Japan J. Indust. Appl. Math., 24 (2007), 307–318 Area ⟨3⟩

An Observation on the Cyclicity of the Group of the $\mathbb{F}_p$-Rational Points of Abelian Surfaces

Takuya YAMAUCHI*

*Department of Mathematics, Graduate School of Science
Hiroshima University, Higashi-hiroshima, 739–8526, Japan
E-mail: yamauchi@math.sci.hiroshima-u.ac.jp

Received October 31, 2006
Revised April 13, 2007

Let A be a principally polarized Abelian surface defined over $\mathbb{Q}$ with $\mathrm{End}(A) = \mathbb{Z}$ and $\widetilde{A}$ be the reduction at a good prime p. In this paper, we study the density of prime numbers p for which $\widetilde{A}(\mathbb{F}_p)$ is a cyclic group and establish a conjecture which relates this density.

Key words: Abelian surface, cyclicity

1. Introduction

Let A be an Abelian variety A defined over $\mathbb{Q}$ and p be a rational prime. Let $\widetilde{A}$ be the reduction of A at a good prime p. In this paper, we study the structure of the group of rational points of the reduction of A modulo a rational prime p. In particular, we want to investigate the density

$$C_A := \lim_{X\to\infty} \frac{\#\{p \in \pi_1(X) \mid \widetilde{A}(\mathbb{F}_p) \text{ is cyclic}\}}{\#\pi_1(X)},$$

for a given Abelian variety A defined over $\mathbb{Q}$. Here $\pi_1(X) = \pi_1(A, X) := \{p \le X \mid A$ has good reduction at a prime $p\}$. We will study this for principally polarized Abelian surfaces defined over $\mathbb{Q}$ to avoid some difficulties that come up when A is higher dimensional.

In the case of elliptic curves E, Serre and Murty studied C_E and obtained the following result by using Hooley's method which is so called simple asymptotic sieve (p. 212 in [8]).

THEOREM 1.1 ([17], [13]). *Let E be an elliptic curve over $\mathbb{Q}$ and p be a rational prime. Let $E[m]$ be the kernel of multiplication by an integer m on E. Assume the generalized Riemann hypothesis (GRH for short). Then,*

$$\{p \le X \mid \widetilde{E}(\mathbb{F}_p) \textit{ is cyclic and } p \textit{ is a good prime}\} \sim C_E \cdot \frac{X}{\log X},$$

where $C_E = \sum_{m:\,squarefree\ge 1} \frac{\mu(m)}{\#\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})}$ *and μ is the Möbius function.*

*The author was supported by the Japan Society for the Promotion of Science Research Fellowships for Young Scientists.

Using Theorem 1.1, we can asymptotically compute the density C_E for a semi-stable elliptic curve E over $\mathbb{Q}$ by Corollary 1 at p. 308 in [15] and Proposition 3.2 in [4]. Gupta obtained a more explicit form for C_E of $E = E_1(a)\colon y^2 = x^3 - ax$ (note $\mathrm{End}(E) = \mathbb{Z}[\sqrt{-1}]$) [6] and Takeuchi did the same for $E = E_2(a)\colon y^2 = x^3 + a$ (note $\mathrm{End}(E) = \mathbb{Z}[\sqrt{-3}]$) [21]. In both cases, the densities are given by the combinatorial formula in the parameter $a \in \mathbb{Z}$. We remark that the assumption of the GRH can be removed if E has complex multiplication ([13] and [3]).

After these works, it is quite natural to expect a similar result for the higher dimensional case and compute the density explicitly. We formulate the following conjecture:

CONJECTURE 1.2. *Let A be a principally polarized Abelian surface defined over $\mathbb{Q}$ and $A[m]$ be the kernel of multiplication by an integer m on A. Assume the GRH. Then,*

$$C_A = \sum_{m:\,squarefree \geq 1} \frac{\mu(m)\,\#T_m}{\#\mathrm{Gal}(\mathbb{Q}(A[m])/\mathbb{Q})},$$

where $T_m = \{\sigma \in \mathrm{Gal}(\mathbb{Q}(A[m])/\mathbb{Q}) \mid \dim_{\mathbb{Z}/\ell\mathbb{Z}}(A[\ell]^\sigma) \geq 2 \ \forall \ell \mid m\}$. Here $A[\ell]^\sigma = \{P \in A[\ell] \mid P^\sigma = P\}$ for a rational prime ℓ. In other words,

$$\#\{p \leq X \mid \widetilde{A}(\mathbb{F}_p) \text{ is cyclic and } p \text{ is a good prime}\} \sim C_A \cdot \frac{X}{\log X}.$$

Then we will prove the following theorem which is the algebraic part in our results.

THEOREM 1.3. *Let ℓ be a rational prime and A be a principally polarized Abelian surface defined over $\mathbb{Q}$. Assume* $\mathrm{End}(A) = \mathbb{Z}$ *and the image of* mod ℓ *Galois representation associated to A is isomorphic to* $\mathrm{GSp}_4(\mathbb{F}_\ell)$ *(see* Section 2*). Then we have*

$$\#T_\ell = \ell^2(2\ell^5 - \ell^4 - \ell^3 - \ell^2 - 3\ell - 1).$$

The above theorem asserts us that a new phenomena appears in the case higher dimension which is greater than one, though it also appears some difficulties by reason of this. We remark that $\#T_m = 1$ for any m in the case elliptic curves.

The following theorem is the analytic part in our results which will be discussed in Section 3.

THEOREM 1.4. *Let A be a principally polarized Abelian surface defined over $\mathbb{Q}$ with* $\mathrm{End}(A) = \mathbb{Z}$. *Assume the GRH and* Conjecture 3.5 *(see p.* 315*), then* Conjecture 1.2 *is true for A.*

The above theorem is easy to prove, since the tools and methods which we apply are already known. Therefore, it is crucial to prove Conjecture 3.5 though it seems to be difficult to do it in the current situation.

This paper is organized as follows. We will study T_ℓ for Abelian surfaces with $\mathrm{End}(A) = \mathbb{Z}$ in Section 2 and give the proof of Theorem 1.3. We will prove

Theorem 1.4 in Section 3. In Section 4, we will give a numerical evidence of Conjecture 1.2 to compute the asymptotical value of C_A for the Jacobian surface of the hyperelliptic curve defined by $y^2 = x^5 - x + 1$.

In this paper, we use the notation $f(x) \ll g(x)$ if there exists a constant $c \geq 0$ such that $f(x) \leq cg(x)$ for any sufficiently large x. For a parameter $X \geq 0$, we denote by $\pi(X)$ the set of rational primes which are less than or equal to X.

2. Computation of T_ℓ

Throughout this section we will assume that $\mathrm{Gal}(\mathbb{Q}(A[\ell])/\mathbb{Q})) \simeq \mathrm{GSp}_4(\mathbb{F}_\ell)$. This assumption is satisfied for all but finitely many ℓ when A is a principally polarized Abelian surface with $\mathrm{End}(A) = \mathbb{Z}$. This well-known fact is a celebrated theorem of Serre (see Theorem 3 in [18]). To compute T_ℓ for an odd prime ℓ, we begin from the following easy exercises in linear algebra.

Let V be a vector space over a field k. Let $f\colon V \times V \to k$ be a non-degenerate, alternating form.

LEMMA 2.1. *Assume* $\mathrm{char}(k) \neq 2$. *Then there exists a basis* $\{u_1, v_1, \ldots, u_n, v_n\}$ *such that* $f(u_i, u_j) = f(v_i, v_j) = 0$ *and* $f(u_i, v_j) = \delta_{ij}$, *where* δ_{ij} *is Kronecker's delta. In particular the dimension of* V *is even.*

Proof. Take a non zero element u_1 in V. Since f is non-degenerate on V, there exists $v_1 \in V$ such that $f(u_1, v_1) = 1$. Since f is an alternating form, u_1 and v_1 are independent over k. Let $W := ku_1 \oplus kv_1$. Clearly, $f|_W$ is non-degenerate on W. Then the following exact sequence splits:

$$0 \to W^\perp \to V \to W^* \to 0,$$

where $W^\perp := \{v \in V \mid f(v, w) = 0 \ (\forall w \in W)\}$, $W^* = \mathrm{Hom}_k(W, k)$ is the dual of W, and the second arrow means that $V \ni v \mapsto f(v, *) \in W^*$. Iterating the same procedure for $W^\perp$, we get the claim. □

Let W be a subspace of V and $W_0 = \mathrm{Ker}(W \ni w \mapsto f(*, w) \in W^*)$. Here W^* means the dual of W.

LEMMA 2.2. *Take the symplectic complement* W_1 *of* W *in* V. *Then there exists a subspace* W_2 *of* V *which satisfies the following conditions*

(a) $\dim(W_0) = \dim(W_2)$,
(b) $f(w_1, w_2) = 0$ *for any* w_1 *in* W_1 *and any* w_2 *in* W_2,
(c) $W \cap W_2 = \{0\}$,
(d) $f|_{W_0 \oplus W_2}$ *is non-degenerate.*

Proof. Let $\dim_k V = n$, $\dim_k W = m$, and $\dim_k W_0 = r$. We denote by $\{v_1, \ldots, v_n\}$ a basis of V such that $\{v_1, \ldots, v_r\}$ is a basis of W_0 and $\{v_{r+1}, \ldots, v_m\}$ is a basis of W_1. Since f is non-degenerate on V, we can take the basis $\{v_1^*, \ldots, v_n^*\}$ which corresponds to the dual basis of V. Let W_2 be the k-vector subspace of V

which is spanned by $\{v_1^*, \dots, v_r^*\}$. Then clearly W_2 satisfies (a) and (b) by choosing a basis of W_1 above.

Let $v \in W_2 \cap W$. Then $f(w_0, v) = 0$ for all $w_0 \in W_0$, since $v \in W$. Then we get $v = 0$, since $v \in W_2$. This asserts (c).

For (d), it follows from that $W_0 \oplus W_2$ has the basis $\{v_1, \dots, v_r, v_1^*, \dots, v_r^*\}$. □

For a subspace $W \subset V$, we define by the degenerate degree $d(W)$ of W the dimension of W_0. Let $S_{r,s} := \{W \subset V \mid \dim(W) = r,\ d(W) = s\}$. Since f is an alternating form, $r - s$ is even, and $r + s \leq \dim(V)$ by Lemma 2.2.

Using above two lemmas, we now compute T_ℓ for any odd prime number ℓ. We assume A has a principal polarization for simplicity. Then the image of mod ℓ Galois representation of ℓ-section points of A can be embedded in $\mathrm{GSp}_4(\mathbb{F}_\ell)$. Namely,

$$\mathrm{Gal}(\mathbb{Q}(A[\ell])/\mathbb{Q}) \hookrightarrow \mathrm{GSp}(A[\ell], e_\ell) \simeq \mathrm{GSp}_4(\mathbb{F}_\ell).$$

Here e_ℓ is the Weil pairing and $\mathrm{GSp}(A[\ell], e_\ell) = \{g \in \mathrm{Aut}(A[\ell]) \mid \exists \chi(g) \in \mathbb{F}_\ell^*\colon e_\ell(gx, gy) = \chi(g) e_\ell(x, y),\ \forall x, y \in A[\ell]\}$. Recall $T_m = \{\sigma \in \mathrm{Gal}(\mathbb{Q}(A[m])/\mathbb{Q}) \mid \dim_{\mathbb{Z}/\ell\mathbb{Z}}(A[\ell]^\sigma) \geq 2\ \forall \ell \mid m\}$ for a squarefree integer $m \geq 1$.

We now prove Theorem 1.2, namely

$$\#T_\ell = \ell^2(2\ell^5 - \ell^4 - \ell^3 - \ell^2 - 3\ell - 1).$$

Assume $\mathrm{Gal}(\mathbb{Q}(A[\ell])/\mathbb{Q}) \simeq \mathrm{GSp}(A[\ell], e_\ell)$. Let $V = A[\ell]$ $(\simeq \mathbb{F}_\ell^{\oplus 4})$ and $f = e_\ell$. Let $S_{r,s} = \{W \subset V \mid \dim(W) = r,\ d(W) = s\}$. Then, $r - s$ is even and $r + s \leq \dim(V) = 4$.

We decompose T_ℓ by using $S_{r,s}$ as follows:

$$T_\ell = \coprod_{(r,s)} \coprod_{W \in S_{r,s}} T_{r,s}(W),$$

where $T_{r,s}(W) = \{g \in \mathrm{Gal}(\mathbb{Q}(A[\ell])/\mathbb{Q}) \mid V^g = W\}$ and (r, s) runs over $\{(2,2), (2,0), (3,1), (4,0)\}$. For any $W, W' \in S_{r,s}$, we can see that $T_{r,s}(W)$ and $T_{r,s}(W')$ are conjugate. So $\#T_{r,s}(W)$ is independent of the choice of W. We define $\#T_{r,s} := \#T_{r,s}(W)$ for some $W \in S_{r,s}$. From this, we have $\#T_\ell = \sum_{(r,s)} \#S_{r,s}\, \#T_{r,s}$.

We take a basis $\langle u_1, v_1, u_2, v_2\rangle$ of V as in Lemma 2.1.

In the case $(r, s) = (2, 2)$. Put $W = \langle u_1, u_2\rangle \in S_{2,2}$. So $g \in T_{2,2}(W)$ if and only if

$$g = \begin{pmatrix} I_2 & B \\ 0 & D \end{pmatrix},$$

where $B, D \in M_2(\mathbb{F}_\ell)$. Since $g \in \mathrm{GSp}(V, f)$, we have

$${}^t\begin{pmatrix} I_2 & B \\ 0 & D \end{pmatrix} \begin{pmatrix} 0 & I_2 \\ -I_2 & 0 \end{pmatrix} \begin{pmatrix} I_2 & B \\ 0 & D \end{pmatrix} = \lambda \begin{pmatrix} 0 & I_2 \\ -I_2 & 0 \end{pmatrix},$$

for some $\lambda \in \mathbb{F}_\ell^*$. Then we get $D = \lambda I_2$, ${}^tB = B$. The number of such g is $\ell^3(\ell-1)$. Furthermore, g fixes some subspace of V of dimension 3 if and only if $\lambda = 1$ and $\det(B) = 0$ (note that ${}^tB = B$). The number of such g is ℓ^2. So $\#T_{2,2} = \ell^3(\ell-1) - \ell^2$.

In the case $(r,s) = (2,0)$, we take $W = \langle u_1, v_1 \rangle \in S_{2,0}$. So $g \in T_{2,0}(W)$ if and only if

$$g = \begin{pmatrix} I_2 & B \\ 0 & D \end{pmatrix},$$

where $B, D \in M_2(\mathbb{F}_\ell)$. Since $g \in \mathrm{GSp}(V,f)$, we have

$${}^t\begin{pmatrix} I_2 & B \\ 0 & D \end{pmatrix}\begin{pmatrix} J & 0 \\ 0 & J \end{pmatrix}\begin{pmatrix} I_2 & B \\ 0 & D \end{pmatrix} = \lambda\begin{pmatrix} J & 0 \\ 0 & J \end{pmatrix}, \quad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

where $B, D \in M_2(\mathbb{F}_\ell)$ and $\lambda \in \mathbb{F}_\ell^*$. From this, we have $\lambda = 1$, $B = 0$, and ${}^tDJD = J$ (i.e. $D \in \mathrm{SL}_2(\mathbb{F}_\ell)$). The number of such g is $\ell(\ell^2-1)$. Furthermore, g fixes some subspace of V of dimension 3 if and only if D fixes some subspace of V of dimension 1. The number of such g is ℓ^2. So $\#T_{2,0} = \ell(\ell^2-1) - \ell^2$.

In the case $(r,s) = (3,1)$, we take $W = \langle u_1, v_1, u_2 \rangle \in S_{3,1}$. So $g \in T_{3,1}(W)$ if and only if

$$g = \begin{pmatrix} I_2 & 0 \\ 0 & D \end{pmatrix}, \quad D = \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_\ell).$$

Since $g \in \mathrm{GSp}(V,f)$, we have

$${}^t\begin{pmatrix} I_2 & 0 \\ 0 & D \end{pmatrix}\begin{pmatrix} J & 0 \\ 0 & J \end{pmatrix}\begin{pmatrix} I_2 & 0 \\ 0 & D \end{pmatrix} = \lambda\begin{pmatrix} J & 0 \\ 0 & J \end{pmatrix},$$

where $\lambda \in \mathbb{F}_\ell^*$. From this, we have $d = 1$. Furthermore, $V^g = V$ if and only if $b = 0$. So $\#T_{3,1} = \ell - 1$.

In the case $(r,s) = (4,0)$. This is the trivial case so that $\#T_{4,0} = 1$.

On the other hand, it is easy to compute $\#S_{r,s}$:

$$\#S_{r,s} = \ell^{4t-2t^2-2ts} \prod_{j=0}^{t-1} \frac{\ell^{4-2j}-1}{\ell^{2t-2j}-1} \prod_{j=0}^{s-1} \frac{\ell^{4-2t-2j}-1}{\ell^{s-j}-1},$$

where $t := \frac{r-s}{2}$ and we set the first (resp. second) product to be 1 if $t = 0$ (resp. if $s = 0$).

Summing up the computations above, we have

$$\begin{aligned} \#T_\ell &= (\ell^3(\ell-1) - \ell^2)S_{2,2} + (\ell^3 - \ell^2 - \ell)S_{2,0} + (\ell-1)S_{3,1} + S_{4,0} \\ &= (\ell^3(\ell-1) - \ell^2)(\ell^3 + \ell^2 + \ell + 1) + (\ell^3 - \ell^2 - \ell)(\ell^4 + \ell^2) \\ &\quad + (\ell-1)(\ell^3 + \ell^2 + \ell + 1) + 1 \\ &= \ell^2(2\ell^5 - \ell^4 - \ell^3 - \ell^2 - 3\ell - 1). \end{aligned}$$

3. Cyclicity of $\widetilde{A}(\mathbb{F}_\ell)$

Let A be a principally polarized Abelian surface defined over $\mathbb{Q}$. In this section, we first give another interpretation of the density C_A. For a squarefree integer m, let $T_m = \{\sigma \in \mathrm{Gal}(\mathbb{Q}(A[m])/\mathbb{Q}) \mid \dim_{\mathbb{Z}/\ell\mathbb{Z}}(A[\ell])^\sigma \geq 2 \ \forall \ell \mid m\}$ and let $S_m(X) := \{p \in \pi_1(X) \mid \mathrm{Frob}_p(\mathbb{Q}(A[\ell])/\mathbb{Q}) \subset T_\ell, \ \forall \ell \neq p, \ \ell \mid m\}$. By Čhebotarev's density theorem, we have

$$\lim_{X\to\infty} \frac{\#S_m(X)}{\#\pi_1(X)} = \frac{\#T_m}{\#\mathrm{Gal}(\mathbb{Q}(A[m])/\mathbb{Q})}.$$

LEMMA 3.1. $S_m(X) = \{p \in \pi_1(X) \mid \widetilde{A}(\mathbb{F}_p) \supset (\mathbb{Z}/\ell\mathbb{Z})^{\oplus 2} \ \forall \ell \neq p, \ \ell \mid m\}$.

Proof. Let $\widetilde{A}$ be the reduction of A at a good prime p and $\ell \neq p$ be a prime. By the proper smooth base change theorem (see [11]), the specialization map $H^1_{\mathrm{et}}(A \times_{\mathbb{Q}} \overline{\mathbb{Q}}, \mathbb{Z}_\ell) \to H^1_{\mathrm{et}}(\widetilde{A} \times_{\mathbb{F}_\ell} \overline{\mathbb{F}}_\ell, \mathbb{Z}_\ell)$ gives a $\mathbb{Z}_\ell$-linear isomorphism and it preserves the action of Frob_p. Since the Tate module $T_\ell(A)$ (resp. $T_\ell(\widetilde{A})$) of A (resp. $\widetilde{A}$) is the dual of $H^1_{\mathrm{et}}(A \times_{\mathbb{Q}} \overline{\mathbb{Q}}, \mathbb{Z}_\ell)$ (resp. $H^1_{\mathrm{et}}(\widetilde{A} \times_{\mathbb{F}_\ell} \overline{\mathbb{F}}_\ell, \mathbb{Z}_\ell)$) as $G_{\mathbb{Q}}$-modules (resp. $G_{\mathbb{F}_\ell}$-modules) (cf. [11]), $A[\ell] = T_\ell(A)/\ell T_\ell(A)$ and $\widetilde{A}[\ell] = T_\ell(\widetilde{A})/\ell T_\ell(\widetilde{A})$ are isomorphic as $\mathbb{F}_\ell$-modules and this isomorphism preserves the action of Frob_p. From this "$\subset$"-part is easy to follow.

For "$\supset$"-part, take p from the right side in the claim, then by the criterion of Néron–Ogg–Shafarevich [20] the lift of Frobenius map is uniquely determined. Then we have the assertion from the same as above. □

We say a finite group M is "cyclic outside p" if its p-primary part is cyclic. Then $\widetilde{A}(\mathbb{F}_p)$ is cyclic outside p if and only if $\widetilde{A}(\mathbb{F}_p) \not\supset (\mathbb{Z}/\ell\mathbb{Z})^{\oplus 2}$ for all primes ℓ different from p. By lemma 3.1, we expect the probabilistic density of $\{p \in \pi_1(X) \mid \widetilde{A}(\mathbb{F}_p)$ is cyclic outside $p\}$ to be $P_A := \prod_\ell \left(1 - \frac{\#T_\ell}{\#\mathrm{Gal}(\mathbb{Q}(A[\ell])/\mathbb{Q})}\right)$ which will be more or less different from C_A by the contribution of the conductor of A (cf. p. 518–520 [4]).

We have to treat the case $l = p$ separately to compute the density. To do this, we compute the density of $U(X) := \{p \in \pi_1(X) \mid \widetilde{A}(\mathbb{F}_p) \supset (\mathbb{Z}/p\mathbb{Z})^{\oplus 2}\}$.

Let $F_p(t) \in \mathbb{Z}[t]$ be the characteristic polynomial of the Frobenius map Frob_p acting on the Tate module $T_\ell(\widetilde{A})$ of $\widetilde{A}$ for some good prime ℓ and α_i, $i = 1, \ldots, 4$ be its roots. By Weil conjecture, $|\alpha_i| = \sqrt{p}$, $i = 1, \ldots, 4$ ([22]). This reads the following:

$$\begin{aligned}
\#\widetilde{A}(\mathbb{F}_p) &= \sum_{i=0}^{4} \mathrm{Trace}(\mathrm{Frob}_p^{-1} \mid H^i_{\mathrm{et}}(\widetilde{A} \times_{\mathbb{F}_\ell} \overline{\mathbb{F}}_\ell, \mathbb{Z}_\ell)) \\
&= \sum_{i=0}^{4} \mathrm{Trace}\left(\mathrm{Frob}_p^{-1} \;\middle|\; \bigwedge^i H^1_{\mathrm{et}}(\widetilde{A} \times_{\mathbb{F}_\ell} \overline{\mathbb{F}}_\ell, \mathbb{Z}_\ell)\right) \\
&= \prod_{i=1}^{4} (1 - \alpha_i) \leq (\sqrt{p} + 1)^4.
\end{aligned}$$

If $\#\widetilde{A}(\mathbb{F}_p) = mp^2$ for some $m \geq 2$, then we have the inequality $p^2 \leq 4p\sqrt{p} + 6p + 4\sqrt{p} + 1$. This inequality does not hold if $p \geq 29$. Therefore we may consider $U_1(X) = \{p \in \pi_1(X) \mid \#\widetilde{A}(\mathbb{F}_p) = p^2\}$ instead of $U(X)$. Take p in $U_1(X)$. Let $F_p(t) = t^4 - a_1t^3 + a_2t^2 - pa_1t + p^2$ be the characteristic polynomial of Frob_p. Since $p^2 = F_p(1)$, we have $|a_1| \leq \frac{|a_2|+1}{p+1} \leq \frac{6p+1}{p+1} \leq 6$. Then $\mathrm{Trace}(\mathrm{Frob}_p) = a_1 \in \{0, \pm1, \pm2, \pm3, \pm4, \pm5, \pm6\}$.

LEMMA 3.2. *Assume* $\mathrm{End}(A) = \mathbb{Z}$. *Then* $\lim_{X\to\infty} \frac{\#U_1(X)}{\#\pi_1(X)} = \lim_{X\to\infty} \frac{\#U(X)}{\#\pi_1(X)} = 0$.

Proof. From Theorem 3 in [18], the image of the ℓ-adic representation ρ_ℓ associated to the ℓ-adic Tate module $T_\ell(A)$ is open in $\mathrm{GSp}(T_\ell, e_\ell) \simeq \mathrm{GSp}_4(\mathbb{Z}_\ell)$ for a sufficiently large ℓ. Since $U_1(X) \subset \bigcup_{i=-6}^{6}\{p \in \pi_1(X) \mid \mathrm{Trace}(\mathrm{Frob}_p) = i\}$, $\rho_\ell(\mathrm{Frob}_p)$ is lying on a finite union of some hyperplanes in $\mathrm{GSp}(T_\ell, e_\ell) \simeq \mathrm{GSp}_4(\mathbb{Z}_\ell)$. Since the Haar measure of hyperplanes in $\mathrm{GSp}_4(\mathbb{Z}_\ell)$ is zero (cf. Chapter 1 in [14]), the assertion follows from this. □

LEMMA 3.3 ([16]). *Let $K/\mathbb{Q}$ be a finite Galois extension which is ramified only at the primes $p_1, \ldots, p_m$, then*

$$\frac{1}{[K:\mathbb{Q}]}\log|d_K| \leq \log[K:\mathbb{Q}] + \sum_{j=1}^{m}\log p_j,$$

where d_K is the discriminant of $K/\mathbb{Q}$.

PROPOSITION 3.4 ([9], [16]). *Let $K/\mathbb{Q}$ be a Galois extension of degree n and $C \subset \mathrm{Gal}(K/\mathbb{Q})$ be closed under conjugation. Assume the GRH. Then,*

$$\#\pi_C(X) = \frac{\#C}{n}\cdot\#\pi(x) + O\left(\frac{\#C}{n}X^{1/2}(\log d_K + n\log X)\right),$$

where $\pi_C(X) = \{p \leq X \mid p$: unramified in K and $\mathrm{Frob}_p(K/\mathbb{Q}) \subset C\}$.

We claim the following under the GRH and Conjecture 3.5 below: if $\mathrm{End}(A) = \mathbb{Z}$, then

$$C_A = \lim_{X\to\infty}\frac{\#\{p \in \pi_1(X) \mid \widetilde{A}(\mathbb{F}_p) \text{ is cyclic outside } p\}}{\#\pi_1(X)}.$$

To see this we apply Hooley's method. Let $f(A, X) := \#\{p \in \pi_1(X) \mid \widetilde{A}(\mathbb{F}_p)$ is cyclic outside $p\}$ for a principally polarized Abelian surface with $\mathrm{End}(A) = \mathbb{Z}$. If $\widetilde{A}(\mathbb{F}_p) \supset (\mathbb{Z}/\ell\mathbb{Z})^{\oplus 2}$ for a good prime p of A, then we have $\ell^2 \leq (\sqrt{p}+1)^4$ by the Weil bound. So $p \leq X$ leads $\ell \leq 3X$. Let

$$N(X, Y) = \#\{p \in \pi_1(X) \mid \widetilde{A}(\mathbb{F}_p) \not\supset (\mathbb{Z}/\ell\mathbb{Z})^{\oplus 2}, \forall \ell \leq Y,\ \neq p\},$$

and

$$M(X, Y) = \#\{p \in \pi_1(X) \mid \widetilde{A}(\mathbb{F}_p) \supset (\mathbb{Z}/\ell\mathbb{Z})^{\oplus 2}, \text{ for some } \ell \neq p, \text{ s.t. } Y \leq \ell \leq 3X\}.$$

Here Y is a parameter depending on X, to be chosen later. Then we have

$$N(X,Y) - M(X,Y) \le f(A,X) \le N(X,Y).$$

First, we estimate $N(X,Y)$. By the inclusion-exclusion principle,

$$N(X,Y) = \sum_m{}' \mu(m)\, \#S_m(X),$$

where the summation is over all squarefree integers m all of whose prime factors are less than or equal to Y. We set $S_1(X) = \pi_1(X)$ if $m = 1$. Applying Proposition 3.4 for $G = G_m := \mathrm{Gal}(\mathbb{Q}(A[m])/\mathbb{Q})$ and $C = T_m$, we have the following under the GRH:

$$S_m(X) = \frac{\#T_m}{\#G_m} \cdot \#\pi(X) + O\bigg(\frac{\#T_m}{\#G_m} X^{1/2}(\log|d_m| + \#G_m \log X)\bigg),$$

where d_m is the discriminant of $\mathbb{Q}(A[m])$. Therefore,

$$N(X,Y) = \sum_m{}' \mu(m)\frac{\#T_m}{\#G_m} \cdot \#\pi(X) + O\bigg(\sum_m{}' \frac{\#T_m}{\#G_m} X^{\frac{1}{2}}(\log d_m + \#G_m \log X)\bigg).$$

Using Lemma 3.3, we have

$$\frac{1}{\#G_m}\log d_m \le \log \#G_m + \log(Nm) \ll \log m,$$

where N is the conductor of A. Then

$$O\bigg(\sum_m{}' \frac{\#T_m}{\#G_m} X^{1/2}(\log d_m + \#G_m \log X)\bigg) = O\bigg(\sum_m{}' (\log m)\ \#T_m X^{1/2} \log X\bigg).$$

Let us observe that $m \le \prod_{\substack{p\mid m\\ p\le Y}} p \le e^{2Y}$. By Theorem 3 in [18] and Theorem 1.2, it is easy to see that

$$\bigg|\sum_m{}' (\log m)\ \#T_m\bigg| \ll \sum_{1\le m\le e^{2Y}} m^8 \ll (e^{2Y})^9 = e^{18Y},$$

since $T_m \subset \prod_{\ell\mid m} T_\ell$. Now we chose Y to be $\frac{1}{18}\log X^\delta$ for a positive constant $\delta < \frac{1}{2}$. Then we have

$$N\bigg(X, \frac{1}{18}\log X^\delta\bigg) = \sum_m{}' \mu(m)\frac{\#T_m}{\#G_m} \cdot \#\pi(X) + o\bigg(\frac{X}{\log X}\bigg),$$

for sufficiently large X.

We remain to estimate $M(X,Y)$ for $Y = \frac{1}{18}\log X^\delta$. We are hopeful that $M\big(X, \frac{1}{18}\log X^\delta\big) = o\big(\frac{X}{\log X}\big)$ to prove Conjecture 1.2. However it seems to be difficult to prove it with the current tools in analytic number theory or algebraic number theory. We set up the following conjecture which we expect to be true from the (naive) numerical evidence in Section 4.

CONJECTURE 3.5. *The notations being as above. Then* $M\big(X, \frac{1}{18}\log X^\delta\big) = o\big(\frac{X}{\log X}\big)$.

The estimation for $N(X,Y)$ and Conjecture 3.5 give us

$$f(A,X) = {\sum_m}' \mu(m)\frac{\#T_m}{\#G_m}\cdot \#\pi(X) + o\left(\frac{X}{\log X}\right),$$

under the GRH. Then we have

$$\begin{aligned}\lim_{X\to\infty}\frac{\#\{p\in\pi_1(X)\mid \widetilde{A}(\mathbb{F}_p) \text{ is cyclic outside } p\}}{\#\pi_1(X)} &= \lim_{X\to\infty}\frac{f(A,X)}{\#\pi(X)}\\ &= {\sum_m}' \mu(m)\frac{\#T_m}{\#G_m}.\end{aligned}$$

REMARK 3.6.

(a) A naive estimation gives us that

$$\begin{aligned}M\left(X, \frac{1}{18}\log X^\delta\right) &\le \sum_{\frac{1}{18}\log X^\delta\le \ell\le 3X} \#S_\ell(X)\\ &= \sum_{\frac{1}{18}\log X^\delta\le \ell\le 3X}\frac{\#T_\ell}{\#G_\ell}\cdot\#\pi(X) + O(X^{\frac{17}{2}}).\end{aligned}$$

(b) In the proofs of Theorem 1.1, Serre and Murty make use of the fact that the division fields $\mathbb{Q}(E[\ell])$ (here ℓ is a prime) contain cyclotomic fields, and thus a prime p splitting completely in $\mathbb{Q}(E[\ell])$ satisfies the congruence condition $p\equiv 1 \pmod{\ell}$. As such, they can invoke the Brun–Titchmarch Theorem to estimate $M(X,Y)$. In current situation of an Abelian surface, this argument can not be invoked because the invariant $\#T_\ell$ becomes large with order ℓ^7 when ℓ is large (see Theorem 1.2). Contrary to this situation, $\#T_\ell = 1$ for any ℓ if A is an elliptic curve.

Proof of Theorem 1.4. By Lemma 3.2 and the observations above,

$$\begin{aligned}{\sum_m}' \mu(m)\frac{\#T_m}{\#G_m} &= \lim_{X\to\infty}\frac{\#\{p\in\pi_1(X)\mid \widetilde{A}(\mathbb{F}_p) \text{ is cyclic outside } p\}}{\#\pi_1(X)}\\ &= \lim_{X\to\infty}\frac{\#\{p\in\pi_1(X)\mid \widetilde{A}(\mathbb{F}_p) \text{ is cyclic}\}}{\#\pi_1(X)} + \lim_{X\to\infty}\frac{\#U(X)}{\#\pi_1(X)}\\ &= C_A.\end{aligned}$$

□

4. Numerical evidence

In this section, we compute the asymptotic values of C_A for some Jacobian surface A and compare this value with the probabilistic density P_A. In general, T_m is not multiplicative function for m and then C_A does not coincide with P_A. However, we expect these two values become close, since P_A is an interpretation of C_A in the probabilistic point of view.

We consider an algebraic curve $C\colon y^2 = x^5 - x + 1$ with $\mathrm{End}(J(C)) = \mathbb{Z}$. Let $A = J(C)$.

We first compute the value of the probabilistic density P_A (see p. 312). The following result is known by L. Dieulefait.

THEOREM 4.1 (see p. 509 in [5]). *Assume the Serre's conjecture (*3.2.4$_?$ [19]*). Then*

$$\mathrm{Gal}(\mathbb{Q}(J(C)[\ell]))/\mathbb{Q} \simeq \mathrm{GSp}_4(\mathbb{F}_\ell),$$

for $\ell \geq 3$.

LEMMA 4.2. *The notations are as above. Then* $\#T_2 = 46$.

Proof. Let $P_i = (\alpha_i, 0)$, $i = 1, 2, 3, 4, 5$ where α_i is a root of $x^5 - x + 1$ and let $D_i = P_i - \infty \in J(C)$, where ∞ is the infinite point on C. Then $J(C)[2] = \bigoplus_{i=1}^4 \mathbb{F}_2 D_i$ (cf. Section 5 in [12]) and $D_1 + D_2 + D_3 + D_4 = D_5$, since the divisor of y is $\left(\sum_{i=1}^5 P_i\right) - 5\infty$. Using this, we have the Galois representation

$$\rho\colon \mathrm{Gal}(\mathbb{Q}_f/\mathbb{Q}) \to GL_4(\mathbb{F}_2),$$

where $\mathbb{Q}_f$ is the decomposition field of $f(x) = x^5 - x + 1$ (note that $\mathbb{Q}_f = \mathbb{Q}(J(C)[2])$). For $\sigma \in \mathrm{Gal}(\mathbb{Q}_f/\mathbb{Q})$, $\sigma \in T_2$ if and only if the rank of the matrix $\rho(\sigma) - I_4$ is less than or equal to 2.

We know $\mathrm{Gal}(\mathbb{Q}_f/\mathbb{Q}) = \mathfrak{S}_5$ by using Pari-gp calculator [1]. To compute T_2, we have only to consider the conjugacy classes of $\mathfrak{S}_5$.

Let $\{(1), (12), (123), (1234), (12345), (12)(34), (12)(345)\}$ be the complete set of conjugacy classes of $\mathfrak{S}_5$. Clearly, $(1) \in T_2$. Let $\{e_i\}_{i=1}^4$ be the canonical basis of $\mathbb{F}_2^{\oplus 4}$. For $\sigma = (12)$, the number of elements of $\mathfrak{S}_5$ conjugate to σ is equal to 10 and we have

$$\rho(\sigma) = (e_2, e_1, e_3, e_4).$$

From the criterion above, $\sigma \in T_2$.

For $\sigma = (123)$, the number of elements of $\mathfrak{S}_5$ conjugate to σ is equal to 20 and we have

$$\rho(\sigma) = (e_3, e_1, e_2, e_4).$$

From the criterion above, $\sigma \in T_2$.

For $\sigma = (1234)$, the number of elements of $\mathfrak{S}_5$ conjugate to σ is equal to 30 and we have

$$\rho(\sigma) = (e_4, e_1, e_2, e_3).$$

From the criterion above, $\sigma \notin T_2$.

For $\sigma = (12345)$, the number of elements of $\mathfrak{S}_5$ conjugate to σ is equal to 24 and we have

$$\rho(\sigma) = (e_4, e_1 + e_4, e_2 + e_4, e_3 + e_4).$$

Here we use the relation $D_1+D_2+D_3+D_4 = D_5$. From the criterion above, $\sigma \notin T_2$.

For $\sigma = (12)(34)$, the number of elements of $\mathfrak{S}_5$ conjugate to σ is equal to 15 and we have

$$\rho(\sigma) = (e_2, e_1, e_4, e_3).$$

From the criterion above, $\sigma \in T_2$.

For $\sigma = (12)(345)$, the number of elements of $\mathfrak{S}_5$ conjugate to σ is equal to 20 and we have

$$\rho(\sigma) = (e_2 + e_4, e_1 + e_4, e_4, e_3 + e_4).$$

Here we use the relation $D_1+D_2+D_3+D_4 = D_5$. From the criterion above, $\sigma \notin T_2$.

From the computations above, we have $\#T_2 = 1 + 10 + 20 + 15 = 46$. □

From Theorem 4.1 and Theorem 1.2, we have

$$P_A = \left(1 - \frac{46}{5!}\right) \prod_{\ell \geq 3} \left(1 - \frac{\ell^2(2\ell^5 - \ell^4 - \ell^3 - \ell^2 - 3\ell - 1)}{\ell^4(\ell - 1)(\ell^2 - 1)(\ell^4 - 1)}\right) = 0.5945\cdots.$$

So we would like to expect that the density

$$C_A = \lim_{X \to \infty} \frac{\#\{p \in \pi_1(X) \mid \widetilde{A}(\mathbb{F}_p) \text{ is cyclic}\}}{\#\pi_1(X)}$$

Table 1. The cyclicity of $\widetilde{J(C)}(\mathbb{F}_p)$

X	$\#\pi_1(X)$	cyclic	Density
1000	163	91	$0.5582\cdots$
2000	298	176	$0.5906\cdots$
3000	425	258	$0.6070\cdots$
4000	544	318	$0.5845\cdots$
5000	663	393	$0.5927\cdots$
6000	777	453	$0.5830\cdots$
7000	894	524	$0.5861\cdots$
8000	1001	578	$0.5774\cdots$

Here we exclude $p = 2, 3, 5$.

is close to P_A. To support this, we calculate $\frac{\#\{p\in\pi_1(X)|\widetilde{A}(\mathbb{F}_p) \text{ is cyclic}\}}{\#\pi_1(X)}$ by 1000 units as $X = 1000, 2000, \ldots, 8000$.

Here "cyclic" in the third column in Table 1 means the number of primes p such that $\widetilde{J(C)}(\mathbb{F}_p)$ is cyclic. We hope that Density above become close to C_A and also P_A.

Acknowledgments. The author expresses sincere thanks to F. Sairaiji for his many valuable comments and warm encouragement during the preparation of his paper. N. Kanayama made the table in Section 4. The author also thanks him for this.

References

[1] H. Cohen et al., available at `http://www.math.u-bordeaux.fr/~belabas/pari/`.
[2] A. Cojocaru, On the cyclicity of the group of $\mathbb{F}_p$-rational points of non-CM elliptic curves. J. Number Theory, **96** (2002), 335–350.
[3] A. Cojocaru, Cyclicity of CM elliptic curves modulo p. Trans. AMS, **355** (2003), 2651–2662.
[4] A. Cojocaru and W. Duke, Reductions of an elliptic curve and their Tate-Shafarevich groups. Math. ann., **329** (2004), 513–534.
[5] L.-V. Dieulefait, Explicit determination of the images of the Galois representations attached to Abelian surfaces with $\mathrm{End}(A) = \mathbb{Z}$. Experiment. Math., **11** (2002), 503–512.
[6] R. Gupta, Division fields of $Y^2 = X^3 - aX$. J. Number Theory, **34** (1990), 335–345.
[7] R. Gupta and R. Murty, Cyclicity and generation of points mod p on elliptic curves. Invent. math., **101** (1990), 225–235.
[8] C. Hooley, On Artin's conjecture. J. Reine Angew. Math., **225** (1967), 209–220.
[9] J.C. Lagarias and A.M. Odlyzko, Effective versions of the Chebotarev density theorem. Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), Academic Press, London, 1977, 409–464.
[10] J.S. Milne, Etale cohomology. Princeton Mathematical Series, **33**, Princeton University Press, Princeton, N. J., 1980.
[11] J.S. Milne, Abelian varieties. Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, 103–150.
[12] K. Murty, The addition law on hyperelliptic Jacobians. Currents trends in number theory (Allahabad, 2000), Hindustan Book Agency, New Delhi, 2002, 101–110.
[13] R. Murty, On Artin's conjecture. J. Number Theory, **16** (1983), 147–168.
[14] J.-P. Serre, Abelian l-adic representations and elliptic curves. McGill University lecture notes written with the collaboration of Willem Kuyk and John Labute, W. A. Benjamin Inc., New York–Amsterdam, 1968.
[15] J.-P. Serre, Proprietes galoisiennes des points d'ordre fini des courbes elliptiques. Invent. Math., **15** (1972), 259–331.
[16] J.-P. Serre, Chebotarev, Quelques applications du théorème de densité de Chebotarev. Publications Mathematiques de l'IHES, **54** (1981), 123–201.
[17] J.-P. Serre, Résumé des cours de 1977–1978. Collected papers, **III**, 465–468.
[18] J.-P. Serre, Résumé des cours de 1984–1985. Collected papers, **IV**, 33–37.
[19] J.-P. Serre, Sur les representations modulaires de degre 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Duke Math. J., **54** (1987), 179–230.
[20] J.-P. Serre and J. Tate, Good reduction of Abelian varieties. Ann. of Math., **88** (1968), 492–517.
[21] R. Takeuchi, On distribution of the group of rational points of reductions of an elliptic curve. Mathematical software (Beijing, 2002), World Sci. Publishing, River Edge, NJ, 2002, 271–280.
[22] A. Weil, Varietes abeliennes et courbes algebriques. Hermann and Cie., Paris, 1948.