J. reine angew. Math. **432** (1992), 151—176

Journal für die reine und
angewandte Mathematik

The Hasse zeta function of a $K3$ surface related to the number of words of weight 5 in the Melas codes

By *C. Peters* at Leiden, *J. Top* at Rotterdam and *M. van der Vlugt* at Leiden

0. Introduction

In a paper on weight distributions of codes R. Schoof and M. van der Vlugt derive formulas for the binary Melas codes [S-V], Table 6.4. Their method is rather roundabout. First, the weight distribution for the dual code is determined. Then they apply the MacWilliams identities and the Eichler-Selberg trace formula for Hecke operators. The final results then follow after involved computations.

It is natural to ask whether these formulas can be derived in a more direct way. In trying to do so for the number w_5 of words of weight 5, an interesting $K3$-surface $\tilde{X}$ defined over $\mathbb{Q}$, came up. It is the minimal resolution of singularities of the surface in $\mathbb{P}^4$ given by the two equations

$$x_1 + x_2 + x_3 + x_4 + x_5 = 0\,,$$

$$x_2 x_3 x_4 x_5 + x_1 x_3 x_4 x_5 + x_1 x_2 x_4 x_5 + x_1 x_2 x_3 x_5 + x_1 x_2 x_3 x_4 = 0\,.$$

This $K3$-surface turns out to have maximal Picard number and we have been able to compute its Hasse zeta function over its field of definition $\mathbb{Q}$.

To put this result into perspective we recall some results from [S-I] where $K3$-surfaces Y with maximal Picard number are classified. One supposes that Y is defined over an algebraic number field L which is large enough so that all twenty algebraic cycles are defined over L. Then the zeta function of the reduction $Y(\mathfrak{p})$ of Y at a good prime ideal $\mathfrak{p}$ of L, is of the form

$$1/Z(Y, t) = (1 - t)(1 - q^2 t)(1 - qt)^{20} Q_2(t), \quad q = \mathrm{Norm}_{L|\mathbb{Q}}\,\mathfrak{p}\,,$$

where the quadratic polynomial $Q_2(t)$ can be found using the geometry of the situation, as we sketch now. Canonically associated to Y we have an elliptic curve E_Y with complex multiplication by $\mathbb{Q}(\sqrt{d})$, where d denotes the discriminant of the Néron-Severi group.

Assuming L is large enough (so that various geometric objects needed in the proof given in [S-I] are defined over L) the zeta function of $E_Y(\mathfrak{p})$ completely determines the polynomial $Q_2(t)$. In fact $Q_2(t) = (1-\beta^2 t)(1-\bar{\beta}^2 t)$, where β and $\bar{\beta}$ are the roots of Frobenius at $\mathfrak{p}$ acting on the Tate module of E_Y. In particular, the Tate conjecture [Ta], Conjecture 2, p. 104, now follows for $Y(\mathfrak{p})$.

In our situation $\tilde{X}$ is defined over $\mathbb{Q}$ and $d = -2^2 \cdot 15$, but the preceding results only apply after replacing $\mathbb{Q}$ by some extension of $\mathbb{Q}$ which we don't know explicitly. It is therefore interesting to show that for $\tilde{X}$ the results of [S-I] can be made precise in every detail.

Using the geometry of $\tilde{X}$ and the Weil conjectures we determine the zeta function $Z(t)$ of the (non-singular) reduction of $\tilde{X}$ modulo a prime $p \neq 3, 5$. We find

$$1/Z(t) = (1-t)(1-p^2 t)(1-pt)^{16}\left(1-\left(\frac{p}{3}\right)pt\right)^4\left(1-A_p t+\left(\frac{p}{15}\right)p^2 t^2\right).$$

The interesting factor in the zeta function for $\tilde{X}(p)$, $p \neq 3, 5$ is the degree two polynomial $Q_2(t)$ which in this case is equal to $1 - A_p t + \left(\frac{p}{15}\right) p^2 t^2$.

It remains to determine the numbers A_p. To do this, we first construct an elliptic curve E over $\mathbb{Q}(\sqrt{5})$ isogenous to $E_{\tilde{X}}$ and show that the polynomial $Q_2(t)$ coincides with the corresponding polynomial $Q_2'(t)$ for the reduction mod p of the Weil-restriction A of E from $\mathbb{Q}(\sqrt{5})$ to $\mathbb{Q}$. This is an abelian surface.

The most direct way to prove this would have been by means of some algebraic correspondence between A and $\tilde{X}$ defined over a small explicitly given field. We have not been able to do this. Instead, we have applied a method due to Faltings, Serre and Livné (cf. [L]) to the L-function with local factors corresponding to the polynomials $Q_2(t)$. In our case this method provides a small list of primes with the property that this L-function is completely determined by the local factors at the primes of the list. Since in our case these local factors $Q_2(t)$ and $Q_2'(t)$ are the same, equality of the L-functions follows.

Moreover, we show that our L-function can be described in a completely different way as the L-function associated to a Hecke eigenform in $S_3(15, (\frac{\cdot}{15}))$. The essential step in proving this consists in showing that our L-function satisfies a functional equation. This functional equation is in perfect agreement with conjecture C. 5.1 of Serre in [Se 2]. Our main result is also in accordance with a generalisation of the Taniyama-Weil conjecture, which fits into Langlands program (see [G] for an excellent introduction).

The main result can now be stated as follows:

(0.1) Theorem. *The number of $\mathbb{F}_p$-rational points of the $K3$-surface $\tilde{X}$ $(p \neq 3, 5)$ is equal to*

$$1 + p^2 + p \cdot \left(16 + 4\left(\frac{p}{3}\right)\right) + A_p,$$

where the number A_p is the coefficient of q^p in the q-expansion of

$$\left(\sum_{m,n\in\mathbb{Z}} q^{m^2+mn+4n^2}\right)\cdot q\cdot\prod_{r=1}^{\infty}(1-q^r)(1-q^{3r})(1-q^{5r})(1-q^{15r}).$$

Now it is easy to find back the formula for w_5 from [S-V], Table 6.4:

$$w_5=\frac{q-1}{5!}(q^2-14q+41+(-1)^r(-6q+30)+B_r),\quad B_r:=\omega^r+\bar{\omega}^r,\ \omega:=\frac{1}{2}(1+\sqrt{-15}).$$

Namely, the shape of the zeta function tells us that the number of $\mathbb{F}_p$-rational points of $\tilde{X}$ determines the number N_q of points of $\tilde{X}$ over $\mathbb{F}_q$ with $q=p^r$. Geometric considerations which we present in detail in section 1, show that the number w_5 is related to N_q with $q=2^r$ in a straightforward manner and we find back the above formula.

We employ the following notation throughout:

For any variety X defined over the integers, we let $X(p)$ be its reduction modulo p and we let $N_q(X)$ be the number of points defined over the field $\mathbb{F}_q$, $q=p^r$, of a variety X in characteristic p or of the reduction $X(p)$ if X is defined over the integers.

We want to thank Bas Edixhoven, Torsten Ekedahl, Ron Livné, Ulf Persson and René Schoof for various enlightening conversations. Also, we want to thank J.-P. Serre for helpful correspondence.

1. Melas codes

Recall that a linear code $\mathscr{C}$ over $\mathbb{F}_q$ is a subspace of the vector space $\mathbb{F}_q^n$, $q=p^r$. The number n is called the length of the code and $\dim\mathscr{C}$ is called its dimension. Its elements are called words and the weight of a word is the number of its non-zero coordinates. The weight enumerator polynomial is

$$\sum_j w_j t^j,\quad w_j:=\{\text{the number of words in }\mathscr{C}\text{ of weight } j\}.$$

With α a generator of the multiplicative group $\mathbb{F}_q^*$, consider the $\mathbb{F}_q$-code of length $q-1$ given by

$$\ker\begin{pmatrix}1 & \alpha & \alpha^2 & \dots & \alpha^{q-2}\\ 1 & \alpha^{-1} & \alpha^{-2} & \dots & \alpha\end{pmatrix}.$$

The p-ary Melas code $\mathscr{M}(q)$ is the restriction to $\mathbb{F}_p$ of this code so that its words are:

$$\{(c_0,\dots,c_{q-2})\in\mathbb{F}_p^{q-1}\mid\sum_j c_jx_j=0,\ \sum_j c_jx_j^{-1}=0\},$$

where $x_j, j=0,\dots,q-2$ are the $q-1$ distinct non-zero elements in $\mathbb{F}_q$ taken in some order.

We are interested in the number w_5 of words of weight 5 in binary Melas codes. Note that in characteristic two, code words of weight k are points on the affine variety in x-space given by

$$X_k' := \{(x_1, x_2, \ldots, x_k) \in (\mathbb{F}_q^*)^k \mid \sum_j x_j = 0, \quad \sum_j x_j^{-1} = 0\}.$$

Only points with all coordinates different actually give code words. To count their number geometrically, we first consider the projective variety

$$X_k := \{(x_1, x_2, \ldots, x_k) \in \mathbb{P}^{k-1} \mid x_1 + \cdots + x_k = 0, \\ x_2 x_3 \cdots x_k + x_1 x_3 \cdots x_k + \cdots + x_1 x_2 \cdots x_{k-1} = 0\}.$$

The affine variety is obtained from X_k by deleting the hyperplanes "at infinity" $x_j = 0$, $j = 1, \ldots, k$, which gives us the projective variety $\mathbb{P}(X_k')$ of lines in X_k'. A point of X_k with one coordinate equal to zero automatically has two coordinates equal to zero and belongs to the hyperplane $x_1 + \cdots + x_k = 0$. Conversely, every point on this hyperplane of weight at most $k - 2$ is a point on the intersection of X_k with a hyperplane at infinity. We denote by $N_q(Y)$ the number of points of a variety Y with all coordinates in $\mathbb{F}_q$. A combinatorial argument then gives:

$$(1.1) \qquad N_q(X_k) = N_q(\mathbb{P}(X_k')) + \sum_{r=1}^{k-2} \binom{k}{r} \frac{(q-1)^{r-1} + (-1)^r}{q}.$$

Let us now specify to $k = 5$. Then X_5 is a surface. The ten points which form the $\mathfrak{S}_5$-orbit of $(1, -1, 0, 0, 0)$ are all singular on X_5; in fact they are ordinary double points which become smooth after one blow up. The resulting surface $\tilde{X}_5$ is smooth. Since every singular point is defined over the ground field $\mathbb{F}_2$ and is replaced by a projective line upon blowing up, we derive

$$N_q(\tilde{X}_5) = N_q(\mathbb{P}(X_5')) + 20q - 10.$$

The number w_5 is the number of $\mathfrak{S}_5$ orbits of points on X_5' with all coordinates different. These points belong to

$$X_5'' := X_5' \setminus \bigcup_{i \neq j} (x_i + x_j = 0),$$

and we find $w_5 = \dfrac{q-1}{5!} \cdot N_q(\mathbb{P}(X_5''))$. The configuration Δ given by the intersection in $\mathbb{P}(X_5')$ of the union of the planes H_{ij} with equations $x_i + x_j = 0$ for $i \neq j$, $i, j = 1, \ldots, 5$ can be studied easily. They do not contain points over $\mathbb{F}_{2^r}$ if r is odd and if r is even an easy counting argument gives $N_q(\Delta) = 20(q - 3)$. Combining this with the previous formula we deduce:

(1.2) Proposition. *With $q = 2^r$ we have*

$$N_q(\tilde{X}_5) = 5!(q-1)w_5 + 30q - 40 + (-1)^r(10q - 30).$$

In order to find the formula for w_5 in a direct way we must compute $N_q(\tilde{X}_5)$ directly. Note that if we use the result for w_5 from [S-V], Table 6.4, we get

$$N_q(\tilde{X}_5) = 1 + q^2 + q\bigl(16 + (-1)^r 4\bigr) + B_r, \tag{1.3}$$

where

$$B_r = \omega^r + \bar{\omega}^r \quad \text{with} \quad \omega = \frac{1}{2}(1 + \sqrt{-15}).$$

Since the variety X_5 is defined by equations having integral coefficients, we can study it in any characteristic; we set

$$\begin{aligned} X := X_5 = \{&(x_1, x_2, x_3, x_4, x_5) \in \mathbb{P}^4 \mid x_1 + x_2 + x_3 + x_4 + x_5 = 0, \\ &x_2x_3x_4x_5 + x_1x_3x_4x_5 + x_1x_2x_4x_5 + x_1x_2x_3x_5 + x_1x_2x_3x_4 = 0\}. \end{aligned}$$

and

$$\tilde{X} := \text{the blow up of } X_5 \text{ in the } \mathfrak{S}_5\text{-orbit of } (1, -1, 0, 0, 0).$$

This surface is considered to be defined over $\mathbb{Q}$. It is non-singular and reduces to a non-singular surface $\tilde{X}(p)$ in all finite characteristics p except 3 and 5.

From now on we assume that:

the characteristic p is different from 3 *and* 5.

2. The Néron-Severi group

The Néron-Severi group $NS(Y)$ of a non-singular algebraic variety Y over a field k is the group of its divisors (over an algebraic closure of k) modulo numerical equivalence. This is a group of finite rank $\varrho(Y)$, the Picard number. If Y is a surface, intersection-pairing induces on $NS(Y)$ modulo torsion the structure of a $\mathbb{Z}$-lattice, which is called the *Picard-lattice*. In characteristic zero, we can find back this lattice inside $H^2(Y, \mathbb{Z})$ as the sublattice generated by classes of (1,1)-type. See e.g. [B-P-V], Chapter I.6. It follows that $\varrho \leqq h^{1,1}(Y)$, where $h^{1,1}(Y)$ is the dimension of the Hodge component $H^{1,1}(Y)$. Later we shall work with l-adic cohomology. In characteristic zero we shall embed the Picard lattice in the vector space $H^2_{\text{ét}}(Y, \mathbb{Q}_l)$ and we write

$$H^2_{\text{alg}}(Y, \mathbb{Q}_l)$$

for the subspace it generates. In finite characteristics we only consider reductions of varieties defined over some number field k and for those H^2_{alg} denotes the subspace of $H^2_{\text{ét}}$ generated by classes of cycles which are reductions of cycles defined over an algebraic closure of k. In both cases we define the *transcendental subspace* by

$$H^2_{\text{trc}}(Y, \mathbb{Q}_l) := H^2_{\text{alg}}(Y, \mathbb{Q}_l)^{\perp} \subset H^2_{\text{ét}}(Y, \mathbb{Q}_l).$$

If Y is a $K3$-surface in characteristic zero, it is well-known that $h^{1,1} = 20$ (see [B-P-V], Chapter VIII, 3). So in characteristic zero $\varrho(Y) \leqq 20$. In positive characteristic p we only have $\varrho(Y) \leqq b_2(Y) = 22$, where $b_2(Y) = \dim H^2_{\text{ét}}(Y, \mathbb{Q}_l)$, $l \neq p$. In fact, if $\varrho(Y) > 20$, it must be equal to 22 and the $K3$-surface is called *supersingular*. See [A] for details.

In this section we set:

$$x := x_2, \quad y := x_3, \quad z := x_4, \quad t := x_5 .$$

In projective three-space with these coordinates the equation of our singular surface X is:

$$(x + y + z + t)(xyz + xyt + xzt + yzt) - xyzt = 0 .$$

Recall that the surface $\tilde{X}$ is obtained from X by blowing up the 10 points which form the $\mathfrak{S}_5$-orbit of $(1, -1, 0, 0, 0)$ (in the 'old' coordinates x_j). One easily checks that in any characteristic these are ordinary double points and that in all characteristics different from 3 and 5 there are no other singular points. So $\tilde{X}$ as well as the reductions $\tilde{X}(p)$, $p \neq 3, 5$ are non-singular.

(2.1) Proposition. *$\tilde{X}$ is a $K3$-surface.*

Proof. In fact, any surface which is the minimal resolution of singularities of a surface given by a degree four equation in projective space with at most rational double points is a $K3$-surface. We see this as follows. First of all, the usual Lefschetz theorem on hyperplane sections [M], section 7, shows that X is simply connected. Since there are finitely many ordinary double points it follows that also the resolution of singularities $\tilde{X}$ of X is simply connected. Secondly, the adjunction formula [B-P-V], Chapter I, Proposition 6.3, shows that the canonical bundle is trivial. □

To understand the Néron-Severi-group of a $K3$-surface it is useful to have an elliptic fibration. To produce one, we consider the following picture, where P_{ij} are the double points of the surface X and where we have drawn all the lines passing through 3 of the singular points. These lines all lie in X.

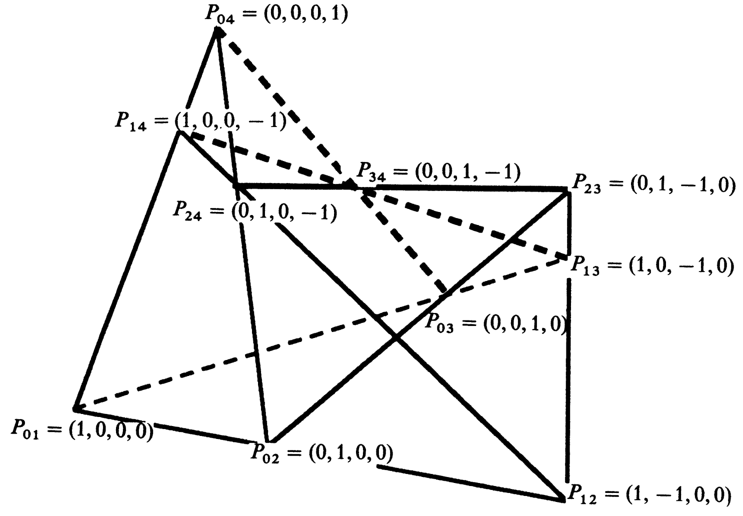

Figure 1. Special lines

Consider the pencil $s_1 t = s_0 z$ of planes through $L_0 := \{t = 0 = z\}$, one of these lines. For simplicity, we set $s = s_0/s_1 \in \mathbb{C} \cup \infty$. Each of these planes cuts X in $L_0 \cup C_s$, with C_s

a curve of degree 3, which for most values of s is non-singular and thus defines an elliptic curve. This gives the desired elliptic fibration

$$f: \tilde{X} \to \mathbb{P}^1(s).$$

The equation of the fibre C_s in the x, y, z-plane is given by:

$$s(x+y)^2 z + (1+s+s^2)xyz + s(1+s)(x+y)z^2 + (1+s)xy(x+y) = 0.$$

This curve has a flex at $(1, -1, 0)$ with tangent line given by

$$x + y + uz = 0, \quad u := (1+s+s^2)/(1+s).$$

Now transform this line to infinity, such that the flex becomes $(0, 1, 0)$ by introducing new coordinates

$$\begin{aligned} X &= x + y, \\ Y &= -y, \\ vZ &= x + y + uz, \quad v = s^2/(1+s+s^2)^2. \end{aligned}$$

We arrive at the following Weierstrass-equation for the cubic curve

$$X^3 + a_2 X^2 Z + a_4 X Z^2 = Y^2 Z + XYZ,$$

$$a_2 = -\frac{(s^{-1}+3+s)}{(s^{-1}+1+s)^2}, \quad a_4 = \frac{(s^{-1}+2+s)}{(s^{-1}+1+s)^4}.$$

Note that the coefficients a_2 and a_4 are functions of $s^{-1}+s$, which makes the computation of the discriminant $\Delta := a_4^2[(1+4a_2)^2 - 64a_4]$ (see [Si], p. 46) a lot easier. In fact, we find in homogeneous coordinates

$$\Delta = \frac{(s_0+s_1)^4 (s_0 s_1)^6 (s_0^2 - 7 s_0 s_1 + s_1^2)}{(s_0^2 + s_0 s_1 + s_1^2)^9}.$$

Consequently, one has singular fibres C_s for $s = 0, \infty, -1, \varrho, \varrho^2, \sigma, \bar{\sigma}$, where ϱ is a primitive third root of unity, while σ and $\bar{\sigma}$ are the roots of $x^2 - 7x + 1 = 0$. As a first step towards the computation of the Néron-Severi group we shall classify these singular fibres according to Kodaira's classification (cf. [B-P-V], Chapter V.7).

(2.2.) Lemma. *The singular fibres are all of type* I_n.

(i) *Type* I_6 *occurs over* $s = 0$ *and* $s = \infty$, *type* I_4 *over* $s = -1$, *type* I_3 *over* $s = \varrho$ *and* $s = \varrho^2$ *and finally over* σ *and* $\bar{\sigma}$ *we have an* I_1*-fibre.*

(i) *For the reduction* $\tilde{X}(p)$, p *odd, the components of the reducible fibres are of the same type. They are defined over the ground field precisely when* $\left(\frac{p}{3}\right) = 1$. *If* $\left(\frac{p}{3}\right) = -1$, *Frobenius interchanges the two fibres of type* I_3 *componentwise. Moreover, only two of the four components of the* I_4*-fibre are defined over the ground field in this case, the other two components are interchanged by Frobenius. The components of the other reducible fibres are all defined over the ground field.*

(iii) *If* $p = 2$, *there are no type* I_1*-fibres and the two* I_3*-fibres reduce to fibres of type* IV.

Proof. (i) Inspection of Fig. 1 immediately shows the nature of the singular fibres over 0 and over ∞. The fibre over -1 consists of the component coming from blowing up P_{34}, the line $t = 0 = z$ and the two lines $\{(\varrho\mu, \varrho^2\mu, \lambda, -\lambda)\}$ and $\{(\varrho^2\mu, \varrho\mu, \lambda, -\lambda)\}$ with $(\lambda, \mu) \in \mathbb{P}^1$. The fibre over ϱ consists of the three lines through the three points $(1, 1, \varrho, \varrho^2)$, $(1, -1, \varrho, \varrho^2)$ and $(-1, 1, \varrho, \varrho^2)$ and a similar property holds for the fibre over ϱ^2. The discriminant Δ has a simple zero for σ and $\bar{\sigma}$ so that the planes $t = \sigma z$ and $t = \bar{\sigma} z$ are simply tangent to the surface X and hence the corresponding singular fibre has precisely one node, which means that it is an I_1-fibre.

(ii) and (iii) Note that $\varrho = \sigma$ if and only if $p = 2$. It follows that after reduction, the fibre types remain the same, except maybe if $p = 2$. The components of the I_3-fibres remain distinct after reduction modulo 2, but the three points of intersection come together, creating a type IV singular fibre. The assertions about the fields of definition of the fibral components and about the action of Frobenius are clear. □

Remark. From the singular fibres we see that the Euler number of the non-singular model $\tilde{X}$ for X is equal to $2 \cdot 6 + 4 + 2 \cdot 3 + 2 \cdot 1 = 24$, as could be expected, since $\tilde{X}$ is a $K3$-surface. A similar remark applies to $\tilde{X}(p)$, $p \neq 3, 5$.

Having studied the fibres, we now consider sections of the elliptic fibration f, i.e. rational points of the corresponding elliptic curve defined over the field of rational functions in s.

Let us first observe that the preceding computation shows that the zero section S_0 corresponds to the blown up point P_{12}.

Next, we note that by Shioda's theorem [Sh], Cor. 1.5, the group of sections of f has rank at most $20 - 2 - 2 \cdot 5 - 3 - 2 \cdot 2 = 1$. Moreover, if the rank is 1, it follows at the same time that the Néron-Severi group has maximal rank, i.e. 20. This is indeed the case, namely we show that the following two lines are sections of infinite order:

$$S := \{(\varrho^2\mu, -\lambda, \lambda, \mu) \mid (\lambda, \mu) \in \mathbb{P}^1\}, \quad S' := \{(\varrho\mu, -\lambda, \lambda, \mu) \mid (\lambda, \mu) \in \mathbb{P}^1\}.$$

(2.3) Lemma. *The sections S and S' have infinite order and hence, the Picard number of $\tilde{X}$ is maximal, i.e.* 20. *In $\tilde{X}(p)$ the cycles S and S' are defined over the ground field precisely when* $\left(\frac{p}{3}\right) = 1$ *and over* $\mathbb{F}_{p^2}$ *otherwise.*

Proof. We show that the order of the point which S defines on the special fibre for $s = \varrho$ is infinite. A similar reasoning can be given for S'. The smooth points on this special fibre (over the complex numbers) form a group isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{C}^{\times}$. In fact, the component through the zero-section is the line $L_{\varrho}^{0} := (x + y = 0) \cap (t = \varrho z)$. We take z/x as inhomogeneous coordinate on this line. Then the zero-section corresponds to 0 and the points Q_1, Q_2 of intersection of L_{ϱ}^{0} with the two other fibre components correspond to ϱ^2 and $-\varrho^2$. If we send these three points to 1, ∞, 0 respectively, we get an explicit isomorphism from $L \backslash \{Q_1, Q_2\}$ to $\mathbb{C}^{\times}$ sending the "origin" to 1. Under this isomorphism, a point with inhomogeneous coordinate b maps to

$$a = D(a, 1, 0, \infty) = D(b, 0, -\varrho^2, \varrho^2) = -(b + \varrho^2)/(b - \varrho^2),$$

where D is the cross ratio. In particular, since the section S meets the fibre in $(1, -1, 1, \varrho)$ with inhomogeneous coordinate $b = 1$, we get $a = \frac{\sqrt{-3}}{3}$, which has infinite order. □

Having determined the rank of the Néron-Severi group, we want to give generators and relations. In order to do so, we need the torsion sections.

(2.4) Lemma. *The torsion subgroup T of the group of all sections of f is isomorphic to $\mathbb{Z}/6\mathbb{Z}$. It is given by the three exceptional curves of self intersection -2 coming from resolving the three double points P_{01}, P_{02} and P_{12} (the last curve in fact corresponds to the zero section in the Weierstrass-model) and the three lines through P_{34} which are drawn more heavily in Fig. 1. These sections are defined over $\mathbb{Z}$.*

Proof. Let us rewrite the Weierstrass-form as

$$X(X - X_1 Z)(X - X_2 Z) = Y^2 Z + YXZ,$$

$$X_1 = \frac{s^2}{(1 + s + s^2)^2}, \quad X_2 = \frac{s(s+1)^2}{(1 + s + s^2)^2}.$$

Let $S_0 = (0, 1, 0)$, $S_1 = (X_1, 0, 1)$, $S_2 = (X_2, 0, 1)$, $S_3 = (0, 0, 1)$, $S_4 = (X_1, -X_1, 1)$, $S_5 = (X_2, -X_2, 1)$. These points precisely correspond to the six given curves. The following relations can be checked:

$$2S_3 = S_0, \quad 2S_1 = S_4 = -S_1, \quad S_1 + S_3 = S_5, \quad S_2 + S_3 = S_4.$$

From these relations it follows that the given curves define a torsion group isomorphic to $\mathbb{Z}/6\mathbb{Z}$. Now, we use [M-P], table 4.5, to see that the only possible torsion group T which contains $\mathbb{Z}/6\mathbb{Z}$ in our case (which corresponds to $\chi = 2$, $R \leqq 1$ in the cited table) must be $\mathbb{Z}/6\mathbb{Z}$. □

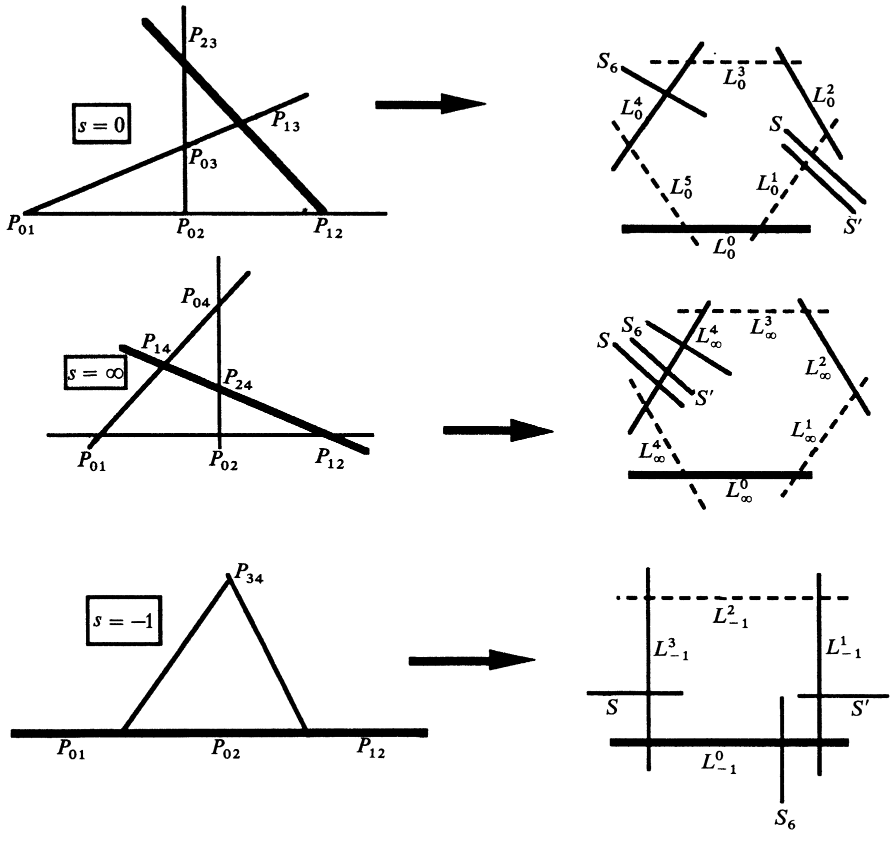

Figure 2. The special fibres at 0, ∞ and -1

Now we come to the main result of this section:

(2.5) Theorem. *The Néron-Severi group of the $K3$-surface $\tilde{X}$ is generated by the following divisor classes:*

– *The class f of a fibre,*

– *the classes s_0, s_6, s of the zero-section S_0, the section S_6 of order six defined by P_{01} and the infinite order section S,*

– *the classes $l_s^{j_s}$ of the components of the special fibres*

$$L_s^{j_s} \quad (s = 0, \infty, -1, \varrho, \varrho^2, \quad j_0, j_\infty = 1,2,3,4,5, \quad j_{-1} = 1,2,3, \quad j_\varrho, j_{\varrho^2} = 1,2)$$

not meeting the zero-section. See Fig. 2 and Fig. 3.

The only relation between these classes is:

$$-3(s_6 - s_0) = -6f + (l_\varrho^l + 2l_\varrho^2) + (l_{\varrho^2} + 2l_{\varrho^2}^2) + (l_0^1 + 2l_0^2 + 3l_0^3 + 4l_0^4 + 2l_0^5)$$
$$+ (l_\infty^1 + 2l_\infty^2 + 3l_\infty^3 + 4l_\infty^4 + 2l_\infty^5)\,.$$

The discriminant of the Picard-lattice is equal to $-4 \cdot 15$.

Proof. Let N be the lattice generated by the classes mentioned in the statement of the theorem and let N' be the sublattice of N spanned by s_0, s, f and the fibre components. As in the proof of [Sh], theorem 1.1, the given relation holds and is the only one. So N' has index 3 in N.

The intersection matrix of the given generators of N' can be found easily using the fact that the self intersection of any rational curve is -2 (see [B-P-V], Chapter VIII, Proposition 3.6), the self intersection of a fibre is zero and the intersection of s with the reducible fibres is as given in Fig. 2 and Fig. 3.

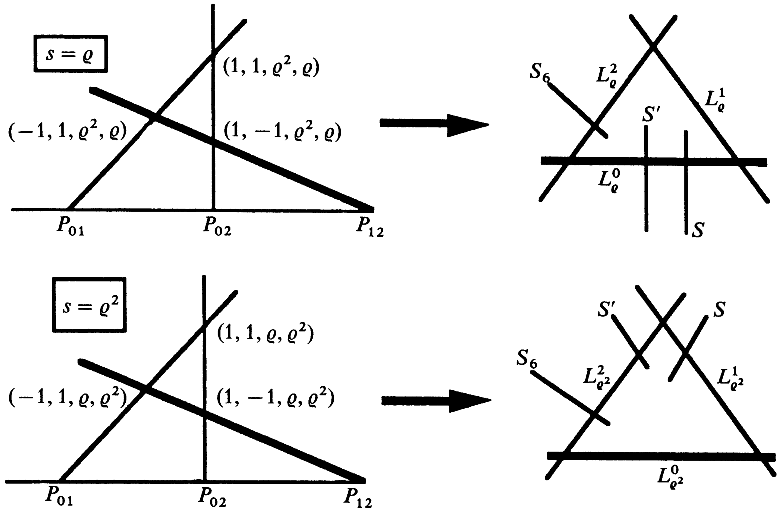

Figure 3. The special fibres at ρ, ρ^2

When the 20 generators of N' are given in the order s_0, s, f, the components of two fibres of type I_3 not meeting s_0, then similarly those for the fibre of type I_4 and the two fibres of type I_6 we find for this matrix

$$\begin{pmatrix}
-2 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & -2 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0\\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & -2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 1 & -2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 1 & 0 & 0 & 0 & -2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 1 & -2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 1 & 0 & 0 & 0 & 0 & 0 & -2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -2 & 1 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -2 & 1 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -2 & 0 & 0 & 0 & 0 & 0\\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -2 & 1 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -2 & 1 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -2 & 1 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -2 & 1\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -2
\end{pmatrix}$$

The determinant of this matrix is $-6^2 \cdot 15$ and hence the discriminant of N equals $-2^2 \cdot 15$. It follows that either N is the full Néron-Severi lattice or is of index 2 in it. Let us now consider the group MW of sections for the fibration f. In the latter case we would have that in this group at least one of the elements $S + kS_6$, $k = 0, \ldots, 5$ belongs to $2MW$. Restricting sections to the fibre at 0 gives a homomorphism $MW \to \mathbb{Z}/6\mathbb{Z} \times \mathbb{C}^*$. Since however any section of the form $S + kS_6$ maps to an element which is not 2-divisible (see Figure 2) this yields a contradiction. So $N = NS$. □

3. The zeta function

If X is a smooth projective variety of dimension n defined over $\mathbb{F}_q$, $q = p^r$, the numbers $N_{q^s}(X)$ are collected in the zeta function

$$Z(t) = Z(X/\mathbb{F}_q, t) := \exp\left(\sum_{s=1}^{\infty} \frac{N_{q^s}}{s} t^s\right).$$

We summarize a few facts concerning the zeta function ([Ha], Appendix C).

The zeta function can be written as

$$Z(t) = \frac{P_1(t) \cdots P_{2n-1}(t)}{P_0(t) \cdots P_{2n}(t)},$$

with $P_i(t) = \det(1 - tF_q | H^i_{\text{ét}}(X, \mathbb{Q}_l))$, where F_q denotes the induced Frobenius operator in cohomology. We always have $P_0(t) = 1 - t$ and $P_{2n}(t) = 1 - q^n t$. The polynomials $P_i(t)$ have integer coefficients and their degree is equal to the i-th Betti number

$$b_i = \dim H^i_{\text{ét}}(X, \mathbb{Q}_l), \quad l \neq p.$$

We have $P_i(t) = \prod_j (1 - \alpha_{ij} t)$ where the reciprocal roots α_{ij} are algebraic numbers with $|\alpha_{ij}| = q^{i/2}$. Finally, the map $\alpha \mapsto q^n/\alpha$ gives a bijection between the reciprocal roots of $P_i(t)$ and those of $P_{2n-i}(t)$.

Using the equation

$$-(td/dt)\log(1 - \alpha_{ij} t) = \sum_{s=1}^{\infty} \alpha_{ij}^s t^s,$$

we find from the definition of the zeta function that

$$N_{q^s} = \sum_{i\,\text{even}} \sum_j \alpha_{ij}^s - \sum_{i\,\text{odd}} \sum_j \alpha_{ij}^s.$$

As a final remark, we recall (cf. [Ta], p. 97) that on the subspace of $H^2_{\text{ét}}$ generated by algebraic cycles defined over $\mathbb{F}_q$, Frobenius acts as multiplication by q.

Example. For a surface with $b_1 = b_3 = 0$ the only relevant factor of the zeta function is $P_2(t)$. If the surface is the reduction of a characteristic zero surface, we find

$$N_q = 1 + q^2 + \operatorname{Tr} F_q | H^2_{\mathrm{alg}} + \operatorname{Tr} F_q | H^2_{\mathrm{trc}}.$$

If we apply this formula to our $K3$-surface in characteristic 2 ($q = 2^r$) and compare the result with formula (1.3), we should have 16 algebraic cycles over the ground field $\mathbb{F}_q$ with Frobenius acting on them by multiplication by q and 4 algebraic cycles which are only defined over a quadratic extension and which are Galois-conjugate. Finally, the number B_r must be the trace of Frobenius on the two-dimensional transcendental space.

Now we determine the factor $P_2(t)$ of the zeta function of $\tilde{X}(p)$.

(3.1) Proposition. *For the surface $\tilde{X}(p)$ with $p \neq 3, 5$, we have*

$$P_2(t) = (1 - pt)^{16} \left(1 - \left(\frac{p}{3}\right) pt\right)^4 Q_2(t)$$

with $Q_2(t)$ a quadratic polynomial.

Proof. If $\left(\frac{p}{3}\right) = 1$, by Theorem 2.5, Lemma 2.2 and Lemma 2.3 there are twenty independent cycles defined over the ground field with Frobenius acting on them by multiplication by p and hence $P_2(t)$ contains a factor of the form $(1 - pt)^{20}$. If $\left(\frac{p}{3}\right) = -1$, Lemma 2.2 shows that six fibral components L_1^1, L_1^3, L_ϱ^1, $L_{\varrho^2}^1$, L_ϱ^2, $L_{\varrho^2}^2$ (see Fig. 2 and Fig. 3), are not defined over the base field and Frobenius interchanges them pairwise. Now Lemma 2.3 shows that the section S is not defined over the ground field. Its Galois conjugate is the section S' and it is easily seen that the six fibral components together with S and S' span an eight dimensional subspace which is invariant under Frobenius F_p. In this subspace $\det(1 - tF_p) = (1 - p^2 t^2)^4$. In the 12-dimensional orthogonal complement (with respect to intersection pairing) of this subspace within the Néron-Severi group Frobenius acts by multiplication by p, since it has a basis consisting of cycles defined over the ground field. □

(3.2) Remark. If $P_2(t)$ has the form $(1 - pt)^{k_1}(1 + pt)^{k_2} Q_2(t)$ with

$$Q_2(t) = (1 - \beta t)(1 - \beta' t) \in \mathbb{Z}[t]$$

then the number N_q of $\mathbb{F}_q$-rational points of $X(p)$, with $q = p^r$, is

$$N_q = 1 + q^2 + q\big(k_1 + (-1)^r k_2\big) + A_q,$$

where $A_q = \beta^r + \beta'^r$.

The properties of the polynomials $P_i(t)$ imply that in case $Q_2(t)$ is irreducible, we have $\beta \cdot \beta' = p^2$ and hence:

$$Q_2(t) = 1 - A_p t + p^2 t^2.$$

(3.3) Proposition. *Let X' be the variety obtained from X by deleting the hyperplanes $x_i = 0$, $i = 1, \ldots, 5$.*

(i) *We have the following relation between A_q and the number N_q' of points of $X'(q)$:*

$$A_q = N_q' + 4q\left(1 - \left(\frac{q}{3}\right)\right) - q^2 - 11 .$$

(ii) *The quadratic factor $Q_2(t)$ is of the form*

$$Q_2(t) = 1 - A_p t + \left(\frac{p}{15}\right) p^2 t^2$$

and $A_p = 0$ precisely when $\left(\frac{p}{15}\right) = -1$.

Proof (suggested by R. Livné). Observe that by Remark 3.2 we have

$$N_q(\tilde{X}) = 1 + q^2 + q\left(16 + 4\left(\frac{q}{3}\right)\right) + A_q .$$

In section 1 we have seen that for $p = 2$ the collection of lines at infinity $(X \setminus X')(q)$ consists of $20q - 10$ points. This computation is also valid in any characteristic different from 3 or 5 and the formula for A_q follows.

In order to prove part (ii), we compute modulo 5. The symmetric group $\mathfrak{S}_5$ acts on $X'(p)$ and points whose orbitsize is not divisible by 5 are fixed by the 5-cycle (12345). The only such points on $X'(q)$ are the points $(1, \zeta, \zeta^2, \zeta^3, \zeta^4)$ with ζ a primitive 5-th root of unity. Such a root belongs to $\mathbb{F}_q$ precisely when $q \equiv 1 \bmod 5$ and so we find that $N_q' \equiv -1 \bmod 5$ in this case and $N_q' \equiv 0 \bmod 5$ otherwise. An elegant way of saying this is $N_q' \equiv 1 + q + q^2 + q^3 \bmod 5$ and then we find that

$$A_q \equiv q\left(\left(\frac{q}{3}\right) + q^2\right) \bmod 5 \equiv q\left(\left(\frac{q}{3}\right) + \left(\frac{q}{5}\right)\right) \bmod 5 .$$

The product of the eigenvalues β, β' of Frobenius at p can be written as $\frac{1}{2}(A_p^2 - A_{p^2})$. So modulo 5 this product is equal to $\left(\frac{p}{15}\right) p^2$ and this fixes the sign of the coefficient $\pm p^2$ of t^2.

The 'only if'-part of the last assertion follows from the congruence modulo 5 for A_p. Conversely, if $\left(\frac{p}{15}\right) = -1$ then $Q_2(t) = 1 - A_p t - p^2 t^2$ has real roots $\pm p$ and hence $A_p = 0$. □

If we combine the results of this section we get:

(3.4) Theorem. *For $p \neq 3, 5$ the zeta function of the $K3$-surface $\tilde{X}(p)$ is given by*

$$1/Z(t) = (1-t)(1-p^2t)(1-pt)^{16}\left(1-\left(\frac{p}{3}\right)pt\right)^4\left(1-A_pt+\left(\frac{p}{15}\right)p^2t^2\right).$$

4. The L-function

First we introduce some notation which will be used throughout this section.

K:	a number field,
$\bar{K}$:	an algebraic closure of K,
G_K:	the Galois group $\operatorname{Gal}(\bar{K}\,|\,K)$,
$\mathfrak{o}_K$:	the ring of integers in K,
v, w:	a (finite or infinite) valuation of K,
Σ_K:	the set of finite valuations of K,
K_v:	the completion of K at v,
$\mathfrak{o}_v$:	local valuation ring for the valuation v,
$\mathfrak{o}_v^\times$:	units of $\mathfrak{o}_v$,
$\mathfrak{p}_v$:	maximal ideal in $\mathfrak{o}_v$,
π_v:	a uniformising element of $\mathfrak{p}_v$,
k_v:	the residue class field $\mathfrak{o}_v/(\pi_v)$,
$\mathrm{N}v = \mathrm{N}\mathfrak{p}_v$:	the number of elements in k_v,
$\mathbb{A}_K^\times$:	the group of idèles of K with the usual topology.

In this section we want to identify the L-functions attached to two systems of 2-dimensional Galois representations of $G_{\mathbb{Q}}$. The first L-function is associated to the transcendental subspace of $H^2(\tilde{X}, \mathbb{Q}_l)$ and the other L-function to the transcendental subspace of $H^2(A, \mathbb{Q}_l)$, where A is an abelian surface defined over $\mathbb{Q}$.

Starting with our $K3$-surface $\tilde{X}$ over $\mathbb{Q}$ we have a system $\varrho = (\varrho_l)$ of 2-dimensional l-adic representations of $G_{\mathbb{Q}}$, namely

$$\varrho_l : G_{\mathbb{Q}} \to \operatorname{Aut} H^2_{\mathrm{trc}}(\tilde{X}, \mathbb{Q}_l).$$

For the basic notions on l-adic Galois representations of G_K in a finite dimensional $\mathbb{Q}_l$-vector space V_l we refer to [Se1], [Se2].

(4.1) Proposition. *The system $\varrho = (\varrho_l)$ has an L-function*

$$L(s, \varrho) = \prod_{p \neq 3,5} \frac{1}{1 - A_p p^{-s} + \left(\frac{p}{15}\right)p^2 p^{-2s}}.$$

Proof. From [Se 2], section 2.1, we deduce that for primes $p \neq 3, 5$ the characteristic polynomial of Frobenius F_{p,ϱ_l}, $l \neq p$, is independent of l. In particular, the system ϱ is strictly compatible. This implies that we may associate an L-function to ϱ:

$$L(s, \varrho) = \prod_{p \neq 3,5} \frac{1}{P_{p,\varrho}(p^{-s})},$$

with $P_{p,\varrho}(t) = \det(1 - tF_{p,\varrho_l} | H^2_{\mathrm{trc}}(\tilde{X}(p), \mathbb{Q}_l))$. From Theorem 3.4 it follows that

$$P_{p,\varrho}(t) = 1 - A_p t + \left(\frac{p}{15}\right) p^2 t^2 \quad \text{if } p \neq 3, 5. \quad \square$$

Let us indicate how we shall proceed in identifying $L(s, \varrho)$ with another L-function. From the Čebotarev density theorem [Se 1], 2.2, and from the fact that a semi-simple representation in a characteristic zero vector space is determined by its traces we deduce the following essential tool for identifying L-functions.

(4.2) Lemma. *Let $\varrho_l, \varrho_l' : G_{\mathbb{Q}} \to \operatorname{Aut} V_l$ be two rational l-adic representations with $\operatorname{Tr} F_{p,\varrho_l} = \operatorname{Tr} F_{p,\varrho_l'}$ for a set of primes p of density one (e.g. for all but finitely many primes). If ϱ_l and ϱ_l' fit into two strictly compatible systems, the L-functions associated to these systems are the same.*

One of the crucial ideas of [F] is that one can replace the set on which one has to check equality of traces by a *finite* set. This has been made effective by Serre in certain cases and elaborated on by Livné in [L]. For brevity, we introduce the following.

Definition. A finite set T of primes is said to be an *effective test set* for a rational Galois representation $\varrho_l : G_{\mathbb{Q}} \to \operatorname{Aut} V_l$ if Lemma 4.2 holds with the set of density one replaced by T.

Before we formulate a simple instance of Livné's criterion for effective test sets [L], section 4, we introduce a map f on sets of primes. Let S be a finite subset of $\Sigma_{\mathbb{Q}}$ of cardinality r. For $s \in S' := S \cup \{-1\}$ and an arbitrary odd prime t we set

$$f_s(t) = \frac{1}{2}\left(1 + \left(\frac{s}{t}\right)\right).$$

If $T \subset \Sigma_{\mathbb{Q}}$ is disjoint from S, we define $f : T \to (\mathbb{Z}/2\mathbb{Z})^{r+1}$ by $f(t) = (f_s(t))_{s \in S'}$.

(4.3) Proposition[1]**).** *Let ϱ and ϱ' be two 2-adic $G_{\mathbb{Q}}$-representations which are unramified outside a finite set S of primes, with $\operatorname{Tr} F_{p,\varrho} \equiv \operatorname{Tr} F_{p,\varrho'} \equiv 0 \bmod 2$ and*

$$\det F_{p,\varrho} \equiv \det F_{p,\varrho'} \bmod 2 \quad \textit{for } p \notin S \cup \{2\}.$$

[1]) Serre remarks that this Proposition is exactly the content of the criterion he communicated to Livné.

Any finite set T of rational primes disjoint from S such that $f(T) = (\mathbb{Z}/2\mathbb{Z})^{r+1} - \{0\}$ is an effective test set for ϱ with respect to ϱ'.

Going back to the system $\varrho = (\varrho_l)$, we remark that the congruence properties which are required in the preceding Proposition can be checked for any prime $l \nmid p$, since the system is strictly compatible. For the trace we first prove:

(4.4) Lemma (Compare [L], proposition 3.1). · *For all primes $p > 5$ Frobenius $F_{p,\varrho}$ at p has even trace.*

Proof. We employ the notation used in Proposition 3.3 and we notice that $A_p \equiv N_p' \bmod 2$. Any point of $X'(p)$ with odd orbitsize under $\mathfrak{S}_5$ must be fixed by a 2-Sylow subgroup, which we can take to be the dihedral group generated by (1234) and (12)(34). It easily follows that there are no such points on $X'(p)$ and thus $A_p \equiv 0 \bmod 2$. □

Next, we note that the Galois representation ϱ is ramified at most in 3 and 5, since $\tilde{X}(p)$ is singular for only these primes. So the exceptional set S consists of the two primes 3 and 5. A quick computation reveals that the set of primes $T = \{11, 13, 17, 19, 23, 29, 61\}$ satisfies the condition on effective test sets from Proposition 4.3. Using Proposition 3.3 and a computer we found a table of the traces A_p of Frobenius of our representation for p belonging to the above set T; we have added the trace at 2:

Prime p	A_p
2	1
7, 11, 13, 14 mod 15	0
17	−14
19	−22
23	34
61	−118

Table 1. Traces of Frobenius

On the other hand, we will consider the L-function associated to the strictly compatible system ϱ' associated to the transcendental subspace of $H^2(A, \mathbb{Q}_l)$, where A is the abelian surface defined over $\mathbb{Q}$ obtained as the Weil restriction from $\mathbb{Q}(\sqrt{5})$ to $\mathbb{Q}$ of an elliptic curve E over $\mathbb{Q}(\sqrt{5})$ with complex multiplication by the ring of integers in $\mathbb{Q}(\sqrt{-15})$. The local factors of this L-function can be explicitly calculated. We then want to use Proposition 4.3 to deduce equality of both L-functions. L-functions of elliptic curves with complex multiplication are completely described by L-functions of Hecke characters.

A Hecke character for any number field K is a continuous homomorphism

$$\chi\colon \mathbb{A}_K^\times / K^* \to \mathbb{C}^*,$$

where we give $\mathbb{C}^*$ the usual topology. We denote the local characters associated to χ by χ_v. For the elementary properties of Hecke characters we refer to [La], Ch. XIV and [T], Ch. 2. Given any Hecke character χ, the L-function of χ with conductor $\mathfrak{f}$ by definition is

$$L(s,\chi)=\prod\frac{1}{1-\chi_v(\pi_v)\cdot(\mathrm{N}v)^{-s}},$$

where the product is over all finite v with $\mathfrak{p}_v \nmid \mathfrak{f}$.

The relation between Hecke characters and the L-function can be made explicit in the following way (see [Gr], 8.2).

(4.5) Proposition. *Let E be an elliptic curve over a number field H such that*

(i) *E has complex multiplication by $K := \mathrm{End}(E)\otimes_{\mathbb{Z}}\mathbb{Q}$,*

(ii) *All endomorphisms are defined over H.*

Then $H^1(E_{\bar{H}},\mathbb{Q}_l)\cong K\otimes_{\mathbb{Q}}\mathbb{Q}_l$.

Furthermore, there exists a Hecke character

$$\chi:\mathbb{A}_H^{\times}/H^*\to\mathbb{C}^*$$

with the following properties:

(i) *$\chi_v(H_v^*)\subset K$ for all finite places v of H.*

(ii) *At a place v where E has good reduction a Frobenius element $F_v\in G_H$ acts on $K\otimes_{\mathbb{Q}}\mathbb{Q}_l$ by multiplication by $\chi_v(\pi_v)$.*

Since the set of Frobenius elements F_v is dense in G_H ([Se1], I.2) the preceding Proposition indeed determines the action of G_H on $H^1(E_{\bar{H}},\mathbb{Q}_l)$ completely.

Before we specialize to our situation, we prove a lemma on algebraic number fields.

(4.6) Lemma. *Fix two odd prime numbers p and q with $p\equiv 3 \bmod 4$ and $q\equiv 1 \bmod 4$. If $K:=\mathbb{Q}(\sqrt{-pq})$ has class number 2, then $H:=\mathbb{Q}(\sqrt{-p},\sqrt{q})$ is the Hilbert class field of K.*

Proof. Since the quadratic subfields $F:=\mathbb{Q}(\sqrt{q})$ resp. $F':=\mathbb{Q}(\sqrt{-p})$ have relatively prime discriminants q, resp. $-p$, we infer that $\mathrm{discr}(H/\mathbb{Q})=p^2q^2$ (see [La], Ch. III). From $\mathrm{discr}(H/\mathbb{Q})=\mathrm{discr}^2(K/\mathbb{Q})N_{K/\mathbb{Q}}(\mathrm{discr}(H/K))$ it follows that $\mathrm{discr}(H/K)=\mathfrak{o}_K$. This implies that the extension H/K is unramified. Since K has class number 2, H is the maximal unramified abelian extension of K and $\mathrm{Gal}(H/K)\cong\mathbb{Z}/2\mathbb{Z}$. □

From the theory of complex multiplication of elliptic curves it follows that there exists an elliptic curve E defined over the Hilbert class field $H=\mathbb{Q}(\sqrt{-p},\sqrt{q})$ of $K=\mathbb{Q}(\sqrt{-pq})$ with complex multiplication by the ring of integers of K. In fact we may assume that E is defined over the maximal real subfield $F=\mathbb{Q}(\sqrt{q})$ of H. The Hecke character corresponding to E according to Proposition 4.5 depends on the chosen model over F of our elliptic curve. However, following [Gr], section 11, there is an 'optimal' model which has bad reduction only at the primes dividing p and q. Denote such a model again by E and its Hecke character by χ (Gross denotes it by χ_D with $D = pq$ in our case). We will state the properties of χ, which we need (see [Gr], 11.2):

(4.7) Proposition. (i) *The conductor of* χ *is equal to* $(\sqrt{-pq})$.

(ii) *If* v *is a place of* H *where* E *has good reduction, then* $\chi_v(\pi_v)$ *is an element of* $\mathfrak{p}_v \cap \mathbb{Z}\left[\frac{1+\sqrt{-pq}}{2}\right]$ *of norm* $\mathrm{N}v$.

(iii) *At the two infinite places* v *of* H, *after normalization, the local character is* $\chi_v(x) = x^{-1}$.

(iv) *At a place* v *dividing* p *or* q, *the restriction of* χ_v *to the units* $\mathfrak{o}_v^\times$ *is the unique non-trivial character with values* $\{\pm 1\}$.

From χ we construct another Hecke-character

$$\psi : \mathbb{A}_K^\times / K^* \to \mathbb{C}^*,$$

by setting

$$\psi_v(x) = \prod_{w \mid v} \chi_w(x).$$

(4.8) Lemma. *The character* ψ *has the following properties*:

(a) *The conductor of* ψ *is* (1).

(b) $\psi_\infty(z) = \frac{1}{z^2}$.

(c) *At a finite place* v *of* K *we have that* $\psi_v(\pi_v)$ *is a generator of the principal ideal* $\mathfrak{p}_v^2$.

Proof. (a) If the place v of K above $p_i = p$ or q splits in H, this follows directly from Proposition 4.7 (iv). In the other case, there is a unique w extending v, and the image of $\mathbb{F}_{p_i}^*/(\mathbb{F}_{p_i}^*)^2 \cong \mathfrak{o}_v^*/(\mathfrak{o}_v^*)^2$ in $\mathfrak{o}_w^*/(\mathfrak{o}_w^*)^2 \cong \mathbb{F}_{p_i^2}^*/(\mathbb{F}_{p_i^2}^*)^2$ is clearly trivial.

The properties (b) and (c) follow from the properties of χ listed above. □

We show that these properties leave very little choice for ψ.

(4.9) Proposition. *Let* r *be any rational prime different from* p *or* q *decomposing in* $\mathfrak{o}_K$ *into non-principal ideals* $(r) = \mathfrak{r} \cdot \bar{\mathfrak{r}}$ *and let* $\mathfrak{r}^2 = (\varrho)$. *Let* v_0 *be the valuation corresponding to* $\mathfrak{r}$. *There are exactly two Hecke characters* $\psi : \mathbb{A}_K^\times / K^* \to \mathbb{C}^*$ *which satisfy* (a), (b) *and* (c) *above. They are distinguished by the sign of the local character at* $\mathfrak{p}_{v_0}$:

$$\psi_{v_0}^{\pm}(\pi_{v_0}) = \pm \varrho.$$

The values of the other local characters at v *with* $\mathfrak{p}_v$ *not dividing* pq *are*:

(i) *if* $\mathfrak{p}_v = (s)$ *then* $\psi_v(\pi_v) = \psi_v(s) = s^2$,

(ii) *if* $\mathfrak{p}_v$ *is non-principal and* $\mathfrak{r} \cdot \mathfrak{p}_v =: (\tau)$ *we have* $\psi_v(\pi_v) = \psi_v(\tau) = \tau^2 \cdot \dfrac{1}{\psi_{v_0}(\tau)}$.

Proof. We first remark that $\psi_{v_0}(\pi_{v_0}) = \pm \varrho$ since ± 1 are the only units in K.

Next, we shall show that the local character at all places v of K are determined by the value of $\psi_{v_0}(\pi_{v_0})$. In case (i) we have $1 = \psi_v(s) \cdot \psi_\infty(s)$ and hence $\psi_v(s) = s^2$. In the remaining case we have $1 = \psi_{v_0}(\tau) \cdot \psi_v(\tau) \cdot \tau^{-2}$, which proves (ii). □

We will now indicate a geometric interpretation of the Hecke character ψ. The Artin isomorphism of class field theory ([La]) implies that ψ corresponds to a 1-dimensional continuous representation of G_K. On the other hand, we can look at the 2-dimensional G_Q-representation on $H^2_{\mathrm{trc}}(A_{\bar{Q}})$, where A is the Weil-restriction from F to Q of E.

(4.10) Proposition. *Let* $A = A^+$ *be the Weil-restriction from* F *to* Q *of* E *and let* A^- *be the Weil-restriction from* F *to* Q *of* E^τ, *where* $1 \neq \tau \in \mathrm{Gal}(F|Q)$. *Both* A^+ *and* A^- *are abelian surfaces defined over* Q. *The model* E *can be chosen in such a way that the restriction to* G_K *of the* G_Q*-representation on* $H^2_{\mathrm{trc}}(A^{\pm}_{\bar{Q}})$ *coincides with the* G_K*-representation* $\psi^{\pm}$.

Proof. The restriction of the G_K-representation defined by ψ to $\mathrm{Gal}(\bar{H}|H)$ corresponds to the Hecke character

$$\psi \circ N_{H/K} = \chi^2 .$$

Recall that χ determines the representation on $H^1 = H^1(E_{\bar{H}}, Q_l)$: the eigenvalues of Frobenius at a 'good' place v of H are given by $\chi_v(\pi_v)$ and its complex conjugate. Hence, on the tensor product $H^1 \otimes H^1$ such a Frobenius has two eigenvalues equal to $\mathrm{N}v$ and the eigenvalues $\chi_v^2(\pi_v)$, $\overline{\chi_v^2(\pi_v)}$. The latter two are precisely the eigenvalues of Frobenius on the Galois-invariant subspace $H^2_{\mathrm{trc}}(E \times E)$ of $H^1 \otimes H^1$. To see this, note that the cycle classes of the graphs of elements in $\mathrm{End}(E)$ generate a two-dimensional piece in $H^1 \otimes H^1$ on which Frobenius acts by multiplication by $\mathrm{N}v$. Thus, the other two eigenvalues belong to eigenvectors in the orthogonal complement with respect to the intersection pairing, i.e. $H^2_{\mathrm{trc}}(E \times E)$. Now the surface A over F is isomorphic to $E \times E^\tau$. In fact E and E^τ are isogenous, with an isogeny defined over H ([Gr], (11.1.1) and (11.2.5)). Hence the restriction to $\mathrm{Gal}(\bar{Q}|H)$ of the representation on $H^2_{\mathrm{trc}}(A_{\bar{Q}})$ is $H^2_{\mathrm{trc}}(E \times E|\bar{H})$, which corresponds to the Hecke character χ^2.

It follows that ψ and $H^2_{\mathrm{trc}}(A/\bar{K})$ give the same representation of G_K up to a character of $\mathrm{Gal}(H|K)$. We have two possibilities for ψ which differ by such a character and two possible abelian surfaces $A = A^+$ and A^-. These two surfaces become isomorphic over F and they are quadratic twists of each other over K. We can choose E in such a way that $\psi^{\pm}$ corresponds to $A^{\pm}$. □

We now consider the special case which is of interest to us, namely $p = 3$ and $q = 5$. We let v_0 be the valuation corresponding to the prime ideal $\mathfrak{r} = (2, \omega)$ above (2) in $K = Q(\sqrt{-15})$. We list some values of the Hecke characters $\psi^{\pm}$ in this case.

(4.11) Proposition. *With the notation as above we have*

(i) $\psi_{v_0}^{\pm}(\pi_{v_0}^{\pm}) = \psi_{v_0}^{\pm}(2) = \pm\omega$, *where* $\omega = \frac{1}{2}(1+\sqrt{-15})$,

(ii) $\psi_3^{\pm}(3+\sqrt{-15}) = -(\pm 3)$,

(iii) $\psi_5^{\pm}(\sqrt{-15}) = \pm 5$.

Proof. (i) We easily verify that $\mathfrak{r}^2 = (\omega)$ and we apply Proposition 4.9.

(ii) Since $(3) = (3, \sqrt{-15})^2$, a uniformizer is $3+\sqrt{-15} = 2\cdot(1+\omega)$. From

$$\begin{aligned} 1 &= \psi_{\infty}(3+\sqrt{-15})\cdot\psi_{v_0}(3+\sqrt{-15})\cdot\psi_{\bar{v}_0}(3+\sqrt{-15})\cdot\psi_3(3+\sqrt{-15}) \\ &= \psi_{\infty}(3+\sqrt{-15})\cdot\psi_{v_0}(2)\cdot\psi_{\bar{v}_0}(2)^2\cdot\psi_3(3+\sqrt{-15}) \end{aligned}$$

we derive the stated result.

(iii) In this case $\sqrt{-15}$ is a uniformizer and we can argue as in (ii) to obtain the desired expression. □

The values of $\psi_v^{\pm}(\pi_v)$ can be explicitly computed by means of the procedure outlined above. We collect some values of their traces $A_p^{\pm} = \mathrm{Tr}_{K/Q}\psi_v^{\pm}(\pi_v)$ in the following table:

Prime p	A_p^+	A_p^-
2	1	−1
7, 11, 13, 14 mod 15	0	0
17	−14	14
19	−22	−22
23	34	−34
61	−118	−118

Table 2. Traces of Frobenius for $\psi_p^{\pm}$

(4.12) Proposition. *The local factors of the L-function corresponding to the G_Q-representation $H_{\mathrm{trc}}^2(A_{\bar{Q}}^{\pm})$ can be described as follows.*

(i) *If $p \equiv 7, 11, 13, 14 \bmod 15$ the local factor is the value at $t = p^{-s}$ of the quadratic polynomial $1 - p^2t^2$.*

(ii) *If $p \equiv 1, 2, 4, 8 \bmod 15$ this polynomial is*

$$1 - A_p^{\pm}t + p^2t^2$$

with $A_p^{\pm} = \mathrm{Tr}_{K/Q}\psi_v^{\pm}(\pi_v)$. All $A_p^{\pm}$ are even.

(iii) *At* 3, *resp.* 5 *we have the polynomial* $1 + \pm 3t$, resp. $1 - \pm 5t$.

Proof. In (i) we have the condition that p remains prime in $\mathbb{Q}(\sqrt{-15})$ and hence $\prod_{v|p} (1 - \psi_v^{\pm}(\pi_v)t) = 1 - p^2 t^2$. In (ii) the prime splits and $\prod_{v|p} (1 - \psi_v^{\pm}(\pi_v)t)$ is the indicated polynomial. Since $A_p^{\pm} = \psi_v^{\pm}(\pi_v) + \overline{\psi_v^{\pm}(\pi_v)} = 2a + b$ if $\psi_v^{\pm}(\pi_v) = a + b\omega$ and since $\psi_v^{\pm}(\pi_v) \cdot \overline{\psi_v^{\pm}(\pi_0)} = a^2 + ab + 4b^2 = p^2$ is odd, we easily conclude that $A_p^{\pm}$ is even. The last case is immediate. □

Remark. The numbers A_p, for $p \neq 3, 5$ and $p \not\equiv 1, 2, 4, 8 \bmod 15$ can be computed by means of the following algorithm.

(i) If $p \equiv 1$ or $4 \bmod 15$, find an integral solution of the equation $x^2 + xy + 4y^2 = p$. Then $A_p = 2x^2 - 7y^2 + 2xy$.

(ii) If $p \equiv 2$ or $8 \bmod 15$, find an integral solution of $2x^2 + xy + 2y^2 = p$. In this case $A_p = x^2 + 8xy + y^2$.

We now can state our main result:

(4.13) Theorem. *There exists an elliptic curve E over $\mathbb{Q}(\sqrt{5})$ which has complex multiplication by the ring of integers in $\mathbb{Q}(\sqrt{-15})$ and which has bad reduction at* 3 *and* 5 *only. If we consider the Weil restriction A to $\mathbb{Q}$ of E, which is an Abelian surface defined over $\mathbb{Q}$ then*

(i) *the restriction of the two-dimensional l-adic $G_{\mathbb{Q}}$-representation $H^2_{\mathrm{trc}}(A)$ to $G_{\mathbb{Q}(\sqrt{-15})}$ is unramified outside of l,*

(ii) *the L-series is the same as the L-series for the two-dimensional $G_{\mathbb{Q}}$-space $H^2_{\mathrm{trc}}(\tilde{X})$ for the K3-surface $\tilde{X}$.*

Proof. The statement (i) follows from Lemma 4.8(a). To prove (ii) we apply Proposition 4.3. By Proposition 4.12(ii) and Lemma 4.4 we see that the first condition is met for both Galois representations, while the second is obvious. The tables give the same answers for the traces of Frobenius at p in the test set and so the two L-functions must be the same. □

Remark. By means of this theorem one can show that both $A(p)$ and $\tilde{X}(p)$ are supersingular if and only if $A_p = 0$.

5. Modular forms and the main result

The L-functions of Hecke characters of imaginary quadratic number fields are strongly related to L-functions associated to modular forms, as has already been pointed out by Hecke [H], no. 23, 27. Before we study this relation for our Hecke L-functions $L(s, \psi^{\pm})$ we recall some facts about modular forms. For the basic notions and properties we refer the reader to [K]. For any natural number N we have

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{Z}) \,|\, c \equiv 0 \bmod N \right\}.$$

A holomorphic function $f(z)$ on the upper half plane is a modular form f of weight k for $\Gamma_0(N)$ with Dirichlet character $\alpha : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}^*$ if

(i) $f(\gamma z) = \alpha(d)(cz + d)^k f(z)$ for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$

and

(ii) $f(z)$ is 'holomorphic at the cusps' (see [K], II.3, for more details).

In particular $f(z) = f(z + 1)$ and we have a q-expansion at infinity:

$$f(q) = a_0 + a_1 q + a_2 q^2 + \ldots, \quad q = e^{2\pi i z}$$

and similarly at the other cusps. We let $M_k(N, \alpha)$ denote this set of functions.

The function f is called a cusp form if it vanishes at all cusps. The space of all cusp forms of weight k for $\Gamma_0(N)$ and with character α is a finite dimensional complex vector space which is denoted by $S_k(N, \alpha)$. For each natural number n the Hecke operators T_n act on this space. Let us recall their definition. If $f = \sum_{m=1}^{\infty} a_m q^m \in S_k(N, \alpha)$, we let

$$T_n f = \sum_{m=1}^{\infty} \left(\sum_{d \,|\, m, n} \alpha(d) d^{k-1} a_{mn/d^2} \right) q^m .$$

There exists a basis of simultaneous eigenvectors of T_n for n coprime with N (see [K], III.5). If the corresponding eigenspaces are one-dimensional, we even have a basis of eigenforms for all T_n. Such eigenforms will be called *Hecke eigenforms.*

Let $f(q) = q + a_2 q^2 + \ldots$ be a normalized Hecke eigenform, then $T_n f = a_n f$ and the L-series

$$L(s, f) := \sum_{n=1}^{\infty} a_n n^{-s},$$

now has an Euler product

$$\prod_{p \,\text{prime}} \frac{1}{Q_p(p^{-s})} \quad \text{with} \quad Q_p(t) = 1 - a_p t + \alpha(p) p^{k-1} t^2 .$$

By means of [T], Ch. 2, we prove the following proposition.

(5.1) Proposition. *The L-functions $L(s, \psi^{\pm})$ attached to the Hecke characters $\psi^{\pm}$ of $\mathbb{A}_K^{\times}/K^*$, with $K = \mathbb{Q}(\sqrt{-15})$ coincide with the L-functions $L(s, f^{\pm})$ attached to the Hecke eigenforms $f^{\pm} \in S_3(15, (\frac{\cdot}{15}))$.*

Proof. It is sufficient to prove this for $\psi := \psi^+$. From Corollary 4.6 and Theorem 4.7 we infer that

$$L(s,\psi) = \frac{1}{1+3.3^{-s}} \cdot \frac{1}{1-5.5^{-s}} \cdot \prod_{p \neq 3,5} \frac{1}{Q_{2,p}(p^{-s})},$$

with $Q_{2,p}(t) = 1 - A_p t + (\frac{p}{15}) p^2 t^2$. The Hecke L-function satisfies the following functional equation

$$L_\infty(s,\psi)\, L(s,\psi) = \varepsilon(s,\psi)\, L_\infty(1-s,\psi^{-1})\, L(1-s,\psi^{-1}).$$

Here $L_\infty(s,\psi)$ depends only on ψ_∞. Since $\psi_\infty(z) = z^{-2}$ we get $L_\infty(s,\psi) = (2\pi)^{-s}\Gamma(s)$ and $L_\infty(s,\psi^{-1}) = (2\pi)^{-2-s}\Gamma(s+2)$. Next, because the two roots of the polynomial $Q_{2,p}(t)$ are β and p^2/β, we have $L(s,\psi^{-1}) = L(s+2,\psi)$. Finally, the ε-factor turns out to be equal to $15^{3/2-s}$ (see [T], 2.2). Combining all of this, we can rewrite the functional equation in the form

$$(2\pi)^{-s}\Gamma(s)\, L(s,\psi) = 15^{3/2-s}(2\pi)^{s-3}\,\Gamma(3-s)\, L(3-s,\psi).$$

From [T], Theorem 2.4.2, it then follows that $L(s,\psi) = L(s,f)$ for a modular form $f \in M_3(15, (\frac{\cdot}{15}))$. To prove that f is a cusp form, we look at convergence of the series

$$L(s,\psi) = \sum_{n=1}^{\infty} A_n n^{-s}.$$

For a prime number p, A_p occurs in the polynomial

$$1 - A_p t + (\tfrac{p}{15}) t^2 = (1-\alpha_p t)(1-\alpha'_p t).$$

Now α_p and α'_p are roots of Frobenius acting on (part of) the 2-cohomology of a smooth variety over $\mathbb{F}_p$, and so the Weil conjectures imply $|\alpha_p| \leqq p$ and $|\alpha'_p| \leqq p$. Consequently $|A_p| \leqq 2p$ and it follows that $|A_n| \leqq \sigma_0(n) \cdot n$, where $\sigma_0(n)$ is the number of divisors of n (see [K], p. 96). So $A_n = O(n^{1+\varepsilon})$ for every positive ε and the series converges for $\operatorname{Re} s > 2$. This means that f is a cusp form. The Euler product for $L(s,\psi)$ from the beginning of the proof implies that f is a Hecke eigenform. □

Remark. The functional equation which we derived in the preceding proof provides an example where Serre's conjecture C. 5.1. in [Se 2] is true. This can be seen as follows. The Hecke eigenforms in $S_3(\Gamma_0(15), (\frac{\cdot}{15}))$ mentioned above, which are newforms, determine our Galois representation. For such representations arising from newforms a general theorem of Carayol [C], Théorème (A), implies that all the local factors in the L-series agree with the ones prescribed by Serre's recipe.

The following way of constructing an explicit basis of $S_3(15, (\frac{\cdot}{15}))$ consisting of Hecke eigenforms has been communicated to us by René Schoof. One starts with the theta-functions

$$\theta_1 = \sum_{m,n \in \mathbb{Z}} q^{m^2+mn+4n^2} = 1 + 2q + 6q^4 + \dots$$

and

$$\theta_2 = \sum_{m,n \in \mathbb{Z}} q^{2m^2+mn+2n^2} = 1 + 4q^2 + 2q^3 + \dots .$$

Note that the quadratic forms in the exponents represent the two $SL(2, \mathbb{Z})$-equivalence classes of positive definite binary quadratic forms of discriminant -15. We conclude from [O], Ch. V, that $\theta_1, \theta_2 \in M_1(15, (\frac{\cdot}{15}))$. Next, we consider the function on the upper half plane given by

$$g(z) = \eta(z)\eta(3z)\eta(5z)\eta(15z),$$

where $\eta(z)$ is the Dedekind eta-function defined by

$$\eta(z) = q^{1/24} \prod_{n=1}^{\infty} (1 - q^n).$$

The q-expansion of the function $g(z)$ starts with $g(z) = q - q^2 - q^3 - q^4 + q^5 + \dots$. From [Li], p. 28–31, we infer that $g(z) \in S_2(15, 1)$, where 1 is the trivial Dirichlet character mod 15. We find the following identification for $f^{\pm}$.

(5.2) Proposition. *We have $f^+ = g\theta_1$ and $f^- = g\theta_2$.*

Proof. Applying [S-V], Cor. 2.2, we find that the space $S := S_3(15, (\frac{\cdot}{15}))$ is two-dimensional. Set $F_i = g\theta_i$, $i = 1, 2$. Since $T_2 F_1 = F_1$ and $T_2 F_2 = -F_2$ it follows that $\{F_1, F_2\}$ is a basis of S consisting of Hecke eigenforms. Since $A_2^+ = 1$ and $A_2^- = -1$ (see Table 2) we necessarily have $F_1 = f^+$ and $F_2 = f^-$. □

Combining the results of this section with Theorem 3.4 and Theorem 4.13, we obtain our main result.

(5.3) Theorem. *The number of $\mathbb{F}_p$-rational points of the $K3$-surface $\tilde{X}$ ($p \neq 3, 5$) is equal to*

$$1 + p^2 + p \cdot \left(16 + 4\left(\frac{p}{3}\right)\right) + A_p,$$

where the number A_p is the coefficient of q^p in the q-expansion of the Hecke eigenform

$$\left(\sum_{m,n \in \mathbb{Z}} q^{m^2+mn+4n^2}\right) \cdot q \prod_{r=1}^{\infty} (1 - q^r)(1 - q^{3r})(1 - q^{5r})(1 - q^{15r}).$$

Remark. Note that the formulas for A_p from the remark following Proposition 4.12 yield a fast algorithm to determine the q-expansion of $f^{\pm}$.

References

[A] *M. Artin*, Supersingular $K3$ surfaces, Ann. É.N.S. **7** (1974), 543–567.

[B-P-V] *W. Barth*, *C. Peters*, *A. van de Ven*, Compact Complex Surfaces, Erg. Math. (3) **4**, Berlin–Heidelberg–New York 1984.

[C] *H. Carayol*, Sur les représentations l-adiques associées aux formes modulaires de Hilbert, Ann. scient. Éc. Norm. Sup. (4) **19** (1986), 409–468.

[F] *G. Faltings*, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, Invent. Math. **73** (1983), 349–366.

[G] *S. Gelbart*, An elementary introduction to the Langlands program, Bull. A.M.S. **10** (1984), 177–219.

[Gr] *B. Gross*, Arithmetic on elliptic curves with complex multiplication, Lect. Notes Math. **776**, Berlin–Heidelberg–New York 1980.

[H] *E. Hecke*, Mathematische Werke, Göttingen 1970.

[Ha] *R. Hartshorne*, Algebraic Geometry, Berlin–Heidelberg–New York 1977.

[K] *N. Koblitz*, Introduction to elliptic curves and modular forms, Berlin–Heidelberg–New York 1984.

[La] *S. Lang*, Algebraic number theory, Reading 1970.

[Li] *G. Ligozat*, Courbes modulaires de genre 1, Bull. Soc. Math. France Mém. **43**, (1975).

[L] *R. Livné*, Cubic exponential sums and Galois representations, Contemp. Math. **67** (1987), 247–261.

[M] *J. Milnor*, Morse Theory, Ann. Math. Stud. **51**, Princeton 1963.

[M-P] *R. Miranda*, *U. Persson*, Torsion groups of elliptic surfaces, Comp. Math. **72** (1989), 249–267.

[O] *A. Ogg*, Modular forms and Dirichlet series, New York–Amsterdam 1969.

[S-V] *R. Schoof*, *M. van der Vlugt*, Hecke operators and the weight distribution of certain codes, J. Comb. Th. A. **57** (1991), 163–186.

[Se1] *J.-P. Serre*, Abelian l-adic representations and elliptic curves, New York–Amsterdam 1968.

[Se2] *J.-P. Serre*, Représentations l-adiques, Kyoto Int. Symp. on Algebraic Number Theory (1977), 177–193.

[Sh] *T. Shioda*, On elliptic modular surfaces, J. Math. Soc. Japan **24** (1972), 20–59.

[S-I] *T. Shioda*, *H. Inose*, On singular $K3$-surfaces, in: Complex Analysis and Algebraic Geometry, Cambridge (1977), 117–136.

[Si] *J. Silverman*, The arithmetic of elliptic curves, Berlin–Heidelberg–New York 1986.

[Ta] *J. Tate*, Algebraic cycles and poles of zeta functions, in: Arithmetical Algebraic Geometry, New York (1965), 93–110.

[T] *J. Top*, Hecke L-series related with algebraic cycles or with Siegel modular forms, thesis Utrecht 1990.

Math. Inst. Rijksuniversiteit te Leiden, P.O. Box 9512, 2300 RA Leiden, The Netherlands

Econometrisch Inst. Erasmus Universiteit, P.O. Box 1738, 3000 DR Rotterdam, The Netherlands

Eingegangen 26. April 1991, in revidierter Fassung 7. Februar 1992