MATHEMATICS OF COMPUTATION
Volume 68, Number 228, Pages 1649–1662
S 0025-5718(99)01061-3
Article electronically published on February 19, 1999

ON THE SATO-TATE CONJECTURE FOR QM-CURVES OF GENUS TWO

KI-ICHIRO HASHIMOTO AND HIROSHI TSUNOGAI

ABSTRACT. An abelian surface A is called a QM-abelian surface if its endomorphism ring includes an order of an indefinite quaternion algebra, and a curve C of genus two is called a QM-curve if its jacobian variety is a QM-abelian surface. We give a computational result about the distribution of the arguments of the eigenvalues of the Frobenius endomorphisms of QM-abelian surfaces modulo good primes, which supports an analogue of the Sato-Tate Conjecture for such abelian surfaces. We also make some remarks on the field of definition of QM-curves and their endomorphisms.

0. INTRODUCTION

In this article we report a computational result about the distribution of the arguments of zeroes of congruence ζ-functions of two-dimensional abelian varieties with quaternionic multiplication (QM) modulo good primes. Our result supports an analogue of the Sato-Tate Conjecture for such abelian surfaces.

An abelian surface A is called a *QM-abelian surface* if it has quaternionic multiplication, that is, there exists an order $\mathcal{O}$ of an indefinite quaternion algebra $\boldsymbol{B}$ over $\boldsymbol{Q}$ and an embedding $\iota : \mathcal{O} \hookrightarrow \operatorname{End} A$. A curve C of genus two is called a *QM-curve* if its Jacobian variety is a QM-abelian surface.

In [HM] N. Murabayashi and one of the authors obtained algebraic families of QM-curves explicitly when the discriminants of $\boldsymbol{B}$ are 6 and 10. In the case of discriminant 6, the following equations give a family of QM-curves:

$$\mathcal{S}_6(t,s) : Y^2 = X(X^4 + (A-B)X^3 + QX^2 + (A+B)X + 1), \tag{0.1}$$
$$A = \frac{s}{2t}, \quad B = \frac{1+3t^2}{1-3t^2},$$
$$Q = -\frac{(1-2t^2+9t^4)(1-28t^2+166t^4-252t^6+81t^8)}{4t^2(1-3t^2)^2(1-t^2)(1-9t^2)},$$

$$S_{\boldsymbol{B}_6} : g(t,s) = s^2 + 3 - 14t^2 + 27t^4 = 0. \tag{0.2}$$

(This is slightly modified from the form in [HM]. We have obtained another family which has different arithmetic properties. See §4.) By specializing (t,s) to points $(t_0, s_0) \in S_{\boldsymbol{B}_6}(\bar{\boldsymbol{Q}})$, we can obtain a lot of examples of QM-curves defined over number fields.

For many examples of QM-curves, we calculated the congruence ζ-functions of their reductions modulo $\mathfrak{p}$ and studied the distribution of the argument of the roots

Received by the editor August 22, 1995 and, in revised form, January 22, 1998.
1991 *Mathematics Subject Classification.* Primary 11G40; Secondary 11G15, 14H10, 14K15.
Key words and phrases. Quaternionic multiplication, L-functions.

©1999 American Mathematical Society

α, β of the characteristic polynomial of the Frobenius endomorphisms. For a curve C of genus two defined over a number field k, the congruence ζ-function of C mod $\mathfrak{p}$ for a good prime $\mathfrak{p}$ of k can be written in the form

$$Z(u) = \frac{(1-\alpha u)(1-\bar{\alpha} u)(1-\beta u)(1-\bar{\beta} u)}{(1-u)(1-qu)}, \tag{0.3}$$

where $\bar{\ }$ denotes the complex conjugate, the absolute values of α, β are $\sqrt{q}$, and $q = N\mathfrak{p}$, the absolute norm of $\mathfrak{p}$. In our case of QM-curves, if all endomorphisms of Jac$C$ are defined over k, we have $\alpha = \beta$. Put $\alpha = \sqrt{q}e^{\sqrt{-1}\theta_\mathfrak{p}}$ with $\theta_\mathfrak{p} \in [0, \pi]$. On the distribution of $\{\theta_\mathfrak{p}\}$ there is a conjecture which is an analogue of the Sato-Tate Conjecture for elliptic curves. Let us explain it.

The original *Sato-Tate Conjecture* is as follows. Let E be an elliptic curve defined over a number field k. For a good prime $\mathfrak{p}$ of k, the congruence ζ-function of E mod $\mathfrak{p}$ is in the form

$$Z(u) = \frac{(1-\sqrt{q}e^{\sqrt{-1}\theta_\mathfrak{p}}u)(1-\sqrt{q}e^{-\sqrt{-1}\theta_\mathfrak{p}}u)}{(1-u)(1-qu)}, \tag{0.4}$$

where $\theta_\mathfrak{p} \in [0, \pi]$. M. Sato conjectured that if E has no complex multiplication the arguments $\{\pm\theta_\mathfrak{p}\}$ would be distributed in proportion to $\sin^2\theta$. Also J. Tate arrived at this conjecture; see [T].

H. Yoshida [Yo1] generalized the above conjecture for higher-dimensional abelian varieties A. He conjectured that the distribution of the arguments is characterized by the image of the Galois group under the l-adic representation (more precisely, the Mumford-Tate group) of A. By Faltings' theorem [F], or earlier work of Ohta [O], for a QM-abelian surface A defined over a number field k, the image of the l-adic representation associated to A is a subgroup of $\mathrm{GSp}(4, \boldsymbol{Z}_l)$ isomorphic to an open subgroup of $\mathrm{GL}(2, \boldsymbol{Z}_l)$ if l does not divide the discriminant of $\boldsymbol{B}$ over $\boldsymbol{Q}$. This suggests the following conjecture for the case of QM-abelian surfaces:

Conjecture 0.5. *Let A be a QM-abelian surface defined over a number field k. Assume also that all endomorphisms of A are defined over k. For a good prime $\mathfrak{p}$ of k, let $\pm\theta_\mathfrak{p}$ be the arguments of the eigenvalues of the Frobenius endomorphisms of A mod $\mathfrak{p}$. Then $\{\pm\theta_\mathfrak{p}\}$ would be distributed in proportion to* $\sin^2\theta$.

Y. Yamamoto reported in [Ya] a result of computation which fits with the generarized conjecture for abelian surfaces A with End$A \simeq \boldsymbol{Z}$.

Yoshida [Yo2] proved an analogue of these conjectures for the cases of elliptic curves and QM-abelian surfaces over a function field over a finite field.

If C is a QM-curve, then $A = \mathrm{Jac}C$ is a QM-abelian surface, and the eigenvalues of Frobenius endomorphisms of A mod $\mathfrak{p}$ coincide with the zeroes of the congruence ζ-function of C mod $\mathfrak{p}$. Hence we can examine the conjecture by calculating the congruence ζ-function of C mod $\mathfrak{p}$. We calculated them for more than twenty curves C and for primes $\mathfrak{p}$ with $N\mathfrak{p} < 2^{20}$, and obtained results which support the conjecture.

We carried out these calculations on a PC with UBASIC and on a UNIX Work Station with GNU C. We thank volunteer helpers in the computer room of our department and the staff of the Centre for Informatics, Waseda University. Especially we would like to express our sincere gratitude to Kazumaro Aoki for useful suggestions for improving the algorithm.

1. Congruence ζ-functions

First we recall some basic facts about congruence ζ-functions. For a curve C over $\boldsymbol{F}_q$, let N_m denote the number of $\boldsymbol{F}_{q^m}$-rational points on C. The *congruence ζ-function* of C is defined to be

$$Z(C/\boldsymbol{F}_q;u) = \exp\left(\sum_{m=1}^{\infty} \frac{N_m}{m} u^m\right). \tag{1.1}$$

Let C be a complete, non-singular curve of genus two. Then, by the Weil conjecture, we have

$$Z(C/\boldsymbol{F}_q;u) = \frac{P(u)}{(1-u)(1-qu)}, \tag{1.2}$$

where $P(u) \in \boldsymbol{Z}[u]$ is of degree 4, and $P(u) = (1-\alpha u)(1-\bar{\alpha}u)(1-\beta u)(1-\bar{\beta}u)$ with $|\alpha| = |\beta| = \sqrt{q}$. Putting $\alpha + \bar{\alpha} = a$ and $\beta + \bar{\beta} = b$, we can write

$$P(u) = (1 - au + qu^2)(1 - bu + qu^2) \tag{1.3}$$

with $a, b \in \boldsymbol{R}$ and $|a|, |b| \leq 2\sqrt{q}$. By (1.1) and (1.3), a and b are evaluated from

$$\begin{aligned} a + b &= 1 + q - N_1, \\ ab &= -q - (1+q)N_1 + \frac{1}{2}(N_2 + N_1^2). \end{aligned} \tag{1.4}$$

Let $J = \mathrm{Jac}C$ be the Jacobian variety of C over $\boldsymbol{F}_q$, l a prime different from the characteristic of $\boldsymbol{F}_q$, and ρ_l the l-adic representation

$$\rho_l : \mathrm{Gal}(\bar{\boldsymbol{F}}_q/\boldsymbol{F}_q) \longrightarrow \mathrm{GSp}(4, \boldsymbol{Z}_l). \tag{1.5}$$

Then, for a Frobenius element σ, the characteristic polynomial of $\rho_l(\sigma)$ does not depend on l and coincides with $P(u)$.

Let C be a QM-curve over a number field k, $J = \mathrm{Jac}C$ its Jacobian variety, and $\mathcal{O}$ an order of an indefinite quaternion algebra $\boldsymbol{B}$ over $\boldsymbol{Q}$ identified with $\mathrm{End}J$. Take a good prime $\mathfrak{p}$ of k and let p be its residue characteristic and $N\mathfrak{p} = q$. For a prime number l different from p, we denote the associated completion of $\mathcal{O}$ (resp. $\boldsymbol{B}$) by $\mathcal{O}_l$ (resp. $\boldsymbol{B}_l$). Then we have $\mathrm{End}T_lJ \otimes_{\boldsymbol{Z}_l} \boldsymbol{Q}_l \simeq \mathrm{M}_4(\boldsymbol{Q}_l)$. Let k' be an extension of k over which all endomorphisms of J are defined. It is known [R, P] that k' can be chosen as a $(2, \dots, 2)$-extention of k. First, consider the l-adic representation ρ_l of $\mathrm{Gal}(\bar{\boldsymbol{Q}}/k')$ attached to J:

$$\rho_l : \mathrm{Gal}(\bar{\boldsymbol{Q}}/k') \longrightarrow \mathrm{GSp}(4, \boldsymbol{Z}_l) \subset \mathrm{M}_4(\boldsymbol{Q}_l). \tag{1.6}$$

Denote by $\mathrm{End}_{\mathrm{Gal}(\bar{k}/k')}T_lJ$ the centralizer of $\mathrm{Im}\rho_l$ in $\mathrm{End}T_lJ$. Then, by Faltings [F], $\mathrm{End}_{\mathrm{Gal}(\bar{k}/k)}T_lJ \otimes_{\boldsymbol{Z}_l} \boldsymbol{Q}_l \simeq \mathrm{End}_{k'}J \otimes \boldsymbol{Q}_l = \boldsymbol{B}_l$. Hence $\mathrm{Im}\rho_l$ is contained in the centralizer of $\boldsymbol{B}_l$ in $\mathrm{M}_4(\boldsymbol{Q}_l)$, which is isomorphic to the opposite algebra $\boldsymbol{B}_l^0$ of $\boldsymbol{B}_l$. For a prime $\mathfrak{P}$ of k' above $\mathfrak{p}$, let $\sigma_{\mathfrak{P}}$ be the Frobenius element. Since $\rho_l(\sigma_{\mathfrak{P}})$ belongs to $\boldsymbol{B}_l^0$, it satisfies a quadratic relation of the form

$$1 - c_{\mathfrak{P}}X + (N\mathfrak{P})X^2 = 0. \tag{1.7}$$

Now consider ρ_l on $\mathrm{Gal}(\bar{\boldsymbol{Q}}/k)$. Let $f = f(\mathfrak{P}/\mathfrak{p})$ be the inertia degree of $\mathfrak{P}$ in k'/k. Then $f = 1$ or 2, and $\rho_l(\sigma_{\mathfrak{p}})$ satisfies

$$1 - c_{\mathfrak{P}}X^f + (qX^2)^f = 0 \tag{1.8}$$

since $\sigma_{\mathfrak{P}} = \sigma_{\mathfrak{p}}^f$. On the other hand, since $\rho_l(\sigma_{\mathfrak{p}})$ belongs to $\mathrm{M}_4(\boldsymbol{Q}_l)$, it satisfies a quartic relation. We can distinguish between the cases $f = 1$ and 2 by the values N_1 and N_2. If $f = 1$, then the characteristic polynomial of $\rho_l(\sigma_{\mathfrak{p}})$ is

$$(1 - c_{\mathfrak{P}}X + qX^2)^2 = (1 - a_{\mathfrak{p}}X + qX^2)^2$$

with $a_{\mathfrak{p}} = c_{\mathfrak{P}}$. By (1.4), we have

$$(1.9) \qquad (1 + q - N_1)^2 = 2(1 + 4q + q^2 - N_2), \quad a_{\mathfrak{p}} = \frac{1}{2}(1 + q - N_1).$$

If $f = 2$, then the characteristic polynomial of $\rho_l(\sigma_{\mathfrak{p}})$ is

$$1 - c_{\mathfrak{P}}X^2 + q^2X^4 = (1 - a_{\mathfrak{p}}X + qX^2)(1 + a_{\mathfrak{p}}X + qX^2)$$

with $a_{\mathfrak{p}}^2 = c_{\mathfrak{P}} + 2q$. By (1.4), we have

$$(1.10) \qquad N_1 = 1 + q, \quad a_{\mathfrak{p}}^2 = \frac{1}{2}(1 + 4q + q^2 - N_2).$$

Now one of the remarkable properties for our family $\mathcal{S}_6$ given in (0.1) is that for any curve $C_{(t_0,s_0)}$ obtained by specializing at (t, s) with $t \in \boldsymbol{Q}$, which is defined over a quadratic field $k = \boldsymbol{Q}(s) = \boldsymbol{Q}(\sqrt{-3 + 14t^2 - 27t^4})$, (numerically) we always have $f = 1$. This shows that, very probably, all endomorphisms of Jac$C$ are defined over k, because if almost all primes of a number fields k are decomposed completely in an extention k'/k then $k' = k$. Based on this assumption, for many primes, we calculated only N_1 to obtain results in reasonable time.

2. Density functions

Let $\Theta = \{\theta_j\}_{j=1}^{\infty}$ be a sequence in the unit circle $T = \boldsymbol{R}/2\pi\boldsymbol{Z}$. A real valued distribution $\Phi = \Phi(\theta)$ on T is called the *density function* of Θ if it has the following property:

For any open interval U of T and any natural number m, let

$$(2.1) \qquad n(U, m) = \#\{j \in \mathbf{N} \mid \theta_j \in U, j < m\}.$$

Then

$$(2.2) \qquad \lim_{m\to\infty} \frac{n(U, m)}{m} = \int_U \Phi(\theta)d\theta,$$

where $d\theta$ denotes the measure on T induced from the Lebesgue measure on $\boldsymbol{R}$.

The next lemma is basic (see, e.g. [Yo2]).

Lemma 2.3. *For a sequence $\Theta = \{\theta_j\}_{j=1}^{\infty}$ on T, assume that the limit*

$$c_k := \lim_{m\to\infty} \frac{1}{2\pi m} \sum_{j=1}^{m} e^{-\sqrt{-1}k\theta_j}$$

exists for all $k \in \boldsymbol{Z}$. Then the series

$$\Phi(\theta) := \sum_{k=-\infty}^{\infty} c_k e^{\sqrt{-1}k\theta}$$

converges in the sense of distributions and is the density function of Θ.

Let E be an elliptic curve defined over a number field k. For a good prime $\mathfrak{p}$ of k, let $\pm\theta_{\mathfrak{p}}$ be the arguments of zeroes of the congruence ζ-function for E mod $\mathfrak{p}$ (see (0.4)). Since we should consider the distribution of a sequence of pairs $\Theta = \{\pm\theta_{\mathfrak{p}}\}_{\mathfrak{p}}$, we define the density function of Θ as a distribution satisfying

$$\lim_{x\to\infty} \frac{\#\{\mathfrak{p} \mid \theta_{\mathfrak{p}} \in U, N\mathfrak{p} < x\}}{\#\{\mathfrak{p} \mid N\mathfrak{p} < x\}} = \int_U \Phi(\theta)d\theta \tag{2.4}$$

for any open interval $U \subset [0,\pi]$. The original Sato-Tate Conjecture asserts that, if E has no complex multiplication, then $\Phi(\theta) = \pi^{-1}\sin^2\theta$.

Let C be a QM-curve defined over a number field k. We assume that all endomorphisms of Jac$C$ are defined over k. Then, for a good prime $\mathfrak{p}$ of k, the congruence ζ-function of C mod $\mathfrak{p}$ has the form

$$Z(u) = \frac{(1-\sqrt{q}e^{\sqrt{-1}\theta_{\mathfrak{p}}}u)^2(1-\sqrt{q}e^{-\sqrt{-1}\theta_{\mathfrak{p}}}u)^2}{(1-u)(1-qu)}, \tag{2.5}$$

where $q = N\mathfrak{p}$ is the absolute norm of $\mathfrak{p}$. Similarly to the case of an elliptic curve, we consider the density function of the pairs $\Theta = \{\pm\theta_{\mathfrak{p}}\}_{\mathfrak{p}}$. A generalization of the Sato-Tate Conjecture by H. Yoshida asserts that the density function Φ of Θ would be

$$\Phi(\theta) = \pi^{-1}\sin^2\theta. \tag{2.6}$$

We checked this conjecture for many QM-curves of discriminant 6 by calculating the Fourier coefficients of $\Phi(\theta)$ approximately. Similarly to Lemma 2.3, we have the following lemma.

Lemma 2.7. *For $\Theta = \{\pm\theta_{\mathfrak{p}}\}_{\mathfrak{p}}$, assume that the limit*

$$c_k := \lim_{x\to\infty} \frac{1}{\#\{\mathfrak{p} \mid \text{good prime}, N\mathfrak{p} < x\}} \sum_{N\mathfrak{p}<x} \cos k\theta_{\mathfrak{p}}$$

exists for all positive integers k. Then the series

$$\Phi(\theta) := \frac{1}{2\pi} + \frac{1}{\pi}\sum_{k=1}^{\infty} c_k \cos k\theta$$

converges in the sense of distributions and is the density function of Θ.

If the conjecture is true, then the Fourier coefficients c_k of Φ must be

$$c_2 = -\frac{1}{2}, \quad c_k = 0 \ (k \neq 2). \tag{2.8}$$

We calculated approximate values of c_k's as

$$c_k \fallingdotseq \frac{1}{\#\{\mathfrak{p} \mid \text{good prime}, N\mathfrak{p} < x\}} \sum_{N\mathfrak{p}<x} \cos k\theta_{\mathfrak{p}} \tag{2.9}$$

for sufficiently large x.

Remark 2.10. In the definition of the Fourier coefficients c_k, we can restrict ourselves to primes degree one. But we calculated the arguments $\pm\theta_{\mathfrak{p}}$ also for primes $\mathfrak{p}$ of absolute degree more than one (in fact, of degree two because we examined QM-curves defined over (imaginary) quadratic fields) to make sure that there was no qualitative difference.

3. Results

Consider the family of QM-curves given by

$$(3.1)\qquad \mathcal{S}_6(t,s): Y^2 = X(X^4+(A-B)X^3+QX^2+(A+B)X+1),$$
$$A=\frac{s}{2t},\quad B=\frac{1+3t^2}{1-3t^2},$$
$$Q=-\frac{(1-2t^2+9t^4)(1-28t^2+166t^4-252t^6+81t^8)}{4t^2(1-3t^2)^2(1-t^2)(1-9t^2)},$$

$$(3.2)\qquad S_{\boldsymbol{B}_6}: g(t,s)=s^2+3-14t^2+27t^4=0.$$

We denote by $C_{(t_0,s_0)}$ the curve obtained by specializing (t,s) to a point (t_0,s_0) on $g(t,s)=0$. We can find that $C_{(t,s)}=C_{(-t,-s)}$ and that $C_{(t,s)}$ and $C_{(t,-s)}$ are generically isomorphic over $\boldsymbol{Q}(\sqrt{-1})$ by

$$(3.3)\qquad C_{(t,s)} \simeq C_{(t,-s)},$$
$$(X,Y)\leftrightsquigarrow(-X^{-1},\sqrt{-1}X^{-3}Y).$$

We checked the following curves and primes:

$$(3.4)\qquad t\in\boldsymbol{Z},\ 2\le t\le 30\ (\#=29)$$
$$N\mathfrak{p}<2^{20}\ \text{(primes of degree one)}.$$

Since t belongs to $\boldsymbol{Q}$, $C_{(t,s)}$ is defined over an imaginary quadratic field $k=\boldsymbol{Q}(s)=\boldsymbol{Q}(\sqrt{-3+14t^2-27t^4})$. Moreover, $C_{(t,s)}$ and $C_{(t,-s)}$ are conjugate over $\boldsymbol{Q}$. If a rational prime p decomposes as $p=\mathfrak{p}\mathfrak{p}'$ in k, then

$$(3.5)\qquad C_{(t,s)} \bmod \mathfrak{p}' \simeq C_{(t,-s)} \bmod \mathfrak{p}\ (\text{over } \boldsymbol{F}_p)$$
$$\simeq C_{(t,s)} \bmod \mathfrak{p}\ (\text{over } \boldsymbol{F}_p(\sqrt{-1})),$$

where $\boldsymbol{F}_p(\sqrt{-1})$ means $\boldsymbol{F}_p$ if $p\equiv 1 \bmod 4$ or $\boldsymbol{F}_{p^2}$ if $p\equiv 3 \bmod 4$. Hence we have $\theta_{\mathfrak{p}'}=\theta_{\mathfrak{p}}$ if $p\equiv 1 \bmod 4$ or $\theta_{\mathfrak{p}'}=\pi-\theta_{\mathfrak{p}}$ if $p\equiv 3 \bmod 4$. This means that we may consider only one prime above p for a splitting prime p.

For each curve $C=C_{(t,s)}$, we first computed the numbers of $\boldsymbol{F}_p$- and $\boldsymbol{F}_{p^2}$-rational points of $C \bmod \mathfrak{p}$ for first thirty splitting primes $\mathfrak{p}$ of k, to check the assumption that all endomorphisms of Jac$C$ are defined over k, and obtained data which shows the assumption is true. Under this assumption, the congruence ζ-function of $C \bmod \mathfrak{p}$ is determined only by the number N_1 of $\boldsymbol{F}_p$-rational points. We computed N_1 of $C \bmod \mathfrak{p}$ for splitting primes $\mathfrak{p}$ of k with $N\mathfrak{p}<2^{20}$ (more than 40000 primes), and calculated the approximate values of the Fourier coefficients c_k ($k\le 20$) of the density function by (2.9). For all curves we checked, all the approximate values of c_k satisfy

$$(3.6)\qquad \left|c_2+\frac{1}{2}\right|<0.007,\qquad |c_k|<0.011\ \ (k>0, k\ne 2).$$

In fact, out of 551 values of $|c_k|$ $(k>0,k\ne 2)$, only 49 values are bigger than 0.005. For c_2, out of 29 values of $|c_2+\frac{1}{2}|$, only 2 values are bigger than 0.005. We also carried out the same computations for the other primes $\mathfrak{p}=(p)$ of k with $N\mathfrak{p}<2^{20}$ $(p<2^{10})$, and found no qualititive difference from splitting primes.

We shall give precise data for $t=2$ in the following. In the examples, Table A gives the approximate values of the Fourier coefficients of the density function and Table B gives the frequency distribution of the arguments and the comparison with $\sin^2\theta$.

Example 1.

$$C_{(2,\sqrt{-379})} : Y^2$$
$$= X\left(X^4 + \left(\frac{\sqrt{-379}}{4} + \frac{13}{11}\right)X^3 - \frac{979961}{203280}X^2 + \left(\frac{\sqrt{-379}}{4} - \frac{13}{11}\right)X + 1\right).$$

We carried out our calculations for 40823 splitting primes (see Tables 1.A, 1.B, Figure 1.C at the end of this paper).

We also calculated some other examples which seem interesting to us in a sense. The following example has relatively small coefficients.

Example 2.

$$C_{(\frac{2}{3},\frac{\sqrt{-19}}{3})} : Y^2 = X\left(X^4 + \left(\frac{\sqrt{-19}}{4} + 7\right)X^3 + \frac{3281}{240}X^2 + \left(\frac{\sqrt{-19}}{4} - 7\right)X + 1\right).$$

We carried out our calculations for 40947 splitting primes (see Tables 2.A, 2.B, Figure 2.C at the end of this paper).

The following example is the case when Jac$C$ is isogenous to a product $E \times E$ of an elliptic curve E with complex multiplication.

Example 3 ([HM] Example 1.5).

$$C_{(\frac{\sqrt{-3}}{3},\frac{4\sqrt{-6}}{3})} : Y^2 = X\left(X^4 + 2\sqrt{2}X^3 + \frac{11}{3}X^2 + 2\sqrt{2}X + 1\right).$$

Via the following morphism ϕ of degree two, Jac$C$ splits into $E \times E$:

$$\phi : C_{(\frac{\sqrt{-3}}{3},\frac{4\sqrt{-6}}{3})} \longrightarrow E : y^2 = (x+2)\left(x^2 + 2\sqrt{2}x + \frac{5}{3}\right), \tag{3.7}$$
$$(X,Y) \longmapsto (x,y) = \left(X + \frac{1}{X}, \frac{Y(X+1)}{X^2}\right),$$

where E is an elliptic curve with complex multiplication by $\boldsymbol{Z}[\sqrt{-6}]$, whose invariant is $j(\sqrt{-6}) = 12^3(1399 + 988\sqrt{2})$.

We carried out our calculations for 41003 splitting primes (see Tables 3.A, 3.B, Figure 3.C at the end of this paper).

Remark 3.8. In this case the Hasse-Weil L-function of C coincides with a square of that of E. For the primes inert in $\boldsymbol{Q}(\sqrt{2},\sqrt{-6})/\boldsymbol{Q}(\sqrt{2})$ (density $\frac{1}{2}$), the arguments of zeroes of the characteristic polynomials of the Frobenius elements are all $\frac{\pi}{2}$, and for the primes splitting in $\boldsymbol{Q}(\sqrt{2},\sqrt{-6})/\boldsymbol{Q}(\sqrt{2})$ they are distributed uniformly on T by the property of größencharacter. Hence the k-th Fourier coefficients of the density function $\Phi(\theta)$ must be $\frac{(-1)^{\frac{k}{2}}}{2}$ for even k and zero for odd k. The above data fits with this fact very well.

Remark 3.9. By arguments similar to Example 1.6 in [HM], we can *prove* that, in Example 1, Jac$C$ are *simple* QM-abelian surfaces, i.e. they never split into a product of CM-elliptic curves. The qualitative difference between Example 1 and Example 3 is so clear that we can distinguish experimantally whether Jac$C$ is simple or not.

4. Some remarks on the defining equations

Although we have carried out our computation mainly for the family of QM-curves defined by (3.1), we also have some defining equations of algebraic families of QM-curves which have different arithmetic properties. In this section we shall make some remarks on them.

The original equation obtained in [HM](Theorem 1.3) is of the following form:

$$\begin{aligned} &(4.1) && \mathcal{S}'_6(t,s) : Y^2 = X(X^4 - PX^3 + QX^2 - RX + 1) \\ &&& P = -2(s+t), \quad R = -2(s-t), \\ &&& Q = \frac{(1+2t^2)(11-28t^2+8t^4)}{3(1-t^2)(1-4t^2)}, \\ &(4.2) && S'_{\boldsymbol{B}_6} : g'(t,s) = 4s^2t^2 - s^2 + t^2 + 2 = 0. \end{aligned}$$

For a value $t \in \boldsymbol{Q}$, s belongs to the quadratic field $k = \boldsymbol{Q}(\sqrt{(2+t^2)(1-4t^2)})$, and hence we get a QM-curve $C = C_{(t,s)}$ defined over k. First we carried out our computation for many fibers $C_{(t,s)}$ corresponding to the values $t \in \boldsymbol{Z}$ and for many primes $\mathfrak{p}$ splitting in $k/\boldsymbol{Q}$. We then found numerically that the case $f = 2$ does occur (see (1.9), (1.10)), in which case we need both N_1 and N_2 to determine the congruence ζ-function of $C_{(t,s)} \mod \mathfrak{p}$. Since this takes very much time when $N_{\mathfrak{p}}$ is large, this family $\mathcal{S}'_6$ is not suitable for our computation. Therefore it is important to observe the following phenomena, which has been checked for many $t \in \boldsymbol{Z}$ and for many prime p.

Numerical Fact 4.3. *There exist a polynomial $D(t) \in \boldsymbol{Z}[t]$ such that, for each value $t \in \boldsymbol{Z}$ and for each prime p splitting in $k/\boldsymbol{Q}$, $f = 1$ if and only if $\left(\frac{D(t)}{p}\right) = 1$. In fact, one can take $D(t) = -3(1-4t^2)$.*

This suggests that all endomorphisms of Jac$C_{(t,s)}$ are defined over $\boldsymbol{Q}(t, s, \sqrt{D(t)})$ $= \boldsymbol{Q}(t, \sqrt{-3(1-4t^2)}, \sqrt{-3(2+t^2)})$ generically. This observation is very helpful to find the defining equation (3.1), in whose case all endomorphisms of Jac$C_{(t,s)}$ are defined over the field $\boldsymbol{Q}(t,s)$ of definition of the curve $C_{(t,s)}$. In fact, we obtained (3.1) from (4.1) by putting

$$(4.4) \qquad a = \frac{\sqrt{D(t)}}{1-2t}, \quad b = \frac{s}{2t}$$

then subtituting a, b for t, s, respectively.

Another remark is concerned with the descent of the base curve $S_{\boldsymbol{B}_6}$.

Lemma 4.5. *The family $\mathcal{S}_6$ of QM-curves has an automorphism w of order two which preserves fibration and is defined over $\boldsymbol{Q}$, described as*

$$w : (t,s,X,Y) \longmapsto \left(-\frac{1}{3t}, -\frac{s}{3t}, X^{-1}, X^{-3}Y\right).$$

Put $\mathcal{S}^0_6 = \mathcal{S}_6/\langle w\rangle$ and $S^0_{\boldsymbol{B}_6} = S_{\boldsymbol{B}_6}/\langle w\rangle$. Then $\mathcal{S}^0_6$ is a family of QM-curves over $S^0_{\boldsymbol{B}_6}$, whose defining equation is

$$\begin{aligned} \mathcal{S}^0_6(\tau,\sigma) : \eta^2 = (\xi^2 - R)\{&(2 - Q + 2A)\xi^4 - 4R\xi^3 \\ &+ 2R(6+Q)\xi^2 + 4R^2\xi + R^2(2 - Q - 2A)\}, \\ A = \frac{\sigma}{\tau}, \quad & R = 1 + 3\tau^2, \\ Q = \frac{(1+\tau^2)(1-4\tau^2+\tau^4)}{\tau^2(1-\tau^2)}&, \\ S^0_{\boldsymbol{B}_6} : g^0(\tau,\sigma) = \sigma^2 + \tau^2 + 3 = 0.& \end{aligned}$$

Proof. It is easy to see that w gives an automorphism of $\mathcal{S}_6$ of order two. To obtain the equation of the base curve $S^0_{\boldsymbol{B}_6}$, we put

$$\sigma = \frac{s}{3t^2-1}, \qquad \tau = \frac{2t}{3t^2-1}.$$

Then σ and τ are w-invariant and the mapping $(t,s) \mapsto (\sigma,\tau)$ gives a 2 : 1-morphism from $S_{\boldsymbol{B}_6}$ with image $\sigma^2+\tau^2+3=0$. In terms of σ and τ, the coefficients A, R, Q are w-invariant and described as above, where $R = B^2$ and B itself is not w-invariant; $B^w = -B$. Now set

$$\xi = \frac{B(X-1)}{X+1} \qquad \eta = \frac{-8R^2Y}{(X+1)^3}.$$

Then ξ and η are w-invariant, and the mapping $(X,Y) \mapsto (\xi,\eta)$ is birational since

$$X = -\frac{\xi+B}{\xi-B}, \qquad Y = \frac{\eta}{B(\xi-B)^3}.$$

Substituting these for X, Y in the defining equation (3.1), we obtain the above equation defining $\mathcal{S}^0_6(\tau,\sigma)$. □

It is noticeable that the equation $g^0(\tau,\sigma)=0$ of the base space $S^0_{\boldsymbol{B}_6}$ coincides with the defining equation of the canonical model of the Shimura curve for discriminant 6 described by A. Kurihara [K]. Our computation for this family suggests that the field of definition of all endomorphisms of $\mathrm{Jac}C_{(\tau,\sigma)}$ is not $\boldsymbol{Q}(\tau,\sigma)$ but $\boldsymbol{Q}(\tau,\sigma,\sqrt{R})$. Hence $\mathcal{S}^0_6(\tau,\sigma)$ is not suitable for our computation similarly to $\mathcal{S}'_6$. For this reason we did not choose $\mathcal{S}^0_6(\tau,\sigma)$ for our computation, although it seems to be very interesting to study the arithmetic properties of this family.

5. Some other examples

While this paper was with the referee, some isolated examples of QM-curves defined over $\boldsymbol{Q}$ were found. We carried out our calculations for these curves and obtained results fitting with the conjecture very well.

Let $C_{(i)}$ $(i=1,2,3)$ be hyperelliptic curves of genus two over $\boldsymbol{Q}$ defined by

$$C_{(1)} : y^2 = x^6 - 33x^5 + 342x^4 - 1040x^3 - 912x^2 + 720x - 96, \tag{5.1}$$

$$C_{(2)} : y^2 = x^6 - 47x^5 - 390x^4 - 92x^3 + 2511x^2 + 899x + 62, \tag{5.2}$$

$$C_{(3)} : y^2 = x^6 + 47x^5 + 365x^4 + 865x^3 + 400x^2 + 38x - 4. \tag{5.3}$$

These curves have the property that their Jacobian varieties $\mathrm{Jac}C_{(i)}$ are of GL_2-type over $\boldsymbol{Q}$ with $\mathrm{End}_{\boldsymbol{Q}}\mathrm{Jac}C_{(i)} = \boldsymbol{Q}(\sqrt{5})$. Moreover, we know the following:

Theorem 5.4 (Hasegawa-Hashimoto-Momose [HHM]). *The curves $C_{(i)}$ $(i=1,2,3)$ are QM-curves such that $\mathrm{End}\mathrm{Jac}C_{(i)} = \mathrm{End}_k\mathrm{Jac}C_{(i)}$ is an order of the indefinite division quaternion algebra over $\boldsymbol{Q}$ of discriminant* 10, *where $k = \boldsymbol{Q}(\sqrt{-2})$, $\boldsymbol{Q}(\sqrt{-58}), \boldsymbol{Q}(\sqrt{-10})$, respectively. Furthermore, $C_{(1)}$ and $C_{(2)}$ are modular.*

We carried out our calculations for these curves $C_{(i)}$ and the primes $p < 2^{20}$ splitting in $k/\boldsymbol{Q}$, and obtained results which support the conjecture. The approximate value of the Fourier coefficients c_k $(k \le 20)$ satisfy

$$\left|c_2 + \frac{1}{2}\right| < 0.004, \qquad |c_k| < 0.009 \ \ (k>0, k\neq 2). \tag{5.5}$$

We give precise data for $C_{(1)}$ in Table 4.A, 4.B, Figure 4.C. The number of the primes we calculated is 40972.

Table 1.A

k	c_k
0	0.500000
1	0.002503
2	−0.500186
3	−0.002054
4	−0.002779
5	0.001513
6	0.000647
7	−0.002529
8	0.000754
9	−0.000483
10	0.002203
11	0.000223
12	−0.000862
13	0.000373
14	−0.001862
15	0.000216
16	−0.002844
17	−0.000214
18	0.006595
19	−0.003201
20	−0.002521

Table 1.B

i	range of θ	rel. frequency	$\frac{1}{10}\sin^2(\frac{i}{20}\pi)$
0	$0 < \theta < 0.025\pi$	0.000073	0.000000
1	$0.025\pi < \theta < 0.075\pi$	0.002682	0.002447
2	$0.075\pi < \theta < 0.125\pi$	0.009615	0.009549
3	$0.125\pi < \theta < 0.175\pi$	0.020858	0.020611
4	$0.175\pi < \theta < 0.225\pi$	0.034980	0.034549
5	$0.225\pi < \theta < 0.275\pi$	0.050584	0.050000
6	$0.275\pi < \theta < 0.325\pi$	0.065564	0.065451
7	$0.325\pi < \theta < 0.375\pi$	0.079453	0.079389
8	$0.375\pi < \theta < 0.425\pi$	0.091652	0.090451
9	$0.425\pi < \theta < 0.475\pi$	0.097286	0.097553
10	$0.475\pi < \theta < 0.525\pi$	0.099135	0.100000
11	$0.525\pi < \theta < 0.575\pi$	0.096575	0.097553
12	$0.575\pi < \theta < 0.625\pi$	0.090207	0.090451
13	$0.625\pi < \theta < 0.675\pi$	0.078742	0.079389
14	$0.675\pi < \theta < 0.725\pi$	0.065294	0.065451
15	$0.725\pi < \theta < 0.775\pi$	0.050927	0.050000
16	$0.775\pi < \theta < 0.825\pi$	0.034662	0.034549
17	$0.825\pi < \theta < 0.875\pi$	0.019781	0.020611
18	$0.875\pi < \theta < 0.925\pi$	0.009272	0.009549
19	$0.925\pi < \theta < 0.975\pi$	0.002633	0.002447
20	$0.975\pi < \theta < \pi$	0.000024	0.000000

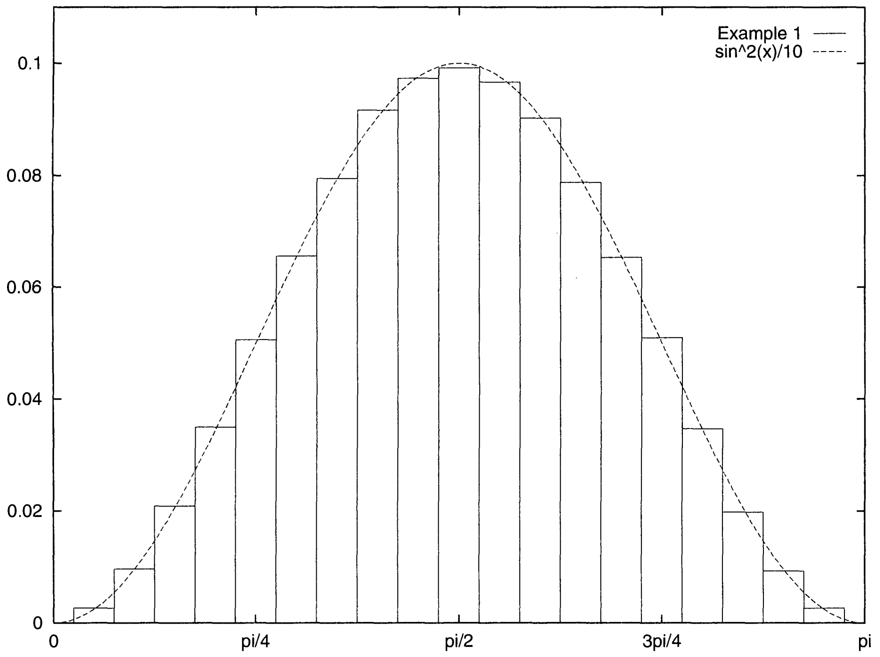

FIGURE 1.C

Table 2.A

k	c_k
0	0.500000
1	0.001908
2	−0.499384
3	−0.002081
4	−0.001489
5	0.001223
6	0.000531
7	−0.001741
8	0.001393
9	0.000938
10	0.000051
11	0.002461
12	−0.006414
13	−0.007648
14	0.001614
15	0.003759
16	0.001708
17	0.001766
18	0.000495
19	−0.003832
20	0.003876

Table 2.B

i	range of θ	rel. frequency	$\frac{1}{10}\sin^2(\frac{i}{20}\pi)$
0	$0 < \theta < 0.025\pi$	0.000037	0.000000
1	$0.025\pi < \theta < 0.075\pi$	0.002613	0.002447
2	$0.075\pi < \theta < 0.125\pi$	0.010453	0.009549
3	$0.125\pi < \theta < 0.175\pi$	0.020136	0.020611
4	$0.175\pi < \theta < 0.225\pi$	0.034801	0.034549
5	$0.225\pi < \theta < 0.275\pi$	0.050907	0.050000
6	$0.275\pi < \theta < 0.325\pi$	0.065621	0.065451
7	$0.325\pi < \theta < 0.375\pi$	0.078553	0.079389
8	$0.375\pi < \theta < 0.425\pi$	0.092046	0.090451
9	$0.425\pi < \theta < 0.475\pi$	0.096368	0.097553
10	$0.475\pi < \theta < 0.525\pi$	0.099836	0.100000
11	$0.525\pi < \theta < 0.575\pi$	0.097223	0.097553
12	$0.575\pi < \theta < 0.625\pi$	0.089848	0.090451
13	$0.625\pi < \theta < 0.675\pi$	0.078260	0.079389
14	$0.675\pi < \theta < 0.725\pi$	0.066208	0.065451
15	$0.725\pi < \theta < 0.775\pi$	0.049637	0.050000
16	$0.775\pi < \theta < 0.825\pi$	0.034972	0.034549
17	$0.825\pi < \theta < 0.875\pi$	0.019867	0.020611
18	$0.875\pi < \theta < 0.925\pi$	0.010111	0.009549
19	$0.925\pi < \theta < 0.975\pi$	0.002393	0.002447
20	$0.975\pi < \theta < \pi$	0.000110	0.000000

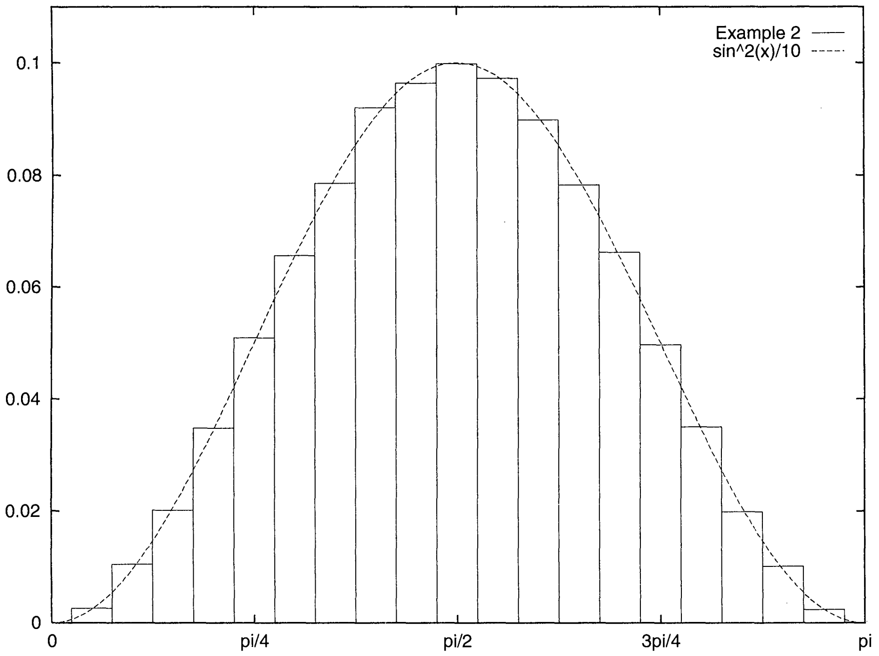

FIGURE 2.C

Table 3.A

k	c_k
0	0.500000
1	−0.000280
2	−0.501998
3	−0.000975
4	0.499924
5	−0.001571
6	−0.502599
7	−0.001873
8	0.499744
9	−0.002418
10	−0.501226
11	−0.001901
12	0.500802
13	−0.000221
14	−0.502897
15	−0.000873
16	0.500289
17	0.000625
18	−0.500966
19	−0.001550
20	0.497862

Table 3.B

i	range of θ	rel. frequency	$\frac{1}{10}\sin^2(\frac{i}{20}\pi)$
0	$0 < \theta < 0.025\pi$	0.011463	0.000000
1	$0.025\pi < \theta < 0.075\pi$	0.024742	0.002447
2	$0.075\pi < \theta < 0.125\pi$	0.025352	0.009549
3	$0.125\pi < \theta < 0.175\pi$	0.025010	0.020611
4	$0.175\pi < \theta < 0.225\pi$	0.025279	0.034549
5	$0.225\pi < \theta < 0.275\pi$	0.025047	0.050000
6	$0.275\pi < \theta < 0.325\pi$	0.024620	0.065451
7	$0.325\pi < \theta < 0.375\pi$	0.025364	0.079389
8	$0.375\pi < \theta < 0.425\pi$	0.024913	0.090451
9	$0.425\pi < \theta < 0.475\pi$	0.025145	0.097553
10	$0.475\pi < \theta < 0.525\pi$	0.526083	0.100000
11	$0.525\pi < \theta < 0.575\pi$	0.025023	0.097553
12	$0.575\pi < \theta < 0.625\pi$	0.024693	0.090451
13	$0.625\pi < \theta < 0.675\pi$	0.025340	0.079389
14	$0.675\pi < \theta < 0.725\pi$	0.024888	0.065451
15	$0.725\pi < \theta < 0.775\pi$	0.024779	0.050000
16	$0.775\pi < \theta < 0.825\pi$	0.025132	0.034549
17	$0.825\pi < \theta < 0.875\pi$	0.024986	0.020611
18	$0.875\pi < \theta < 0.925\pi$	0.024498	0.009549
19	$0.925\pi < \theta < 0.975\pi$	0.025108	0.002447
20	$0.975\pi < \theta < \pi$	0.012536	0.000000

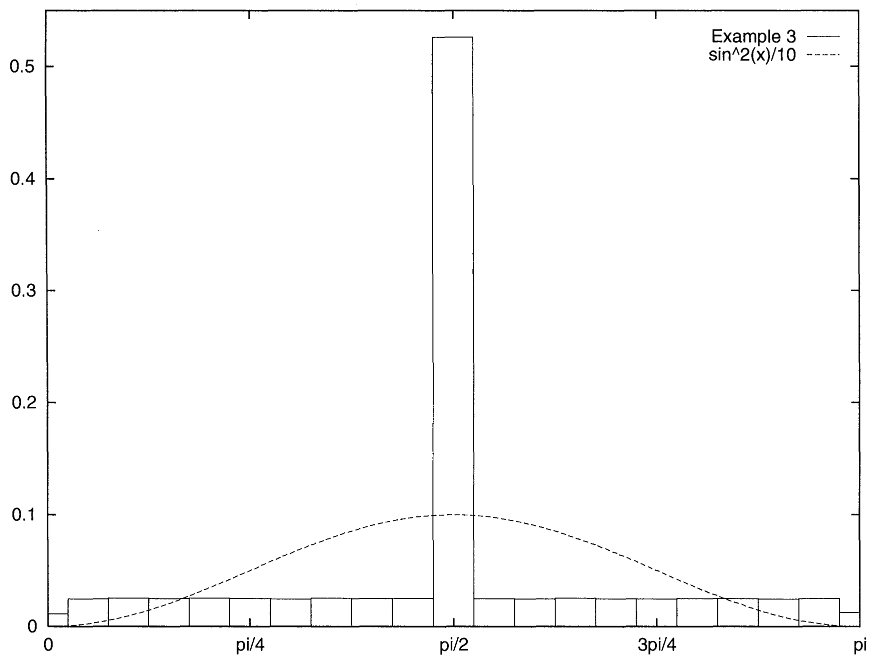

Figure 3.C

Table 4.A

k	c_k
0	0.500000
1	−0.005620
2	−0.503954
3	0.008570
4	−0.000414
5	−0.000747
6	0.005640
7	−0.007312
8	−0.002358
9	0.005689
10	0.004150
11	−0.003570
12	−0.006671
13	0.002887
14	0.005516
15	−0.002321
16	−0.003407
17	−0.001983
18	0.003538
19	0.002949
20	−0.001526

Table 4.B

i	range of θ	rel. frequency	$\frac{1}{10}\sin^2(\frac{i}{20}\pi)$
0	$0 < \theta < 0.025\pi$	0.000024	0.000000
1	$0.025\pi < \theta < 0.075\pi$	0.002343	0.002447
2	$0.075\pi < \theta < 0.125\pi$	0.009177	0.009549
3	$0.125\pi < \theta < 0.175\pi$	0.020599	0.020611
4	$0.175\pi < \theta < 0.225\pi$	0.034170	0.034549
5	$0.225\pi < \theta < 0.275\pi$	0.047813	0.050000
6	$0.275\pi < \theta < 0.325\pi$	0.064922	0.065451
7	$0.325\pi < \theta < 0.375\pi$	0.078297	0.079389
8	$0.375\pi < \theta < 0.425\pi$	0.090720	0.090451
9	$0.425\pi < \theta < 0.475\pi$	0.097554	0.097553
10	$0.475\pi < \theta < 0.525\pi$	0.099116	0.100000
11	$0.525\pi < \theta < 0.575\pi$	0.096676	0.097553
12	$0.575\pi < \theta < 0.625\pi$	0.092258	0.090451
13	$0.625\pi < \theta < 0.675\pi$	0.081275	0.079389
14	$0.675\pi < \theta < 0.725\pi$	0.067290	0.065451
15	$0.725\pi < \theta < 0.775\pi$	0.052353	0.050000
16	$0.775\pi < \theta < 0.825\pi$	0.033242	0.034549
17	$0.825\pi < \theta < 0.875\pi$	0.020209	0.020611
18	$0.875\pi < \theta < 0.925\pi$	0.008982	0.009549
19	$0.925\pi < \theta < 0.975\pi$	0.002831	0.002447
20	$0.975\pi < \theta < \pi$	0.000146	0.000000

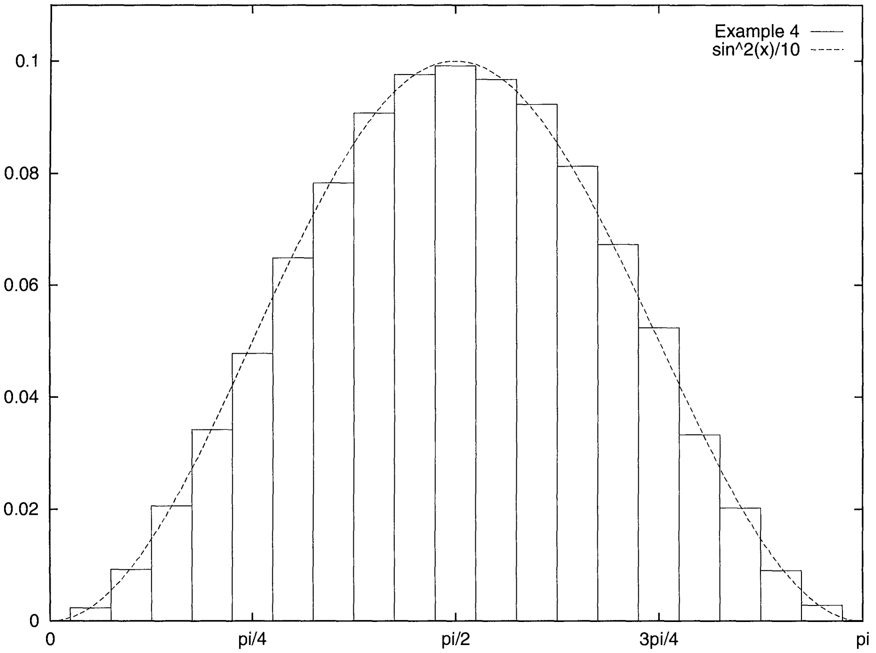

FIGURE 4.C

References

[D] Deuring, M., Die Typen der Multiplicatorenringe der elliptischer Funktionenkörper, Abh.Math.Sem. Hamburg 14 (1941), 197–272. MR **3:**104f

[F] Faltings, G., Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, Invent. Math. 73 (1983), 349–366. MR **85g:**11026a

[HHM] Hasegawa, Y., Hashimoto, K., Momose, F., Modular conjecture for $\boldsymbol{Q}$-curves and QM-curves, preprint, 1997.

[HM] Hashimoto, K., Murabayashi, N., Shimura curves as intersection of Humbert surfaces and defining equations of QM-curves of genus two, Tohoku Math. J. 47 (1995), 271–296. MR **96b:**14023

[K] Kurihara, A., On some examples of equations defining Shimura curves and the Mumford uniformization, F. Fac. Sci. Univ. Tokyo, 25 (1979), 277–301. MR **80e:**14010

[M] Mumford, D., Abelian varieties, Oxford Univ. Press, London, 1970. MR **44:**219

[O] Ohta, M., On l-adic representations of Galois groups obtained from certain two dimensional abelian varieties, J. Fac. Sci. Univ. Tokyo, 21 (1974), 299–308. MR **54:**7389

[P] Pyle, E., Abelian varieties over $\boldsymbol{Q}$ with large endmorphism algebras and thier simple components over $\bar{\boldsymbol{Q}}$, Doctor's thesis, Univ. of California at Berkeley, 1995.

[R] Ribet, K., Fields of definition of abelian varieties with real multiplication, Contemp. Math. 174 (1994), 107–118. MR **95i:**11057

[T] Tate, J., Algebraic Cycles and Poles of Zeta Functions, in "Arithmetical Algebraic Geometry", (F.G. Schilling, ed.), Harper and Row, New York, 1965, pp. 93–110. MR **37:**1371

[Ya] Yamamoto, Y., On Sato Conjecture for two-dimensional abelian varieties (in Japanese), Number Theory Symposium at Kinosaki (1979), 236–244.

[Yo1] Yoshida, H., Mumford-Tate groups and its application to abelian varieties (in Japanese), "Shimura varieties and algebraic geometry" Symposium at Kinosaki (1983), 106–131.

[Yo2] Yoshida, H., On an Analogue of the Sato Conjecture, Invent. Math. 19 (1973), 261–277. MR **49:**2746

Department of Mathematics, Waseda University, 3-4-1, Ōkubo, Shinjuku-ku, Tōkyō, 169-8555, Japan

E-mail address: khasimot@mn.waseda.ac.jp

Department of Mathematics, Sophia University, 7-1, Kioi-chō, Chiyoda-ku, Tōkyō, 102-8554, Japan

E-mail address: tsuno@mm.sophia.ac.jp