Arithmetic on a Family of Picard Curves

Rolf-Peter Holzapfel and Florin Nicolae

Humboldt-Universität zu Berlin, Institut für Mathematik, Rudower Chaussee 25, D-10099 Berlin, Germany

Abstract. The L-function of the curve $C_a : Y^3 = X^4 - aX$ over an algebraic number field k which contains $\zeta_9 := \exp(\frac{2\pi i}{9})$ is the inverse of a product of six Hecke L-functions with Grössencharakter. The Euler factors at primes of good reduction are determined by means of Jacobi sums associated to certain powers of the 9-th power residue character. The number of points of C_a over a finite field is given in terms of such sums. The jacobian variety of C_a over the field of complex numbers has complex multiplication by the ring $\mathbb{Z}[\zeta_9]$.

Let k be a perfect field of characteristic different from 3. The curves

$$C_a : Y^3 = X^4 - aX, a \in k^*$$

are smooth of genus 3 over k, with one point $(0 : 0 : 1)$ at infinity. The main result of this paper is that the L-function of the curve C_a over an algebraic number field k which contains $\zeta_9 := \exp(\frac{2\pi i}{9})$ is the inverse of a product of six Hecke L-functions with Grössencharakter (Theorem 1). As a consequence of this it follows that Hasse's conjecture on the meromorphic continuation and the functional equation of the zeta function is true for the family C_a. Since the Jacobians of the curves C_a have complex multiplication, the result on the zeta function fits into the theory of zeta functions of abelian varieties with complex multiplication ([De],[Ta]).

Let N_1 denote the number of points of the curve C_a over a finite field $k = \mathbb{F}_q$. If $q \not\equiv 1(\bmod 9)$ then $N_1 = q + 1$. This is proved in propositions 1 and 2. If $q \equiv 1(\bmod 9)$ then

$$N_1 = q + 1 - \mathrm{Tr}_{\mathbb{Q}(\zeta_9)/\mathbb{Q}}(\eta),$$

where

$$\eta := \psi^4(a)\iota(\psi^3, \psi),$$

ψ a character of k^* of order 9, $\iota(\psi^3, \psi)$ the Jacobi sum over $\mathbb{F}_q$ associated to ψ^3 and ψ. This is proved in proposition 3. Corollaries 1, 2 and proposition 4 give explicit forms of the L-polynomial of the curve C_a over $\mathbb{F}_q$ in all cases $q(\bmod 9)$. Proposition 5 gives the arithmetic characterization of the algebraic number $\iota(\psi^3, \psi)$ in the ring $\mathbb{Z}[\zeta_9]$.

Over the field $k = \mathbb{C}$ of complex numbers, all curves C_a are isomorphic to $C_1 : Y^3 = X^4 - X$. The moduli point of C_1 is the only orbitally isolated singularity on the modular surface of Picard curves. The endomorphism ring of the jacobian variety $J(C_1)$ of C_1 is the ring $\mathbb{Z}[\zeta_9]$. Up to isomorphism, C_1 is the only Picard curve whose jacobian variety has a cyclotomic maximal order as endomorphism ring. This is proved in proposition 7. In proposition 8 is given explicitly a period matrix of $J(C_1)$:

$$\Pi = \begin{pmatrix} -\zeta_9+1 & 0 & -2{\zeta_9}^2-2\zeta_9 & -{\zeta_9}^2-1 & 1 & 2{\zeta_9}^2+\zeta_9 \\ {\zeta_9}^2-1 & 0 & -{\zeta_9}^2+2\zeta_9 & -{\zeta_9}^2+\zeta_9+1 & -1 & {\zeta_9}^2-2\zeta_9 \\ -\zeta_9+1 & 0 & -2{\zeta_9}^2-2\zeta_9 & -{\zeta_9}^2-1 & 1 & 2{\zeta_9}^2+\zeta_9 \end{pmatrix} \cdot {\zeta_9}^3 +$$

$$+ \begin{pmatrix} 2{\zeta_9}^2+\zeta_9+1 & 1 & -\zeta_9+1 & -2{\zeta_9}^2-\zeta_9 & 0 & {\zeta_9}^2+\zeta_9-1 \\ -{\zeta_9}^2+2\zeta_9 & 1 & -2{\zeta_9}^2+2\zeta_9+1 & -\zeta_9+1 & -1 & {\zeta_9}^2-\zeta_9-1 \\ 2{\zeta_9}^2+\zeta_9+1 & 1 & -\zeta_9+1 & -2{\zeta_9}^2-\zeta_9 & 0 & {\zeta_9}^2+\zeta_9-1 \end{pmatrix}.$$

Picard curves of equation type $Y^3 = X^4 - a$ are considered in [Lac].

This research was supported by the Deutsche Forschungsgemeinschaft.

1 The curves $C_a : Y^3 = X^4 - aX$ over $\mathbb{F}_q$

Let $k = \mathbb{F}_q$ be a finite field of characteristic $p \neq 3$ with $q = p^f$ elements, and let $a \in k^*$. The curve

$$C_a : y^3 = x^4 - ax$$

is smooth of genus 3 over k. Let F_a/k be the function field of C_a, let $\mathbb{P}_{F_a}$ denote the set of places, and let $\mathrm{Div}F_a$ denote the group of divisors of F_a/k. The absolute norm $\mathfrak{N}(\mathfrak{P})$ of a place $\mathfrak{P} \in \mathbb{P}_{F_a}$ is the cardinality of its residue class field. It holds $\mathfrak{N}(\mathfrak{P}) = q^{\deg \mathfrak{P}}$, with a natural number $\deg \mathfrak{P} \geq 1$, the degree of $\mathfrak{P}$. The Zeta function of the curve C_a is a meromorphic function in the complex plane, defined for $\Re s > 1$ by

$$\zeta_{C_a}(s) = \prod_{\mathfrak{P} \in \mathbb{P}_{F_a}} \frac{1}{1 - \frac{1}{\mathfrak{N}(\mathfrak{P})^s}} = \sum_{\mathfrak{A} \in \mathrm{Div}F_a,\, \mathfrak{A} \geq 0} \frac{1}{\mathfrak{N}(\mathfrak{A})^s}.$$

Denoting for $n \geq 0$ by A_n the number of positive divisors of degree n it holds

$$\zeta_{C_a}(s) = \sum_{n=0}^{\infty} \frac{A_n}{q^{ns}}.$$

The power series

$$Z_{C_a}(t) := \sum_{n=0}^{\infty} A_n t^n$$

is convergent for $|t| < q^{-1}$ and represents a rational function

$$Z_{C_a}(t) = \frac{L_{C_a}(t)}{(1-t)(1-qt)},$$

where $L_{C_a}(t)$ is a polynomial with coefficients in $\mathbb{Z}$ of the form:

$$L_{C_a}(t) = 1 + a_1 t + a_2 t^2 + a_3 t^3 + q a_2 t^4 + q^2 a_1 t^5 + q^3 t^6.$$

For $r \geq 1$ let N_r be the number of $\mathbb{F}_{q^r}$-rational points of the complete curve C_a, and let $S_r := N_r - (q^r + 1)$. It holds

$$a_1 = S_1,$$

$$2a_2 = S_2 + S_1 a_1,$$

$$3a_3 = S_3 + S_2 a_1 + S_1 a_2.$$

The plane curve C_a has only one point at infinity, hence

$$N_1 = N + 1$$

where N is the number of solutions (x, y) in k of the equation

$$y^3 = x^4 - ax.$$

Proposition 1. *If* $q \equiv 2(\bmod 3)$ *then* $N_1 = q + 1$.

P r o o f: If $q \equiv 2(\bmod 3)$ the order $q-1$ of the cyclic multiplicative group k^* is not divisible by 3, so $k^* = k^{*3}$. This implies that for each $x \in k$ there exists exactly one $y \in k$ with $y^3 = x^4 - ax$. Hence $N = q$. □

Proposition 2. *If* $q \equiv 4(\bmod 9)$ *or* $q \equiv 7(\bmod 9)$ *then* $N_1 = q + 1$.

P r o o f: If $q \equiv 4(\bmod 9)$ or $q \equiv 7(\bmod 9)$ then the cyclic multiplicative group k^* of order $q-1$ is equal to the internal direct product of its subgroup of order 3, generated by ζ, and of its subgroup of order $\frac{q-1}{3}$, denoted by $U_{\frac{q-1}{3}}$. Each element $c \in \mathbb{F}_q^*$ can be uniquely written in the form $c = d\zeta^j$ with $d \in U_{\frac{q-1}{3}}$ and $0 \leq j \leq 2$. Let χ be a character of k^* of order 3. Put $\chi(0) := 0$. The number of solutions in k of the equation $y^3 = x^4 - ax$ is

$$N = q + \sum_{c \in \mathbb{F}_q} \chi(c^4 - ac) + \sum_{c \in \mathbb{F}_q} \chi^2(c^4 - ac) = q + \alpha + \bar{\alpha},$$

where

$$\alpha = \sum_{c \in \mathbb{F}_q} \chi(c^4 - ac) = \sum_{d \in U_{\frac{q-1}{3}}} \sum_{j=0}^{2} \chi(d^4 \zeta^{4j} - ad\zeta^j) =$$

$$= \sum_{d \in U_{\frac{q-1}{3}}} \sum_{j=0}^{2} \chi[\zeta^j (d^4 - ad)] = [\sum_{d \in U_{\frac{q-1}{3}}} \chi(d^4 - ad)] \cdot [\sum_{j=0}^{2} \chi(\zeta^j)] =$$

$$= [\sum_{d \in U_{\frac{q-1}{3}}} \chi(d^4 - ad)] \cdot [\chi(1) + \chi(\zeta) + \chi(\zeta)^2].$$

If $q \equiv 4(\bmod 9)$ or $q \equiv 7(\bmod 9)$ then $\frac{q-1}{3}$ is prime to 3, so χ is not trivial on the subgroup of k^* of order 3. This implies

$$\chi(1) + \chi(\zeta) + \chi(\zeta)^2 = 0,$$

so $\alpha = 0$ and $N = q$. □

Corollary 1. *If* $q \equiv 2(\bmod 9)$ *or* $q \equiv 5(\bmod 9)$ *then*

$$L_{C_a}(t) = 1 + q^3 t^6.$$

P r o o f: If $q \equiv 2(\bmod 9)$ or $q \equiv 5(\bmod 9)$ then $q \equiv 2(\bmod 3)$, $q^2 \equiv 4(\bmod 9)$ or $q^2 \equiv 7(\bmod 9)$, and $q^3 \equiv 2(\bmod 3)$. By Propositions 9 and 10 it holds $N_1 = q+1$, $N_2 = q^2+1$, $N_3 = q^3+1$. So $S_i = N_i - (q^i+1) = 0$ for $i = 1,2,3$ and $a_1 = a_2 = a_3 = 0$. Hence $L_{C_a}(t) = 1 + q^3 t^6$. □

For a character φ of the multiplicative group k^* let

$$\tau(\varphi) := -\sum_{c \in k^*} \varphi(c) \exp(\frac{2\pi i}{p} \mathrm{Tr}_{\,k/\mathbb{F}_p} c)$$

be the corresponding Gauss sum ([Da-Ha]). For an element $d \in k^*$ define

$$\tau_d(\varphi) := -\sum_{c \in k^*} \varphi(c) \exp(\frac{2\pi i}{p} \mathrm{Tr}_{\,k/\mathbb{F}_p} cd).$$

It holds

$$\tau_d(\varphi) = \varphi^{-1}(d)\tau(\varphi). \tag{1}$$

For two characters φ_1 and φ_2 of k^* let

$$\iota(\varphi_1, \varphi_2) := -\sum_{c \in k} \varphi_1(c)\varphi_2(1-c)$$

be the corresponding Jacobi sum. If $\varphi_1 \cdot \varphi_2 \neq 1$ then

$$\iota(\varphi_1, \varphi_2) = \frac{\tau(\varphi_1)\tau(\varphi_2)}{\tau(\varphi_1\varphi_2)}. \tag{2}$$

For each natural number $m \geq 1$ let $\zeta_m := \exp \frac{2\pi i}{m}$ and let $\mu_m := \{\zeta_m^l \mid 0 \leq l \leq m-1\}$ be the group of complex m-th roots of unity.

Proposition 3. *If* $q \equiv 1(\bmod 9)$ *then*

$$N_1 = q + 1 - \mathrm{Tr}_{\,\mathbb{Q}(\zeta_9)/\mathbb{Q}}(\eta),$$

where

$$\eta := \psi^4(a)\iota(\psi^3, \psi),$$

ψ *a character of* k^* *of order* 9.

The number of elements of a finite set X is denoted by $|X|$. It holds

Lemma 1. *Let $k = \mathbb{F}_q$ be a finite field of characteristic $p \neq 3$, and let ξ be a generator of the cyclic multiplicative group k^*. If $B(x) \in k[x]$ is a polynomial with a simple root $x_1 \in k$:*

$$B(x) = (x - x_1)B_1(x), B_1(x) \in k[x], B_1(x_1) \neq 0,$$

then the number of solutions in k of the equation

$$y^3 = B(x)$$

is

$$N = \frac{1}{3}(|\mathcal{A}_{11}| + |\mathcal{A}_{\xi\xi^2}| + |\mathcal{A}_{\xi^2\xi}|),$$

where

$$\mathcal{A}_{11} := \{(t, u) \in k \times k \mid B_1(t^3 + x_1) = u^3\},$$
$$\mathcal{A}_{\xi\xi^2} := \{(t, u) \in k \times k \mid B_1(\xi t^3 + x_1) = \xi^2 u^3\},$$
$$\mathcal{A}_{\xi^2\xi} := \{(t, u) \in k \times k \mid B_1(\xi^2 t^3 + x_1) = \xi u^3\}.$$

P r o o f: I) The case $q \equiv 1(\bmod 3)$. Let χ be a character of k^* of order 3 such that

$$\chi(\xi) = \omega = e^{\frac{2\pi i}{3}}.$$

Put $\chi(0) := 0$. It holds

$$N = q + \alpha + \bar{\alpha},$$

with

$$\alpha = \sum_{c \in k} \chi(B(c)) = \sum_{c \in k} \chi((c - x_1)B_1(c)) = \sum_{c \in k} \chi(c - x_1)\chi(B_1(c)) =$$

$$= \sum_{i,j=0}^{2} \sum_{c \in A, \chi(c-x_1)=\omega^i, \chi(B_1(c))=\omega^j} \omega^{i+j} =$$

$$= |A_{11}| + |A_{\omega\omega^2}| + |A_{\omega^2\omega}| + \omega(|A_{1\omega}| + |A_{\omega 1}| + |A_{\omega^2\omega^2}|) +$$
$$+ \omega^2(|A_{1\omega^2}| + |A_{\omega\omega}| + |A_{\omega^2 1}|),$$

where

$$A := \{c \in k \mid B(c) \neq 0\},$$
$$A_{\omega^i\omega^j} = \{c \in A \mid \chi(c - x_1) = \omega^i, \chi(B_1(c)) = \omega^j\},$$

for $i, j = 0, 1, 2$. It follows that

$$\alpha + \bar{\alpha} = 2(|A_{11}| + |A_{\omega\omega^2}| + |A_{\omega^2\omega}|) + (\omega + \omega^2)(|A_{1\omega}| + |A_{\omega 1}| + |A_{\omega^2\omega^2}|) +$$

$$+ (\omega^2 + \omega)(|A_{1\omega^2}| + |A_{\omega\omega}| + |A_{\omega^2 1}|) = 2(|A_{11}| + |A_{\omega\omega^2}| + |A_{\omega^2\omega}|) -$$

$$-(|A_{1\omega}|+|A_{\omega 1}|+|A_{\omega^2\omega^2}|)-(|A_{1\omega^2}|+|A_{\omega\omega}|+|A_{\omega^2 1}|)=$$

$$=3(|A_{11}|+|A_{\omega\omega^2}|+|A_{\omega^2\omega}|)-\sum_{i,j=0}^{2}|A_{\omega^i\omega^j}|=$$

$$3(|A_{11}|+|A_{\omega\omega^2}|+|A_{\omega^2\omega}|)-|A|, \tag{3}$$

since the sets $A_{\omega^i\omega^j}$, $i,j=0,1,2$, form a partition of the set A.
It holds

$$A_{11}=\{c\in A\mid \chi(c-x_1)=1,\chi(B_1(c))=1\}=$$
$$=\{c\in A\mid(\exists)(t,u)\in k^*\times k^*: c-x_1=t^3, B_1(c)=u^3\}.$$

Let

$$\mathcal{B}_{11}:=\{(0,u)\mid u\in k, u^3=B_1(x_1)\}\cup\{(t,0)\mid t\in k, B_1(t^3+x_1)=0\}.$$

The map

$$g_{11}:\mathcal{A}_{11}\setminus\mathcal{B}_{11}\to A_{11}$$
$$g_{11}(t,u):=t^3+x_1$$

is precisely 9:1 : For $c\in A_{11}$ and $(t,u)\in g_{11}^{-1}(c)$ it holds:

$$g_{11}^{-1}(c)=\{(\zeta^i t,\zeta^j u)\mid 0\le i,j\le 2\},$$

where ζ is an element of k^* of order 3, so $|g_{11}^{-1}(c)|=9$. Hence

$$|A_{11}|=\frac{1}{9}|\mathcal{A}_{11}|-\frac{1}{9}|\{c\in k\mid c^3=B_1(x_1)\}|-\frac{1}{9}|\{c\in k\mid B_1(c^3+x_1)=0\}|. \tag{4}$$

It holds

$$A_{\omega\omega^2}=\{c\in A\mid \chi(c-x_1)=\omega,\chi(B_1(c))=\omega^2\}=$$
$$=\{c\in A\mid(\exists)(t,u)\in k^*\times k^*: c-x_1=\xi t^3, B_1(c)=\xi^2u^3\}.$$

Let

$$\mathcal{B}_{\xi\xi^2}:=\{(0,u)\mid u\in k,\xi^2u^3=B_1(x_1)\}\cup\{(t,0)\mid t\in k, B_1(\xi t^3+x_1)=0\}.$$

The map

$$g_{\omega\omega^2}:\mathcal{A}_{\xi\xi^2}\setminus\mathcal{B}_{\xi\xi^2}\to A_{\omega\omega^2}$$
$$g_{\omega\omega^2}(t,u):=\xi t^3+x_1$$

is also precisely 9:1 : For $c\in A_{\omega\omega^2}$ and $(t,u)\in g_{\omega\omega^2}^{-1}(c)$ it holds:

$$g_{\omega\omega^2}^{-1}(c)=\{(\zeta^i t,\zeta^j u)\mid 0\le i,j\le 2\},$$

so $|g^{-1}_{\omega\omega^2}(c)| = 9$. Hence

$$|A_{\omega\omega^2}| = \frac{1}{9}|\mathcal{A}_{\xi\xi^2}| - \frac{1}{9}|\{c \in k \mid \xi^2 c^3 = B_1(x_1)\}| -$$

$$-\frac{1}{9}|\{c \in k \mid B_1(\xi c^3 + x_1) = 0\}|. \tag{5}$$

Analogously:

$$|A_{\omega^2\omega}| = \frac{1}{9}|\mathcal{A}_{\xi^2\xi}| - \frac{1}{9}|\{c \in k \mid \xi c^3 = B_1(x_1)\}| -$$

$$-\frac{1}{9}|\{c \in k \mid B_1(\xi^2 c^3 + x_1) = 0\}|. \tag{6}$$

From (3), (4), (5) and (6) it follows that

$$\alpha + \bar{\alpha} = 3(|A_{11}| + |A_{\omega\omega^2}| + |A_{\omega^2\omega}|) - |A| =$$

$$= \frac{1}{3}(|\mathcal{A}_{11}| + |\mathcal{A}_{\xi\xi^2}| + |\mathcal{A}_{\xi^2\xi}|) -$$

$$-\frac{1}{3}(|\{c \in k \mid c^3 = B_1(x_1)\}| + |\{c \in k \mid \xi c^3 = B_1(x_1)\}| +$$

$$+|\{c \in k \mid \xi^2 c^3 = B_1(x_1)\}|) -$$

$$-\frac{1}{3}(|\{c \in k \mid B_1(c^3 + x_1) = 0\}| + |\{c \in k \mid B_1(\xi c^3 + x_1) = 0\}| +$$

$$+|\{c \in k \mid B_1(\xi^2 c^3 + x_1) = 0\}|) - |A| =$$

$$= \frac{1}{3}(|\mathcal{A}_{11}| + |\mathcal{A}_{\xi\xi^2}| + |\mathcal{A}_{\xi^2\xi}|) - 1 - |\{d \in k \mid B_1(d) = 0\}| - |A|.$$

It holds

$$|A| = q - |\{c \in k \mid B(c) = 0\}| = q - 1 - |\{d \in k \mid B_1(d) = 0\}|,$$

hence

$$\alpha + \bar{\alpha} = \frac{1}{3}(|\mathcal{A}_{11}| + |\mathcal{A}_{\xi\xi^2}| + |\mathcal{A}_{\xi^2\xi}|) - q$$

and

$$N = q + \alpha + \bar{\alpha} = \frac{1}{3}(|\mathcal{A}_{11}| + |\mathcal{A}_{\xi\xi^2}| + |\mathcal{A}_{\xi^2\xi}|).$$

II) The case $q \equiv 2(\bmod 3)$. Each element of k has one and only one third root in k. It holds

$$N = q,\ |\mathcal{A}_{11}| = |\mathcal{A}_{\xi\xi^2}| = |\mathcal{A}_{\xi^2\xi}| = q. \square$$

P r o o f of Proposition 3: The polynomial $B(x) = x^4 - ax = x(x^3 - ax)$ has the root $x_1 = 0$ in k. Let $B_1(x) := x^3 - a \in k[x]$. With the notations of Lemma 1 it holds:

$$\mathcal{A}_{11} = \{(t,u) \in k \times k \mid B_1(t^3 + x_1) = u^3\} = \{(t,u) \in k \times k \mid -u^3 + t^9 = a\},$$

$$\mathcal{A}_{\xi\xi^2} = \{(t,u) \in k \times k \mid -\xi^2 u^3 + \xi^3 t^9 = a\},$$

$$\mathcal{A}_{\xi^2\xi} = \{(t,u) \in k \times k \mid -\xi u^3 + \xi^6 t^9 = a\}.$$

The equation

$$a_1 u^3 + a_2 t^9 = a_3$$

with $a_1, a_2, a_3 \in k \setminus \{0\}$ has by ([Da-Ha], 6.2 and 6.5)

$$N(a_1, a_2, a_3) =$$

$$= q - \psi^3(-\frac{a_1}{a_2}) - \psi^6(-\frac{a_1}{a_2}) - \sum_{\chi^\mu \neq 1, \psi^\nu \neq 1, \chi^\mu \psi^\nu \neq 1} \frac{\tau_{a_1}(\chi^\mu)\tau_{a_2}(\psi^\nu)}{\tau_{a_3}(\chi^\mu \psi^\nu)} =$$

$$= q - \chi(-\frac{a_1}{a_2}) - \chi^2(-\frac{a_1}{a_2}) - \sum_{1 \le \mu \le 2} \sum_{1 \le \nu \le 8, 3\mu + \nu \neq 9} \frac{\tau_{a_1}(\psi^{3\mu})\tau_{a_2}(\psi^\nu)}{\tau_{a_3}(\psi^{3\mu+\nu})} =$$

$$= q - \chi(-\frac{a_1}{a_2}) - \chi^2(-\frac{a_1}{a_2}) - \sum_{\nu=1, \nu \neq 6}^{8} \frac{\tau_{a_1}(\psi^3)\tau_{a_2}(\psi^\nu)}{\tau_{a_3}(\psi^{3+\nu})} - \sum_{\nu=1, \nu \neq 3}^{8} \frac{\tau_{a_1}(\psi^6)\tau_{a_2}(\psi^\nu)}{\tau_{a_3}(\psi^{6+\nu})}$$

solutions in k. Hence

$$|\mathcal{A}_{11}| = N(-1, 1, a) = q - 2 - \sum_{\nu=1, \nu \neq 6}^{8} \frac{\tau_{-1}(\psi^3)\tau_1(\psi^\nu)}{\tau_a(\psi^{3+\nu})} -$$

$$- \sum_{\nu=1, \nu \neq 3}^{8} \frac{\tau_{-1}(\psi^6)\tau_1(\psi^\nu)}{\tau_a(\psi^{6+\nu})},$$

$$|\mathcal{A}_{\xi\xi^2}| = N(-\xi^2, \xi^3, a) =$$

$$= q - \chi(\xi^{-1}) - \chi^2(\xi^{-1}) - \sum_{\nu=1, \nu \neq 6}^{8} \frac{\tau_{-\xi^2}(\psi^3)\tau_{\xi^3}(\psi^\nu)}{\tau_a(\psi^{3+\nu})} -$$

$$- \sum_{\nu=1, \nu \neq 3}^{8} \frac{\tau_{-\xi^2}(\psi^6)\tau_{\xi^3}(\psi^\nu)}{\tau_a(\psi^{6+\nu})} =$$

$$= q + 1 - \sum_{\nu=1, \nu \neq 6}^{8} \frac{\tau_{-\xi^2}(\psi^3)\tau_{\xi^3}(\psi^\nu)}{\tau_a(\psi^{3+\nu})} - \sum_{\nu=1, \nu \neq 3}^{8} \frac{\tau_{-\xi^2}(\psi^6)\tau_{\xi^3}(\psi^\nu)}{\tau_a(\psi^{6+\nu})}$$

and

$$|\mathcal{A}_{\xi^2\xi}| = N(-\xi, \xi^6, a) =$$

$$q-\chi(\xi^{-5})-\chi^2(\xi^{-5})-\sum_{\nu=1,\nu\neq 6}^{8}\frac{\tau_{-\xi}(\psi^3)\tau_{\xi^6}(\psi^\nu)}{\tau_a(\psi^{3+\nu})}-\sum_{\nu=1,\nu\neq 3}^{8}\frac{\tau_{-\xi}(\psi^6)\tau_{\xi^6}(\psi^\nu)}{\tau_a(\psi^{6+\nu})}=$$

$$=q+1-\sum_{\nu=1,\nu\neq 6}^{8}\frac{\tau_{-\xi}(\psi^3)\tau_{\xi^6}(\psi^\nu)}{\tau_a(\psi^{3+\nu})}-\sum_{\nu=1,\nu\neq 3}^{8}\frac{\tau_{-\xi}(\psi^6)\tau_{\xi^6}(\psi^\nu)}{\tau_a(\psi^{6+\nu})}.$$

It follows that

$$|\mathcal{A}_{11}|+|\mathcal{A}_{\xi\xi^2}|+|\mathcal{A}_{\xi^2\xi}|=$$

$$=3q-\sum_{\nu=1,\nu\neq 6}^{8}\frac{\tau_{-1}(\psi^3)\tau_1(\psi^\nu)+\tau_{-\xi^2}(\psi^3)\tau_{\xi^3}(\psi^\nu)+\tau_{-\xi}(\psi^3)\tau_{\xi^6}(\psi^\nu)}{\tau_a(\psi^{3+\nu})}-$$

$$-\sum_{\nu=1,\nu\neq 3}^{8}\frac{\tau_{-1}(\psi^6)\tau_1(\psi^\nu)+\tau_{-\xi^2}(\psi^6)\tau_{\xi^3}(\psi^\nu)+\tau_{-\xi}(\psi^6)\tau_{\xi^6}(\psi^\nu)}{\tau_a(\psi^{6+\nu})}. \tag{7}$$

By (1) it holds

$$\tau_{-1}(\psi^3)\tau_1(\psi^\nu)+\tau_{-\xi^2}(\psi^3)\tau_{\xi^3}(\psi^\nu)+\tau_{-\xi}(\psi^3)\tau_{\xi^6}(\psi^\nu)=\psi^{-3}(-1)\tau(\psi^3)\tau(\psi^\nu)+$$

$$+\psi^{-3}(-1)\psi^{-3\nu-6}(\xi)\tau(\psi^3)\tau(\psi^\nu)+\psi^{-3}(-1)\psi^{-6\nu-3}(\xi)\tau(\psi^3)\tau(\psi^\nu)=$$

$$=\tau(\psi^3)\tau(\psi^\nu)(1+\psi^{-3\nu-6}(\xi)+\psi^{-6\nu-3}(\xi))=$$

$$=\tau(\psi^3)\tau(\psi^\nu)(1+\chi^{-\nu-2}(\xi)+\chi^{-2\nu-1}(\xi))=$$

$$=\tau(\psi^3)\tau(\psi^\nu)(1+\omega^{-\nu-2}+\omega^{2(-\nu-2)}),$$

so

$$\sum_{\nu=1,\nu\neq 6}^{8}\frac{\tau_{-1}(\psi^3)\tau_1(\psi^\nu)+\tau_{-\xi^2}(\psi^3)\tau_{\xi^3}(\psi^\nu)+\tau_{-\xi}(\psi^3)\tau_{\xi^6}(\psi^\nu)}{\tau_a(\psi^{3+\nu})}=$$

$$=3\frac{\tau(\psi^3)\tau(\psi)}{\tau_a(\psi^4)}+3\frac{\tau(\psi^3)\tau(\psi^4)}{\tau_a(\psi^7)}+3\frac{\tau(\psi^3)\tau(\psi^7)}{\tau_a(\psi)}. \tag{8}$$

Analogously:

$$\tau_{-1}(\psi^6)\tau_1(\psi^\nu)+\tau_{-\xi^2}(\psi^6)\tau_{\xi^3}(\psi^\nu)+\tau_{-\xi}(\psi^6)\tau_{\xi^6}(\psi^\nu)=\psi^{-6}(-1)\tau(\psi^6)\tau(\psi^\nu)+$$

$$+\psi^{-6}(-1)\psi^{-3\nu-12}(\xi)\tau(\psi^6)\tau(\psi^\nu)+\psi^{-6}(-1)\psi^{-6\nu-6}(\xi)\tau(\psi^6)\tau(\psi^\nu)=$$

$$=\tau(\psi^6)\tau(\psi^\nu)(1+\psi^{-3\nu-12}(\xi)+\psi^{-6\nu-6}(\xi))=$$

$$=\tau(\psi^6)\tau(\psi^\nu)(1+\chi^{-\nu-4}(\xi)+\chi^{-2\nu-2}(\xi))=$$

$$=\tau(\psi^6)\tau(\psi^\nu)(1+\omega^{-\nu-1}+\omega^{2(-\nu-1)}),$$

so
$$\sum_{\nu=1,\nu\neq 3}^{8}\frac{\tau_{-1}(\psi^6)\tau_1(\psi^\nu)+\tau_{-\xi^2}(\psi^6)\tau_{\xi^3}(\psi^\nu)+\tau_{-\xi}(\psi^6)\tau_{\xi^6}(\psi^\nu)}{\tau_a(\psi^{6+\nu})}=$$

$$=3\frac{\tau(\psi^6)\tau(\psi^2)}{\tau_a(\psi^8)}+3\frac{\tau(\psi^6)\tau(\psi^5)}{\tau_a(\psi^2)}+3\frac{\tau(\psi^6)\tau(\psi^8)}{\tau_a(\psi^5)}. \qquad (9)$$

By (7), (8) and (9) it holds

$$|\mathcal{A}_{11}|+|\mathcal{A}_{\xi\xi^2}|+|\mathcal{A}_{\xi^2\xi}|=3q-3\frac{\tau(\psi^3)\tau(\psi)}{\tau_a(\psi^4)}-3\frac{\tau(\psi^3)\tau(\psi^4)}{\tau_a(\psi^7)}-3\frac{\tau(\psi^3)\tau(\psi^7)}{\tau_a(\psi)}-$$

$$-3\frac{\tau(\psi^6)\tau(\psi^2)}{\tau_a(\psi^8)}-3\frac{\tau(\psi^6)\tau(\psi^5)}{\tau_a(\psi^2)}-3\frac{\tau(\psi^6)\tau(\psi^8)}{\tau_a(\psi^5)},$$

by Lemma 1

$$N=q-\frac{\tau(\psi^3)\tau(\psi)}{\tau_a(\psi^4)}-\frac{\tau(\psi^3)\tau(\psi^4)}{\tau_a(\psi^7)}-\frac{\tau(\psi^3)\tau(\psi^7)}{\tau_a(\psi)}-$$

$$-\frac{\tau(\psi^6)\tau(\psi^2)}{\tau_a(\psi^8)}-\frac{\tau(\psi^6)\tau(\psi^5)}{\tau_a(\psi^2)}-\frac{\tau(\psi^6)\tau(\psi^8)}{\tau_a(\psi^5)}=$$

$$=q-\psi^4(a)\iota(\psi^3,\psi)-\psi^7(a)\iota(\psi^3,\psi^4)-\psi(a)\iota(\psi^3,\psi^7)-$$

$$-\psi^8(a)\iota(\psi^6,\psi^2)-\psi^2(a)\iota(\psi^6,\psi^5)-\psi^5(a)\iota(\psi^6,\psi^8),$$

by (1) and (2).

Let A be the automorphism of the field extension $\mathbb{Q}(\zeta_9)/\mathbb{Q}$ defined by $\zeta_9^A:=\zeta_9^2$. It holds

$$\eta^A=(\psi^4(a)\iota(\psi^3,\psi))^A=(\psi^4(a))^A(-\sum_{c\in k}\psi^3(c)\psi(1-c))^A=$$

$$=\psi^8(a)(-\sum_{c\in k}\psi^6(c)\psi^2(1-c))=\psi^8(a)\iota(\psi^6,\psi^2),$$

$$\eta^{A^2}=(\psi^4(a)\iota(\psi^3,\psi))^{A^2}=(\psi^4(a))^{A^2}(-\sum_{c\in k}\psi^3(c)\psi(1-c))^{A^2}=$$

$$=\psi^7(a)(-\sum_{c\in k}\psi^3(c)\psi^4(1-c))=\psi^7(a)\iota(\psi^3,\psi^4),$$

$$\eta^{A^3}=(\psi^4(a)\iota(\psi^3,\psi))^{A^3}=(\psi^4(a))^{A^3}(-\sum_{c\in k}\psi^3(c)\psi(1-c))^{A^3}=$$

$$=\psi^5(a)(-\sum_{c\in k}\psi^6(c)\psi^8(1-c))=\psi^5(a)\iota(\psi^6,\psi^8),$$

$$\eta^{A^4} = (\psi^4(a)\iota(\psi^3,\psi))^{A^4} = (\psi^4(a))^{A^4}(-\sum_{c\in k}\psi^3(c)\psi(1-c))^{A^4} =$$

$$= \psi(a)(-\sum_{c\in k}\psi^3(c)\psi^7(1-c)) = \psi(a)\iota(\psi^3,\psi^7),$$

$$\eta^{A^5} = (\psi^4(a)\iota(\psi^3,\psi))^{A^5} = (\psi^4(a))^{A^5}(-\sum_{c\in k}\psi^3(c)\psi(1-c))^{A^5} =$$

$$= \psi^2(a)(-\sum_{c\in k}\psi^6(c)\psi^5(1-c)) = \psi^2(a)\iota(\psi^6,\psi^5),$$

hence

$$N = q - \eta - \eta^A - \eta^{A^2} - \eta^{A^3} - \eta^{A^4} - \eta^{A^5} = q - \mathrm{Tr}_{\mathbb{Q}(\zeta_9)/\mathbb{Q}}(\eta).\Box$$

Corollary 2. *If* $q \equiv 4(\bmod 9)$ *or* $q \equiv 7(\bmod 9)$ *then*

$$L_{C_a}(t) = 1 - \frac{1}{3}\mathrm{Tr}_{\mathbb{Q}(\zeta_9)/\mathbb{Q}}(\eta)t^3 + q^3t^6,$$

where $\eta = \psi^4(a)\iota(\psi^3,\psi)$, ψ *a character of order* 9 *of the multiplicative group of the field* $\mathbb{F}_{q^3}$.
If $q \equiv 8(\bmod 9)$ *then*

$$L_{C_a}(t) = 1 - \frac{1}{2}\mathrm{Tr}_{\mathbb{Q}(\zeta_9)/\mathbb{Q}}(\eta)t^2 - q\frac{1}{2}\mathrm{Tr}_{\mathbb{Q}(\zeta_9)/\mathbb{Q}}(\eta)t^4 + q^3t^6,$$

where $\eta = \psi^4(a)\iota(\psi^3,\psi)$, ψ *a character of order* 9 *of the multiplicative group of the field* $\mathbb{F}_{q^2}$.

P r o o f: If $q \equiv 4(\bmod 9)$ or $q \equiv 7(\bmod 9)$ then $q^2 \equiv 7(\bmod 9)$ or $q^2 \equiv 4(\bmod 9)$ and $q^3 \equiv 1(\bmod 9)$. By proposition 2 it holds $N_1 = q+1$ and $N_2 = q^2+1$, so the coefficients a_1 and a_2 of $L_{C_a}(t)$ vanish and the coefficient a_3 equals $\frac{1}{3}(N_3 - q^3 - 1)$, which by proposition 3 equals $-\frac{1}{3}\mathrm{Tr}_{\mathbb{Q}(\zeta_9)/\mathbb{Q}}(\eta)$.
If $q \equiv 8(\bmod 9)$ then $q^2 \equiv 1(\bmod 9)$ and $q^3 \equiv 2(\bmod 9)$. By proposition 1 it holds $N_1 = q+1$ and $N_3 = q^3+1$, so $a_1 = 0$, $a_3 = 0$ and a_2 equals $\frac{1}{2}(N_2 - q^2 - 1)$, which by proposition 3 equals $-\frac{1}{2}\mathrm{Tr}_{\mathbb{Q}(\zeta_9)/\mathbb{Q}}(\eta)$. $\Box$

Remark 1. Corollary 2 explains some computations done in ([CER]).

Proposition 4. *If* $q \equiv 1(\bmod 9)$ *then*

$$L_{C_a}(t) = (1-\eta t)(1-\eta^A t)(1-\eta^{A^2}t)(1-\eta^{A^3}t)(1-\eta^{A^4}t)(1-\eta^{A^5}t),$$

where $\eta = \psi^4(a)\iota(\psi^3,\psi)$, ψ *a character of order* 9 *of the multiplicative group* k^*, A *the automorphism of the field extension* $\mathbb{Q}(\zeta_9)/\mathbb{Q}$ *defined by* $\zeta_9^A := \zeta_9^2$.

P r o o f: The L-polynomial of the curve C_a/k can be written in the form $L_{C_a}(t) = \prod_{j=1}^{6}(1-\alpha_j t)$, where $\alpha_1, \dots, \alpha_6$ are algebraic integers. For $r \geq 1$ it holds

$$N_r = q^r + 1 - \sum_{j=1}^{6} \alpha_j^r \tag{10}$$

Let ψ be a character of order 9 of the cyclic group k^*. The map

$$\psi_r : \mathbb{F}_{q^r}^* \to \mathbb{C}^*, \psi_r(x) := \psi(N_{\mathbb{F}_{q^r}|\mathbb{F}_q}(x))$$

is a character of order 9 of the cyclic group $\mathbb{F}_{q^r}^*$. It holds ([Da-Ha],0.8)

$$\tau_d^{(r)}(\psi_r^l) = \tau_d(\psi^l)^r \tag{11}$$

for $1 \leq l \leq 8$ and $d \in \mathbb{F}_q^*$, where $\tau_d^{(r)}(\psi_r^l)$ denotes the Gauss sum of the character ψ_r^l on $\mathbb{F}_{q^r}$.
By Proposition 4 it holds

$$N_r = q^r + 1 - \frac{\tau^{(r)}(\psi_r^3)\tau^{(r)}(\psi_r)}{\tau_a^{(r)}(\psi_r^4)} - \frac{\tau^{(r)}(\psi_r^3)\tau^{(r)}(\psi_r^4)}{\tau_a^{(r)}(\psi_r^7)} - \frac{\tau^{(r)}(\psi_r^3)\tau^{(r)}(\psi_r^7)}{\tau_a^{(r)}(\psi_r)} -$$

$$- \frac{\tau^{(r)}(\psi_r^6)\tau^{(r)}(\psi_r^2)}{\tau_a^{(r)}(\psi_r^8)} - \frac{\tau^{(r)}(\psi_r^6)\tau^{(r)}(\psi_5)}{\tau_a^{(r)}(\psi_r^2)} - \frac{\tau^{(r)}(\psi_r^6)\tau^{(r)}(\psi_r^8)}{\tau_a^{(r)}(\psi_r^5)},$$

hence by (11)

$$N_r = q^r + 1 - \frac{\tau(\psi^3)^r\tau(\psi)^r}{\tau_a(\psi^4)^r} - \frac{\tau(\psi^3)^r\tau(\psi^4)^r}{\tau_a(\psi^7)^r} - \frac{\tau(\psi^3)^r\tau(\psi^7)^r}{\tau_a(\psi)^r} -$$

$$- \frac{\tau(\psi^6)^r\tau(\psi^2)^r}{\tau_a(\psi^8)^r} - \frac{\tau(\psi^6)^r\tau(\psi^5)^r}{\tau_a(\psi^2)^r} - \frac{\tau(\psi^6)^r\tau(\psi^8)^r}{\tau_a(\psi^5)^r},$$

so one can choose in (10)

$$\alpha_1 = \frac{\tau(\psi^3)\tau(\psi)}{\tau_a(\psi^4)} = \eta, \alpha_2 = \frac{\tau(\psi^3)\tau(\psi^4)}{\tau_a(\psi^7)} = \eta^{A^2}, \alpha_3 = \frac{\tau(\psi^3)\tau(\psi^7)}{\tau_a(\psi)} = \eta^{A^4},$$

$$\alpha_4 = \frac{\tau(\psi^6)\tau(\psi^8)}{\tau_a(\psi^5)} = \eta^{A^3}, \alpha_5 = \frac{\tau(\psi^6)\tau(\psi^5)}{\tau_a(\psi^2)} = \eta^{A^5}, \alpha_6 = \frac{\tau(\psi^6)\tau(\psi^2)}{\tau_a(\psi^8)} = \eta^{A}. \square$$

Let $m \geq 1$ be a natural number and let K be an algebraic number field with ring of integers $\mathcal{O}_K$ such that $\zeta_m \in \mathcal{O}_K$. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ not dividing m, and let $x \in \mathcal{O}_K$ not divisible by $\mathfrak{p}$. The number $x^{\frac{N_{K/\mathbb{Q}}(\mathfrak{p})-1}{m}}$ is congruent modulo $\mathfrak{p}$ to one and only one root of unity $\zeta_m^l \in \mu_m$. The map

$$(\mathcal{O}_K/\mathfrak{p}) \setminus \{0\} \to \mu_m, x \bmod \mathfrak{p} \mapsto \zeta_m^l$$

is a character of order m of the multiplicative group of the finite field $\mathcal{O}_K/\mathfrak{p}$ called the m-th power residue character modulo $\mathfrak{p}$.

Proposition 5. *Let $q \equiv 1(\bmod 9)$ and let $\mathfrak{p}$ be a prime divisor of p in the ring $\mathbb{Z}[\zeta_{q-1}]$. Let ψ be the 9-th power residue character modulo $\mathfrak{p}$ in $\mathbb{Z}[\zeta_{q-1}]$. Identifying the finite field $\mathbb{F}_q$ with the residue class field $\mathbb{Z}[\zeta_{q-1}]/\mathfrak{p}$ it holds:*
a) The absolute value of the complex number $\iota(\psi^3, \psi)$ is

$$|\iota(\psi^3, \psi)| = \sqrt{q};$$

b) The prime ideal decomposition of the principal ideal generated by $\iota(\psi^3, \psi)$ in the ring of integers $\mathbb{Z}[\zeta_9]$ is

$$\iota(\psi^3, \psi)\mathbb{Z}[\zeta_9] = (\mathfrak{q} \cdot \mathfrak{q}^{A^4} \cdot \mathfrak{q}^{A^5})^{f(\mathfrak{p}|\mathfrak{q})},$$

where $\mathfrak{q} := \mathfrak{p} \cap \mathbb{Z}[\zeta_9]$, A is the automorphism of $\mathbb{Q}(\zeta_9)/\mathbb{Q})$ defined by $\zeta_9^A := \zeta_9^2$ and $N_{\mathbb{Q}(\zeta_{q-1})/\mathbb{Q}(\zeta_9)}(\mathfrak{p}) = \mathfrak{q}^{f(\mathfrak{p}|\mathfrak{q})}$.
c) In the ring $\mathbb{Z}[\zeta_9]$ it holds

$$\iota(\psi^3, \psi) \equiv 1(\bmod (\zeta_9 - 1)^4).$$

The number $\iota(\psi^3, \psi) \in \mathbb{Z}[\zeta_9]$ is uniquely determined by the properties a), b) and c).

P r o o f:
a): Every Jacobi sum in a finite field with q elements has absolute value $\sqrt{q}$.
b): By ([Ha1], p.40, (6.)) it holds

$$\iota(\psi^3, \psi)\mathbb{Z}[\zeta_9] = (\mathfrak{q}^{\sum_J d(-3j,-j)J})^{f(\mathfrak{p}|\mathfrak{q})},$$

where J runs over the set $\{A^k \mid 0 \le k \le 5\}$ of automorphisms of $\mathbb{Q}(\zeta_9)$, $j \bmod 9$ is defined by

$$\zeta_9^{J^{-1}} = \zeta_9^j$$

and

$$d(-3j, -j) = \frac{r(-3j) + r(-j) - r(-4j)}{9},$$

$r(x)$ the smallest non-negative residue of $x \bmod 9$. It holds

$$\zeta_9^{(A^0)^{-1}} = \zeta_9,\ d(-3, -1) = \frac{r(-3) + r(-1) - r(-4)}{9} = 1,$$

$$\zeta_9^{(A^1)^{-1}} = \zeta_9^{A^5} = \zeta_9^5,\ d(-15, -5) = \frac{r(-15) + r(-5) - r(-20)}{9} = 0,$$

$$\zeta_9^{(A^2)^{-1}} = \zeta_9^{A^4} = \zeta_9^7,\ d(-21, -7) = \frac{r(-21) + r(-7) - r(-28)}{9} = 0,$$

$$\zeta_9^{(A^3)^{-1}} = \zeta_9^{A^3} = \zeta_9^8,\ d(-24, -8) = \frac{r(-24) + r(-8) - r(-32)}{9} = 0,$$

$$\zeta_9^{(A^4)^{-1}} = \zeta_9^{A^2} = \zeta_9^4,\ d(-12, -4) = \frac{r(-12) + r(-4) - r(-16)}{9} = 1,$$

$$\zeta_9^{(A^5)^{-1}} = \zeta_9^A = \zeta_9^2,\ d(-6,-2) = \frac{r(-6)+r(-2)-r(-8)}{9} = 1,$$

$$\iota(\psi^3,\psi)\mathbb{Z}[\zeta_9] = (\mathfrak{q}^{1+A^4+A^5})^{f(\mathfrak{p}|\mathfrak{q})} = (\mathfrak{q}\cdot\mathfrak{q}^{A^4}\cdot\mathfrak{q}^{A^5})^{f(\mathfrak{p}|\mathfrak{q})}.$$

c): For $c \in \mathbb{F}_q^*$ it holds

$$\psi(c) \equiv 1 \bmod (\zeta_9 - 1)$$

and

$$\psi^3(c) \equiv 1 \bmod (\zeta_9 - 1)^3.$$

Indeed, if $\psi(c) = \zeta_9^k$, $0 \le k \le 8$, then $\psi(c) - 1 = \zeta_9^k - 1$ is divisible by $\zeta_9 - 1$ in $\mathbb{Z}[\zeta_9]$ and $\psi^3(c) - 1$ is divisible by $\zeta_9^3 - 1$ which is associate with $(\zeta_9 - 1)^3$. Then

$$\iota(\psi^3,\psi) = -\sum_{c\in\mathbb{F}_q}\psi^3(c)\psi(1-c) = -\sum_{c\in\mathbb{F}_q}\psi(c)\psi^3(1-c) =$$

$$= -\sum_{c\neq 1}\psi(c) - \sum_{c\neq 0,1}\psi(c)(\psi^3(1-c)-1) =$$

$$= 1 - \sum_{c\neq 0,1}\psi(c)(\psi^3(1-c)-1) \equiv 1 - \sum_{c\neq 0,1}(\psi^3(1-c)-1) \bmod (\zeta_9-1)^4 \equiv$$

$$\equiv 1 - \sum_{c\neq 0,1}\psi^3(1-c) + \sum_{c\neq 0,1} 1 \bmod (\zeta_9-1)^4 \equiv$$

$$\equiv 1 + 1 + q - 2 \bmod (\zeta_9-1)^4 \equiv q \bmod (\zeta_9-1)^4 \equiv 1 \bmod (\zeta_9-1)^4.$$

Two numbers in $\mathbb{Z}[\zeta_9]$ with the same absolute value and the same prime ideal decomposition differ by a root of unity. The group of roots of unity in $\mathbb{Z}[\zeta_9]$ is μ_{18}. The only element of μ_{18} which is $\equiv 1 \bmod (\zeta_9 - 1)^4$ is 1. The properties a), b), c) determine the number $\iota(\psi^3,\psi)$ in $\mathbb{Z}[\zeta_9]$. □

2 The curves $C_a : Y^3 = X^4 - aX$ over an algebraic number field

Let k be an algebraic number field which contains ζ_9. Let $a \in k^*$, and let $\mathfrak{m}_a$ be the product of 3 and of all prime divisors $\mathfrak{p}$ of k which appear in the decomposition of a. Let $\mathfrak{p}$ be a prime divisor of k which does not divide $\mathfrak{m}_a$. The curve C_a has good reduction at $\mathfrak{p}$: By reducing modulo $\mathfrak{p}$ the equation $y^3 = x^4 - ax$ one obtains a curve $C_{a(\mathfrak{p})}$ over the residue class field $k(\mathfrak{p})$ at $\mathfrak{p}$ with the equation

$$C_{a(\mathfrak{p})} : y^3 = x^4 - a(\mathfrak{p})x, a(\mathfrak{p}) := a \bmod \mathfrak{p} \in k(\mathfrak{p})^*$$

which is smooth of genus 3 over $k(\mathfrak{p})$. Let $L_{C_{a(\mathfrak{p})}}(t)$ be the L-polynomial of $C_{a(\mathfrak{p})}/k(\mathfrak{p})$. By proposition 4 it holds

$$L_{C_a}(t) = \prod_{j=0}^{5}(1 - \eta(\mathfrak{p})^{A^j} t),$$

where $\eta(\mathfrak{p}) := {\psi_\mathfrak{p}}^4(a(\mathfrak{p}))\iota({\psi_\mathfrak{p}}^3, \psi_\mathfrak{p})$, $\psi_\mathfrak{p}$ the 9-th power residue character modulo $\mathfrak{p}$, A the automorphism of the field extension $\mathbb{Q}(\zeta_9)/\mathbb{Q}$ defined by $\zeta_9^A := \zeta_9^2$.

The *L-function of C_a over k* is defined by

$$L(s, C_a, k) := \prod_{(\mathfrak{p}, \mathfrak{m}_a)=1} L_{C_{a(\mathfrak{p})}}(N(\mathfrak{p})^{-s}). \tag{12}$$

The product on the right hand side of (12) is absolutely convergent for $\Re s > \frac{3}{2}$ ([Ha1], [We], [De]). It holds

$$L(s, C_a, k) = \prod_{j=0}^{5} L_j(s),$$

where

$$L_j(s) := \prod_{(\mathfrak{p}, \mathfrak{m}_a)=1} (1 - \eta(\mathfrak{p})^{A^j} N(\mathfrak{p})^{-s}), \tag{13}$$

for $j = 0, \dots, 5$. Extend the function $\eta(\mathfrak{p})$ multiplicatively on the group $\mathrm{Div}_{\mathfrak{m}_a} k$ of divisors of k prime to $\mathfrak{m}_a$ and define

$$\lambda_j : \mathrm{Div}_{\mathfrak{m}_a} k \mapsto \mathbb{C}^*, \lambda_j(\mathfrak{a}) := \frac{\eta(\mathfrak{a})^{A^j}}{\sqrt{N(\mathfrak{a})}},$$

for $j = 0, \dots, 5$. The functions $\lambda_0, \dots, \lambda_5$ are *Grössencharaktere* of k ([Ha1], [We]) in the sense of Hecke ([He]). Let $\mathrm{Div}^+_{\mathfrak{m}_a} k$ denote the set of positive divisors in $\mathrm{Div}_{\mathfrak{m}_a} k$. By (13) it holds for $\Re s > \frac{3}{2}$

$$L_j(s)^{-1} = \prod_{(\mathfrak{p}, \mathfrak{m}_a)=1} (1 - \lambda_j(\mathfrak{p}) N(\mathfrak{p})^{-s+\frac{1}{2}})^{-1} =$$

$$= \sum_{\mathfrak{a} \in \mathrm{Div}^+_{\mathfrak{m}_a} k} \frac{\lambda_j(\mathfrak{a})}{N(\mathfrak{a})^{s-\frac{1}{2}}} = L(s - \frac{1}{2}, \lambda_j, k),$$

where

$$L(s, \lambda_j, k) := \sum_{\mathfrak{a} \in \mathrm{Div}^+_{\mathfrak{m}_a} k} \frac{\lambda_j(\mathfrak{a})}{N(\mathfrak{a})^s}, \Re s > 1,$$

is the Hecke L-function corresponding to λ_j, $j = 0, \dots, 5$. So

Theorem 1. *The L-function $L(s, C_a, k)$ of the curve C_a over k equals the product of the inverses of Hecke L-functions $L(s - \frac{1}{2}, \lambda_j, k)$, $j = 0, \dots, 5$.*

3 The curves $C_a \ : Y^3 = X^4 - aX$ over $\mathbb{C}$

A complex *Picard curve* is the projective closure of an affine plane curve of equation type $Y^3 = p_4(X)$, where $p_4(X)$ is a polynomial of degree 4. We exclude all polynomials $p_4(X)$ with only one zero. So one avoids unstable curves in order to get a compact algebraic moduli space $\hat{M}$ of (isomorphy classes of semistable) Picard curves, which we choose in a very canonical way. Smooth Picard curves have genus 3. They correspond to a Zariski-open part $M^{\#}$ of $\hat{M}$. Let $K = \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\omega)$, $\omega := e^{\frac{2\pi i}{3}}$, be the field of Eisenstein numbers. The cyclic group $\mathbb{Z}/3\mathbb{Z}$ of order 3 acts via $(x, y) \mapsto (x, \omega y)$ on each Picard curve C. If C is smooth, we get $\mathbb{P}^1$ as quotient curve $C/(\mathbb{Z}/3\mathbb{Z})$ with $\mathbb{Z}/3\mathbb{Z}$ as Galois group of $C \,/\, \mathbb{P}^1$. The action of $\mathbb{Z}/3\mathbb{Z}$ induces a K-multiplication of type $(2, 1)$ on the jacobian variety $J(C)$ of C, which means that the diagonalized representation group of $\mathbb{Z}/3\mathbb{Z}$ on the tangent space $T_0J(C)$ of $J(C)$ is generated by $\begin{pmatrix} \omega & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \bar{\omega} \end{pmatrix}$. Let

$$\mathbb{B} := \{z = (z_1, z_2) \in \mathbb{C}^2;\ |z|^2 \ := |z_1|^2 + |z_2|^2 < 1\},$$

be the two-dimensional complex unit ball. The moduli space of abelian threefolds with K-multiplication of type $(2, 1)$ is the Shimura surface $\mathbb{B}/\Gamma$, $\Gamma = \mathbb{U}((2, 1), \mathfrak{O})$, $\mathfrak{O} = \mathfrak{O}_K = \mathbb{Z} + \mathbb{Z}\omega$ the ring of Eisenstein integers. Define the congruence subgroup $\Gamma(\sqrt{-3})$ by the exact group sequence

$$1 \longrightarrow \Gamma(\sqrt{-3}) \longrightarrow \Gamma \longrightarrow \mathbb{U}((2, 1), \mathfrak{O}/(1 - \omega)\mathfrak{O}) \longrightarrow 1.$$

In ([Ho1], Ch. I, Prop. 3.2.3) it is proved the following

Theorem 2. *The Baily-Borel compactification* $\widehat{\mathbb{B}/\Gamma(\sqrt{-3})}$ *coincides with the projective plane* $\mathbb{P}^2$*. The compactifying cusp points are four points* $K_1, K_2, K_3, K_4 \in \mathbb{P}^2$ *in general position. The open part* $\mathbb{P}_2^{\#} \subset \mathbb{P}^2$ *coming from smooth Picard curves is precisely the complement of the six projective lines* $L_{ij} = L_{ji}$ *going through pairs* K_i, K_j *of different cusp points.*

It turns out that

$$M^{\#} = \mathbb{P}_2^{\#}/S_4\ ,\ \hat{M} = \mathbb{P}^2/S_4\ ,\ M = \mathbb{P}_2^*/S_4,$$

where $\mathbb{P}_2^* := \mathbb{P}^2 \setminus \{K_1, K_2, K_3, K_4\}$. Now identify $\mathbb{P}^2$ with

$$\mathbb{P}_0^3 = \{(t_1 : t_2 : t_3 : t_4) \in \mathbb{P}^3;\ t_1 + t_2 + t_3 + t_4 = 0\},$$

and introduce projective coordinates such that

$$K_1 = (-3 : 1 : 1 : 1),\ K_2 = (1 : -3 : 1 : 1),$$
$$K_3 = (1 : 1 : -3 : 1),\ K_4 = (1 : 1 : 1 : -3).$$

Each Picard curve is isomorphic to a *normal form* representative

$$C_{\mathfrak{t}}:\ Y^3=(X-t_1)(X-t_2)(X-t_3)(X-t_4),\ t_1+t_2+t_3+t_4=0.$$

The correspondence

$$C_{\mathfrak{t}}\mapsto \mathfrak{t}=(t_1,t_2,t_3,t_4)\mapsto (t_1:t_2:t_3:t_4)\in \mathbb{P}_2^*$$

restricted to $\mathbb{P}_2^{\#}$ and composed with the S_4- quotient map yields the precise parametrisation of isomorphy classes ([Ho1] I, Prop.5.2.3). Especially, all curves of the family

$$C_a\ :Y^3=X^4-aX\ ,a\in\mathbb{C}^*,$$

are isomorphic over $\mathbb{C}$ to

$$C_1:\ Y^3=X^4-X,$$

whose moduli point is the image of $(0:1:\omega:\omega^2)$.

The Jacobians of smooth Picard curves are (principally polarized) abelian threefolds. Via period matrices they are represented by points in the generalized Siegel upper half plane

$$\mathbb{H}_3=\{\Omega\in Mat_3(\mathbb{C});\ {}^t\Omega=\Omega\ ,\ Im\,\Omega\, positive\ definite\},$$

uniquely up to $\mathbb{S}p(6,\mathbb{Z})$-equivalence, where

$$\mathbb{S}p(6,\mathbb{Z})=\{G\in\mathbb{G}l_6(\mathbb{Z});\ {}^tG\cdot\left(\begin{smallmatrix}O & E_3\\ -E_3 & O\end{smallmatrix}\right)\cdot G=\left(\begin{smallmatrix}O & E_3\\ -E_3 & O\end{smallmatrix}\right)\},E_3\ :=diag(1,1,1),$$

denotes the symplectic group acting on $\mathbb{H}_3$ in the well-known manner. By Torelli's theorem there is a canonical algebraic embedding $M^{\#}\hookrightarrow\mathfrak{A}_3$ into the moduli space $\mathfrak{A}_3=\mathbb{H}_3/\mathbb{S}p(6,\mathbb{Z})$ of principally polarized abelian threefolds. Restricting to the Zariski-open subspace $\mathfrak{A}_3^{\#}\subset\mathfrak{A}_3$ corresponding to Jacobians of smooth genus 3 curves one gets a closed embedding $M^{\#}\hookrightarrow\mathfrak{A}_3^{\#}$, which determines $M^{\#}$ uniquely, up to isomorphy. The closed algebraic embedding $M^{\#}\hookrightarrow\mathfrak{A}_3^{\#}$ can be *uniformized* in the following sense. In the analytic category there is a commutative *Shimura diagram*

$$\begin{array}{cccccc}
\mathbb{B} & & \hookrightarrow & & \mathbb{H}_3\\
 & \nwarrow & & \nearrow & \\
 & \mathbb{B}^{\#} & \hookrightarrow & \mathbb{H}_3^{\#} & \\
\downarrow & \downarrow & & \downarrow & \downarrow\\
 & M^{\#} & \hookrightarrow & \mathfrak{A}_3^{\#} & \\
 & \swarrow & & \searrow & \\
M & & \rightarrow & & \mathfrak{A}_3
\end{array}$$

where $\mathbb{H}_3\longrightarrow\mathfrak{A}_3$ is the $\mathbb{S}p(6,\mathbb{Z})$-quotient morphism, $\mathbb{H}_3^{\#}$is the preimage of $\mathfrak{A}_3^{\#}$ in $\mathbb{H}_3$, $\mathbb{B}\hookrightarrow\mathbb{H}_3$ is a closed embedding, $\mathbb{B}^{\#}=\mathbb{B}\cap\mathbb{H}_3^{\#}$, and $\mathbb{B}\longrightarrow M$ is the analytic quotient morphism of the arithmetic group

$$N_{\mathbb{S}p(6,\mathbb{Z})}(\mathbb{B})\ :=\{G\in\mathbb{S}p(6,\mathbb{Z});\ G(\mathbb{B})=\mathbb{B}\}$$

acting on $\mathbb{B}$. In ([Ho3]) it is proved that this ball lattice coincides with Γ.

Identifying for a moment the ball with its image in $\mathbb{H}_3$ we call $\mathbb{B}$ the *period space of Picard curves* and its points are called *Picard period points* (of the family of Picard curves). An element $\gamma \in \Gamma$ is called *elliptic*, iff γ has an isolated fixed point $P \in \mathbb{B}$. Let Γ' be a subgroup of Γ. We call the elliptic element γ *purely Γ'-elliptic*, iff all non-trivially on $\mathbb{B}$ acting elements of the stationary group Γ'_P are elliptic. The images of purely Γ'-elliptic points on $\mathbb{B}/\Gamma'$ are isolated (cyclic quotient) singularities. Notice that the fixed point P is uniquely determined by the elliptic element γ because the group of biholomorphic automorphisms of $\mathbb{B}$ coincides with $\mathbb{PU}((2,1),\mathbb{C})$, so γ has only one negative eigenline in $V = (\mathbb{C}^3, <.,.>)$ with respect to the hermitian metric $<.,.>$ of signature $(2,1)$ on $\mathbb{C}^3$.
In ([Ho1], Ch. I, 3.4.4) it is proved the following

Theorem 3. *(see [Ho1] I, Prop. 3.4.4). The only singularities of $\hat{M}$ are the image points of $S := (0 : 1 : \omega : \omega^2)$ and $N := (1 : i : -1 : -i)$, along the S_4-quotient morphism.* □

This is a simple application of a theorem of Chevalley stating that the singularities of a finite (more generally: locally finite) Galois quotient X/G of a smooth complex manifold X come precisely from points $x \in X$ with isotropy group G_x not generated by reflections at x, where reflections at x are defined as elements of G_x acting trivially on a submanifold of X through x of codimension 1. Looking at finite subgroups of S_4 and their fixed points on $\mathbb{P}^2$ one finds up to S_4-equivalence the points S, N as only singular possibilities. The S_4-isotropy group of S is generated by the cyclic permutation (234) of order 3. The S_4-isotropy group of N is generated by the cyclic permutation (1234) of order 4. The (13)(24)-reflection line on $\mathbb{P}^2$ contains N.

Proposition 6. *The set of Picard period points of C_1 coincides with the set of purely Γ-elliptic points on $\mathbb{B}$. It coincides with the Γ-orbit of*

$$P_{\zeta_9} := ({\zeta_9}^4 - {\zeta_9}^2 \ : \ 1 \ : \ {\zeta_9}^5 + {\zeta_9}^4 - 1) \in \mathbb{B}.$$

P r o o f: For an arbitrary group G let G_{tor} be the set of elements of finite order of G (torsion elements), and let G_{k-tor} be the subset of elements of precise order $k \in \mathbb{N}_+$. G acts by conjugation on G_k and on G_{tor}. It holds

Lemma 2. *For $\Gamma = \mathbb{U}((2,1),\mathfrak{O})$ the set Γ_{9-tor} is not void. It consists of precisely six Γ-conjugation classes. They are projected onto two $\mathbb{P}\Gamma$-conjugation classes in $(\mathbb{P}\Gamma)_{3-tor}$.*

P r o o f of Lemma 2: For the first statement we consider the element

$$\varphi_1 := \begin{pmatrix} -\omega^2 & -1 & \omega^2 \\ \omega & 1 & 1 \\ 1 & -1 & \omega^2 - 1 \end{pmatrix}$$

with

$$det\,\varphi_1 = \omega\ ,\ \varphi_1^3 = \omega E_3.$$

found by Feustel in [Feu]. It is easy to check that φ_1 belongs to Γ. The eigenvalues are ζ_9, ${\zeta_9}^4$, ${\zeta_9}^7$. The powers φ_1^k, $k = 1, 2, 4, 5, 7, 8$, yield six different conjugation classes in Γ_{9-tor} (compare determinants and eigenvalues) and two conjugation classes in $(\mathbb{P}\Gamma)_{3-tor}$. □

Now let φ be an arbitrary element of Γ_{9-tor} with eigenvalues ζ_9, ${\zeta_9}^j$, ${\zeta_9}^k$, say. The Galois group of $F := K(\zeta_9)$ over K is generated by $\sigma\ :\ \zeta_9 \mapsto {\zeta_9}^4$. The characteristic polynomial $\chi_\varphi(T)$ of φ belongs to $K[T]$. Looking at trace and determinant of φ, which must belong to K, it is easy to see that φ has three different eigenvalues. They must be conjugated over K, hence ${\zeta_9}^j = {\zeta_9}^4 = \sigma(\zeta_9)$, ${\zeta_9}^k = {\zeta_9}^7 = \sigma^2(\zeta_9)$. The eigenvectors $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ of ζ_9, $\sigma(\zeta_9)$, $\sigma^2(\zeta_9)$, respectively, can be choosen in F^3. They form an orthogonal basis of F^3 endowed with our hermitian $(2,1)$-metric because of different eigenvalues. From $\varphi(\mathfrak{a}) = \zeta_9 \cdot \mathfrak{a}$ it follows that

$$\sigma(\varphi(\mathfrak{a})) = \sigma(\zeta_9)\sigma(\mathfrak{a}) = {\zeta_9}^4\sigma(\mathfrak{a})$$

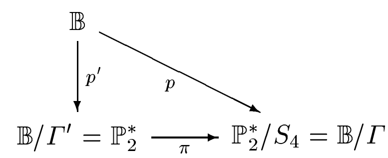
because φ belongs to $Mat_3(K)$. Therefore

$$\mathfrak{a},\ \mathfrak{b} = \sigma(\mathfrak{a}),\ \mathfrak{c} = \sigma^2(\mathfrak{a}) \in F^3,$$

satisfying

$$< \mathfrak{a}, \mathfrak{a} > < 0,\ < \mathfrak{b}, \mathfrak{b} > > 0,\ < \mathfrak{c}, \mathfrak{c} > > 0, \tag{14}$$

(without loss of generality) is an orthogonal φ-eigenbasis of $\mathbb{C}^3$. The elliptic element φ has the unique elliptic fixed point $P = \mathbb{P}\mathfrak{a} \in \mathbb{B}$. We show that P is a purely Γ-elliptic point. With $\Gamma' := \Gamma(\sqrt{-3})$ we have a commutative diagram of quotient morphisms



In [Ho1] I, Prop. 3.4.4, there are listed on $\mathbb{P}_2^*$ the p'- images of all Γ-elliptic points $Q \in \mathbb{B}$ together with their (abstract) isotropy groups Γ_Q. Our P cannot be an intersection point of two Γ-reflection discs because the reflections have eigenvalues only in K. Otherwise $P \in \mathbb{B} \subset \mathbb{P}^2$ would be the intersection point of two projective lines (the projectivized orthogonal complements of the one-dimensional eigenspaces) defined over K. This leads to $\mathbb{P}\mathfrak{a} = P = \mathbb{P}\mathfrak{a}'$, $\mathfrak{a}' \in K^3$, $\sigma(P) = P$, which contradicts to $\sigma(P) \notin \mathbb{B} = \mathbb{P}V_-$, by (14). There are precisely two Γ-orbits $\Gamma\tilde{N}$, $\Gamma\tilde{S}$ of Γ-elliptic points whose isotropy groups are not generated by reflections. The projective isotropy groups $\mathbb{P}\Gamma_{\tilde{N}}$ or $\mathbb{P}\Gamma_{\tilde{S}}$

are cyclic of order 4 or 3, respectively. Since $\mathbb{P}\varphi \in \mathbb{P}\Gamma_P$ is elliptic of order 3 the point P must belong to the second orbit. The image $p(\tilde{S})$ coincides with $p'(S)$, which is an orbitally isolated singularity with respect to Γ. This means that $\tilde{S}$ is a purely Γ-elliptic point, hence $\mathbb{P}\Gamma_{\tilde{S}} \cong <\mathbb{P}\varphi>$ of order 3. □

Let F be a number field and A a complex abelian variety of dimension g. We say that A has F*-multiplication*, if there is a $\mathbb{Q}$-algebra embedding ι of F into the endomorphism algebra $End^\circ A = \mathbb{Q} \otimes End\, A$ of A. If, moreover, the degree $[F : \mathbb{Q}]$ of F is equal to $2g$ and ι is an isomorphism, then A is called an abelian CM-*variety*. It is well-known in this case that A is simple and F is a CM-field, which is, by definition, a totally imaginary quadratic field extension of a totally real number field, see [La]. A CM-curve is a (smooth complex) projective curve C whose jacobian variety $J(C)$ is an abelian CM-variety.

Proposition 7. *The endomorphism ring* $End\, J(C_1)$ *is isomorphic to* $\mathbb{Z}[\zeta_9]$. *Up to isomorphy,* C_1 *is the only Picard CM-curve with a cyclotomic maximal order as endomorphism ring.*

P r o o f: Our special Picard curve $C_1 : Y^3 = X(X^3 - 1)$ has an obvious non-trivial automorphism of 9-th order fixing $\infty = (0 : 0 : 1)$:

$$(x, y) \mapsto (\omega x,\ \zeta_9 y)\ ,\ ({\zeta_9}^3 = \omega).$$

It extends to an automorphism of the Jacobian threefold of C_1. With Theorem 6 below we will see that this automorphism generates a subfield in the endomorphism algebra of the Jacobian. Therefore we get embeddings

$$\mathbb{Z}[\zeta_9] \hookrightarrow End\, J(C_1)\ ,\ F = \mathbb{Q}(\zeta_9) \hookrightarrow End^\circ J(C_1). \tag{15}$$

The representing period point $P_{\zeta_9} = \mathbb{P}\mathfrak{a} \in \mathbb{B}$ is purely Γ-elliptic by Proposition 3, fixed by φ_1 of nine-th order. Therefore the ring $End_K(\mathfrak{a}, \mathfrak{a}^\perp)$ of K-endomorphisms of V with eigenvector $\mathfrak{a}$ and invariant subspace $\mathfrak{a}^\perp$ is bigger than K. Such ball points have been called *exceptional* in [Ho2], Corollary 7.10. Moreover, $\mathfrak{a}$ is eigenvector of a simple eigenvalue of $\varphi_1 \in End_K(\mathfrak{a}, \mathfrak{a}^\perp)$. Therefore P_{ζ_9} is an *isolated exceptional* point in the sense of Definition 7.12 of [Ho2]. The K-degree $[K(P_{\zeta_9}) : K]$ of P_{ζ_9} is equal to 3. Now apply the following theorem to see that $J(C_1)$ is a simple CM-threefold with multiplication field $K(\zeta_9)$.

Theorem 4. (see [Ho2], section 7.) *The endomorphism algebra of the jacobian variety* $J_\tau \cong J(C_t)$ *of a Picard curve with period point* $\tau \in \mathbb{B}$ *and moduli point* $t = (t_1 : t_2 : t_3 : t_4) \in \mathbb{P}_2^*$ *is greater than* K *if and only if* τ *is exceptional.* J_τ *splits up to isogeny into abelian CM- subvarieties if and only if* τ *is an isolated exceptional point. Thereby Jacobians with CM-field* F *(of degree* 3 *over* K*) correspond to isolated exceptional points of* K*-degree* 3 *and* $F \cong K(\tau)$. *All other isolated exceptional points (of* K*-degree* 2 *or* 1*) ly on* K*-discs on* $\mathbb{B}$ *(defined as non-empty intersections* $L \cap \mathbb{B}$, L *projective lines on* $\mathbb{P}^2$ *defined over* K*). Thereby* $\tau \in \mathbb{B}(K)$ *if and only if* J_τ *splits into*

$E \times E \times E$. The degree 2 case happens if and only if J_τ splits into $E \times (E'^2)$, where E is an elliptic CM-curve with K-multiplication and E' elliptic CM with imaginary quadratic multiplication field $L \neq K$. Moreover, it holds that $K(L) = K(\tau)$ in the latter case. $\square$

The endomorphism ring of any abelian CM-variety is an order in the corresponding CM-field. Each order of a number field L is contained in the maximal order, the ring $\mathfrak{O}_L$ of integers in L. The maximal order of a cyclotomic field $L = \mathbb{Q}(\zeta)$ is equal to $\mathbb{Z}[\zeta]$, ζ a generating unit root, see e.g. [Neu], I, Prop. 10.2. So the embeddings (15) must be isomorphisms, especially

$$\mathfrak{O}_F = \mathbb{Z}[\zeta_9] \cong End J(C_1) \subseteq End^\circ J(C_1) \cong F.$$

The first part of Proposition 5 is proved.
F is the only cyclotomic field of degree 3 over K. Therefore the Jacobian threefolds of CM-Picard curves C with cyclotomic endomorphism algebra $End^\circ J(C)$, which must be isomorphic to F, have to be isogeneous. There is a bijective correspondence between the ideal classes of $\mathfrak{O}_F$ and the isomorphy classes of principally polarized abelian CM-threefolds A (of same multiplication type) with endomorphism rings $\mathfrak{O}_F$, see e.g. [La], III.2, Cor. 2.7. It is well-known that the class number of F is equal to 1, see e.g. [Ha2], III, end of 29. Therefore, up to isomorphy, there is only one such A. Then, by Torelli's theorem, also the isomorphy class of Picard CM-curves with $End\, J(C) \cong \mathfrak{O}_F$ is uniquely determined. This completes the proof of Proposition 5. $\square$

Remark 2. The *type* of F-multiplication is a lift (F-extension) from the type $(2,1)$ of K-multiplication on $J(C_1)$. This lifted type is unique by [La], I.3, Theorem 3.6.

Proposition 8. *A period matrix of the Jacobian $J(C_1)$ is:*

$$\varPi = \begin{pmatrix} -\zeta_9+1 & 0 & -2\zeta_9{}^2-2\zeta_9 & -\zeta_9{}^2-1 & 1 & 2\zeta_9{}^2+\zeta_9 \\ \zeta_9{}^2-1 & 0 & -\zeta_9{}^2+2\zeta_9 & -\zeta_9{}^2+\zeta_9+1 & -1 & \zeta_9{}^2-2\zeta_9 \\ -\zeta_9+1 & 0 & -2\zeta_9{}^2-2\zeta_9 & -\zeta_9{}^2-1 & 1 & 2\zeta_9{}^2+\zeta_9 \end{pmatrix} \cdot \omega +$$

$$+ \begin{pmatrix} 2\zeta_9{}^2+\zeta_9+1 & 1 & -\zeta_9+1 & -2\zeta_9{}^2-\zeta_9 & 0 & \zeta_9{}^2+\zeta_9-1 \\ -\zeta_9{}^2+2\zeta_9 & 1 & -2\zeta_9{}^2+2\zeta_9+1 & -\zeta_9+1 & -1 & \zeta_9{}^2-\zeta_9-1 \\ 2\zeta_9{}^2+\zeta_9+1 & 1 & -\zeta_9+1 & -2\zeta_9{}^2-\zeta_9 & 0 & \zeta_9{}^2+\zeta_9-1 \end{pmatrix}.$$

The set of $\mathbb{H}_3$-(Siegel-)period points of $J(C_1)$ coincides with the $\mathbb{S}p(6,\mathbb{Z})$-orbit of

$$\begin{pmatrix} \frac{-2rs-1}{3r^2} & \frac{1}{r} & \frac{rs-1}{3r^2} \\ \frac{1}{r} & -1 & 0 \\ \frac{rs-1}{3r^2} & 0 & \frac{-2rs+2}{3r^2} \end{pmatrix} \cdot \omega + \begin{pmatrix} \frac{2rs-2}{3r^2} & \frac{1}{r} & \frac{-rs+1}{3r^2} \\ \frac{1}{r} & -1 & \frac{-1}{r} \\ \frac{-rs+1}{3r^2} & \frac{-1}{r} & \frac{2rs+1}{3r^2} \end{pmatrix}$$

with

$$r := -\zeta_9{}^4 + \zeta_9{}^3 + 2\zeta_9{}^2 + \zeta_9 + 1\ ,\ s := -(\zeta_9{}^5 + \zeta_9{}^3 + 2\zeta_9{}^2 + \zeta_9).$$

P r o o f: In [Ho3], sections 2.4-2.5, it is described a procedure to receive the period matrices starting from the coordinates of the fixed point P_{ζ_9}. First one has to move the "diagonal ball" $\mathbb{B} \subset \mathbb{P}^2$ by a plane projective linear transformation to the "Picard ball" (Siegel domain) $\mathbb{B}' \subset \mathbb{P}^2$. This is done by the inverse of

$$M := \begin{pmatrix} \omega & 0 & -1 \\ 0 & 1 & 0 \\ -\omega^2 & 0 & -1 \end{pmatrix},$$

(see [Ho3], p. 28) acting on row-vectors from the right. Let $P' := (a : b : c) \in \mathbb{B}'$ be the image point of $P_{\zeta_9} \in \mathbb{B}$. Setting $b = 1$ and applying Proposition 3 one gets $a,\, c \in \mathbb{Z}[\zeta_9]$. From the vector $(a, 1, c)$ one gets the period matrices via orthogonal fillings and $*$-procedure coming from Picard period integrals, all described in [Ho3] around Lemma 2.22. The numbers r, s appear in the period matrix Π at places $(1, 1)$ or $(1, 4)$, respectively. □

References

[CER] *Cherdieu, J.-P., Estrada-Sarlabous, J., Reinaldo-Barreiro, E.*, Efficient Reduction on the Jacobian Variety of Picard Curves, in: Coding Theory, Cryptography and Related Areas, Proceedings of the ICCC-98, J. Buchmann, T. Hohold, H. Stichtenoth, H. Tapia-Recillas (eds.), pp. 13-28, Springer-Verlag, 2000.

[Da-Ha] *Davenport, H., Hasse, H.*, Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen, J.Reine Angew. Math. **172**(1934), 151-182.

[De] *Deuring, M.*, Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins, Nachr. Akad. Wiss. Göttingen, 1953, 85-94.

[Feu] *Feustel, J.M.*, Kompaktifizierung und Singularitäten des Faktorraumes einer arithmetischen Gruppe, die in der zweidimensionalen Einheitskugel wirkt, Diplomarbeit, Humboldt-Univ. Berlin, 1976 (unpublished)

[Ha1] *Hasse, H.*, Zetafunktion und L-Funktionen zu einem arithmetischen Funktionenkörper vom Fermatschen Typus, Abhandlungen der Deutschen Akademie der Wissenschaften Berlin, Math.-Nat. Kl. 1954, Nr. 4, 5-70

[Ha2] *Hasse, H.*, Zahlentheorie, Akademie Verlag, Berlin, 1963

[He] *Hecke, E.*, Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen, Math. Zeitschr. **1**(1918), 357-376, **6**(1920), 11-51.

[Ho1] *Holzapfel, R.-P.*, Geometry and Arithmetic around Euler partial differential equations, Dt. Verlag d. Wiss., Berlin/Reidel Publ. Comp., Dordrecht, 1986

[Ho2] *Holzapfel, R.-P.*, Hierarchies of endomorphism algebras of abelian varieties corresponding to Picard modular surfaces, Schriftenreihe Komplexe Mannigfaltigkeiten **190**, Univ. Erlangen, 1994

[Ho3] *Holzapfel, R.-P.*, The ball and some Hilbert problems, Lect. in Math. ETH Zürich, Birkhäuser, Basel-Boston-Berlin, 1995

[Lac] *Lachaud, G.*, Courbes diagonales et courbes de Picard, Prétirage No. 97-30, Institut de Mathematiqués de Luminy, 1997

[La] *Lang, S.*, Complex multiplication, Grundl. Math. Wiss. **255**, Springer, 1983

[Neu] *Neukirch, J.*, Algebraische Zahlentheorie, Springer, Berlin-Heidelberg, 1992

[Ta] *Taniyama, Y.*, L-functions of number fields and zeta functions of abelian varieties, J. Math. Soc. Japan **9**(1957), 330-366.

[We] *Weil, A.*, On Jacobi sums as "Grössencharaktere", Transact. Amer. Math. Soc. **73**(1952), 487-495.