



UvA-DARE (Digital Academic Repository)

K3 surfaces over finite fields with given L-function

Taelman, L.D.J.

DOI

[10.2140/ant.2016.10.1133](https://doi.org/10.2140/ant.2016.10.1133)

Publication date

2016

Document Version

Final published version

Published in

Algebra & Number Theory

[Link to publication](#)

Citation for published version (APA):

Taelman, L. D. J. (2016). K3 surfaces over finite fields with given L-function. *Algebra & Number Theory*, 10(5), 1133–1146. <https://doi.org/10.2140/ant.2016.10.1133>

General rights

It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations

If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: <https://uba.uva.nl/en/contact>, or a letter to: Library of the University of Amsterdam, Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.

K3 surfaces over finite fields with given L -function

Lenny Taelman

The zeta function of a K3 surface over a finite field satisfies a number of obvious (archimedean and ℓ -adic) and a number of less obvious (p -adic) constraints. We consider the converse question, in the style of Honda–Tate: given a function Z satisfying all these constraints, does there exist a K3 surface whose zeta-function equals Z ? Assuming semistable reduction, we show that the answer is yes if we allow a finite extension of the finite field. An important ingredient in the proof is the construction of complex projective K3 surfaces with complex multiplication by a given CM field.

Introduction

Let X be a K3 surface over \mathbb{F}_q . The zeta function of X has the form

$$Z(X/\mathbb{F}_q, T) = \frac{1}{(1-T)L(X/\mathbb{F}_q, qT)(1-q^2T)}$$

where the polynomial $L(X/\mathbb{F}_q)$ is defined by

$$L(X/\mathbb{F}_q, T) := \det(1 - T \text{Frob}, H^2(X_{\overline{\mathbb{F}}_q}, \mathbb{Q}_\ell(1))) \in \mathbb{Q}[T].$$

We have $L(X/\mathbb{F}_q, T) = \prod_{i=1}^{22} (1 - \gamma_i T)$ with the γ_i of complex absolute value 1. The polynomial $L(X/\mathbb{F}_q, T)$ factors in $\mathbb{Q}[T]$ as $L = L_{\text{alg}} L_{\text{trc}}$ with

$$L_{\text{alg}}(X/\mathbb{F}_q, T) = \prod_{\gamma_i \in \mu_\infty} (1 - T\gamma_i), \quad L_{\text{trc}}(X/\mathbb{F}_q, T) = \prod_{\gamma_i \notin \mu_\infty} (1 - T\gamma_i),$$

where μ_∞ is the group of complex roots of unity.

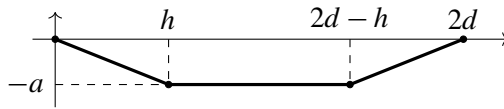
Theorem 1. *Let X be a K3 surface over \mathbb{F}_q with $q = p^a$. Assume that X is not supersingular. Then*

- (1) *all complex roots of $L_{\text{trc}}(X/\mathbb{F}_q, T)$ have absolute value 1;*
- (2) *no root of $L_{\text{trc}}(X/\mathbb{F}_q, T)$ is a root of unity;*

MSC2010: primary 14J28; secondary 14G15, 14K22, 11G25.

Keywords: K3 surfaces, zeta functions, finite fields.

- (3) $L_{\text{trc}}(X/\mathbb{F}_q, T) \in \mathbb{Z}_\ell[T]$ for all $\ell \neq p$;
- (4) the Newton polygon of $L_{\text{trc}}(X/\mathbb{F}_q, T)$ at p is of the form



with h and d integers satisfying $1 \leq h \leq d \leq 10$;

- (5) $L_{\text{trc}}(X/\mathbb{F}_q, T) = Q^e$ for some $e > 0$ and some irreducible $Q \in \mathbb{Q}[T]$, and Q has a unique irreducible factor in $\mathbb{Q}_p[T]$ with negative slope.

The above theorem collects results of Deligne, Artin, Mazur, Yu and Yui, and slightly expands on these, see Section 1 for the details. The integer h in the theorem is the height of X (which is finite by the assumption that X is not supersingular), and assuming the Tate conjecture (which is now known in almost all cases [Charles 2013; 2014; Madupusi Pera 2015]) the Picard rank of $X_{\mathbb{F}_q}$ is $22 - 2d$.

Definition 2 (Property (\star)). A K3 surface X over a finite extension k of \mathbb{Q}_p is said to satisfy (\star) if there exists a finite extension $k \subset \ell$ and a proper flat algebraic space $\mathfrak{X} \rightarrow \text{Spec } \mathcal{O}_\ell$ such that

- (1) $\mathfrak{X} \times_{\text{Spec } \mathcal{O}_\ell} \text{Spec } \ell \cong X \times_{\text{Spec } k} \text{Spec } \ell$,
- (2) \mathfrak{X} is regular,
- (3) the special fiber of \mathfrak{X} is a reduced normal crossings divisor with smooth components,
- (4) $\omega_{\mathfrak{X}/\mathcal{O}_\ell} \cong \mathcal{O}_{\mathfrak{X}}$.

Property (\star) is a strong form of potential semistability. It is expected that every X satisfies (\star) , but this is presently only known for special classes of K3 surfaces, see [Maulik 2014, §4] and [Liedtke and Matsumoto 2015, §2]. Our main result is the following partial converse to Theorem 1.

Theorem 3. Assume every K3 surface X over a p -adic field satisfies (\star) . Let

$$L = \prod_{i=1}^{2d} (1 - \gamma_i T) \in 1 + T\mathbb{Q}[T]$$

be a polynomial which satisfies properties (1)–(5) of Theorem 1. Then there exists a positive integer n and a K3 surface X over \mathbb{F}_{q^n} such that

$$L_{\text{trc}}(X/\mathbb{F}_{q^n}, T) = \prod_{i=1}^{2d} (1 - \gamma_i^n T).$$

The proof of Theorem 3 follows the same strategy as the proof of the Honda–Tate theorem [Tate 1971]: given L_{trc} , one constructs a K3 surface over a finite field by first producing a complex projective K3 surface with CM by a suitably chosen CM field, then descending it to a number field, and finally reducing it to the residue field at a suitably chosen prime above p . In the final step a criterion of good reduction is needed, which has been obtained recently by Matsumoto [2015] and Liedtke and Matsumoto [2015], under the assumption (\star) .

A crucial intermediate result, that may be of independent interest, is the following theorem.

Theorem 4. *Let E be a CM field with $[E : \mathbb{Q}] \leq 20$. Then there exists a K3 surface over \mathbb{C} with CM by E .*

See Section 2 for the definition of “CM by E ”, and see Section 3 for the proof of this theorem.

Remark 5. I do not know if one can take $n = 1$ in Theorem 3. Finite extensions are used in several parts of the proof, both in constructing a K3 surface X over some finite field, and in verifying that the action of Frobenius on H^2 is the prescribed one.

Recently Kedlaya and Sutherland [2015] obtained some computational evidence suggesting that the theorem might hold with $n = 1$. They enumerated all polynomials L satisfying (1)–(5) with $q = 2$, $\deg L = \deg Q = 20$ and with $L(1) = 2$ and $L(-1) \neq 2$. There are 1995 such polynomials. If $L = L_{\text{trc}}(X/\mathbb{F}_2, T)$ for a K3 surface over \mathbb{F}_2 , then the Artin–Tate formula [Milne 1975; Elsenhans and Jahnke 2015] puts strong restrictions on the Néron–Severi lattice of X . These restrictions suggest that X should be realizable as a smooth quartic, and indeed for each of the 1995 polynomials Kedlaya and Sutherland manage to identify a smooth quartic X defined over \mathbb{F}_2 with $L = L_{\text{trc}}(X/\mathbb{F}_2, T)$.

If one can take $n = 1$ in Theorem 3, then new ideas will be needed to prove this. Indeed, there is no reason at all that the X constructed in the current proof is defined over \mathbb{F}_q . A similar problem occurs in the proof of the Honda–Tate theorem [Tate 1971]: given a q -Weil number one first constructs an abelian variety over a finite extension of \mathbb{F}_q , and then identifies the desired abelian variety as a simple factor of the Weil restriction to \mathbb{F}_q . Perhaps a variation of this argument in the context of hyperkähler varieties can be made to work in our setting?

Remark 6. By the work of Madapusi Pera [2015], for every d there is an étale map $M_{2d} \rightarrow \text{Sh}_{2d}$ from the moduli space of quasipolarized K3 surfaces of degree $2d$ to an integral model of a certain Shimura variety, over $\mathbb{Z}[1/2]$. It is surjective over \mathbb{C} , and assuming (\star) , one can deduce from the criterion of Liedtke and Matsumoto that it is surjective on $\bar{\mathbb{F}}_p$ -points. In odd characteristic, Kottwitz [1990] and Kisin [2013] have given a group-theoretic description of the isogeny classes in $\text{Sh}_{2d}(\bar{\mathbb{F}}_p)$,

for every d . With arguments similar to those in Section 3, it should be possible to deduce Theorem 1 and Theorem 3 from the above results.

1. p -adic properties of zeta functions of K3 surfaces

1.1. Recap on the formal Brauer group of a K3 surface. Let X be a K3 surface over a field k . Artin and Mazur [1977] have shown that the functor

$$R \mapsto \ker(\mathrm{Br} X_R \rightarrow \mathrm{Br} X)$$

on Artinian k -algebras is prorepresentable by a (one-dimensional) formal group $\hat{\mathrm{Br}} X$ over k . This formal group is called the *formal Brauer group* of X .

Assume now that k is a perfect field of characteristic $p > 0$ and that X is not supersingular. Then $\hat{\mathrm{Br}} X$ has finite height h satisfying $1 \leq h \leq 10$. We denote by $\mathbb{D}(\hat{\mathrm{Br}} X)$ the (covariant) Dieudonné module of $\hat{\mathrm{Br}} X$. This has the structure of an F -crystal over k . It is free of rank h over the ring W of Witt vectors of k .

We denote by $H^2_{\mathrm{crys}}(X/W)_{<1}$ the maximal sub- F -crystal of $H^2_{\mathrm{crys}}(X/W)$ that has all slopes < 1 .

Proposition 7. *If X is not supersingular, then there is a canonical isomorphism*

$$H^2_{\mathrm{crys}}(X/W)_{<1} \cong \mathbb{D}(\hat{\mathrm{Br}} X)$$

of F -crystals over k .

Proof. By [Illusie 1979, §7.2] there is a canonical isomorphism of F -crystals

$$H^2_{\mathrm{crys}}(X/W) = H^2(X, W\mathcal{O}_X) \oplus H^1(X, W\Omega^1_{X/k}) \oplus H^0(X, W\Omega^2_{X/k}), \tag{1}$$

coming from the de Rham–Witt complex, and by [Artin and Mazur 1977, Corollary 4.3] we have an isomorphism of F -crystals

$$H^2(X, W\mathcal{O}_X) = \mathbb{D}(\hat{\mathrm{Br}} X).$$

Since $\hat{\mathrm{Br}} X$ is a formal group, the slopes of $H^2(X, W\mathcal{O}_X) = \mathbb{D}(\hat{\mathrm{Br}} X)$ are < 1 . On the other hand, since F is divisible by p^i on $H^{2-i}(X, W\Omega^i_{X/k})$, the slopes of the other summands in (1) are ≥ 1 . This proves the theorem. □

1.2. Proof of Theorem 1.

Proof. Property (2) holds by definition, (3) is a formal consequence of the trace formula in ℓ -adic cohomology (see, e.g., [Deligne 1974, §1]), and (1) is part of the Weil conjectures [Deligne 1972; 1974].

The other properties make use of crystalline cohomology. Property (4) is well known. It follows for example from Mazur’s proof of “Newton above Hodge” [Mazur 1972; 1973] for liftable varieties with torsion-free cohomology, see [Mazur

1972, §2]. Property (5) is a sharpening of a result of Yu and Yui [2008, Proposition 3.2]. The argument is essentially the same as in [loc. cit.], we repeat it for completeness.

For a polynomial $Q = \prod(1 - \gamma_i T) \in \mathbb{Q}_p[T]$ we denote by $Q_{<0}$ the product

$$Q_{<0} = \prod_{v_p(\gamma_i) < 0} (1 - \gamma_i T) \in \mathbb{Q}_p[T].$$

Let K be the field of fractions of W . If $q = p^a$, then by Proposition 7 we have

$$L_{\text{trc}, <0} := L_{\text{trc}, <0}(X/\mathbb{F}_q, T) = \det_K(1 - F^a T, K \otimes_W \mathbb{D}(\hat{\text{Br}} X)(1))$$

in $\mathbb{Q}_p[T] \subset K[T]$. Since $\hat{\text{Br}} X$ is a one-dimensional formal group of finite height, the crystal $\mathbb{D}(\hat{\text{Br}} X)$ is indecomposable. It follows that the endomorphism F^a of $\mathbb{D}(\hat{\text{Br}} X)$ has an irreducible minimum polynomial over K , and hence $L_{\text{trc}, <0} = P_{<0}^e$ for some irreducible $P_{<0} \in \mathbb{Q}_p(T)$. Let Q be an irreducible factor of L_{trc} . Then Q has a reciprocal root γ with $v_p(\gamma) < 0$, for otherwise the roots of Q would be algebraic integers and hence roots of unity. In particular $Q_{<0} = P_{<0}$. Apparently any two irreducible factors of L_{trc} share a common root, hence $L_{\text{trc}} = Q^e$. This proves (5). □

2. CM theory of K3 surfaces

This section collects results of Zarhin, Shafarevich and Rizov.

2.1. Hodge theoretic aspects. For a projective K3 surface X over \mathbb{C} we denote by $\text{NS}(X)$ its Néron–Severi group and by $T(X) \subset H^2(X, \mathbb{Z}(1))$ the transcendental lattice, i.e., $T(X)$ is the orthogonal complement of $\text{NS}(X)$. We have a decomposition

$$H^2(X, \mathbb{Q}(1)) = \text{NS}(X)_{\mathbb{Q}} \oplus T(X)_{\mathbb{Q}}.$$

The Hodge structure $T(X)_{\mathbb{Q}}$ is irreducible [Zarhin 1983, Theorem 1.4.1]. The cup product pairing defines even symmetric bilinear forms on $\text{NS}(X)$ and $T(X)$ of signature $(1, \rho - 1)$ and $(2, 20 - \rho)$, with $\rho = \text{rk NS}(X)$.

Proposition 8 [Zarhin 1983, §2]. *Let X be a projective K3 surface over \mathbb{C} . Then the following are equivalent:*

- (1) *The Hodge group of $T(X)_{\mathbb{Q}}$ is commutative.*
- (2) *$E := \text{End}_{\text{HS}} T(X)_{\mathbb{Q}}$ is a CM field and $\dim_E T(X)_{\mathbb{Q}} = 1$.* □

Definition 9. If X satisfies the equivalent conditions (1) and (2) of Proposition 8, then we say that X is a K3 surface *with CM* (by E).

Remark 10. Another equivalent condition is that $T(X)_{\mathbb{Q}}$ is contained in the Tannakian category of Hodge structures generated by the H^1 of CM abelian varieties.

If E is a CM field, then we denote the canonical complex conjugation of E by $z \mapsto \bar{z}$, and its fixed field by E_0 . We have $[E : E_0] = 2$, and E_0 is a totally real number field.

Proposition 11. *Let X be a K3 surface with CM by E . Then*

- (1) $ax \cdot y = x \cdot \bar{a}y$ for all $a \in E$ and $x, y \in T(X)_{\mathbb{Q}}$;
- (2) the group of Hodge isometries of $T(X)_{\mathbb{Q}}$ is $\ker(\text{Nm} : E^{\times} \rightarrow E_0^{\times})$.

Proof. The cup product pairing induces an isomorphism

$$T(X)_{\mathbb{Q}} \xrightarrow{\sim} \text{Hom}(T(X)_{\mathbb{Q}}, \mathbb{Q})$$

of Hodge structures, and hence the action of E on $T(X)$ induces an “adjoint” homomorphism $\varphi : E \rightarrow E$ such that $ax \cdot y = x \cdot \varphi(a)y$. Considering the induced action on $H^{0,2}(X)$ one sees that $\varphi(a) = \bar{a}$, which proves the first assertion. The second is an immediate consequence of the first. \square

2.2. Arithmetic aspects: the Main Theorem of CM. Let X be a K3 surface over \mathbb{C} with CM by E . Consider the algebraic torus G over \mathbb{Q} which is the kernel of the norm map $E^{\times} \rightarrow E_0^{\times}$ (seen as map of tori over \mathbb{Q}). Then $G(\mathbb{Q})$ is the group of E -linear isometries of $T(X)_{\mathbb{Q}}$.

If X is defined over a subfield $k \subset \mathbb{C}$, then we have canonical isomorphisms

$$H_{\text{et}}^2(X_{\bar{k}}, \mathbb{Q}_{\ell}(1)) = H^2(X(\mathbb{C}), \mathbb{Q}(1)) \otimes_{\mathbb{Q}} \mathbb{Q}_{\ell}.$$

Since the Galois action on the left-hand side respects the intersection pairing and the subgroup $\text{NS}(X_{\bar{k}}) = \text{NS}(X_{\mathbb{C}})$, we see that both Gal_k and $G(\mathbb{Q}_{\ell})$ act on $T(X)_{\mathbb{Q}_{\ell}}$. If we denote by \mathbb{A}_f the finite adèles of \mathbb{Q} , i.e., $\mathbb{A}_f = \mathbb{Q} \otimes \hat{\mathbb{Z}}$, then we obtain actions of Gal_k and $G(\mathbb{A}_f)$ on $T(X)_{\mathbb{A}_f}$.

Theorem 12 (Main Theorem of CM for K3 surfaces [Rizov 2010]). *There exists a number field $k \subset \mathbb{C}$ containing E such that*

- (1) X is defined over k ,
- (2) the Galois action on $T(X)_{\mathbb{A}_f}$ factors over a map $\rho : \text{Gal}_k \rightarrow G(\mathbb{A}_f)$
- (3) the diagram

$$\begin{array}{ccc} \text{Gal}_k & \hookrightarrow & \text{Gal}_E \xrightarrow{\text{CFT}} \mathbb{A}_{E,f}^{\times} / E^{\times} \\ \downarrow \rho & & \downarrow z \mapsto \bar{z}/z \\ G(\mathbb{A}_f) & \longrightarrow & G(\mathbb{A}_f) / G(\mathbb{Q}) \end{array}$$

commutes.

Proof. This is a reformulation of [Rizov 2010, Corollary 3.9.2]. Note however that the stated definition of complex multiplication [Rizov 2010, Definition 1.4.3] needs to be corrected (the condition $\dim_E T_{\mathbb{Q}} = 1$ is missing) for the proof and statement to be correct. \square

Remark 13. A priori, the moduli space of polarized complex K3 surfaces has two natural models over \mathbb{Q} : the “canonical model” of the theory of Shimura varieties [Deligne 1971, §3], which is defined in terms of the Galois action on special points, and the model coming from the moduli interpretation. The essential content of Theorem 12 is that these two models coincide. (See also [Madapusi Pera 2015, §3]).

3. Existence of K3 surface with CM by a given CM field

In this section we prove Theorem 4. By the surjectivity of the period map for K3 surfaces, this reduces to a problem about quadratic forms over \mathbb{Q} .

3.1. Invariants of quadratic forms over \mathbb{Q} . We quickly recall some basic facts about quadratic forms over \mathbb{Q} . We refer to [Cassels 1978; Scharlau 1985; Serre 1970] for details and proofs. Let k be a field of characteristic different from 2. A *quadratic space* over k is a pair $V = (V, q)$ consisting of a finite-dimensional vector space over k and a nondegenerate symmetric bilinear form $q : V \times V \rightarrow k$. To such a space one associates the following invariants:

- (1) the *dimension* $\dim(V)$;
- (2) the *determinant* $\det(V) \in k^\times / k^{\times 2}$;
- (3) the *Hasse invariant* $w(V) \in \text{Br}(k)[2]$.

Any form V over k is isomorphic to a diagonal form $\langle \alpha_1, \dots, \alpha_n \rangle$ with $n = \dim V$, and for such a form the invariants are

$$\det(V) = \prod_i \alpha_i \in k^\times / k^{\times 2},$$

$$w(V) = \sum_{i < j} (\alpha_i, \alpha_j)_k \in \text{Br}(k)[2],$$

where $(\alpha, \beta)_k$ denotes the class of the quaternion algebra generated by i and j with $i^2 = \alpha, j^2 = \beta, ij = -ji$.

We denote the orthogonal sum of two quadratic spaces by $V \oplus W$.

Lemma 14. *Let V and W be quadratic spaces over k . Then*

- (1) $\det(V \oplus W) = \det(V) \det(W)$;
- (2) $w(V \oplus W) = w(V) + w(W) + (\det(V), \det(W))_k$.

Proof. This follows from the above formulas for the determinant and Hasse invariant of a diagonal quadratic form, and the bilinearity of $(\alpha, \beta)_k$. \square

Theorem 15. *Two forms over \mathbb{Q}_p are isomorphic if and only if they have the same dimension, determinant and Hasse invariant. For every $d \geq 3$, $\delta \in \mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2}$ and $w \in \text{Br}(\mathbb{Q}_p)[2]$ there exists a form of dimension d , determinant δ and Hasse invariant w . \square*

If $k = \mathbb{Q}$ then a fourth invariant is given by the signature of the form $V_{\mathbb{R}}$.

Theorem 16. *Two forms over \mathbb{Q} are isomorphic if and only if they have the same signature, determinant, and Hasse invariant. All forms V over \mathbb{Q} of signature (r, s) satisfy*

- (1) *the sign of $\delta(V)$ is $(-1)^s$;*
- (2) *the image of $w(V)$ in $\text{Br}(\mathbb{R})[2] = \mathbb{Z}/2\mathbb{Z}$ is $s(s - 1)/2 \pmod 2$.*

If $r + s \geq 3$, and if δ and w satisfy (1) and (2) above, then there exists a quadratic space over \mathbb{Q} with signature (r, s) , determinant δ and Hasse invariant w . \square

Lemma 17. *For $\Lambda_{K3, \mathbb{Q}} = \mathbb{Q} \otimes_{\mathbb{Z}} \Lambda_{K3}$, the Hasse invariant $w(\Lambda_{K3, \mathbb{Q}}) \in \text{Br}(\mathbb{Q})[2]$ is the class of the quaternion algebra $(-1, -1)_{\mathbb{Q}}$, and $\det(\Lambda_{K3, \mathbb{Q}}) = -1$.*

Proof. We have $\Lambda_{K3} \cong (-E_8) \oplus (-E_8) \oplus U \oplus U \oplus U$ where U is the standard hyperbolic plane. Using this explicit description, one computes (over \mathbb{Q}) an orthogonal basis, and computes the invariants using the formula for diagonal forms. \square

3.2. The form q_λ . Let E be a CM field with maximal totally real subfield E_0 . Put $d := [E_0 : \mathbb{Q}]$. Denote by $z \mapsto \bar{z}$ the complex conjugation on E . For $\lambda \in E_0^\times$ the map

$$q_\lambda : E \times E \mapsto \mathbb{Q}, \quad (x, y) \mapsto \text{tr}_{E_0/\mathbb{Q}}(\lambda x \bar{y})$$

is a nondegenerate symmetric bilinear form over \mathbb{Q} .

We denote the discriminant of the number field E by $\Delta(E/\mathbb{Q})$.

Lemma 18 [Bayer-Fluckiger 2014, Lemma 1.3.2].

$$\det(q_\lambda) = (-1)^d \Delta(E/\mathbb{Q}) \quad \text{in } \mathbb{Q}^\times / \mathbb{Q}^{\times 2}.$$

Lemma 19. *If $\lambda \in E_0^\times$ has signature (r, s) , then q_λ has signature $(2r, 2s)$. \square*

3.3. Construction of a K3 surface with CM by E . A key ingredient in the proof of Theorem 4 is the following proposition on rational quadratic forms. I am grateful to Eva Bayer for pointing me to her work on maximal tori in orthogonal groups [Bayer-Fluckiger 2014], and for explaining how it simplifies an earlier version of the proof below.

Proposition 20. *Let E be a CM field with maximal totally real subfield E_0 , and assume $d := [E_0 : \mathbb{Q}] \leq 10$. Then there exists a $\lambda \in E_0^\times$ of signature $(1, d - 1)$ and a quadratic space V such that, as quadratic spaces over \mathbb{Q} ,*

$$(E, q_\lambda) \oplus V \cong \Lambda_{K3, \mathbb{Q}} \quad \square$$

Proof. If $d < 10$ then we claim that for every choice of λ a complement V exists. Indeed, given a choice of λ , then the dimension, signature, determinant and Hasse invariant of V are determined by Lemma 14. These invariants satisfy conditions (1) and (2) of Theorem 16 because they are satisfied by the invariants of (E, q_λ) and $\Lambda_{K3, \mathbb{Q}}$. Since $\dim(V) > 2$, the theorem then guarantees the existence of a form V with $(E, q_\lambda) \oplus V \cong \Lambda_{K3, \mathbb{Q}}$.

So we assume $d = 10$. Let $\delta = \Delta(E/\mathbb{Q}) \in \mathbb{Q}^\times / \mathbb{Q}^{\times 2}$. Note that $\delta > 0$ (since d is even). Consider the diagonal quadratic space $V = \langle -1, \delta \rangle$. By the same reasoning as above, there exists a unique quadratic space W of dimension 20 such that

$$W \oplus \langle -1, \delta \rangle \cong \Lambda_{K3, \mathbb{Q}}.$$

We will show that W can be realized as (E, q_λ) for a suitable choice of $\lambda \in E_0^\times$. Note that W has signature $(2, 18)$, so by Lemma 19 the scalar λ will automatically have signature $(1, 9)$.

By Corollary 4.0.3 and Proposition 1.3.1 of [Bayer-Fluckiger 2014], there exists a λ with $(E, q_\lambda) \cong W$ if and only if the following three conditions hold:

- (1) the signature of W is even;
- (2) $\text{disc}(W) = \delta$;
- (3) for every prime p such that all places of E_0 above p split in E , we have that $W_{\mathbb{Q}_p}$ is isomorphic to an orthogonal sum of 10 hyperbolic planes.

Our W clearly satisfies the first two conditions. For the third, consider a prime p such that all places of E_0 above p split in E . Then the image of δ in $\mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2}$ is 1. Together with Lemma 14 and Lemma 17 this allows us to compute the invariants of $W_{\mathbb{Q}_p}$, and we find $\det(W_{\mathbb{Q}_p}) = 1$ and $w(W_{\mathbb{Q}_p}) = (-1, -1)_{\mathbb{Q}_p}$. These are the same as the invariants for 10 copies of the hyperbolic plane, so with Theorem 15 we see that W satisfies the third condition, which finishes the proof of the proposition. \square

Finally, we show that for every CM field E of degree at most 20 there exists a projective K3 surface X with CM by E .

Proof of Theorem 4. Choose $\lambda \in E_0$ and V as in Proposition 20. This guarantees that there exists an integral lattice

$$\Lambda \subset (E, q_\lambda) \oplus V$$

with $\Lambda \cong \Lambda_{K3}$. Choose such a Λ , and choose an embedding $\epsilon : E \hookrightarrow \mathbb{C}$ with $\epsilon(\lambda) > 0$. Then we have a splitting

$$\Lambda_{\mathbb{C}} = \mathbb{C}_\epsilon \oplus \mathbb{C}_{\bar{\epsilon}} \oplus (\oplus_{\sigma \neq \epsilon, \bar{\epsilon}} \mathbb{C}_\sigma) \oplus V_{\mathbb{C}}.$$

We make Λ into a pure \mathbb{Z} -Hodge structure of weight 0 by declaring \mathbb{C}_ϵ to be of type $(1, -1)$, its conjugate $\mathbb{C}_{\bar{\epsilon}}$ of type $(-1, 1)$, and all the other terms of type $(0, 0)$.

By construction, the bilinear form $\Lambda \otimes \Lambda \rightarrow \mathbb{Z}$ is a morphism of Hodge structures. Note that E acts on $E \subset \Lambda_{\mathbb{Q}}$ via Hodge structure endomorphisms, so that E is irreducible and hence

$$\Lambda^{0,0} \cap \Lambda_{\mathbb{Q}} = V.$$

For every nonzero $z \in H^{2,0}$ we have $z \cdot \bar{z} \in \mathbb{R}_{>0}$ since $\epsilon(\lambda) > 0$, so that the surjectivity of the period map [Todorov 1980] gives the existence of a complex analytic K3 surface X and a Hodge isometry $\Lambda \cong H^2(X, \mathbb{Z}(1))$. A priori, it may not be clear that X is algebraic. However, as $\text{Pic}(X)_{\mathbb{Q}} \cong V$ has signature $(1, 21 - 2d)$, there exists an $h \in \text{Pic}(X)$ with $h \cdot h > 0$. By [Barth et al. 2004, Theorem IV.6.2] this implies that the surface X is projective. By construction, X is a K3 surface with CM by E . □

Remark 21. A similar construction has been used by Piatetski-Shapiro and Shafarevich [1973, §3] in showing the existence of some K3 surfaces with CM. The new ingredients that allow us to obtain a stronger result are the use of rational (as opposed to integral) quadratic forms, the results of Bayer on quadratic forms q_{λ} , and the use of the algebraicity criterion from [Barth et al. 2004], which avoids the delicate question of identifying an ample $h \in \text{Pic}(X)$.

4. Existence of K3 surface with given L_{trc}

In this section we will prove Theorem 3. So let

$$L = \prod_{i=1}^{2d} (1 - \gamma_i T) \in 1 + T\mathbb{Q}[T]$$

be a polynomial satisfying properties (1)–(5) of Theorem 1. Consider the number field $F := \mathbb{Q}(\gamma_1)$.

Lemma 22. *F is a CM field and $\bar{\gamma}_1 \gamma_1 = 1$.*

Proof. The image γ of γ_1 under any homomorphism $F \rightarrow \mathbb{C}$ satisfies $|\gamma| = 1$, hence $\bar{\gamma} = \gamma^{-1}$. Moreover γ cannot be real, since then $\gamma = \pm 1$, contradicting the fact that γ_1 is not a root of unity. It follows that F is a CM field with complex conjugation $\gamma_1 \mapsto \gamma_1^{-1}$. □

By property (5), the number field F has a unique valuation v above the prime p such that $v(\gamma_1) < 0$.

Lemma 23. *There exists an extension E of F with $[E : \mathbb{Q}] = 2d$, and such that*

- (1) *E is a CM field;*
- (2) *the valuation v has a unique extension to E .*

Proof. Let F_0 be the maximal totally real subfield of F . Let v_0 be the place of F_0 under v . Now choose a polynomial $P(X) \in F_0[X]$ such that

- (1) $\deg P = e$;
- (2) P has e real roots for every embedding $F_0 \hookrightarrow \mathbb{R}$;
- (3) P is irreducible in $(F_0)_{v_0}[X]$.

Note that v_0 splits in F , since by the preceding lemma $\bar{v}(\gamma_1) > 0$ and hence $\bar{v} \neq v$. In particular $P(X)$ is irreducible in $F_v[X]$, and it follows that $E := F[X]/P(X)$ is a field satisfying the desired conditions. \square

We fix an E satisfying the conditions of the lemma. Abusing notation, we will denote the unique extension of v to E by the same symbol v .

Lemma 24. $[E_v : \mathbb{Q}_p] = h$.

Proof. Since $L = Q^e$, and since v is the unique place with $v(\gamma_1) < 0$, we see from properties (4) and (5) in Theorem 1 that $[F_v : \mathbb{Q}_p] = h/e$. But $[E : F] = e$ and v has a unique extension to E , hence $[E_v : \mathbb{Q}_p] = h$. \square

Let X be a K3 surface over \mathbb{C} with CM by E . By the Main Theorem of CM (Theorem 12) this surface is defined over a number field k containing E . Let w be a place of k lying above v . We extend the commutative diagram of Theorem 12 to include the local-global compatibility of class field theory:

$$\begin{array}{ccccc}
 W_{k_w} & \hookrightarrow & W_{E_v} & \xrightarrow{\text{LCFT}} & E_v^\times \\
 \downarrow & & \downarrow & & \downarrow \\
 \text{Gal}_k & \hookrightarrow & \text{Gal}_E & \xrightarrow{\text{GCFT}} & \mathbb{A}_{E,f}^\times / E^\times \\
 \downarrow \rho & & & & \downarrow z \mapsto z/\bar{z} \\
 G(\mathbb{A}_f) & \longrightarrow & & & G(\mathbb{A}_f)/G(\mathbb{Q})
 \end{array} \tag{2}$$

Here $W_{k_w} \subset \text{Gal}_{k_w}$ denotes the Weil group of the local field k_w . Extending k if necessary, we may assume that the residue field \mathbb{F}_w is an extension of \mathbb{F}_q .

Choose a prime $\ell \neq p$. Then the image of inertia I_{k_w} in $G(\mathbb{Z}_\ell)$ is finite, hence after replacing k by a finite extension, we may assume that the action of Gal_{k_w} on $H_{\text{et}}^2(X_{\bar{k}}, \mathbb{Q}_\ell(1))$ is unramified.

Now assume X_{k_w} satisfies (\star) . Then, replacing k once more by a finite extension, we may assume by the criterion of Liedtke and Matsumoto [2015, Theorem 2.5] that X has good reduction at w . Let \bar{X}/\mathbb{F}_w be the reduction of X/k at w .

Let $\sigma \in W_{k_w}$ be a Frobenius element. Note that γ_1 lies in $G(\mathbb{Q}) \subset E^\times$.

Proposition 25. *There is an $m > 0$ such that for all $\ell \neq p$ we have in $G(\mathbb{Q}_\ell)$*

$$\rho(\sigma^m)_\ell = \gamma_1^{m[\mathbb{F}_w:\mathbb{F}_q]}.$$

Proof. Let $\pi \in E_v^\times$ be the image of σ under the CFT map. Then

$$v(\pi) = \frac{e(k_w : E_v)}{f(E_v : \mathbb{Q}_p)}.$$

The image of π in $G(\mathbb{A}_f)/G(\mathbb{Q})$ is the class of the idèle

$$(1, \dots, 1, \pi, \bar{\pi}^{-1}, 1, \dots, 1) \in \mathbb{A}_{E,f}^\times,$$

where $\bar{\pi} \in E_{\bar{v}}$ denotes the image of π under the isomorphism $E_v \rightarrow E_{\bar{v}}$ induced by complex conjugation on E .

We have $v(\gamma_1) = -[\mathbb{F}_q : \mathbb{F}_p]/h$ from which we compute

$$v(\gamma_1^{[\mathbb{F}_w : \mathbb{F}_q]}) = -v(\pi),$$

and hence $\bar{v}(\gamma_1^{[\mathbb{F}_w : \mathbb{F}_q]}) = v(\pi)$. Moreover, γ_1 is a unit at all places of E different from v and \bar{v} . It follows that the idèle

$$\alpha := \gamma_1^{[\mathbb{F}_w : \mathbb{F}_q]} \cdot (1, \dots, 1, \pi, \bar{\pi}, 1, \dots, 1) \in \mathbb{A}_{E,f}^\times.$$

lies in the maximal compact subgroup

$$\mathcal{K} = \{g \in (\mathcal{O}_E \otimes \hat{\mathbb{Z}})^\times \mid g\bar{g} = 1\} \subset G(\mathbb{A}_f).$$

Since Gal_k is compact also, $\rho(\sigma)$ lies in \mathcal{K} . From the commutativity of the diagram (2) we conclude that $\rho(\sigma)/\alpha$ lies in the kernel of the map

$$\mathcal{K} \rightarrow G(\mathbb{A}_f)/G(\mathbb{Q}).$$

This kernel equals $\{g \in \mathcal{O}_E^\times \mid g\bar{g} = 1\}$, which is finite by the Dirichlet unit theorem. We conclude that $\rho(\sigma^m) = \alpha^m$ for some m , and hence

$$\rho(\sigma^m)_\ell = \gamma_1^m$$

in $G(\mathbb{Q}_\ell)$ for all $\ell \neq p$. □

We have

$$L(\bar{X}/\mathbb{F}_w) = \det_{\mathbb{Q}_\ell}(1 - \sigma T, H_{\text{et}}^2(X_{\bar{\mathbb{F}}_w}, \mathbb{Q}_\ell(1))).$$

Since none of the conjugates of γ_1 are roots of unity, we conclude from the preceding proposition that there is a finite extension $\mathbb{F}_w \subset \mathbb{F}'_w$ such that

$$L_{\text{trc}}(\bar{X}_{\mathbb{F}'_w}/\mathbb{F}'_w) = \det_{\mathbb{Q}}(1 - \gamma_1^{[\mathbb{F}'_w : \mathbb{F}_q]} T, E),$$

or in other words

$$L_{\text{trc}}(\bar{X}_{\mathbb{F}'_w}/\mathbb{F}'_w) = \prod_i (1 - \gamma_i^{[\mathbb{F}'_w : \mathbb{F}_q]} T),$$

which finishes the proof of Theorem 3.

Acknowledgements

This paper has benefited significantly from enlightening discussions with Eva Bayer, Christophe Cornut, Johan de Jong, Nick Katz, Mark Kisin, Christian Liedtke, Ronald van Luijk, Yuya Matsumoto, Davesh Maulik, Ben Moonen and Raman Parimala — I am most grateful for their questions, answers, comments and suggestions. Most of the research leading to this paper was performed while I was a member at the IAS. My gratitude to the Institute and its staff for maintaining the most stimulating research environment cannot be overstated. Special thanks go to Momota Ganguli who promptly and enthusiastically fulfilled even my most obscure bibliographical requests. Finally, I wish to thank Lotte Meijer and Michel Reymond for the necessary diversions outside geometry.

The author acknowledges financial support of the National Science Foundation (NSF) and the Netherlands Organization for Scientific Research (NWO).

References

- [Artin and Mazur 1977] M. Artin and B. Mazur, “Formal groups arising from algebraic varieties”, *Ann. Sci. École Norm. Sup. (4)* **10**:1 (1977), 87–131. MR 56 #15663 Zbl 0351.14023
- [Barth et al. 2004] W. P. Barth, K. Hulek, C. A. M. Peters, and A. Van de Ven, *Compact complex surfaces*, 2nd ed., *Ergebnisse der Mathematik und ihrer Grenzgebiete (3)* **4**, Springer, Berlin, 2004. MR 2004m:14070 Zbl 1036.14016
- [Bayer-Fluckiger 2014] E. Bayer-Fluckiger, “Embeddings of maximal tori in orthogonal groups”, *Ann. Inst. Fourier (Grenoble)* **64**:1 (2014), 113–125. MR 3330542 Zbl 1318.11054
- [Cassels 1978] J. W. S. Cassels, *Rational quadratic forms*, London Mathematical Society Monographs **13**, Academic Press, London, 1978. Reprinted by Dover, Mineola, NY, 2008. MR 80m:10019 Zbl 0395.10029
- [Charles 2013] F. Charles, “The Tate conjecture for K3 surfaces over finite fields”, *Invent. Math.* **194**:1 (2013), 119–145. MR 3103257 Zbl 1282.14014
- [Charles 2014] F. Charles, “Birational boundedness for holomorphic symplectic varieties, Zarhin’s trick for K3 surfaces, and the Tate conjecture”, preprint, 2014. arXiv 1407.0592
- [Deligne 1971] P. Deligne, “Travaux de Shimura”, pp. 123–165 in *Séminaire Bourbaki 1970/1971* (Exposé 389), *Lecture Notes in Mathematics* **244**, Springer, Berlin, 1971. MR 58 #16675 Zbl 0225.14007
- [Deligne 1972] P. Deligne, “La conjecture de Weil pour les surfaces K3”, *Invent. Math.* **15** (1972), 206–226. MR 45 #5137 Zbl 0219.14022
- [Deligne 1974] P. Deligne, “La conjecture de Weil, I”, *Inst. Hautes Études Sci. Publ. Math.* **43** (1974), 273–307. MR 49 #5013 Zbl 0287.14001
- [Elsenhans and Jahnel 2015] A.-S. Elsenhans and J. Jahnel, “On the characteristic polynomial of the Frobenius on étale cohomology”, *Duke Math. J.* **164**:11 (2015), 2161–2184. MR 3385131 Zbl 06486373
- [Illusie 1979] L. Illusie, “Complexe de de Rham–Witt et cohomologie cristalline”, *Ann. Sci. École Norm. Sup. (4)* **12**:4 (1979), 501–661. MR 82d:14013 Zbl 0436.14007
- [Kedlaya and Sutherland 2015] K. S. Kedlaya and A. V. Sutherland, “A census of zeta functions of quartic K3 surfaces over F_2 ”, preprint, 2015. arXiv 1511.06945

- [Kisin 2013] M. Kisin, “Mod p points on Shimura varieties of abelian type”, preprint, Harvard University, 2013, Available at <http://www.math.harvard.edu/~kisin/dvifiles/lr.pdf>.
- [Kottwitz 1990] R. E. Kottwitz, “Shimura varieties and λ -adic representations”, pp. 161–209 in *Automorphic forms, Shimura varieties, and L-functions* (Ann Arbor, MI, 1988), vol. 1, edited by L. Clozel and J. S. Milne, Perspectives in Mathematics **10**, Academic Press, Boston, MA, 1990. MR 92b:11038 Zbl 0743.14019
- [Liedtke and Matsumoto 2015] C. Liedtke and Y. Matsumoto, “Good reduction of K3 surfaces”, preprint, 2015. arXiv 1411.4797
- [Madapusi Pera 2015] K. Madapusi Pera, “The Tate conjecture for K3 surfaces in odd characteristic”, *Invent. Math.* **201**:2 (2015), 625–668. MR 3370622 Zbl 06480962
- [Matsumoto 2015] Y. Matsumoto, “Good reduction criterion for K3 surfaces”, *Math. Z.* **279**:1–2 (2015), 241–266. MR 3299851 Zbl 1317.14089
- [Maulik 2014] D. Maulik, “Supersingular K3 surfaces for large primes”, *Duke Math. J.* **163**:13 (2014), 2357–2425. MR 3265555 Zbl 1308.14043
- [Mazur 1972] B. Mazur, “Frobenius and the Hodge filtration”, *Bull. Amer. Math. Soc.* **78** (1972), 653–667. MR 48 #8507 Zbl 0258.14006
- [Mazur 1973] B. Mazur, “Frobenius and the Hodge filtration (estimates)”, *Ann. of Math. (2)* **98** (1973), 58–95. MR 48 #297 Zbl 0261.14005
- [Milne 1975] J. S. Milne, “On a conjecture of Artin and Tate”, *Ann. of Math. (2)* **102**:3 (1975), 517–533. MR 54 #2659 Zbl 0343.14005
- [Piatetski-Shapiro and Shafarevich 1973] I. I. Piatetski-Shapiro and I. R. Shafarevich, “Арифметика поверхностей типа K3”, *Trudy Mat. Inst. Steklov.* **132** (1973), 44–54. Translated as “The arithmetic of surfaces of type K3” in *Proc. Steklov Inst. Math.* **132** (1973), 45–57. MR 49 #302 Zbl 0293.14010
- [Rizov 2010] J. Rizov, “Kuga–Satake abelian varieties of K3 surfaces in mixed characteristic”, *J. Reine Angew. Math.* **648** (2010), 13–67. MR 2012e:14089 Zbl 1208.14031
- [Scharlau 1985] W. Scharlau, *Quadratic and Hermitian forms*, Grundlehren der Mathematischen Wissenschaften **270**, Springer, Berlin, 1985. MR 86k:11022 Zbl 0584.10010
- [Serre 1970] J.-P. Serre, *Cours d’arithmétique*, Collection SUP: “Le Mathématicien” **2**, Presses Universitaires de France, Paris, 1970. Translated as *A course in arithmetic*, Graduate Texts in Mathematics **7**, Springer, New York, 1973. MR 41 #138 Zbl 0225.12002
- [Tate 1971] J. Tate, “Classes d’isogénie des variétés abéliennes sur un corps fini (d’après T. Honda)”, pp. 95–110 in *Séminaire Bourbaki 1968/1969* (Exposé 352), Lecture Notes in Mathematics **175**, Springer, Berlin, 1971. MR 3077121 Zbl 0212.25702
- [Todorov 1980] A. N. Todorov, “Applications of the Kähler–Einstein–Calabi–Yau metric to moduli of K3 surfaces”, *Invent. Math.* **61**:3 (1980), 251–265. MR 82k:32065 Zbl 0472.14006
- [Yu and Yui 2008] J.-D. Yu and N. Yui, “K3 surfaces of finite height over finite fields”, *J. Math. Kyoto Univ.* **48**:3 (2008), 499–519. MR 2010j:11099 Zbl 1174.14034
- [Zarhin 1983] Y. G. Zarhin, “Hodge groups of K3 surfaces”, *J. Reine Angew. Math.* **341** (1983), 193–220. MR 84g:14009 Zbl 0506.14034

Communicated by Kiran S. Kedlaya

Received 2015-08-17

Revised 2015-11-27

Accepted 2015-12-27

l.d.j.taelman@uva.nl

Korteweg-de Vries Instituut, Universiteit van Amsterdam,
P.O. Box 94248, 1090 GE Amsterdam, Netherlands

Algebra & Number Theory

msp.org/ant

EDITORS

MANAGING EDITOR

Bjorn Poonen
Massachusetts Institute of Technology
Cambridge, USA

EDITORIAL BOARD CHAIR

David Eisenbud
University of California
Berkeley, USA

BOARD OF EDITORS

Dave Benson	University of Aberdeen, Scotland	Susan Montgomery	University of Southern California, USA
Richard E. Borcherds	University of California, Berkeley, USA	Shigefumi Mori	RIMS, Kyoto University, Japan
John H. Coates	University of Cambridge, UK	Raman Parimala	Emory University, USA
J-L. Colliot-Thélène	CNRS, Université Paris-Sud, France	Jonathan Pila	University of Oxford, UK
Brian D. Conrad	Stanford University, USA	Anand Pillay	University of Notre Dame, USA
Hélène Esnault	Freie Universität Berlin, Germany	Victor Reiner	University of Minnesota, USA
Hubert Flenner	Ruhr-Universität, Germany	Peter Sarnak	Princeton University, USA
Sergey Fomin	University of Michigan, USA	Joseph H. Silverman	Brown University, USA
Edward Frenkel	University of California, Berkeley, USA	Michael Singer	North Carolina State University, USA
Andrew Granville	Université de Montréal, Canada	Vasudevan Srinivas	Tata Inst. of Fund. Research, India
Joseph Gubeladze	San Francisco State University, USA	J. Toby Stafford	University of Michigan, USA
Roger Heath-Brown	Oxford University, UK	Ravi Vakil	Stanford University, USA
Craig Huneke	University of Virginia, USA	Michel van den Bergh	Hasselt University, Belgium
Kiran S. Kedlaya	Univ. of California, San Diego, USA	Marie-France Vignéras	Université Paris VII, France
János Kollár	Princeton University, USA	Kei-Ichi Watanabe	Nihon University, Japan
Yuri Manin	Northwestern University, USA	Efim Zelmanov	University of California, San Diego, USA
Philippe Michel	École Polytechnique Fédérale de Lausanne	Shou-Wu Zhang	Princeton University, USA

PRODUCTION

production@msp.org
Silvio Levy, Scientific Editor


See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2016 is US \$290/year for the electronic version, and \$485/year (+\$55, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscribers address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW[®] from MSP.

PUBLISHED BY

 **mathematical sciences publishers**
nonprofit scientific publishing

<http://msp.org/>

© 2016 Mathematical Sciences Publishers