N \to \infty$.*

1.4. Notation

If L is a perfect field we will let $\bar{L}$ denote the algebraic closure of L. If L is a number field, we let $\mathbb{A}_L$ denote the ring of adeles over L, and $\mathbb{A}_L^\infty$ denote the ring of finite adeles over L. If $L = \mathbb{Q}$, we write $\mathbb{A}$ and $\mathbb{A}^\infty$ for $\mathbb{A}_\mathbb{Q}$ and $\mathbb{A}_\mathbb{Q}^\infty$, respectively.

Let Σ be a set of primes of F. If a group U has the form $U = \prod_{v\in\Sigma} U_v$, and J is an ideal which is a product of some elements in Σ, we will write U^J for the subgroup of U given by $U^J = \prod_{v\in\Sigma, v\nmid J} U_v$ and U_J for the subgroup of U given by $U_J = \prod_{v\in\Sigma, v|J} U_v$.

In this paper, F will be a totally real field. If $\mathfrak{p}$ is a finite place of F, we will write $F_\mathfrak{p}$ for the completion of F at $\mathfrak{p}$, $\mathcal{O}_{F_\mathfrak{p}}$ the ring of integers of $F_\mathfrak{p}$, and $k_\mathfrak{p}$ the residue field of $\mathcal{O}_{F_\mathfrak{p}}$. We also write $k'_\mathfrak{p}$ for the degree two extension of $k_\mathfrak{p}$.

2. Local points of $X_0^D(N)$

In this section, we apply Hensel's lemma (Proposition 2.1) to study local points on Shimura curves with Γ_0^D level. More precisely, we compute $m_\mathfrak{p}(X_0^D(N))$. The results in this section hold for general totally real field F. In particular, the results hold in the case $F = \mathbb{Q}$.

Proposition 2.1 (Hensel's Lemma). *Let R be a complete DVR with quotient field K and residue field k. Let X be a smooth algebraic variety over K. Suppose that $\mathcal{X}_{/R}$ is a regular model of $X_{/K}$. Then X has a $K-$rational point if and only if the special fiber $\mathcal{X}_{/R} \times k$ has a smooth $k-$rational point.*

Proof. See for example Lemma 1.1 of [5]. ■

2.1. Case $\mathfrak{p} \nmid NS_D$

If $(\mathfrak{p}, NS_D) = 1$, then $X_0^D(N)_{/F_\mathfrak{p}}$ has a smooth integral model $M_0^D(N)_{/\mathcal{O}_{F_\mathfrak{p}}}$ which has good reduction at $\mathfrak{p}$. We consider another Shimura curve $X_0^D(\mathfrak{p}N)$ with regular integral model $M_0^D(\mathfrak{p}N)_{/\mathcal{O}_{F_\mathfrak{p}}}$. The curve $M_0^D(\mathfrak{p}N)_{/\mathcal{O}_{F_\mathfrak{p}}}$ has semistable reduction at $\mathfrak{p}$. The special fiber $M_0^D(\mathfrak{p}N)_{/k_\mathfrak{p}}$ is isomorphic to a union of two copies of $M_0^D(N)_{/k_\mathfrak{p}}$ intersecting transversely above a finite set of points $\Sigma_0^D(N)$. (See for example Theorem 10.2 of [4].) The points in $\Sigma_0^D(N)$ are called supersingular points.

Lemma 2.2. *The finite set $\Sigma_0^D(N)$ is not empty. Moreover, every supersingular point is defined over $k'_\mathfrak{p}$.*

Proof. Let D' be another quaternion algebra over F such that D' is ramified at primes $S_D \cup \{\mathfrak{p}\} \cup \{v : v \mid \infty\}$. Then from section 11 of [2], we have the following bijection:

$$\Sigma_0^D(N) \cong (D')^\times \backslash (D' \otimes_F \mathbb{A}_F^{\mathfrak{p}\infty})^\times \times F_\mathfrak{p}^\times / \Gamma_0^{D'}(N)^\mathfrak{p} \times \mathcal{O}_{F_\mathfrak{p}}^\times.$$

Therefore, $\Sigma_0^D(N)$ is non empty (and finite).

The supersingular points are defined over $k'_\mathfrak{p}$ follows from Theorem 10.2 of [4]. (See also Theorem 2.4.) ∎

Corollary 2.3. *If $\mathfrak{p} \nmid NS_D$, then $m_\mathfrak{p}(X_0^D(N)) \leqslant 2$.*

Proof. This follows from the above lemma and Hensel's lemma. ∎

2.2. Case $\mathfrak{p} \mid N$

The following theorem is proved in section 10 of [4]. We already used it above.

Theorem 2.4. *If $\mathfrak{p} \mid N$, then the special fiber $M_0^D(N)_{/k_\mathfrak{p}}$ has two irreducible components, each isomorphic to the smooth curve $M_0^D(N/\mathfrak{p})_{/k_\mathfrak{p}}$. The two irreducible components intersect transversely at the supersingular points, a corresponding point on the first copy being glued to its image under the Frobenius map.*

Furthermore, at each supersingular point $x \in M_0^D(N)_{/k'_\mathfrak{p}}$, the complete local ring is isomorphic to $W(k'_\mathfrak{p})[1/p][[X,Y]]/(XY - \varpi_\mathfrak{p}^{a_x})$ for some positive integer a_x.

Corollary 2.5. *If $\mathfrak{p} \mid N$, then $m_\mathfrak{p}(X_0^D(N)) \leqslant 4$.*

Proof. The proof is the same as the proof of Proposition 14 of [3]. We sketch it here. Let $z \in M_0^D(N)_{k'_\mathfrak{p}}$ be a point coming from a supersingular point in $M_0^D(N/\mathfrak{p})(k'_\mathfrak{p})$. Then the complete local ring at z is isomorphic to $W(k'_\mathfrak{p})[1/p][[X,Y]]/(XY - \varpi_\mathfrak{p}^{a_z})$ for some positive integer a_z. If $a_z > 1$, then we have to blow up z $(a_z - 1)$ times to obtain a regular model. This procedure produces $(a_z - 1)$ rational curves over $k'_\mathfrak{p}$. Each such rational curve has $(|k'_\mathfrak{p}| - 1)$ smooth points over $k'_\mathfrak{p}$, which lift to give rational points of $X_0^D(N)$ over $K_0 = Frac(W(k'_\mathfrak{p}))$.

If $a_z = 1$, let $K = K_0(\sqrt{\varpi})$ be a ramified quadratic extension of K_0. Let R be the ring of integers of K. Then the complete local ring of $z \in M_0^D(N)_{/R}$ is isomorphic to $R[[X,Y]]/(XY - (\sqrt{\varpi})^2)$. The same argument as above shows that $X_0^D(N)$ has rational points over K. Since $[K : F_\mathfrak{p}] = 4$, the statement follows. ∎

2.3. Case $\mathfrak{p} \mid S_D$

We recall the $p-$adic uniformization theory for Shimura curves. Let v be a finite place of F at which D is ramified. Let P be an open compact subgroup of $(D \otimes \mathbb{A}^\infty)^\times$ such that $P_v = (\mathcal{O}_D \otimes_F \mathcal{O}_{F_v})^\times$. We have a Shimura curve X_P (with level P) which is defined over F.

Let F_v^{ur} be the maximal unramified extension of F_v, let Ω_{F_v} be Drinfeld's upper half plane. Consider the analytic space $\Omega_{F_v}^{nr} = \Omega_{F_v} \otimes_{F_v} {F_v}^{nr}$ over F_v. We let $g \in GL_2(F_v)$ act on $\Omega_{F_v}^{nr}$ via the natural (left) action on Ω_{F_v} and the action of $Frob_{F_v}^{val(det\ g)}$ on ${F_v}^{ur}$. We also let $n \in \mathbb{Z}$ act on $\Omega_{F_v}^{nr}$ through the action of $Frob_{F_v}^{-n}$ on ${F_v}^{nr}$. This gives an F_v-rational action of $GL_2(F_v) \times \mathbb{Z}$ on $\Omega_{F_v}^{nr}$. Moreover, the F_v-analytic space $GL_2(F_v)\backslash(\Omega \times (P^v\backslash(D \otimes \mathbb{A}_F^{\infty v})^\times/D^\times))$ algebraizes canonically to a scheme $\mathfrak{X}_P$ over F_v. Let X and $\mathfrak{X}$ be the inverse limits of X_P and $\mathfrak{X}_P$ over all P. Then a special case of Theorem 5.3 of [11] gives the following theorem. (See also section 1 of [6].)

Theorem 2.6. *There exists a $(D \otimes \mathbb{A}_F^{\infty v})^\times \times \mathbb{Z}-$equivariant, F_v-rational isomorphism*

$$X \otimes_F F_v \cong \mathfrak{X}.$$

In particular, we have an F_v-rational isomorphism

$$X_P \otimes_F F_v \cong \mathfrak{X}_P.$$

Furthermore, there exists an integral model M_P for X_P over $\mathcal{O}_{F_v}$, and the above isomorphism can be extended to schemes over $\mathcal{O}_{F_v}$.

Corollary 2.7. *If $\mathfrak{p} \mid S_D$, then $m_{\mathfrak{p}}(X_0^D(N) \leqslant 2$.*

Proof. In our case, we have $M_P = X_0^D(N)_{/\mathcal{O}_{F_\mathfrak{p}}}$, $\mathfrak{X}_P = \mathfrak{X}_0^D(N)$. The special fiber of $\mathfrak{X}_0^D(N)_{/\mathcal{O}_{F_\mathfrak{p}}}$ has non-degenerate quadratic singular points. The dual graph $\mathfrak{G}$ attached to the special fiber of $\mathfrak{X}_0^D(N)_{/\mathcal{O}_F}$ is the quotient

$$GL_2(F_\mathfrak{p})^+\backslash(\Delta \times (\Gamma_0^D(N)^\mathfrak{p}\backslash(D \otimes \mathbb{A}_F^{\infty\mathfrak{p}})^\times/D^\times)),$$

where Δ is the well-known tree attached to $SL_2(F_\mathfrak{p})$. The singular points of $\mathfrak{X}_0^D(N) \times k_\mathfrak{p}$ correspond to the edges of $\mathfrak{G}$.

To prove the corollary, it suffices to find a smooth $k'_\mathfrak{p}-$rational point on $M_0^D(N) \cong_{k'_\mathfrak{p}} \mathfrak{X}_0^D(N)$. Because every vertex of $\mathfrak{G}$ has degree at most $|k_\mathfrak{p}|+1$, every irreducible component $\mathfrak{X}_i$ (which is isomorphic to $\mathbf{P}^1$) of $\mathfrak{X}_0^D(N)_{/k_\mathfrak{p}}$ has at most $|k_\mathfrak{p}|+1$ singular points, hence at least $|k_\mathfrak{p}|^2+1-(|k_\mathfrak{p}|+1)$ smooth $k'_\mathfrak{p}-$rational points. ■

From the above analysis, we have the following result.

Corollary 2.8. *For any finite prime $\mathfrak{p}$ of F, $X_0^D(N)(k'_\mathfrak{p})$ is non empty.*

3. $\bar{\mathbb{F}}_p-$gonality of $X_0^D(N)$

If $F \neq \mathbb{Q}$, $X_0^D(N)$ is not geometrically integral in general. From now on, we assume that $F = \mathbb{Q}$.

In Theorem 1.1 of [1], the author gives a linear lower bound on the $\mathbb{C}-$gonality of Shimura curves. In [3], the author uses this bound and some other ingredients to show that almost all Shimura curves $X_0^D(N)$ are potentially Hasse principle violation. In this section, we study the $\bar{\mathbb{F}}_p-$gonality of Shimura curve $X_0^D(N)$. More precisely, we give lower bounds of the $\bar{\mathbb{F}}_p-$gonality of Shimura curve $X_0^D(N)$ by an idea of [8] and some counting arguments. The following theorem is proved in Theorem 2.5 of [8].

Theorem 3.1. *Let X be a geometrically integral curve over a perfect field K. Let $L \supset K$ be an algebraic field extension. Assume that $X(K) \neq \emptyset$. Then $\gamma_L(X) \geqslant \sqrt{\gamma_K(X)}$.*

By Corollary 2.8, $X_0^D(N)(\mathbb{F}_{p^2})$ is non empty for any p. We may apply this theorem to give a lower bound for $\gamma_{\bar{\mathbb{F}}_p}(X_0^D(N))$ by computing $\gamma_{\mathbb{F}_{p^2}}(X_0^D(N))$.

3.1. Case $p \nmid NS_D$

We count the number of $\mathbb{F}_{p^r}-$rational points of $X_0^D(N)_{/\mathbb{F}_p}$. To do this, we follow the approach of [5]. Let p be a prime number not dividing NS_D. The Eichler-Shimura relation leads to the following formula for the Zeta-function of $X_0^D(N)_{/\mathbb{F}_p}$.

$$Z(X_0^D(N)_{/\mathbb{F}_p}, t) = \frac{\det(1 - T_p t + \langle p \rangle p t^2)}{(1-t)(1-pt)}.$$

Here T_p is the Hecke operator acting on the space $H^0(X_0^D(N), \Omega^1)$, $\langle p \rangle$ is the diamond operator. Set $T_1 = Id$, $T_{p^{-1}} = 0$, then we have identity

$$T_{p^{r+1}} = T_{p^r} T_p - \langle p \rangle p T_{p^{r-1}}.$$

By taking $\frac{d}{dt}\log$ on both sides of the Zeta-function, we have the following equality for $r \geqslant 1$:

$$|X_0^D(N)(\mathbb{F}_{p^r})| = 1 + p^r + \mathrm{Trace}(\langle p \rangle p T_{p^{r-2}} - T_{p^r}). \tag{3.1}$$

In our setting, for $(n, NS_D) = 1$, $\mathrm{Trace}(T_n)$ can be computed in a very explicit way. We state the following theorem which is a special case of Theorem 6.8.4 of [7].

Theorem 3.2 (Eichler-Selberg trace formula). *Let χ be a Dirichlet character* (mod N)*, $S_2(\Gamma_0^D(N), \chi)$ be the space of forms of weight two, level $\Gamma_0^D(N)$, and character χ. Then we have the following formula.*

$$\begin{aligned}\mathrm{Trace}(T_n) &:= \mathrm{Trace}(T_n | S_2(\Gamma_0^D(N), \chi)) \\ &= \frac{1}{12}\chi(\sqrt{n}) N \prod_{p|N}(1 + p^{-1}) \prod_{p|S_D}(p-1) - \sum_t a(t) \sum_f b(t,f) c(t,f).\end{aligned} \tag{3.2}$$

Here each term is as follows.

(1) $\chi(\sqrt{n}) = 0$ *if n is not a square.*
(2) *t runs over all integers such that $t^2 - 4n$ are negative or square. For such t, $a(t)$ is some number depends on n and S_D.*

(3) *f runs over all positive divisors of m, where m is a positive integer given by $t^2 - 4n = m^2 d$ if $d \neq 0$; otherwise $m = 1$. For such an f, $b(t, f)$ is some number depends on n and S_D, $c(t, f)$ is some number depends on n, S_D, and N.*

For the explicit formulaes of $a(t)$, $b(t, f)$, and $c(t, f)$, see Theorem 6.8.4 of [7]. To compute equation (3.1), we have $\chi = 1$.

Corollary 3.3. *If $p \nmid N_S D$, then*

$$\gamma_{\mathbb{F}_{p^2}}(X_0^D(N)) \geqslant \frac{1 + p^2 + \mathrm{Trace}(\langle p \rangle p - T_{p^2})}{p^2 + 1}.$$

Here, the right hand side of the inequality can be computed by Eichler-Selberg trace formula, denote it by $G_2(p, N, S_D)$. We then have

$$\gamma_{\bar{\mathbb{F}}_p}(X_0^D(N)) \geqslant \sqrt{G_2(p, N, S_D)}.$$

Proof. The first inequality follows from the fact that

$$|X_0^D(N)(\mathbb{F}_{p^2})| \leqslant \gamma_{\mathbb{F}_p^2}(X_0^D(N))|\mathbf{P}^1(\mathbb{F}_{p^2})| = \gamma_{\mathbb{F}_p^2}(X_0^D(N))(p^2 + 1).$$

The second inequality follows from Theorem 3.1. ∎

Remark 3.4. In the above computation, we did not write down all the terms explicitly. The reason is that the formulaes in Theorem 6.8.4 of [7] are complicated, even in the simple case where N is a prime number. In this case, from equation (5) of [10], we have

$$|X_0^D(N)(\mathbb{F}_{p^2})| = \Sigma_2(N) - p\Sigma_0(N) + \frac{1}{12}(N + 1)(p - 1) \prod_{d | S_D, d \text{ prime}} (d - 1).$$

Here $\Sigma_m(M)$ are some number defined at the beginning of section 1.3 of [10], which are related to a, b, and c in Eichler-Selberg trace formula. In particular, $\Sigma_2(N) - p\Sigma_0(N) \geqslant 0$ by Proposition 1.3 of [10]. Therefore we have the following lower bound of $\gamma_{\mathbb{F}_{p^2}}(X_0^D(N))$.

$$\gamma_{\mathbb{F}_{p^2}}(X_0^D(N)) \geqslant \frac{1}{12(p^2 + 1)}(N + 1)(p - 1) \prod_{d | S_D, d \text{ prime}} (d - 1).$$

Note that we have $12(p^2 + 1)$ as the denominator. See Proposition 3.1 of [8] for a similar result in the case of modular curves.

Corollary 3.5. *Fix a prime p. If N is square free and $p \nmid NS_D$, then*

$$\gamma_{\mathbb{F}_{p^2}}(X_0^D(N)) \geqslant \frac{1}{12(p^2 + 1)}(p - 1)(n_N + 1) \prod_{d | S_D, d \text{ prime}} (d - 1),$$

where n_N is the maximal prime divisor of N. Therefore,

$$\gamma_{\bar{\mathbb{F}}_p}(X_0^D(N)) \geqslant \sqrt{\frac{1}{12(p^2+1)}(p-1)(n_N+1)\prod_{d|S_D, d \text{ prime}}(d-1)}.$$

Proof. There exists a dominant rational map $X_0^D(N) \to X_0^D(N/n)$ for any prime divisor n of N. By Proposition A.1 of [8], $\gamma_{\mathbb{F}_{p^2}}(X_0^D(N)) \geqslant \gamma_{\mathbb{F}_{p^2}}(X_0^D(N/n))$. The corollary follows from the computation in Remark 3.4. ■

3.2. Case $p \mid N$

We have the following inequality

$$\gamma_{\mathbb{F}_{p^2}}(X_0^D(N)) \geqslant \frac{|X_0^D(N)(\mathbb{F}_{p^2})|}{p^2+1}.$$

Note that $X_0^D(N)_{/\mathbb{F}_p}$ is a union of two copies of a smooth curve $X_0^D(N/p)_{/\mathbb{F}_p}$ intersect at supersingular points, which are rational over $\mathbb{F}_{p^2}$. The set of supersingular points is bijective to the following double quotient

$$\bar{D}^\times \backslash (\bar{D} \otimes \mathbb{A}^{\infty p})^\times \times \mathbb{Q}_p^\times / \Gamma_0^{\bar{D}}(N/p)^p \mathbb{Z}_p^\times.$$

Here $\bar{D}$ is another definite quaternion algebra over $\mathbb{Q}$ obtained by changing the local invariants of D at p and ∞. This double quotient is a finite set. Let $\sigma(p, N/p, S_D)$ be the number of elements of this set. We have the following result.

Corollary 3.6. *If $p \mid N$, then*

$$\gamma_{\mathbb{F}_{p^2}}(X_0^D(N)) \geqslant 2G_2(p, N/p, S_D) - \frac{\sigma(p, N/p, S_D)}{p^2+1}.$$

Therefore,

$$\gamma_{\bar{\mathbb{F}}_p}(X_0^D(N)) \geqslant \sqrt{2G_2(p, N/p, S_D) - \frac{\sigma(p, N/p, S_D)}{p^2+1}}.$$

Notice that $G_2(p, N/p, S_D) \geqslant \frac{\sigma(p,N/p,S_D)}{p^2+1}$. Therefore

$$2G_2(p, N/p, S_D) - \frac{\sigma(p, N/p, S_D)}{p^2+1} \geqslant G_2(p, N/p, S_D) \geqslant \frac{\sigma(p, N/p, S_D)}{p^2+1} > 0.$$

Remark 3.7. Since N is square free, we have an explicit bound for $G_2(p, N/p, S_D)$. The same argument as in the case $p \nmid S_D N$ gives us the following inequality.

$$\gamma_{\mathbb{F}_{p^2}}(X_0^D(N)) \geqslant \frac{1}{12(p^2+1)}(p-1)(n_{N/p}+1)\prod_{d|S_D, d \text{ prime}}(d-1).$$

3.3. Case $p \mid S_D$

Let $\bar{D}$ be another definite quaternion algebra over $\mathbb{Q}$ obtained by changing the local invariants of D at p and ∞. By Proposition 4.4 of [9], the set of irreducible components of $\mathfrak{X}_0^D(N)$ is bijective to the set of vertices of its dual graph, which is bijective to two copies of the following double quotient

$$\bar{D}^\times \backslash (\bar{D} \otimes \mathbb{A}^\infty)^\times / \Gamma_0^{\bar{D}}(N).$$

This is a finite set. Let $v(p, N, S_D)$ be the number of elements of this double quotient. The set of singular points of $\mathfrak{X}_0^D(N)_{/\mathbb{F}_p}$ is bijective to the set of edges of its dual graph, which is bijective to the following double quotient

$$\bar{D}^\times \backslash (\bar{D} \otimes \mathbb{A}^\infty)^\times / \Gamma_0^{\bar{D}}(Np).$$

This is also a finite set. Let $e(p, N, S_D)$ be the number of elements of this set.

From the proof of Corollary 2.7, the number of smooth $\mathbb{F}_{p^2}$ points on $\mathfrak{X}_0^D(N)$ is at least $2(p^2 - p)v(p, N, S_D)$. The number of rational $\mathbb{F}_{p^2}$ points on $\mathfrak{X}_0^D(N)$ is at least $2(p^2 - p)v(p, N, S_D) + e(p, N, S_D)$. We have the following result.

Corollary 3.8. *If $p \mid S_D$, then*

$$\gamma_{\mathbb{F}_p^2}(X_0^D(N)) \geqslant \frac{2(p^2 - p)v(p, N, S_D) + e(p, N, S_D)}{p^2 + 1}.$$

Therefore,

$$\gamma_{\bar{\mathbb{F}}_p}(X_0^D(N)) \geqslant \sqrt{\frac{2(p^2 - p)v(p, N, S_D) + e(p, N, S_D)}{p^2 + 1}}.$$

References

[1] D. Abramovich, *A Linear Lower Bound on the Gonality of Modular Curves*, Internat. Math. Res. Notices 1996, no. 20, 1005–1011.

[2] M. Carayol, *Sur la mauvaise réduction des courbes de Shimura*, Compositio Math. **59** (1986), no. 2, 151–230.

[3] P. Clark, *On the Hasse principle for Shimura curves*, Israel J. Math. **171** (2009), no. 1, 349–365.

[4] F. Jarvis, *Mazur's Principle for totally real fields of odd degree*, Compositio Mathematica **116** (1999) 39–79.

[5] B.W. Jordan, B. Livne, *Local diophantine properties of Shimura curves*, Math. Ann. **270** (1993), 385–390.

[6] B. Jordan, B. Livne, Y. Varshavsky, *Local points on p-adically uniformized Shimura varieties.*

[7] T. Miyake, *Modular Forms.* Springer-Verlag, 2006

[8] B. Poonen, *Gonality of modular curves in characteristic p*, Math. Res. Lett. **14** (2007), no. 4, 691–701.

[9] K.A. Ribet, *On modular representations of* $Gal(\bar{Q}/Q)$ *arising from modular forms*. Invent. Math. **100** (1990), no. 2, 431–476.

[10] A. Skorobogatov, A. Yafaev, *Descent on certain Shimura curves*. Israel J. Math. **140** (2004), 319–332.

[11] Y. Varshavsky, *p-adic uniformization of unitary Shimura varieties*. J. Differential Geometry **49** (1998), 75–113

Address: Chuangxun Cheng: Department of Mathematics, Bielefeld University, Germany.

E-mail: ccheng@math.uni-bielefeld.de

Received: 18 October 2012; **revised:** 26 October 2012