Quotients of Fermat curves and a Hecke character

Bert van Geemen

Università di Milano, Dipartimento di Matematica

Via Saldini 50, 20133 Milano, Italy

Kenji Koike

Division of School Education, Faculty of Education and Human Sciences

University of Yamanashi, Takeda 4-4-37

Kofu, Yamanashi, Japan

Annegret Weng*

Johannes Gutenberg-Universität

Fachbereich Mathematik, Staudingerweg 9

D-55128 Mainz, Germany

September 19, 2003

The third address is also the address for manuscript correspondence.

Email address: weng@mathematik.uni-mainz.de.

Telephone: 0049 6131 3922833

Fax: 0049 6131 3921295

*The third author was supported by the Maria Sybilla Merian program of the University of Essen.

Abstract

We explicitly identify infinitely many curves which are quotients of Fermat curves. We show that some of these have simple Jacobians with complex multiplication by a non-cyclotomic field. For a particular case we determine the local zeta functions with two independent methods. The first uses Jacobi sums and the second applies the general theory of complex multiplication, we verify that both methods give the same result.

Keywords: Fermat curves, complex multiplication, Jacobi sums, Hecke characters

1 Introduction

In [5] and [10], we studied a method for constructing CM-hyperelliptic curves of genus 3 and CM-Picard curves suitable for cryptography. The construction in the cited articles was done by computing approximations of the invariants of the curves (that are rational functions of theta constants) using a computer. Although these methods give cryptographically interesting examples of curves defined over $\mathbb{F}_p$, we do not have a rigorous mathematical proof that they really have complex multiplication with the stated CM-field.

In this paper we show that some of the examples given in [5] and [10] are obtained as quotients of Fermat curves, and that they indeed are Jacobians of the stated CM type.

It seems that the algebraic curves whose Jacobian is a simple factor of Jacobians of Fermat curves are not completely known. We give a sequence of such curves as cyclic d-gonal curves in Section 2.

In a special case, we find a Picard curve whose Jacobian has complex multiplication with the CM-field $\mathbb{Q}(\zeta_3, \zeta_7 + \zeta_7^{-1})$. We compute the local zeta functions for this curve by two different methods: with Jacobi sums based on a result in [4] (Section 3) by Hecke characters (Section 4). It is very well known that both methods give the same result and we verify this explicitly in section 4.8.

2 Fermat quotient curves

2.1

We consider a cyclic d-gonal curve

$$C_{d,n,k} \ : \ y^d = x^k(x^{nd-2k}+1), \quad n \geq 1, \ d > k \geq 0, \ nd - 2k > 0 \tag{2.1}$$

over $\mathbb{C}$, which is obtained as a quotient of the Fermat curve

$$F_{d(nd-2k)} \ : \ t^{d(nd-2k)} = s^{d(nd-2k)} + 1$$

by the quotient map $(s,t) \mapsto (x,y) = (s^d, t^{nd-2k}s^k)$.

The curve $C_{d,n,k}$ has automorphisms

$$\rho : \ (x,y) \longmapsto (x, \zeta_d y), \qquad \sigma : \ (x,y) \longmapsto (\zeta_{nd-2k}^d x, \zeta_{nd-2k}^k y),$$

$$\tau : \ (x,y) \longmapsto (1/x, y/x^n),$$

where $\zeta_n = \exp(2\pi/n)$. The involution τ commutes with ρ, and it acts on the quotient curve $X_{d,n,k} = C_{d,n,k}/\langle\tau\rangle$. Namely, the following diagram is commutative.

$$\begin{tikzcd} C_{d,n,k} \arrow[r, "\varepsilon"] \arrow[d, "\pi"'] & X_{d,n,k} \arrow[d, "\pi'"'] \\ \mathbb{P}^1 \arrow[r, "\gamma"] & \mathbb{P}^1 \end{tikzcd} \tag{2.2}$$

where π, π' and ε are quotient maps by actions of ρ and τ, and γ is defined by $x \mapsto x + x^{-1}$. Moreover we have $\tau\sigma = \sigma^{-1}\tau$, so $\sigma + \sigma^{-1}$ commutes with τ on the Jacobian $J(C_{d,n,k})$. Therefore we see that

Lemma 2.1. *We have an automorphism ρ on $X_{d,n,k}$ and an endomorphism $\sigma+\sigma^{-1}$ on $J(X_{d,n,k})$.*

Let us write down an equation of $X_{d,n,k}$. Let $B_{d,n,k}$ be the set of roots of $x^{nd-2k}+1=0$. Because the restriction of ε over $\mathbb{P}^1-\{\pm1\}$ gives an étale double cover $\pi^{-1}(\mathbb{P}^1-\{\pm1\})\to(\pi')^{-1}(\mathbb{P}^1-\{\pm2\})$, $X_{d,n,k}$ has an affine model of the form model

$$Y^d=(X-2)^a(X+2)^b\prod(X-\xi_i),\quad d>a,b\geq 0, \tag{2.3}$$

where $\xi_i\in\gamma(B_{d,n,k})$ and $\xi_i\neq-2$. Note that each element in the fiber $\pi^{-1}(1)$ is fixed by τ. So $(\pi')^{-1}(2)$ consists of d distinct points, and we have $b=0$.

Lemma 2.2. *The exponent a in (2.3) is 0 if n is even. In the case that n is odd, we have $a=d/2$ if d is even, and $a=(d+1)/2$ if d is odd.*

Proof. If n is even, each element in the fiber $\pi^{-1}(-1)$ is fixed by τ. So we have $a=0$ in this case. Now let n be an odd number. If d is odd, -1 is a branch point of π and $\gamma(B_{d,n,k})$ consists of -2 and other $(nd-2k-1)/2$ points. Because the branch divisor of π' has the multiplicity k at ∞, the degree of the branch divisor is

$$a+(nd-2k-1)/2+k,$$

and this must be divided by d. So $a \mod d$ is uniquely determined, and we see that $a=(d+1)/2$ satisfies this condition and $d>a\geq0$. The same argument works for the case that d is even. □

Next let us consider the polynomial $\prod(X-\xi_i)$. This is defined over $\mathbb{Z}$ since this is a product of minimal polynomials for algebraic integers in the real subfield of cyclotomic field.

To compute this polynomial, let us consider the rational functions $u_n(x) = x^n + x^{-n}$. These are determined inductively by $u_{n+1}(x) = X \cdot u_n(x) - u_{n-1}(x)$ where $X = x + x^{-1}$. Therefore we can regard $u_n(x)$ as a polynomial in X and we denote this by $U_n(X)$. Namely, $U_n(X) \in \mathbb{Z}[X]$ is the monic polynomial of degree n determined by the relation

$$U_{n+1}(X) = X \cdot U_n(X) - U_{n-1}(X), \quad U_1(X) = X, \; U_2(X) = X^2 - 2. \tag{2.4}$$

Lemma 2.3. *The polynomial $\prod(X - \xi_i)$ in (2.3) is given by $U_{(nd-2k)/2}(X)$ if $nd - 2k$ is even, and by $V_{(nd-2k-1)/2}(X)$ if $nd - 2k$ is odd where $V_m(X) \in \mathbb{Z}[X]$ is the monic polynomial of degree m defined by $U_{2m+1}(X) + 2 = (X+2)V_m(X)^2$.*

Proof. In the case of $nd - 2k = 2m$, the assertion follows from that

$$U_m(x + x^{-1}) = 0 \;\Leftrightarrow\; u_m(x) = x^m + x^{-m} = 0 \;\Leftrightarrow x^{2m} + 1 = 0.$$

Next let us consider the case of $nd - 2k = 2m + 1$. We have

$$\begin{aligned} U_{2m+1}(x + x^{-1}) + 2 = 0 \;&\Leftrightarrow\; x^{2m+1} + x^{-2m-1} + 2 = 0 \\ &\Leftrightarrow\; x^{4m+2} + 2x^{2m+1} + 1 = 0 \;\Leftrightarrow (x^{2m+1} + 1)^2 = 0. \end{aligned}$$

On the other hand, we have $x^{2m+1} + x^{-2m-1} + 2 = (\sqrt{x}^{2m+1} + \sqrt{x}^{-2m-1})^2$ and

$$\begin{aligned} \sqrt{x}^{2m+1} + \sqrt{x}^{-2m-1} &= (\sqrt{x} + \sqrt{x}^{-1}) \sum_{j=0}^{2m} (-1)^j (\sqrt{x})^j (\sqrt{x}^{-1})^{2m-j} \\ &= (\sqrt{x} + \sqrt{x}^{-1}) \sum_{j=0}^{2m} (-1)^j x^{j-m}, \end{aligned}$$

so $U_{2m+1}(x + x^{-1}) = (x + x^{-1} + 2)v_m(x)^2$ with a rational function $v_m(x)$ in x. Therefore $U_{2m+1}(X)$ must be of the form $(X+2)V_m(X)^2$. Now the assertion is obvious. □

Summarizing, we proved that

Theorem 2.1. *The curve $X_{d,n,k} = C_{d,n,k}/\langle\tau\rangle$ is defined by*

$$Y^d = U_{(nd-2k)/2}(X) \qquad (n \text{ even})$$

$$Y^d = (X+2)^{d/2} U_{(nd-2k)/2}(X) \qquad (n \text{ odd, } d \text{ even})$$

$$Y^d = (X+2)^{(d+1)/2} V_{(nd-2k-1)/2}(X) \qquad (n \text{ odd, } d \text{ odd})$$

for $n \geq 1$, $d > k \geq 0$ and $nd - 2k > 0$. The Jacobian $J(X_{d,n,k})$ has an endomorphism μ induced from $\sigma + \sigma^{-1} \in End(J(C_{d,n,k}))$.

Because we can identify the τ-invariant subspace $H^0(C_{d,n,k}, \Omega^1)^\tau$ with $H^0(X_{d,n,k}, \Omega^1)$, we can compute the type of endomorphism μ explicitly.

Example 2.1. Let $p > 3$ be an odd prime number. Then the hyperelliptic curve

$$C_{2,p+1,1} \ : \ y^2 = x(x^{2p} + 1)$$

has the following base

$$(1 - x^{p-1})dx/y, \quad (x - x^{p-2})dx/y, \ \cdots, \ (x^{(p-3)/2} - x^{(p-1)/2})dx/y$$

of $H^0(C_{2,p+1,1}, \Omega^1)^\tau$. Let σ be the automorphism $(x, y) \mapsto (\zeta_p^2 x, \zeta_p y)$. Above 1-forms correspond to eigenvectors of $\mu = \sigma + \sigma^{-1}$ with eigenvalues

$$\zeta_p + \zeta_p^{-1}, \quad \zeta_p^2 + \zeta_p^{-2}, \ \cdots, \ \zeta_p^{(p-3)/2} + \zeta_p^{(p-1)/2}$$

changing orders if necessary.

Also the automorphism $\rho : (x, y) \mapsto (-x, \zeta_4 y)$ induces an action on $X_{2,p+1,1}$, and we see that ρ and μ give a simple CM-type, that is

$$End(J(X_{2,p+1,1})) \otimes \mathbb{Q} = \mathbb{Q}(\zeta_4, \zeta_p + \zeta_p^{-1}).$$

In the case of $p = 7$, the curve $X_{2,8,1}$

$$Y^2 = U_7(X) = X(X^6 - 7X^4 + 14X^2 - 7)$$

is found in [10].

Example 2.2. Next we consider the hyperelliptic curve $C_{2,n,0} : y^2 = x^{2n} + 1$ for an odd number $n = 2m + 1$. Let C_n be the hyperelliptic curve defined by $y^2 = x^n + 1$. Then we have a morphism

$$p : C_{2,n,0} \longrightarrow C_n, \quad (x, y) \longmapsto (x^2, y),$$

and a decomposition $H^0(C_{2,n,0}, \Omega^1) = p^* H^0(C_n, \Omega^1) \oplus V_-$. Let us take a base

$$\varphi_i = x^{2i+1} dx/y, \quad (i = 0, \cdots, m - 1)$$

of $p^* H^0(C_n, \Omega^1)$, and a base

$$\psi_i = x^{2i} dx/y, \quad (i = 0, \cdots, m - 1)$$

of V_-. Then $\{\varphi_i - \psi_{2m-i}\}_{i=0,\cdots m-1}$ gives a base of $H^0(C_n, \Omega^1)^\tau$. Thus we have $J(C_{2,n,0}) \sim J(C_n)^2$ and $J(C_n) \sim J(X_{2,n,0})$ (isogenous).

Example 2.3. Let us consider the curve

$$C_{3,3,1} : y^3 = x(x^7 + 1). \tag{2.5}$$

The trigonal curve $X_{3,3,1}$

$$Y^3 = (X + 2)^2 V_3(X) = (X + 2)^2 (X^3 - X^2 - 2X + 1)$$

gives an example of a Picard curve (see [3]) of CM-type. The Jacobian has the endomorphism ring $End(J(X_{3,3,1})) \otimes \mathbb{Q} = \mathbb{Q}(\zeta_3, \zeta_7 + \zeta_7^{-1})$. Putting

$$X = (7 - 2x)/x, \quad Y = -7y/x^2,$$

we obtain a smooth model

$$y^3 = x(x^3 - 14x^2 + 49x - 49). \tag{2.6}$$

Note that the Jacobian $J(C_{3,3,1})$ is isogenous to the product $J(X_{3,3,1})^2 \times E$ with a CM-elliptic curve E. To see this, note that we have a non-trivial morphism

$$C_{3,3,1} \longrightarrow E, \quad (x,y) \longmapsto (t,s) = (x^7, y^7/(x^7+1)^2)$$

to a CM elliptic curve $E : s^3 = t(t+1)$. A base of $H^0(C_{2,p+1,1}, \Omega^1)^\tau$ is given by

$$(1-x)dx/y, \quad (1-x^4)dx/y^2, \quad (x-x^3)dx/y^2$$

and they are eigenvectors for the action of $\zeta_7 + \zeta_7^{-1}$. The -1-eigenspace of $H^0(C_{2,p+1,1}, \Omega^1)$ for the action of τ is given by

$$(1+x)dx/y, \quad (1+x^4)dx/y^2, \quad (x+x^3)dx/y^2$$

and x^2dx/y^2 (this 1-form is pulled back from E). Considering the CM-type, we can conclude the desired isogeny.

3 Computation of the zeta function of $C_{3,3,1}$

3.1

We would like to compute the local zeta-function

$$Z_{C,p}(t) = \exp\left(\sum_{r=1}^{\infty} \frac{\#C(\mathbb{F}_{p^r})}{r} t^r\right)$$

for the curves $C_{3,3,1}$ given by equation (2.5) and $X_{3,3,1}$ given by equation (2.6) at primes $p \neq 3, 7$. It is well-known that we can write

$$Z_{C_{3,3,1}}(t) = \frac{L_{C_{3,3,1}}(t)}{(1-t)(1-pt)} \quad \text{and} \quad Z_{X_{3,3,1}}(t) = \frac{L_{X_{3,3,1}}(t)}{(1-t)(1-pt)}.$$

where $L_{C_{3,3,1}}(t)$ resp. $L_{X_{3,3,1}}(t)$ is the L-polynomial of $C_{3,3,1}$ resp. $X_{3,3,1}$. The reciprocal of the L-polynomial of a curve is the characteristic polynomial of the Frobenius endomorphism on its Jacobian.

It is well-known that the L-polynomial of a curve C is of degree $2g$ and has a special form, i.e it satisfies $L(t) = a_0 + a_1 t + \ldots + a_{2g} t^{2g} \in \mathbb{Z}[t]$ with $a_{2g-1} = p^{g-i} a_i$ for $0 \leq i \leq g$ and $a_0 = a_{2g} = 1$. It is therefore determined by the g coefficients $a_1, \ldots, a_g$ which can be determined from the number of points $\#C(\mathbb{F}_{p^r})$ for $r = 1, \ldots, 7$.

Let $S_r = \#C(\mathbb{F}_{p^r}) - (p^r + 1)$ and a_i be the undetermined coefficients. We have

$$a_1 = S_1, \qquad a_i = 1/i \left(S_i + \sum_{j+k=i, 1 \leq j, k \leq i-1} a_k S_j \right).$$

In this section we compute $L_{C_{3,3,1}}$ and $L_{X_{3,3,1}}$ using Jacobi sums.

For $\alpha \in \mathbb{F}_q$, we set

$$e(\alpha) = \exp\left(2\pi i \frac{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p} \alpha}{p} \right).$$

Let χ be a character on a finite field $\mathbb{F}_q$. The Gauss sum (resp. Jacobi sum) is defined by

$$\tau(\chi) = \tau_1(\chi) = -\sum_{\alpha \in \mathbb{F}_q} \chi(\alpha) e(\alpha) \text{ resp. } J(\chi^s, \chi^t) = -\sum_{\alpha} \chi^s(\alpha) \chi^t(1-\alpha).$$

We have the relation

$$J(\chi^s, \chi^t) = \frac{\tau(\chi^s)\tau(\chi^t)}{\tau(\chi^{s+t})}.$$

Some Jacobi sums are easy to compute.

Lemma 3.1 ([1],Theorem 11.6.1). *Let χ be character of order m in $\mathbb{F}_{p^{2t}}$ with $p > 2$ and suppose that $p^t \equiv -1 \mod m$ for some positive integer t. Then*

$$p^{-t}\tau(\chi) = \begin{cases} -1 & \textit{if } p = 2, \\ -(-1)^{\frac{p^t+1}{m}} & \textit{if } p > 2. \end{cases}$$

3.2

We are now going to compute the number of points on $C_{3,3,1}(\mathbb{F}_q)$ over finite fields $\mathbb{F}_q$. We reduce our problem to counting the number of points of curves of the form $a_1x_1^{n_1} + a_2x_2^{n_2} = a_3$. These curves have already been considered by Davenport and Hasse [2].

Lemma 3.2. *Let q be a prime power.*

1. *Suppose $q \equiv 2 \mod 3$, then $\#C_{3,3,1}(\mathbb{F}_q) = \#X_{3,3,1}(\mathbb{F}_q) = q + 1$.*

2. *Let $q = p^r$, $q \equiv 1 \mod 3$ but $q \not\equiv 1 \mod 7$. We distinguish two cases:*

   (a) $p \equiv 1 \mod 3$. Then

$$\#C_{3,3,1}(\mathbb{F}_q) = q + 1 - \pi^r - \overline{\pi}^r$$

   where $\pi\overline{\pi} = p$ and $\pi = a + b\zeta_3 \equiv 1 \mod 3$ in $Z[\zeta_3]$, $\zeta_3^2 + \zeta_3 + 1 = 0$.

   (b) $p \equiv 2 \mod 3$. Then

$$\#C_{3,3,1}(\mathbb{F}_q) = \begin{cases} p^r + 1 & \text{if } r \text{ odd} \\ p^r + 1 - 2(-p)^{\frac{r}{2}} & \text{if } r \text{ even.} \end{cases}$$

Proof. 1. Obvious, since every element in $\mathbb{F}_q$ is a third power of a unique element in $\mathbb{F}_q$.

2. Let ξ be a generator of $\mathbb{F}_q^*$. By Lemma 1 in [4], the number of affine solutions in $\mathbb{F}_q$ of the equation $y^3 = x^8 + x$ is equal to

$$N = \frac{1}{3}\left(|A_{11}| + |A_{\xi\xi^2}| + |A_{\xi^2\xi}|\right),$$

where

$$A_{\eta_1\eta_2} = \{(t, u) \in k \times k|\ \eta_1^7 t^{21} + 1 = \eta_2 u^3\}.$$

Since $q \not\equiv 1 \mod 7$, the map $t \to t^7$ is an isomorphism and we are looking for the points on the affine part of the elliptic curves $E_{\eta_1\eta_2}$ given by $\eta_1^7 t^3 + 1 = \eta_2 u^3$ resp. $\eta_1^7 t^3 + \eta_2 u^3 = 1$.

For an elliptic curve defined over a prime field $\mathbb{F}_p$, the number of points over $\mathbb{F}_{p^r}$ is already determined by $\#E(\mathbb{F}_p)$.

If $p \not\equiv 1 \mod 3$, all three elliptic curves obtained from A_{11}, $A_{\xi\xi^2}$ and $A_{\xi^2\xi}$ are supersingular. Hence, $\#C_{3,3,1}(\mathbb{F}_q)$ is equal to the number of points of a supersingular elliptic curve.

Now assume that $p \equiv 1 \mod 3$. We apply the technique explained in [7], Section 10.3.

Embed $\mathbb{F}_p$ into $\mathbb{Z}[\zeta_3]/(\pi)$ where $\pi \in \mathbb{Z}[\zeta_3]$ is an element above p satisfying $\pi \equiv 1 \mod 3$. Let χ be the character of order 3 given by the cubic residue symbol $\left(\frac{\cdot}{\pi}\right)_3$. We get

$$\begin{aligned}
|A_{11}| &= \sum_{a+b=1} \sum_{j=0}^{2} \chi^j(a) \sum_{k=0}^{2} \chi^k(b) = \sum_{j=0}^{2}\sum_{k=0}^{2}\sum_{a+b=1} \chi^j(a)\chi^k(b) \\
&= \sum_{j=0}^{2}\sum_{k=0}^{2}\sum_{a\in\mathbb{F}_p} \chi^j(a)\chi^k(1-a) = -\sum_{j=0}^{2}\sum_{k=0}^{2} J(\chi^j,\chi^k) \\
&= q - \sum_{j=1}^{2}\sum_{k=1}^{2} J(\chi^j,\chi^k) = q - 2 - J(\chi,\chi) - J(\chi^2,\chi^2).
\end{aligned}$$

Now $J(\chi,\chi) = \pi$ ([7], Proposition 7.5).

Similar computations show that $|A_{\xi\xi^2}| = |A_{\xi^2\xi}| = q + 1 - J(\chi,\chi) - J(\chi^2,\chi^2)$. Hence, the assertion follows.

Note that we can do the same computation for q with $p \not\equiv 1 \mod 3$. This shows that

$$J(\chi,\chi) + J(\chi^2,\chi^2) = 2(-p)^r \tag{3.1}$$

for $q = p^{2r}$ with $p \not\equiv 1 \mod 3$. We will use this observation later.

□

Theorem 3.1. *Finally let $q \equiv 1 \mod 21$. Let ψ be a character of order 21 on $\mathbb{F}_q$ and set $\eta = J(\psi^7, \psi)$. We have*

$$\#C_{3,3,1}(\mathbb{F}_q) = q + 1 - Tr_{\mathbb{Q}(\zeta_{21})/\mathbb{Q}}(\eta) - J(\psi^7, \psi^7) - J(\psi^{14}, \psi^{14}).$$

Proof. We follow very closely the proof of Proposition 3 in [4].

Let ξ be generator of $\mathbb{F}_q^*$. Again we form the sets $A_{\eta_1\eta_2}$ for $(\eta_1, \eta_2) = \{(1,1), (\xi, \xi^2), (\xi^2, \xi)\}$.

By the theorem of Davenport-Hasse [2] the number of solutions of the equation $a_1u^3 + a_2t^{21} = a_3$ in $\mathbb{F}_q$ is given by

$$N(a_1, a_2, a_3) = q - \chi(-\frac{a_1}{a_2}) - \chi^2(-\frac{a_1}{a_2}) - \sum_{1 \le \nu \le 2} \sum_{1 \le \mu \le 20} \frac{\tau_{a_1}(\psi^{7\nu})\tau_{a_2}(\psi^{\mu})}{\tau_{a_3}(\psi^{7\nu+\mu})}$$

where $\tau_x(\psi) = -\sum_{\alpha \in \mathbb{F}_q} \psi(\alpha)e^x(\alpha)$.

We deduce

$$|A_{11}| = N(-1, 1, -1) = q - 2 - \sum_{\mu=1, \mu \neq 14}^{20} \frac{\tau_{-1}(\psi^7)\tau_1(\psi^\mu)}{\tau_{-1}(\psi^{7+\mu})} - \sum_{\mu=1, \mu \neq 7}^{20} \frac{\tau_{-1}(\psi^{14})\tau_1(\psi^\mu)}{\tau_{-1}(\psi^{14+\mu})},$$

$$|A_{\xi\xi^2}| = N(-\xi^2, \xi^7, -1) = q + 1 - \sum_{\mu=1, \mu \neq 14}^{20} \frac{\tau_{-\xi^2}(\psi^7)\tau_{\xi^7}(\psi^\mu)}{\tau_{-1}(\psi^{7+\mu})} - \sum_{\mu=1, \mu \neq 7}^{20} \frac{\tau_{-\xi^2}(\psi^{14})\tau_{\xi^7}(\psi^\mu)}{\tau_{-1}(\psi^{14+\mu})} \text{ and}$$

$$|A_{\xi^2\xi}| = N(-\xi, \xi^{14}, -1) = q + 1 - \sum_{\mu=1, \mu \neq 14}^{20} \frac{\tau_{-\xi}(\psi^7)\tau_{\xi^{14}}(\psi^\mu)}{\tau_{-1}(\psi^{7+\mu})} - \sum_{\mu=1, \mu \neq 7}^{20} \frac{\tau_{-\xi^2}(\psi^{14})\tau_{\xi^14}(\psi^\mu)}{\tau_{-1}(\psi^{14+\mu})}.$$

Hence,

$$\begin{aligned} &|A_{11}| + |A_{\xi\xi^2}| + |A_{\xi^2\xi}| = 3q \\ &- \sum_{\mu=1, \mu \neq 14}^{20} \left(\frac{\tau_{-1}(\psi^7)\tau_1(\psi^v) + \tau_{\xi^2}(\psi^7)\tau_{\xi^7}(\psi^\mu) + \tau_{-\xi}(\psi^7)\tau_{\xi^{14}}(\psi^\mu)}{\tau_{-1}(\psi^{7+v})} \right) \\ &- \sum_{\mu=1, \mu \neq 7}^{20} \left(\frac{\tau_{-1}(\psi^{14})\tau_1(\psi^v) + \tau_{-\xi^2}(\psi^{14})\tau_{\xi^7}(\psi^\mu) + \tau_{-\xi}(\xi^{14})\tau_{\xi^{14}}(\psi^\mu)}{\tau_{-1}(\psi^{14+v})} \right). \end{aligned}$$

Since $\psi(-1) = 1$, we get $\tau_{-1}(\psi^s) = \tau_1(\psi^s)$ and using $\tau_d(\psi) = \psi^{-1}(d)\tau(\psi)$ we find

$$\begin{aligned}
&\tau_{-1}(\psi^7)\tau_1(\psi^\mu) + \tau_{\xi^2}(\psi^7)\tau_{\xi^7}(\psi^\mu) + \tau_{-\xi}(\psi^7)\tau_{\xi^{14}}(\psi^\mu) \\
&= \tau(\psi^7)\tau(\psi^\mu)\left(1 + w^{-v-2} + w^{-2(v-2)}\right) \text{ and} \\
&\tau_{-1}(\psi^{14})\tau_1(\psi^\mu) + \tau_{-\xi^2}(\psi^{14})\tau_{\xi^7}(\psi^\mu) + \tau_{-\xi}(\psi^{14})\tau_{\xi^{14}}(\psi^\mu) \\
&= \tau(\psi^{14})\tau(\psi^\mu)\left(1 + w^{-v-1} + w^{-2(v-1)}\right)
\end{aligned}$$

where $w = \psi^7(\xi)$ is a third root of unity.

Therefore

$$\begin{aligned}
&\frac{1}{3}\left(|A_{11}| + |A_{\xi\xi^2}| + |A_{\xi^2\xi}|\right) = \\
&q - J(\psi^7,\psi^7) - J(\psi^{14},\psi^{14}) - \sum_{i=0}^{6} J(\psi^7,\psi^{3i+1}) - \sum_{i=0}^{6} J(\psi^{14},\psi^{3i+2}). \qquad (3.2)
\end{aligned}$$

The Galois group of the field extension $\mathbb{Q}(\zeta_{21})$ is generated by two elements A, B of order six resp. two, say $\zeta_{21}^A := \zeta_{21}^5$ and $\zeta_{21}^B := \zeta_{21}^8$. We easily see that the 12 elements $J(\psi^{7i},\psi^k)$ with $7 \nmid k$ in (3.2) are conjugate over $\mathbb{Q}(\zeta_{21})$ and the result follows. □

Corollary 3.1. *For $p \equiv 5, 17 \mod 21$ we get*

$$\begin{aligned}
&L_{C_{3,3,1}}(t) = 1 + pt^2 + 2p^3t^6 + 2p^4t^8 + p^6t^{12} + p^7t^{14} \\
&= (p^2t^4 - pt^2 + 1)^2(pt^2+1)^3.
\end{aligned}$$

Proof. Using Lemma 3.2 we get $S_1 = S_3 = S_5 = S_7 = 0$, $S_2 = 2p$ and $S_4 = -2p^2$. From Lemma 3.1, the observation (3.1) and the fact that $p^3 + 1 \equiv 0 \mod 42$ we deduce $S_6 = 14p^3$. □

3.3

Let us consider the Jacobi sum $J(\psi^7,\psi)$ more closely.

Theorem 3.2. *Let $q = p^r \equiv 1 \mod 21$ and let ψ be a character of order 21 in $\mathbb{F}_q$. Suppose that n is the smallest integer such that $p^n \equiv 1 \mod 21$.*

1. *The absolute value of every Jacobi sum is $\sqrt{q}$.*

2. *There exists a prime ideal $\mathfrak{p}$ above p in $\mathbb{Z}[\zeta_{21}]$ such that we have the following prime ideal decomposition*

$$J(\psi^7, \psi)\mathbb{Z}[\zeta_{21}] = \left(\mathfrak{p}\mathfrak{p}^{A^4}\mathfrak{p}^{A^5}\mathfrak{p}^{AB}\mathfrak{p}^{A^2B}\mathfrak{p}^{A^3B}\right)^{\frac{r}{n}}$$

   where A and B have been defined in the proof of Theorem 3.1.

   Moreover, $Norm_{\mathbb{Q}(\zeta_{21})/\mathbb{Q}(\zeta_3,\sqrt{-7})}(J(\psi^7, \psi)) = qJ(\psi^7, \psi^7)$.

3. *Let $\mathfrak{p}_7$ be a prime ideal in $\mathbb{Q}(\zeta_{21})$ lying above 7. We get*

$$J(\psi^7, \psi) \equiv 1 \mod (1 - \zeta_{21}^7) \text{ and } J(\psi^7, \psi) \equiv J(\psi^7, \psi^7) \mod \mathfrak{p}_7.$$

The properties 1), 2), 3) determine $J(\psi^7, \psi)$ (up to conjugation in $\mathbb{Q}(\zeta_{21})$) uniquely.

Proof. 1. Well known fact on Jacobi sums ([2], equation (4.2)).

2. By Stickelberger's theorem (see e.g. [1], Chapter 11.2), the decomposition of the Jacobi sum is given by

$$J(\psi^7, \psi)\mathbb{Z}[\zeta_{21}] = \left(\prod_J \mathfrak{p}_j^{d(-7j,-j)}\right)^{\frac{r}{n}}$$

   where J runs through all automorphisms of $\mathbb{Q}(\zeta_{21})$ (where $\sigma : \zeta \mapsto \zeta^k$ is identified with $k \in (\mathbb{Z}/21\mathbb{Z})^*$), $j = J^{-1} \mod 21$ and d is given by

$$d(-7j, -j) = \frac{r(-7j) + r(-j) - r(-8j)}{21}.$$

   where $r(x)$ is the smallest non-negative residue of $x \mod 21$. Both assertions follow from straight forward calculations.

3. By Theorem 2.1.7 in [1] we have $J(\psi^7, \psi) = q \mod (1 - \zeta_{21}^7)$. The prime ideal (7) is the sixth power of a product of two prime ideals in $\mathbb{Q}(\zeta_{21})$. Let $\mathfrak{p}_7$ be a prime ideal lying above 7. Using the Frobenius in $\mathbb{Z}[\zeta_{21}]/\mathfrak{p}_7 \simeq \mathbb{F}_7$ we get

$$\begin{aligned} J(\psi^7, \psi) &= -\sum_{a \in \mathbb{F}_q} \psi^7(a)\psi(1-a) \\ &\equiv -\sum_{a \in \mathbb{F}_q} \psi^7(a)\psi^7(1-a) \mod \mathfrak{p}_7 \\ &\equiv J(\psi^7, \psi^7) \mod \mathfrak{p}_7. \end{aligned}$$

Property 2) fixes $J(\psi^7, \psi)$ up to units, Property 1) fixes it up to roots of unity and Property 3) fixes the root of unity, since 1 is the only root of unity in $\mathbb{Q}(\zeta_{21})$ congruent to $1 \mod (1 - \zeta_{21}^7)\mathfrak{p}_7$.

□

Corollary 3.2. *Let p be a prime.*

1. *If $p \equiv 2, 11 \mod 21$, we have*

$$L_{C_{3,3,1}}(t) = 1 + pt^2 + 2p^3t^6 + 2p^4t^8 + p^6t^{12} + p^7t^{14}.$$
$$= (p^2t^4 - pt^2 + 1)^2(pt^2 + 1)^3.$$

2. *If $p \equiv 8, 20 \mod 21$, we have*

$$L_{C_{3,3,1}}(t) = p^7t^{14} + 7p^6t^{12} + 21p^5t^{10} + 35p^4t^8$$
$$+ 35p^3t^6 + 21p^2t^4 + 7pt^2 + 1 = (1 + pt^2)^7.$$

Proof. 1. We have $S_1 = S_3 = S_5 = S_7 = 0$ and $S_2 = 2p$, $S_4 = -2p^2$. By Theorem 3.2, A^3B fixes the ideal generated by $\eta = J(\psi^7, \psi)$. Moreover, every prime ideal above p is fixed by A^4B ($\equiv 2 \mod 21$) resp. A^2B ($\equiv 11$

mod 21). Hence $(\eta)\mathbb{Z}[\zeta_{21}] = (p^3)\mathbb{Z}[\zeta_{21}]$ and using part 3 of Theorem 3.2 we get $S_6 = 14p^3$.

2. This can be shown analogously to part 1 and is left to the reader.

□

Corollary 3.3. *Let p be a prime such that $p \equiv 1 \mod 3$ and let π be an element in $\mathbb{Z}[\zeta_3]$ such that $\pi\overline{\pi} = p$ and $\pi \equiv 1 \mod 3$.*

1. *Suppose $p \equiv 4, 16 \mod 21$. Let ζ_3^k be a third root of unity such that*

$$7|N_{\mathbb{Q}(\zeta_3)/\mathbb{Q}}\left(\zeta_3^k \pi p - \pi^3\right).$$

Then

$$L_{C_{3,3,1}}(t) = (pt^2 - (\pi + \overline{\pi})t + 1) \cdot (p^3t^6 - p(\zeta_3^k\pi + \overline{\zeta_3^k\pi})t^3 + 1)^2.$$

2. *Suppose $p \equiv 10, 19 \mod 21$. Let ζ_3^k be a third root of unity such that*

$$7|N_{\mathbb{Q}(\zeta_3)/\mathbb{Q}}(\zeta_3^k\pi^2p^2 - \pi^6).$$

Then

$$L_{C_{3,3,1}}(t) = (t^2p - (\pi + \overline{\pi})t + 1)$$
$$(p^3t^6 - (\zeta_3^{2k}\pi + \overline{\zeta_3^{2k}\pi})pt^3 + 1)(p^3t^6 + (\zeta_3^{2k}\pi + \overline{\zeta_3^{2k}\pi})pt^3 + 1).$$

Proof. 1. Let ψ be a character of order 21 in $\mathbb{F}_{p^3}$ such that $\psi^7 = \chi \circ N_{\mathbb{F}_{p^3}/\mathbb{F}_p}$ where χ is the character given by the cubic residue symbol $\left(\frac{\cdot}{\pi}\right)_3$. We have $S_i = -\pi^i - \overline{\pi}^i$ for $i = 1, 2, 4, 5, 7$ and $S_j = -\pi^j - \overline{\pi}^j - Tr_{\mathbb{Q}(\zeta_{21})/\mathbb{Q}}\eta^{j/3}$ for $j = 3, 6$ and $\eta = J(\psi^7, \psi)$. By Theorem 3.2 we get $(\eta)\mathbb{Z}[\zeta_{21}] = (\pi p)\mathbb{Z}[\zeta_{21}]$. Using Corollary 4.33 and Proposition 7.5. in [7] we find $J(\psi^7, \psi^7) = \pi^3$. Hence, $J(\psi, \psi^7) \equiv \pi^3 \mod \mathfrak{p}_7$ by Theorem 3.2. Hence we can choose η

such that $\eta \equiv \pi^3 \mod \mathfrak{p}_7$ where $\mathfrak{p}_7$ is any prime ideal lying above 7 in $\mathbb{Q}(\zeta_{21})$. We get $S_j = -\pi^j - \overline{\pi}^j - 6p^{j/3}((\zeta_3^k\pi)^{j/3} + \overline{(\zeta_3^k\pi)}^{j/3})$ for $j = 3, 6$ and ζ given as above.

2. Similar to (1) and left to the reader.

□

Corollary 3.4. *Let $K = \mathbb{Q}(\zeta_3, \zeta_7 + \zeta_7^{-1})$ and let $p \equiv 1 \mod 21$ (resp. $p \equiv 13 \mod 21$) and let η be an integer in K such that $\eta\overline{\eta} = p$ (resp. $\eta\overline{\eta} = p^2$). Let $\pi \in \mathbb{Z}[\zeta_3]$, $\pi \equiv 1 \mod 3$, be such that $p\pi$ generates the ideal $Norm_{K/\mathbb{Q}(\zeta_3)}(\eta)$ (resp. $p^2\pi^2$ generates the ideal $Norm_{K/\mathbb{Q}(\zeta_3)}(\eta^2)$). After multiplying η by a suitable root of unity we may assume that $\eta \equiv 1 \mod (1 - \zeta_3)$ and $\eta \equiv \pi \mod \mathfrak{p}_7$ (resp. $\eta^2 \equiv 1 \mod (1 - \zeta_3)$ and $\eta^2 \equiv \pi^2 \mod \mathfrak{p}_7$)) where $\mathfrak{p}_7$ is any prime lying above 7 in K. Let $\{\eta_i\}$ be the set of Galois conjugates of η.*

1. *If $p \equiv 1 \mod 21$, then*

$$L_{C_{3,3,1}}(t) = (1 - \pi t)(1 - \overline{\pi} t) \prod_{i=1}^{6} (1 - \eta_i t)^2.$$

2. *If $p \equiv 13 \mod 21$, then*

$$L_{C_{3,3,1}}(t) = (1 - \pi t)(1 - \overline{\pi} t) g_1(t) g_1(-t).$$

where $g_1(t) = \prod_{i=1}^{6}(1 - \eta_i t)$.

Proof. 1. The reciprocals of the zeros of the L-polynomial are the numbers α_j of absolute value $\sqrt{p}$ such that

$$N_r = q^r - 1 - S_r = q^r + 1 - \sum_{j=1}^{14} \alpha_j^r.$$

We have

$$S_i = -\pi^i - \overline{\pi}^i - \sum_{j=1}^{12} (\eta^{\sigma_j})^i.$$

The first equation follows. The Jacobian over $\mathbb{Q}$ has a factor of dimension 6 (see example 2.3). Since this factor has CM by $K = \mathbb{Q}(\zeta_3, \zeta_7 + \zeta_7^{-1})$, η lies in K.

The conditions on η follow from Theorem 3.2.

2. We have $S_i = -\pi^i - \overline{\pi}^i$ for $i = 1, 3, 5, 7$ and $S_i = -\pi^i - \overline{\pi}^i - T_i$ for $i = 2, 4, 6$ for some integers T_i and π with $\pi\overline{\pi} = p$. Plugging this into the formula for the computation of $L_{C_{3,3,1}}(t)$ we find

$$L_{C_{3,3,1}}(t) = (1 - \pi t)(1 - \overline{\pi} t) f_{\text{even}}(t)$$

where $f_{\text{even}}(t)$ is an even polynomial.

Set $\eta^2 = J(\xi^7, \xi)$ as in Theorem 3.1. We have $f_{\text{even}}(t) = g(t^2)$ where $g(\eta^2) = 0$. Since the Jacobian over $\mathbb{Q}$ has a factor of dimension 6 with CM by K, every root of $f_{\text{even}}(t)$ lies in K.

The conditions on η follow from Theorem 3.2.

□

We now consider the L-polynomial of the curve $X_{3,3,1}$.

Theorem 3.3. *Let K be as above and let $p \neq 3, 7$ be a rational prime. We distinguish the following four cases:*

1. *Suppose p is inert in $K/\mathbb{Q}$ (i.e. $p \equiv 2, 5, 11, 17 \mod 21$). Then $L_{X_{3,3,1}}(t) = p^3 t^6 + 1$. The curve $X_{3,3,1}$ is a supersingular curve, i.e. its Jacobian is isogenous to a product of supersingular elliptic curves.*

2. *Suppose p splits into three prime ideals (i.e. $p \equiv 8, 20 \mod 21$). Then $X_{3,3,1}/\mathbb{F}_p$ is supersingular and $L_{X_{3,3,1}}(t) = (pt^2 + 1)^3$.*

3. *Suppose p splits into two prime ideals. Let $p \equiv 4, 16 \mod 21$ (resp. $10, 19 \mod 21$) and let $\pi \equiv 1 \mod 3$ be an integer in $\mathbb{Z}[\zeta_3]$ such that $\pi\overline{\pi} = p$. Let ζ_3^k be a third root of unity such that $7 | N_{\mathbb{Q}(\zeta_3)/\mathbb{Q}}\left(\zeta_3^k \pi p - \pi^3\right)$ (resp. $7 | N_{\mathbb{Q}(\zeta_3)/\mathbb{Q}}(\zeta_3^{2k}\pi^2 p^2 - \pi^6)$.) Then*

$$L_{X_{3,3,1}}(t) = p^3 t^6 - p(\zeta_3^k \pi + \overline{\zeta_3^k \pi}) t^3 + 1.$$

4. *Suppose p splits completely. Let η be an integer in K such that $\eta\overline{\eta} = p$ and $\eta \equiv 1 \mod (1 - \zeta_3)$ (resp. $\eta^2 \equiv 1 \mod (1 - \zeta_3)$). Let $\pi \in \mathbb{Z}[\zeta_3]$, $\pi \equiv 1 \mod 3$, be such that $p\pi$ generates the ideal $Norm_{K/\mathbb{Q}(\zeta_3)}(\eta)$ (resp. $p^2\pi^2$ generates the ideal $Norm_{K/\mathbb{Q}(\zeta_3)}(\eta^2)$). Assume moreover that $\eta \equiv \pi \mod \mathfrak{p}_7$ (resp. $\eta^2 \equiv \pi^2 \mod \mathfrak{p}_7$) where $\mathfrak{p}_7$ is any prime lying above 7 in K. Then $L_{X_{3,3,1}}(t) = \prod_{i=1}^6 (1 - \eta_i t)$, where the η_i are the Galois conjugates of η.*

Proof. This follows easily from the local L-series of $C_{3,3,1}$. For 3), $p \equiv 10, 19 \mod 21$ and 4), $p \equiv 13 \mod 21$ we use the fact that the local L-series evaluated at 1 gives the order of group of $\mathbb{F}_p$-rational points on the Jacobian which must be divisible by 27 (see also Remark 4.6). This tells us which factor of $L_{C_{3,3,1}}(t)$ we have to take. □

4 The Hecke character of $X_{3,3,1}$

4.1

It is well known that the L-function of an abelian variety with CM is the L-function of a Hecke character (cf. [6]). In particular, if the abelian variety is the Jacobian of a curve, one finds the number of points on that curve over finite fields with very little effort. We will determine the Hecke character associated to $A = Jac(X_{3,3,1})$ explicitly and use it to determine the zeta function of $X_{3,3,1}$. The values of the Hecke character are essentially Jacobi sums, and we already considered that point of view in the previous section.

4.2

A basis of $H^0(X_{3,3,1}, \Omega^1) \cong H^0(C_{2,p+1,1}, \Omega^1)^\tau$ is given by

$$(1-x)dx/y, \qquad (1-x^4)dx/y^2, \qquad (x-x^3)dx/y^2.$$

The automorphism of order three $(x,y) \mapsto (x, \zeta_3 y)$ acts as $diag(\zeta_3^2, \zeta_3, \zeta_3)$. The endomorphism $\mu = \sigma + \sigma^{-1}$ of $A = Jac(X_{3,3,1})$ is induced by the automorphism σ of $C_{3,3,1}$ given by $(x,y) \mapsto (\zeta_7^3 x, \zeta_7 y)$, thus μ acts as $diag(\zeta_7^2 + \zeta_7^{-2}, \zeta_7 + \zeta_7^{-1}, \zeta_7^3 + \zeta_7^{-3})$. These endomorphisms of A generate a ring isomorphic to the ring of integers $\mathcal{O}_K = \mathbb{Z}[\zeta_3, \zeta_7 + \zeta_7^{-1}]$ where

$$K = \mathbb{Q}(\zeta_3, \alpha), \qquad \alpha = \zeta_7 + \zeta_7^{-1},$$

thus K is CM field of degree 6 over $\mathbb{Q}$ with totally real subfield $K_0 = \mathbb{Q}(\alpha)$. The minimum polynomial of α is $X^3 + X^2 - 2X - 1$.

Let $Sq = \{1,4,2\} \subset (\mathbb{Z}/7\mathbb{Z})^*$ be the subgroup of squares, then the Galois group $G_K = Gal(K/\mathbb{Q}) \cong (\mathbb{Z}/3\mathbb{Z})^* \times Sq$ acts as:

$$\sigma_{(a,b)} : K \longrightarrow K, \qquad \zeta_3 \longmapsto \zeta_3^a, \qquad \alpha = \zeta_7 + \zeta_7^{-1} \longmapsto \zeta_7^b + \zeta_7^{-b}.$$

Embedding $K \hookrightarrow \mathbb{C}$ by $\zeta_7 \mapsto e^{2\pi i/7}$, the set of complex embeddings of K is identified with G_K by $K \xrightarrow{\sigma} K \hookrightarrow \mathbb{C}$. The CM type of A is then the subset

$$\Sigma = \{\sigma_1 = (1,1),\ \sigma_2 = (2,2),\ \sigma_3 = (1,4)\} \qquad (\subset G_K = (\mathbb{Z}/3\mathbb{Z})^* \times Sq)$$

It is easy to verify that this CM type is simple.

The curve $X_{3,3,1}$ has good reduction away from 3 and 7 and in $\mathcal{O}_K$ we have

$$(3) = \wp_3^2, \qquad (7) = \wp_{7,1}^3 \wp_{7,2}^3$$

with prime ideals $\wp_3 = (1-\zeta_3)$, $\wp_{7,1} = (2-\zeta_3, 2-\alpha)$, $\wp_{7,2} = (4-\zeta_3, 2-\alpha)$.

4.3

We briefly recall how to find the Frobenius endomorphism $Fr_\wp$ of $A_\wp$ at a prime of good reduction $\wp$ of A. Here $A_\wp$ is the abelian variety over the finite field $\mathcal{O}/\wp$ which is the reduction of A at $\wp$. Since $\mathcal{O}_K$ is a principal ideal domain, we can choose a generator $\pi_\wp$ for each prime ideal $\wp$ in $\mathcal{O}_K$. Let ω_i, $i = 1,2,3$, be a basis of the regular 1-forms of $A_\wp$ on which $x \in \mathcal{O}_K$ acts as $x^*\omega_i = \sigma_i(x)\omega_i$, such a basis can be obtained by reduction mod $\wp$ of a basis of 1-forms of A. Note that $x^*\omega_i = 0$ if $\sigma_i(x) \in \wp$. Thus the element $\prod_j \sigma_j^{-1}(\pi_\wp) \in \mathcal{O}_K$ acts trivially on the 1-forms. This implies that it is an inseparable endomorphism. The degree of this endomorphism is $N_{K/\mathbb{Q}}(\pi_\wp)^3$, which is also the degree of $Fr_\wp$. Therefore $Fr_\wp = u\prod_j \sigma_j^{-1}(\pi_\wp)$ where u is some automorphism of $A_\wp$. The theory of complex multiplication (which uses results from class field theory) allows one to determine $Fr_\wp$ precisely.

4.4

The Hecke character χ of K which describes the action of $Gal(\overline{\mathbb{Q}}/K)$ on the first étale cohomology group of A is a homomorphism

$$\chi : \mathbb{A}_K^* \longrightarrow K^*, \qquad \chi(\ldots, x_\wp, \ldots) = \prod_\wp \chi_\wp(x_\wp)$$

where $\mathbb{A}_K^*$ are the ideles of K (the restricted product of the $K_\wp^*$) and the product is taken over all places of K. A Hecke character is trivial on $K^* \hookrightarrow \mathbb{A}_K^*$ (diagonal embedding).

The main result of complex multiplication is that for a prime $\wp$ where A has good reduction $A_\wp$ the Frobenius endomorphism $Fr_\wp \in \mathcal{O}_K \subset End(A_\wp)$ is given by:

$$Fr_\wp = \chi(1, \ldots, 1, \pi_\wp, 1, \ldots)$$

where the idele $(1, \ldots, 1, \pi_\wp, 1, \ldots)$ has all components equal to one except at the place $\wp$ where $\pi_\wp$ is a(ny) generator of the maximal ideal of the local ring $\mathcal{O}_\wp$. The Hecke character is unramified outside the places of bad reduction, which are the primes dividing 21, hence if $\wp$ does not divide 21 then $\chi_\wp$ is trivial on the units of the local ring $\mathcal{O}_\wp$ of the local field $K_\wp^*$.

As before, we choose a generator $\pi_\wp \in \mathcal{O}_K$ for each prime ideal $\wp$. Then for any idele $\xi = (\xi_\wp)$ there is an element $x_\xi \in K$, unique up to a unit of $\mathcal{O}_K$, such that $x_\xi \xi_\wp$ is in $\mathcal{O}_\wp^*$ for all finite places. Hence χ is determined by the infinity and the ramified components:

$$\chi(\xi) = \chi(\xi x_\xi) = \left(\prod_{\sigma|\infty} \chi_\sigma(\xi_\wp x_\xi)\right)\left(\prod_{\wp|21} \chi_\wp(\xi_\wp x_\xi)\right)$$

Thus χ is determined by the infinity components and the restrictions of the $\chi_\wp$ to $\mathcal{O}_\wp^*$ for $\wp|21$.

From the discussion in section 4.3 it follows that the infinity component χ_σ is non-trivial only if $\sigma^{-1} \in \Sigma$, the CM type of A, and then $\chi_{\sigma^{-1}}(x_\sigma) = \sigma^{-1}(x_\sigma^{-1})$. In our case it is easy to see that $\prod \sigma_i^{-1}(x) = \prod \sigma_i(x)$ for all $x \in K$, hence we will omit the inverse on the σ_i from now on. The Frobenius elements are then given by:

$$\begin{aligned} Fr_\wp &= \chi(1,\ldots,1,\pi_\wp,1,\ldots) \\ &= \chi(\pi_\wp^{-1},\ldots,\pi_\wp^{-1},1,\pi_\wp^{-1},\ldots) \\ &= \chi_{\wp_3}(\pi_\wp^{-1})\chi_{\wp_{7,1}}(\pi_\wp^{-1})\chi_{\wp_{7,2}}(\pi_\wp^{-1})\textstyle\prod_{\sigma\in\Sigma}\sigma(\pi_\wp) \end{aligned}$$

(so we took $x_\xi = \pi_\wp^{-1}$). The fact that x_ξ is unique up to a unit of $\mathcal{O}_K$ implies that

$$\chi_{\wp_3}(u^{-1})\chi_{\wp_{7,1}}(u^{-1})\chi_{\wp_{7,2}}(u^{-1})\prod_{\sigma\in\Sigma}\sigma(u) = 1 \qquad \forall u \in \mathcal{O}_K^*.$$

Note that for $u \in \mathcal{O}_{K_0}^*$ we have $\prod_{\sigma\in\Sigma}\sigma(u) = N_{K_0/\mathbb{Q}}(u) = \pm 1$, hence it is not so surprising that Hecke characters actually exist. The continuity of χ implies that the $\chi_\wp$ take values in the subgroup of roots of unity of K^* which is the group of order six generated by $\omega := -\zeta_3$.

At this point it is natural to define a homomorphism

$$\psi : K^* \longrightarrow K^*, \qquad x \longmapsto \chi_{\wp_3}(x^{-1})\chi_{\wp_{7,1}}(x^{-1})\chi_{\wp_{7,2}}(x^{-1})\prod_{\sigma\in\Sigma}\sigma(x).$$

Then we have:

$$Fr_\wp = \psi(\pi_\wp), \qquad \psi(u) = 1$$

for all units $u \in \mathcal{O}_K^*$. We will determine ψ explicitly using these conditions.

4.5

To determine the $\chi_\wp$ we note that any homomorphism $(\mathcal{O}_K/\wp_3^k)^* \to \mathbb{Z}/6\mathbb{Z}$ is trivial on the subgroup of elements $\equiv 1 \bmod 3$ (consider the $\wp_3$-adic valuation of $(1+3x)^3$), hence it factors over $(\mathcal{O}_K/\wp_3^2)^*$. This group has 3^6-1 elements, it has a subgroup of $3^3-1 = 26$ elements which is $(\mathcal{O}_{K_0}/(3))^*$. This subgroup maps isomorphically onto $(\mathcal{O}_K/\wp_3)^*$ under the homomorphism below. The subgroup

$$(\mathcal{O}_K/\wp_3^2)_1^* := \ker\left((\mathcal{O}_K/\wp_3^2)^* \longrightarrow (\mathcal{O}_K/\wp_3)^*\right)$$

has order 3^3 and every element is 3-torsion, hence this subgroup is isomorphic to $(\mathbb{Z}/3\mathbb{Z})^3$. To be explicit, any element in $(\mathcal{O}_K/\wp_3^2)_1^*$ can be written uniquely as $x_{a,b,c} = 1 + (a + b\alpha + c\alpha^2)(1 - \zeta_3)$ with $a, b, c \in \mathbb{Z}/3\mathbb{Z}$ and any $x \in (\mathcal{O}/\wp_3^2)^*$ as $x_1 x_{a,b,c}$ with $x_1 \in (\mathcal{O}_{K_0}/(3))^*$. Then

$$\chi_{\wp_3}(x) = \epsilon(x)\zeta_3^{ka+lb+mc}, \qquad x = x_1(1 + (a + b\alpha + c\alpha^2)(1 - \zeta_3)),$$

where ϵ is either trivial or is onto $\{\pm 1\}$ and $\epsilon(x) = \epsilon(x_1)$.

Similarly, but easier, any homomorphism $(\mathcal{O}_K/\wp_{7,i}^k)^* \to \mathbb{Z}/6\mathbb{Z}$ factors over the cyclic group $(\mathcal{O}_K/\wp_{7,i})^* \cong \mathbb{Z}/6\mathbb{Z}$. We will fix an isomorphism $(\mathcal{O}_K/\wp_{7,i})^* = (\mathbb{Z}/7\mathbb{Z})^* \cong \mathbb{Z}/6\mathbb{Z}$ using the generator 3 of $(\mathbb{Z}/7\mathbb{Z})^*$. Then the characters are determined by elements $n_i \in \mathbb{Z}/6\mathbb{Z}$ as follows

$$(\chi_{\wp_{7,1}}\chi_{\wp_{7,2}})(x) = \omega^{d_1 n_1 + d_2 n_2} \qquad x \equiv (\omega^{d_1}, \omega^{d_2}) \in (\mathcal{O}_K/\wp_{7,1})^* \times (\mathcal{O}_K/\wp_{7,2})^*,$$

when the image of x in $(\mathcal{O}_K/\wp_{7,i})^*$ is 3^{d_i}.

Lemma 4.1. *With the notation above, the characters $\chi_{\wp_3}$, $\chi_{\wp_{7,1}}$ and $\chi_{\wp_{7,2}}$ are determined by:*

$$k = 0,\ l = m = 2,\ n_1 = 4,\ n_2 = 2,$$

and the character ϵ is non-trivial.

Proof. To determine ϵ and k, l, m, n_1, n_2 from 4.5 we first consider a prime $p \equiv 8$, 20 mod 21, such a prime splits as

$$(p) = \wp_1\wp_2\wp_3 \qquad p \equiv 8,\ 20 \bmod 21.$$

Since (p) already splits in $\mathcal{O}_{K_0}$, also a principal ideal domain, we can choose a generator $\pi \in \mathcal{O}_{K_0}$ for the the ideal $\wp_1 \subset \mathcal{O}_K$. Then $\chi_{\wp_3}(\pi) = \epsilon(\pi)$. Since $-\alpha \in \mathcal{O}_{K_0}^*$ maps to -2, a generator $(\mathbb{Z}/7\mathbb{Z})^*$, we may assume (after multiplying

π by a power of the unit $-\alpha$) that $\chi_{\wp_{7,i}}(\pi) = 1$ for $i = 1, 2$. (One may take $p = 29$, $\pi = \alpha^2(2 - 2\alpha + \alpha^2)$ for example). Then we get

$$\psi(\pi) = \epsilon(\pi)N_{K/K_0}(\pi) = \epsilon(-\pi)N_{K/K_0}(-\pi) = -\epsilon(-\pi)N_{K/K_0}(\pi),$$

the second equality holds because the character ψ is trivial on units, so $\psi(-1) = 1$. Hence ϵ must be the non-trivial character on $(\mathcal{O}_K/\wp_3)^*$.

Next we exploit that ψ must be trivial on units of $\mathcal{O}_K$. Since $\epsilon(-1) = -1$, $\epsilon(\alpha) = 1$ (since $\alpha \equiv (\alpha - \alpha^2)^2 \bmod \wp_3$) and $N_{K_0/\mathbb{Q}}(\alpha) = 1$ we find:

$$1 = \chi(-1) = (-1)\zeta_3^0\omega^{3n_1+3n_2}(-1), \qquad 1 = \chi(\alpha) = \zeta_3^0\omega^{4n_1+4n_2}$$

hence $n_1 \equiv -n_2 \bmod 2$ and $n_1 \equiv -n_2 \bmod 3$, hence $n_1 \equiv -n_2 \bmod 6$, so we may take $n_2 = -n_1$ from now on. Next we consider:

$$1 = \chi(\zeta_3) = \zeta_3^k(-\zeta_3)^{4n_1+2n_2}\zeta_3\bar{\zeta}_3\zeta_3 = \zeta_3^{k+n_1+2n_2+1},$$

hence $k - n_1 + 1 \equiv 0 \bmod 3$.

We can also use the action of the Galois group to get restrictions on ψ. For example if a prime p splits completely, and if $\wp$ is prime dividing p, then $\sigma_{a,b}(\psi(\pi_\wp))$ must be a Galois conjugate of $\psi(\pi_\wp)$ (both are roots of the characteristic polynomial of the Frobenius $x \mapsto x^p$), hence, considering the infinity type, $\sigma_{a,b}(\psi(\pi_\wp)) = \psi(\sigma_{a,b}(\pi_\wp))$. If $\sigma_{a,b}$ is trivial on $\mathbb{Q}(\zeta_3)$ (so $a = 1$), then it acts trivially on the values of $\chi_{\wp_3}$ and $\chi_{\wp_{7,i}}$, and it acts trivially on $\mathcal{O}/\wp_{7,i}$. However, it acts non-trivially on $(\mathcal{O}/\wp_3^2)_1$. As $\sigma_{1,2}(a + b\alpha + c\alpha^2) = a + b + 2c\alpha + (b + 2c)\alpha^2 \bmod 3$, we get $ka + bl + cm = k(a + b) + 2lc + m(b + 2c)$, this must hold for all a, b, c, hence $k \equiv 0$ and $l \equiv m \bmod 3$.

Finally we can use explicit computations to determine ψ. We considered some primes $p \equiv 1, 13 \bmod 21$ which split completely in $\mathcal{O}_K$. Let $\wp$ be prime dividing such a p, then we have:

$$N_p := \sharp X_{3,3,1}(\mathbb{F}_p) = 1 - tr_{K/\mathbb{Q}}(Fr_{\wp}) + p.$$

Taking $p = 43$, we counted points and found $N_{43} = 62$. We also found that $1 - \alpha - \zeta_3$ has norm 43 hence generates a prime ideal $\wp$ dividing 43. Therefore we must have:

$$tr_{K/\mathbb{Q}}(\psi(1 - \alpha - \zeta_3)) = -18.$$

On the other hand, computing the character gives:

$$\psi(1-\alpha-\zeta_3) = (-1)\zeta_3^{-k-l-m}(-\zeta_3)^{2n_1+4n_2}(-4-\alpha+3\alpha^2+(-9-2\alpha+3\alpha^2)\zeta_3).$$

Here we must have that the trace of $\psi(1 - \alpha - \zeta_3)$ is -18. Using the previous results, this is the case iff

$$\zeta_3^{l+n_1} = 1, \qquad \text{hence} \qquad l + n_1 \equiv 0 \bmod 3,$$

using also $n_1 \equiv 1 \bmod 3$ we get $l \equiv 2 \bmod 3$ and $n_1 = 1$ or $n_1 = 4 \bmod 6$. Using the prime $\wp = (\alpha + \zeta_3)$ over 13 and $N_{13} = 8$ we found that $n_1 = 4$ and $n_2 = 2$, which completes the determination of ψ. □

4.6 Remark.

The $\wp_3$-torsion points $A[\wp_3]$ of A form a subgroup of $A(K)$ isomorphic to $\mathcal{O}/\wp_3(\cong \mathbb{F}_{3^3})$. The divisor class $a = P - Q$, where $P = (0,0)$, $Q = (x_0, 0) \in X_{3,3,1}(K)$, with $x_0 \neq 0$, is a non-trivial element in this group. Using the $\mathcal{O}_K$-action on A we see that all points of $A[\wp_3]$ are indeed rational over K. This implies that $Fr_{\wp} \equiv 1 \bmod \wp_3$ for any prime of $\wp$ of good reduction.

4.7

To determine the local zeta function of $X_{3,3,1}$ at the prime p, it suffices to give the eigenvalue polynomial $P_p \in \mathbb{Z}[T]$ of the Frobenius $F_p : x \mapsto x^p$, in fact:

$$L_{X_{3,3,1}}(t) = p^3 t^6 P_p(t^{-1}).$$

Let $N_{K/\mathbb{Q}}(\wp) = p^n$, then $F_p^n = Fr_\wp = \psi(\pi_\wp)$ and we have:

$$P_p(T) = \prod_{\wp|p} \left(T^n - \psi(\pi_\wp)\right).$$

In case $p \equiv 1, 13 \bmod 21$, the ideal (p) splits completely in $\mathcal{O}_K$, hence

$$P_p(T) = \prod_{\wp|p}(T - \psi(\pi_\wp)), \qquad (p \equiv 1, 13 \bmod 21),$$

hence $L_{X_{3,3,1}}(t) = \prod_{\wp|p}(1 - \psi(\pi_\wp)t)$. We also have $\psi(\pi_\wp) = Fr_\wp \equiv 1 \bmod \wp_3$ (and $\wp_3 = (1 - \zeta_3)$) for all $\wp$ dividing p.

The case $p \equiv 8,\ 20 \bmod 21$ was discussed earlier. We have $(p) = \wp_1\wp_2\wp_3$ in $\mathcal{O}_K$, we can choose generators $\pi_\wp \in \mathcal{O}_{K_0}$ and $\psi(\pi_\wp) = N_{K/K_0}(\pi_\wp) = \pm p$. By the previous remark (or by using the explicit form of ψ) one finds that $\psi(\wp) = -p$, hence

$$P_p(T) = (T^2 + p)^3, \qquad (p \equiv 8, 20 \bmod 21),$$

so $L_{X_{3,3,1}}(t) = (pt^2 + 1)^3$.

In case $p \equiv 4, 10, 16, 19 \bmod 21$, we have $(p) = \wp_1\wp_2$ and we can choose generators $\pi_\wp \in \mathbb{Z}[\zeta_3]$, in fact, the condition $\pi_\wp \equiv 1 \bmod 3$ determines the generator uniquely. Then $\psi(\pi_\wp) = \omega^a \pi_\wp \overline{\pi_\wp} \pi_\wp = \omega^a p \pi_\wp$ for some $a \in \mathbb{Z}/6\mathbb{Z}$ which can be determined explicitly. Then we find:

$$P_p(T) = T^6 - (\psi(\pi_\wp) + \overline{\psi(\pi_\wp)})T^3 + p^3, \qquad (p \equiv 4, 10, 16, 19 \bmod 21),$$

hence $L_{X_{3,3,1}}(t) = p^3 t^6 - (\psi(\pi_\wp) + \overline{\psi(\pi_\wp)})t^3 + 1$.

In the remaining cases, the ideal (p) is prime in $\mathcal{O}_K$ and $Fr_p = \psi(p) = -p^3$, hence

$$P_p(T) = T^6 + p^3, \quad (p \equiv 2, 5, 11, 17 \bmod 21),$$

hence $L_{X_{3,3,1}}(t) = p^3 t^6 + 1$.

4.8 Comparison.

Comparing the theorem above with Theorem 3.3 it is clear that they give consistent results, except maybe in the case that p splits in two or six prime ideals. However it is easy to check that also in these cases both methods give the same result.

In fact, assume $p = \wp_1 \wp_2$ and choose a generator $\pi \in \mathbb{Z}[\zeta_3]$ for $\wp_1$, so $\pi\overline{\pi} = p$. Multiplying π by a suitable power of $\omega = -\zeta$, we may assume that $\pi \equiv 1 \bmod 3$ and hence that $\chi_{\wp_3}(\pi^{-1}) = 1$. Let $r, s \in \mathbb{Z}/6\mathbb{Z}$ be such that

$$\pi \longmapsto (3^r, 3^s) \in (\mathbb{Z}/7\mathbb{Z})^2 \cong \mathcal{O}_K/\wp_{7,1} \times \mathcal{O}_K/\wp_{7,2}.$$

Then $(\chi_{\wp_{7,1}} \chi_{\wp_{7,2}})(\pi^{-1}) = (-\zeta_3)^{-4r-2s} = \zeta_3^{2r+s}$. Thus we get

$$\psi(\pi) = \zeta_3^{2r+s} p\overline{\pi}.$$

Now assume that $p \equiv 16 \bmod 21$, hence $p \equiv 2 \equiv 3^2 \bmod 7$. Then $p = \pi\overline{\pi} \mapsto (3^r, 3^s)(3^s, 3^r) = (3^{r+s}, 3^{r+s})$, hence $r = 2 - s$ and $\psi(\pi) = \zeta_3^{1-s} p\overline{\pi}$. Next we show that, with $k = 1 - s$, $\zeta_3^k p\overline{\pi} - \pi^3$ has Norm divisible by 7, hence the L function from Theorem 3.3(3) coincides with the one computed with the Hecke character. We have (recall $\zeta_3 \mapsto (2, 4) = (3^2, 3^4)$ and $r = 2 - s$):

$$\zeta_3^{1-s} p\overline{\pi} - \pi^3 \longmapsto (3^{2(1-s)+2+r} - 3^{3r},\ 3^{4(1-s)+2+s} - 3^{3s}) \equiv (0, 0)$$

so indeed $N_{\mathbb{Q}(\zeta_3)/\mathbb{Q}}(\zeta_3^{1-s}\overline{\pi}p - \pi^3) \equiv 0 \bmod 7$. The cases $p \equiv 4, 10, 19 \bmod 21$ can be done similarly.

Finally we consider the case $p \equiv 1 \bmod 21$ (the case $p \equiv 13 \bmod 21$ is similar). Let $\wp$ be a prime ideal in $\mathcal{O}_K$ dividing p and let $\pi_\wp \in \mathcal{O}_K$ be a generator. Multiplying $\pi_\wp$ with -1 if necessary, we may assume that $\pi_\wp$ is congruent to a square mod $(1-\zeta_3)$, in particular $\epsilon(\pi_\wp^{-1}) = 1$ and $\chi_{\wp_3}(\pi_\wp^{-1})$ is a cube root of unity. Then

$$\eta := \psi(\pi_\wp) = (\chi_{\wp_3}\chi_{\wp_{7,1}}\chi_{\wp_{7,2}})(\pi_\wp^{-1}) \cdot \sigma_{1,1}(\pi_\wp)\sigma_{2,2}(\pi_\wp)\sigma_{1,4}(\pi_\wp),$$

and it is easy to see that $\eta \equiv 1 \mod (1-\zeta_3)$.

Let $\pi \in \mathbb{Z}[\zeta_3]$, $\pi \equiv 1 \bmod 3$, be the unique element such that πp generates the ideal $(N_{K/\mathbb{Q}(\zeta_3)}(\eta))$ in $\mathbb{Z}[\zeta_3]$. Thus

$$\pi p = \zeta_3^k \sigma_{1,1}(\pi_\wp)\sigma_{1,2}(\pi_\wp)\sigma_{1,4}(\pi_\wp),$$

where k is chosen such that $\pi \equiv 1 \bmod 3$ (as $\pi_\wp$ is a square mod $(1-\zeta_3)$, also $\sigma_{1,1}(\pi_\wp)\sigma_{1,2}(\pi_\wp)\sigma_{1,4}(\pi_\wp) \in \mathbb{Z}[\zeta_3]$ is a square mod $(1-\zeta_3)$ and hence is 1 mod $(1-\zeta_3)$). Theorem 3.3(4) asserts that

$$(\chi_{\wp_3}\chi_{\wp_{7,1}}\chi_{\wp_{7,2}})(\pi_\wp^{-1})\sigma_{2,2}(\pi_\wp) \equiv \zeta_3^k \sigma_{1,2}(\pi_\wp) \qquad \bmod \wp_{7,i}$$

for each of the primes $\wp_{7,i}$ over 7.

To compute k and $\chi_{\wp_3}(\pi_\wp)$, we write $\pi_\wp = x_1(1 + x_2(1-\zeta_3)) \bmod 3$ with $x_2 = a + b\alpha + c\alpha^2$. Then $\sigma_{1,1}(\pi_\wp)\sigma_{1,2}(\pi_\wp)\sigma_{1,4}(\pi_\wp)$ is congruent to $\zeta_3^{-tr(x_2)}$ mod 3, so $k = tr(x_2)$, with

$$tr(x_2) := tr_{K/\mathbb{Q}(\zeta_3)}(a + b\alpha + c\alpha^2) \equiv b + c \mod 3.$$

As $\epsilon(\pi_\wp) = 1$, $\chi_{\wp_3}(\pi_\wp^{-1}) = \zeta_3^{-2(b+c)} = \zeta_3^{tr(x_2)}$, so it remains to prove that:

$$(\chi_{\wp_{7,1}}\chi_{\wp_{7,2}})(\pi_\wp^{-1})\sigma_{2,2}(\pi_\wp) \equiv \sigma_{1,2}(\pi_\wp) \qquad \bmod \wp_{7,i}.$$

Since $Gal(K/\mathbb{Q}(\zeta_3))$ acts trivially modulo each of the $\wp_{7,i}$'s, we have $\sigma_{2,2}(\pi_\wp) \equiv \overline{\pi_\wp}$ and $\sigma_{1,2}(\pi_\wp) \equiv \pi_\wp$ modulo $\wp_{7,i}$. Let r, s be such that $\pi_\wp \mapsto (3^r, 3^s) \in$

$(\mathbb{Z}/7\mathbb{Z})^2$, so $\overline{\pi_\wp} \mapsto (3^s, 3^r)$. The fact that $p \equiv 1 \mod 7$ implies that $(\pi_\wp \overline{\pi_\wp})^3 \mapsto (1,1)$, so $r+s \equiv 0 \mod 2$. As above, $(\chi_{\wp_{7,1}} \chi_{\wp_{7,2}})(\pi_\wp^{-1}) = \zeta_3^{2r+s} \mapsto (3^{4r+2s}, 3^{2r+4s})$. Therefore

$$(\chi_{\wp_{7,1}} \chi_{\wp_{7,2}})(\pi_\wp^{-1}) \cdot \overline{\pi_\wp} \longmapsto (3^{4r+3s}, 3^{3r+4s}) \equiv (3^r, 3^s),$$

which coincides with the image of $\pi_\wp$. Hence we verified the congruence from Theorem 3.3(4).

References

[1] Berndt, B.C., Evans, R.J., Williams, K.S.,*Gauss and Jacobi Sums*, Wiley-Interscience Publication, 1997

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

[3] R. P. Holzapfel, *The Ball and Some Hilbert Problems*, Birkhäuser (1995).

[4] R. P. Holzapfel and F. Nicolae, *Arithmetic on a Family of Picard curves*, Proceedings of the Sixth International Conference on Finite Fields with Applications 2001, Springer (2003) 187–208.

[5] K. Koike and A. Weng, *Construction of CM-Picard curves with application to cryptography*, preprint (2003).

[6] S. Lang, *Complex Multiplication*, Springer (1983).

[7] F. Lemmermeyer, *Reciprocity laws*, Springer (2000).

[8] P. van Wamelen, *Examples of genus two CM curves defined over the rationals*, Math. Computation **68** (1999), no. 225 307–320.

[9] P. van Wamelen, *Proving that a genus 2 curve has complex multiplication*, Math. Computation **68** (1999), no. 228, 1663–1677.

[10] A. Weng, *A class of hyperelliptic CM-curves of genus three*, J. Ramanujan Math. Soc. **16** (2001), no. 4, 339–372.