View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Elsevier - Publisher Connector

Journal of Number Theory 130 (2010) 1939–1963

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Lines on Fermat surfaces ☆

Matthias Schütt [a,*], Tetsuji Shioda [b,c], Ronald van Luijk [d]

[a] Institute for Algebraic Geometry, Leibniz University Hannover, Welfengarten 1, 30167 Hannover, Germany
[b] Department of Mathematics, Rikkyo University, Tokyo 171-8501, Japan
[c] RIMS, Kyoto University, Kyoto 606-8502, Japan
[d] Mathematisch Instituut, Universiteit Leiden, Postbus 9512, 2300 RA, Leiden, The Netherlands

ARTICLE INFO

Article history:
Received 30 September 2009
Revised 21 January 2010
Available online 2 April 2010
Communicated by Jean-Louis Colliot-Thélène

MSC:
primary 14J25
secondary 11G25, 14C22

Keywords:
Fermat surface
Néron–Severi group
Supersingular reduction

ABSTRACT

We prove that the Néron–Severi groups of several complex Fermat surfaces are generated by lines. Specifically, we obtain these new results for all degrees up to 100 that are relatively prime to 6. The proof uses reduction modulo a supersingular prime. The techniques are developed in detail. They can be applied to other surfaces and varieties as well.

© 2010 Elsevier Inc. All rights reserved.

1. Introduction

Fermat varieties have been a classical object of study in geometry and arithmetic. Here we consider the smooth projective surface of degree $m \in \mathbb{N}$

$$S\colon \quad \{x_0^m + x_1^m + x_2^m + x_3^m = 0\} \subset \mathbb{P}^3. \tag{1}$$

This paper is concerned with the Néron–Severi group $\mathrm{NS}(S)$ of S over the complex numbers, consisting of divisors up to algebraic equivalence.

☆ Partial funding from DFG under grant Schu 2266/2-2 and JSPS under Grant-in-Aid for Scientific Research (C) No. 20540051 is gratefully acknowledged.

* Corresponding author.
E-mail addresses: schuett@math.uni-hannover.de (M. Schütt), shioda@rikkyo.ac.jp (T. Shioda), rvl@math.leidenuniv.nl (R. van Luijk).
URLs: http://www.iag.uni-hannover.de/~schuett/ (M. Schütt), http://www.rkmath.rikkyo.ac.jp/math/shioda/ (T. Shioda), http://www.math.leidenuniv.nl/~rvl (R. van Luijk).

0022-314X/$ – see front matter © 2010 Elsevier Inc. All rights reserved.
doi:10.1016/j.jnt.2010.01.008

In general, it is hard to compute the Néron–Severi group of a variety. The cohomology of Fermat surfaces, however, admits a decomposition into eigenspaces with respect to an abelian subgroup of the automorphism group. Combinatorial data give the Picard number $\rho(S)$, the rank of $\mathrm{NS}(S)$. A rational basis of $\mathrm{NS}(S)$ (i.e. a basis of $\mathrm{NS}(S) \otimes \mathbb{Q}$) was determined in [1] up to certain cycles induced from Fermat surfaces with degree m in the range $12 \leqslant m \leqslant 180$.

The cycles exhibited in [1] involve some particularly prominent divisors on S, namely the $3m^2$ obvious lines. The lines generate $\mathrm{NS}(S)$ rationally if and only if $m \leqslant 4$ or $(m, 6) = 1$. In Proposition 4.1, we will improve the results from [1] in the sense that we identify a rational basis consisting of lines explicitly.

A natural question now is: in which of the above cases do the lines generate the full Néron–Severi group? As opposed to *rational generation*, we refer to this property as *integral generation*. Integral generation is known to hold true for $m \leqslant 4$, as we will review in Section 3. Our main result is the following:

Theorem 1.1. *Let $m \leqslant 100$ be a positive integer. Then the Néron–Severi group of the complex Fermat surface S of degree m is integrally generated by lines if and only if $m \leqslant 4$ or $(m, 6) = 1$.*

We shall use supersingular reduction to prove the theorem. The technique is briefly outlined below; a full account will be given in Section 5. For the degrees $m < 17$, the method is applied separately in Sections 6.2–6.5 to exhibit a proof of the corresponding part of Theorem 1.1. In Section 7, we develop an extension of the supersingular reduction technique that is less involved computationally. This technique is applied to the remaining degrees in Section 7.4 to complete the proof of Theorem 1.1. The explicit approach in Section 6 has two advantages over the extension in Section 7: first the reader may find that it illustrates the methods more clearly; secondly it provides extra information, for instance a basis of the Néron–Severi group of the reduction of the surface.

We give a brief outline of the supersingular reduction technique. Starting from a complex Fermat surface S, we consider the reduction S_p of the integral model (1) modulo a good prime p. By choosing a supersingular prime, we achieve good control of the discriminant of the Néron–Severi lattice of the reduction S_p (Theorem 5.2). Then we compare the discriminants of two lattices: on the one hand the sublattice of finite index in $\mathrm{NS}(S)$ generated by lines, on the other hand a suitable (often finite-index) sublattice of $\mathrm{NS}(S_p)$ where we complement the reductions of the original lines by some divisors that are peculiar to the chosen characteristic (cf. Section 5.1). Unless these discriminants have a common square factor, this method suffices to prove that the sublattice generated by lines is already the full Néron–Severi lattice by Criterion 5.3.

In spirit the supersingular reduction technique is related to a method to compute the Picard number of a projective surface which was introduced by one of the authors in [20]. Namely it was proved that certain K3 surfaces have Picard number one by reducing modulo two different primes. From the Lefschetz fixed point formula, one would derive that the reductions had Picard number (at most) two. Then one would find divisors peculiar to the respective characteristic and compare the resulting discriminants of the Néron–Severi lattices. Once they did not match up to a square factor, it would follow that the original surface had Picard number one.

The supersingular reduction technique compares sublattices of $\mathrm{NS}(S)$ and $\mathrm{NS}(S_p)$ for a supersingular prime p, while the method in [20] required two suitable reductions. Both methods are greatly inspired by the Tate conjecture [19], and in fact the equivalent statement of the Artin–Tate conjecture [11] plays a crucial role for several aspects (cf. Theorem 5.2 and [10]).

The computations were carried out with MAGMA. Programs and scripts are available from the third author's webpage. We are indebted to Bas Edixhoven for the use of his computer.

2. Preliminaries on projective surfaces and lattices

In this section, we recall some basic facts about lattices, projective surfaces and divisors that are relevant for our purposes. In view of Fermat surfaces, we will mostly be concerned with smooth surfaces in $\mathbb{P}^3$. For general background, the reader might confer [3] or [13].

Throughout this paper, every lattice is assumed to be integral unless otherwise stated. In other words, a lattice is a finitely generated free abelian group Λ, together with a symmetric bilinear pairing $\langle\cdot,\cdot\rangle : \Lambda \times \Lambda \to \mathbb{Z}$ that is non-degenerate, i.e., the induced map $\Lambda \to \mathrm{Hom}(\Lambda, \mathbb{Z})$ is injective. The discriminant of a lattice Λ is the determinant of the Gram matrix $(\langle x, y\rangle)_{x,y}$, where x and y run through any chosen basis of Λ; the discriminant is independent of the choice of basis. If L is a finite-index sublattice of a lattice Λ, then their discriminants are related through the equality

$$\mathrm{disc}(L) = [\Lambda : L]^2 \cdot \mathrm{disc}(\Lambda).$$

We say that a sublattice L is primitive in Λ if the quotient Λ/L is torsion-free. This is only possible if L has positive corank in Λ or $L = \Lambda$.

If k is a field and L a lattice, then L_k denotes the vector space $L \otimes_{\mathbb{Z}} k$. For any vector space V over a field k, we denote its dual $\mathrm{Hom}(V, k)$ by V^*.

On any projective surface X, the curves generate the group $\mathrm{Div}(X)$ freely. This group can be endowed with a meaningful structure by dividing out by some equivalence relation such as linear equivalence $\sim$, algebraic equivalence $\approx$ or numerical equivalence $\equiv$ (with implications from left to right).

Two curves are algebraically equivalent if they move within a family of divisors on X over some curve (for instance any fibration has algebraically equivalent fibers). The Néron–Severi group of a projective surface X is defined as the quotient

$$\mathrm{NS}(X) = \mathrm{Div}(X)/\approx.$$

Its rank is called the Picard number, denoted by $\rho(X)$. The Néron–Severi group depends on the chosen base field of the variety (such as number fields, finite fields). In this paper, we are concerned with geometric invariants; hence we always consider the geometric Néron–Severi groups, i.e. for a base change of the surface to an algebraic closure of its base field $(\mathbb{C}, \bar{\mathbb{Q}}, \bar{\mathbb{F}}_p)$. Whenever X is a Fermat surface over $\mathbb{C}$ of degree m and we want to reduce it modulo a prime $p \nmid m$, it is implicitly understood that we work with the integral model (1) of X that has good reduction at p; the surface in the reduction can then be considered over $\bar{\mathbb{F}}_p$.

Two divisors are numerically equivalent if they return the same intersection numbers with all divisors on X (or equivalently with all divisor classes in $\mathrm{NS}(X)$). The corresponding quotient is denoted by $\mathrm{Num}(X)$. It is known that the only difference between algebraic and numerical equivalence lies in the torsion in $\mathrm{NS}(X)$:

$$\mathrm{Num}(X) = \mathrm{NS}(X)/\mathrm{torsion}.$$

In particular, these notions coincide if X is (algebraically) simply connected. This holds for large classes of varieties such as complete smooth intersection in $\mathbb{P}^n$ of dimension greater than one. In consequence, for any smooth surface X in $\mathbb{P}^3$, the Néron–Severi group is torsion-free. The intersection form endows $\mathrm{NS}(X)$ with the structure of a lattice, also called the Néron–Severi lattice. By the Hodge index theorem, the Néron–Severi lattice has signature $(1, \rho(X) - 1)$.

We have seen that it suffices to compute intersection numbers to understand the Néron–Severi groups of Fermat surfaces. Self-intersection numbers involve a subtlety as they can be negative. For a (smooth) irreducible curve C on a surface X, one can compute C^2 through the adjunction formula:

$$2g(C) - 2 = C^2 + C.K_X.$$

Here $g(C)$ is the genus of C and K_X denotes the canonical divisor of X. Often the canonical divisor can be expressed through a hyperplane section H. For a smooth surface of degree m in $\mathbb{P}^3$, one has $K_X = (m-4)H$. For a line $\mathfrak{l}$ and a conic Q (both rational curves, thus of genus zero), one obtains the following self-intersection numbers on such a surface X:

$$\mathfrak{l}^2 = 2 - m, \qquad Q^2 = 6 - 2m.$$

More generally, if C is a rational curve of degree d on a smooth surface of degree m in $\mathbb{P}^3$, then $C^2 = 4d - 2 - dm$.

We conclude this section by indicating how to compute the Betti numbers and Hodge numbers of a smooth (complex) surface X of degree m in $\mathbb{P}^3$. We have already mentioned that $b_1(X) = q(X) = 0$. By Serre duality, the geometric genus equals

$$p_g(X) = h^2(X, \mathcal{O}_X) = h^0(X, K_X) = h^0\big(\mathbb{P}^3, \mathcal{O}_{\mathbb{P}^3}(m-4)\big) = \binom{m-1}{3}.$$

Thus we compute the Euler characteristic $\chi(\mathcal{O}_X) = h^0(\mathcal{O}_X(X)) - q + p_q(X) = 1 + p_g(X)$. The topological Euler number $e(X)$ (which can be defined as the alternating sum of Betti numbers in arbitrary characteristic) can be computed by Noether's formula

$$12\chi(\mathcal{O}_X) = e(X) + K_X^2.$$

Here $K_X^2 = m(m-4)^2$. Then the second Betti number is calculated as $b_2(X) = e(X) - 2$, as we have $b_0 = b_4 = 1$ and $b_1 = b_3 = 0$ by Poincaré duality. One finds

$$b_2(X) = m^3 - 4m^2 + 6m - 2.$$

Over $\mathbb{C}$, we obtain the Hodge number $h^{1,1} = b_2(X) - 2p_g(X)$. The Picard number relates to these invariants as follows:

- in characteristic zero, $\rho(X) \leqslant h^{1,1}(X)$ by Lefschetz' theorem;
- in positive characteristic, $\rho(X) \leqslant b_2(X)$ by Igusa's theorem.

Surfaces attaining an equality in the latter setting are often called *supersingular*. We will recall some of their properties in Section 5 and use them for our supersingular reduction technique.

3. Rational generation of NS

The cohomology of Fermat varieties admits a decomposition into eigenspaces with respect to an abelian subgroup of the automorphism group. According to work by Weil, it splits into one-dimensional eigenspaces; we review these concepts below starting with (2). It is well known which eigenspaces are algebraic, and in the surface case, even which eigenspaces correspond to lines.

Theorem 3.1. *(See Shioda [17].) Let S denote the complex Fermat surface of degree m. The $\mathbb{Q}$-vector space $\mathrm{NS}(S) \otimes_{\mathbb{Z}} \mathbb{Q}$ is generated by divisor classes of lines if and only if $m \leqslant 4$ or m is coprime to 6.*

Before reviewing the proof of the theorem, we comment on the main problem of this paper whether, for the appropriate degrees, lines generate $\mathrm{NS}(S)$ fully or only up to finite index. We now review the current knowledge about this problem.

For $m \leqslant 3$, the integral generation problem has a positive answer. These Fermat surfaces are rational. For $m = 1, 2$, the statement is almost trivial, corresponding to $\mathbb{P}^2$ and $\mathbb{P}^1 \times \mathbb{P}^1$. Any smooth projective cubic complex surface contains 27 lines. Their configuration has been studied in great detail. In fact, any smooth cubic surface is isomorphic to the projective plane $\mathbb{P}^2$ blown up in six distinct points.

For $m = 4$, the K3 case, rational generation must have been known since the 1950's. Meanwhile for integral generation, the answer was conjectured to be positive, but unknown until Mizukami in 1975 proved the affirmative [12]. We will review the history of the original proof and provide an alternative proof using our technique of supersingular reduction in Section 6.1. Our Theorem 1.1 provides the first answer to the question for Fermat surfaces of general type.

In the sequel we shall sketch the line of argument for rational generation from [17] for later use in the next section. In order to prove Theorem 3.1 it clearly suffices to prove the corresponding statement for $\mathrm{NS}(S)\otimes\mathbb{C}$. Hence we will mostly work with the latter vector space in this section and analyse when it is generated by lines.

First we fix notation for the $3m^2$ lines on S, the Fermat surface of degree m. More precisely, we consider the model (1) over an algebraically closed field K of characteristic $p\geqslant 0$ relatively prime to m. Throughout the paper, we denote by μ_n the group of n-th roots of unity of K. Let $\omega\in\mu_{2m}$ such that $\omega^m=-1$. Then for any $\zeta,\eta\in\mu_m$ we have the lines

$$\begin{aligned}
\mathfrak{l}_1(\zeta,\eta)&=\bigl\{[\lambda,\omega\zeta\lambda,\mu,\omega\eta\mu];\ [\lambda,\mu]\in\mathbb{P}^1\bigr\},\\
\mathfrak{l}_2(\zeta,\eta)&=\bigl\{[\lambda,\mu,\omega\zeta\lambda,\omega\eta\mu];\ [\lambda,\mu]\in\mathbb{P}^1\bigr\},\\
\mathfrak{l}_3(\zeta,\eta)&=\bigl\{[\lambda,\mu,\omega\eta\mu,\omega\zeta\lambda];\ [\lambda,\mu]\in\mathbb{P}^1\bigr\}.
\end{aligned}$$

On the model (1) of S over K, the abelian group μ_m^4/μ_m acts by multiplication on homogeneous coordinates:

$$g=[\zeta_1,\zeta_1,\zeta_2,\zeta_3]\in\mu_m^4/\mu_m:[x_0,x_1,x_2,x_3]\mapsto[\zeta_0x_0,\zeta_1x_1,\zeta_2x_2,\zeta_3x_3]. \tag{2}$$

The character group of μ_m^4/μ_m is isomorphic to the kernel of the map

$$\Sigma:(\mathbb{Z}/m\mathbb{Z})^4\to\mathbb{Z}/mZ,\qquad \alpha=(a_0,a_1,a_2,a_3)\mapsto\sum_i a_i,$$

where α sends $g=[\zeta_0,\zeta_1,\zeta_2,\zeta_3]\in\mu_m^4/\mu_m$ to $\alpha(g)=\prod_i\zeta_i^{a_i}\in\mu_m$. We shall consider the eigenspaces of $H^2(S)$ for the induced action of μ_m^4/μ_m with character α in the following subset of the character group

$$\mathfrak{A}_m:=\bigl\{\alpha=(a_0,a_1,a_2,a_3)\in\ker\Sigma\ \bigm|\ a_i\neq 0\ \forall i=0,\dots,3\bigr\}.$$

For $\alpha\in\mathfrak{A}_m$, the corresponding eigenspace $V(\alpha)\subset H^2(S)$ with character α is defined by the condition that $g^*|_{V(\alpha)}$ acts as multiplication by $\alpha(g)$ for all $g\in\mu_m^4/\mu_m$. By results that go back to Weil [21,22] (see also Katz [9, §6] and Ogus [14, §3]), each $V(\alpha)$ is one-dimensional, and

$$H^2(S)=V_0\oplus\bigoplus_{\alpha\in\mathfrak{A}_m}V(\alpha).$$

Here V_0 corresponds to the trivial character and is spanned by the hyperplane section. One easily checks that $\#\mathfrak{A}_m=(m-1)(m^2-3m+3)$, so that indeed $\#\mathfrak{A}_m+1=b_2(S)$.

Up to this point, the whole argument does not depend on the characteristic and works for any appropriate cohomology theory. From now on, we specialise to the complex case. Writing $\alpha=(a_0,\dots,a_3)\in\mathfrak{A}_m$ with canonical representatives $0<\tilde a_i<m$, we define

$$|\alpha|=(\tilde a_0+\cdots+\tilde a_3)/m.$$

Then the eigenspace $V(\alpha)$ has the Hodge weights $(|\alpha|-1,3-|\alpha|)$. In order to decide whether $V(\alpha)$ is algebraic, we let $(\mathbb{Z}/m\mathbb{Z})^*$ operate on $\mathfrak{A}_m$ coordinatewise by multiplication. As a consequence of Lefschetz' theorem, $V(\alpha)$ is algebraic if and only if every element in the $(\mathbb{Z}/m\mathbb{Z})^*$-orbit of α has Hodge weight $(1,1)$, i.e., if and only if $|r\alpha|=2$ for all $r\in(\mathbb{Z}/m\mathbb{Z})^*$.

To collect the corresponding α, we define the subset $\mathfrak{B}_m \subset \mathfrak{A}_m$ as follows:

$$\alpha \in \mathfrak{B}_m \quad \Longleftrightarrow \quad \forall r \in (\mathbb{Z}/m\mathbb{Z})^*\colon\ |r\alpha| = 2.$$

The space $V(\alpha)$ is algebraic if and only if $\alpha \in \mathfrak{B}_m$. Hence

$$\rho(S) = \#\mathfrak{B}_m + 1.$$

By [17], the span of the lines is also known: In $\mathrm{NS}(S) \otimes \mathbb{C}$, this is

$$V_0 \oplus \bigoplus_{\alpha \in \mathfrak{D}_m} V(\alpha), \tag{3}$$

where $\mathfrak{D}_m \subseteq \mathfrak{B}_m$ denotes the subset of decomposable elements α, i.e., those $\alpha \in \mathfrak{B}_m$ for which there is some index $j > 0$ such that $a_0 + a_j = 0$. Then one easily computes

$$\#\mathfrak{D}_m = 3(m-1)(m-2) + \begin{cases} 0, & \text{if } m \text{ is odd,} \\ 1, & \text{if } m \text{ is even.} \end{cases} \tag{4}$$

We now recall why the lines generate the space in (3). This will be achieved by establishing a $\mathbb{C}$-linear combination of lines which is a non-zero eigendivisor for the character $\alpha \in \mathfrak{D}_m$.

More specifically, let $\mathfrak{D}_m^j$ denote the subset of decomposable elements in $\mathfrak{D}_m$ such that $a_0 + a_j = 0$. Note that $\mathfrak{D}_m^j \cap \mathfrak{D}_m^k \neq \emptyset$ for all $1 \leqslant j, k \leqslant 3$ – a fact that will be crucial to our later analysis of an explicit basis of lines. Depending on j, we give an eigendivisor with character for each $\alpha \in \mathfrak{D}_m^j$:

$$\begin{aligned}
\alpha \in \mathfrak{D}_m^1\colon &\quad w_1(\alpha) = \sum_{\zeta,\eta} \zeta^{a_1} \eta^{a_3} \mathfrak{l}_1(\zeta, \eta), \\
\alpha \in \mathfrak{D}_m^2\colon &\quad w_2(\alpha) = \sum_{\zeta,\eta} \zeta^{a_2} \eta^{a_3} \mathfrak{l}_2(\zeta, \eta), \\
\alpha \in \mathfrak{D}_m^3\colon &\quad w_3(\alpha) = \sum_{\zeta,\eta} \zeta^{a_3} \eta^{a_2} \mathfrak{l}_3(\zeta, \eta),
\end{aligned}$$

where the sum is over all $\zeta, \eta \in \mu_m$. By construction, almost all of these eigendivisors are orthogonal:

$$w_i(\alpha).H = 0, \qquad w_i(\alpha).w_j(\beta) = 0 \quad \text{if } \alpha \neq -\beta \ (i, j = 1, 2, 3), \tag{5}$$

which is easily computed thanks to the following intersection behaviour:

$$\mathfrak{l}_i(\zeta, \eta).\mathfrak{l}_j\big(\zeta', \eta'\big) \neq 0 \quad \Leftrightarrow \quad \begin{cases} \zeta = \zeta' \text{ or } \eta = \eta', & i = j, \\ \zeta\eta' = \zeta'\eta, & (i, j) = (1, 2), \\ \zeta' = \omega^2 \eta\zeta\eta', & (i, j) = (1, 3), \\ \zeta\eta = \zeta'\eta', & (i, j) = (2, 3). \end{cases} \tag{6}$$

From the intersection number

$$w_j(\alpha).w_j(-\alpha) = -m^3 \tag{7}$$

it follows that $w_j(\alpha) \neq 0$. We conclude that $V(\alpha) \subset \mathrm{NS}(S) \otimes \mathbb{C}$ is contained in the span of the lines. Denote this span by L. Clearly, also H and thus V_0 can be expressed by lines (cf. (10), (11)), so we derive the inclusion $\subset$ of the following equality

$$V_0 \oplus \bigoplus_{\alpha \in \mathfrak{D}_m} V(\alpha) = L. \tag{8}$$

The other inclusion follows from the fact that every line can be expressed in terms of H and the $w_j(\alpha)$ for $\alpha \in \mathfrak{D}_m$ (cf. [17, (17)]). In particular, we have

$$\mathrm{rank}(L) = 1 + \#\mathfrak{D}_m.$$

Proof of Theorem 3.1. We have seen that the span of lines L has rank $1 + \#\mathfrak{D}_m$. On the other hand, $\rho(S) = 1 + \#\mathfrak{B}_m$. From [17, Theorem 6] we know that

$$\mathfrak{D}_m = \mathfrak{B}_m \quad \Longleftrightarrow \quad m \leqslant 4 \quad \text{or} \quad (m, 6) = 1. \tag{9}$$

This proves that the lines generate $\mathrm{NS}(S) \otimes \mathbb{C}$ exactly in the cases of Theorem 3.1. The corresponding statement for $\mathrm{NS}(S) \otimes \mathbb{Q}$ follows. □

We also note the following consequence of the above computations that is not conditional in terms of the degree m (since it does not require the equivalence (9)). For $m \leqslant 4$ or relatively prime to 6, the corollary specialises to the according statement for $\mathrm{NS}(S)$.

Corollary 3.2. *Let S be the complex Fermat surface of degree m. Then the lattice $\Lambda \subset \mathrm{NS}(S)$ generated by the lines on S has rank $1 + \#\mathfrak{D}_m$ and discriminant dividing m^r for $r = 3\#\mathfrak{D}_m + 1$.*

Proof. Consider the $\mathbb{Z}[\zeta_m]$-lattice $\Lambda \otimes \mathbb{Z}[\zeta_m]$. It contains the finite-index sublattice Λ' generated by H and the $w_j(\alpha)$ for $j = 1, 2, 3$ and $\alpha \in \mathfrak{D}_m^j$. The given generators of Λ' have intersection matrix Q' of determinant m^r for $r = 3\#\mathfrak{D}_m + 1$ by (5) and (7). The determinant of Q' equals the discriminant of Λ times a square in $\mathbb{Z}[\zeta_m]$ (the square of the determinant of the matrix in $M_\rho(\mathbb{Z}[\zeta_m]) \cap GL_\rho(\mathbb{Q}[\zeta_m])$ that expresses the given basis of Λ' in terms of a basis of Λ). Hence Λ has discriminant that divides m^r. □

4. Rational basis of lines

In this section, we will work out an explicit rational basis of the lattice L generated by the lines in $\mathrm{NS}(S)$ for the complex Fermat surface S of degree m. For this, we fix another notation for the lines. Since we are concerned with odd m, we can set $\omega = -1$. Then we fix a primitive m-th root of unity γ. We introduce the short-hand notation

$$\mathfrak{l}_j\left(\gamma^k, \gamma^l\right) = \mathfrak{l}_j(k, l).$$

Proposition 4.1 *(Rational basis for m coprime to 6). Assume that $(m, 6) = 1$ and that the ground field has characteristic zero. Then the following lines form a basis of $\mathrm{NS}(S) \otimes \mathbb{Q}$:*

$$\mathcal{B} = \left\{\mathfrak{l}_j(k, l);\ j = 1, 2, 3,\ 0 \leqslant k < m - 1,\ 0 < l < m - 1\right\} \cup \left\{\mathfrak{l}_1(m - 1, 1)\right\}.$$

Proof. We shall use relations between lines and the hyperplane class H. Clearly

$$H = \sum_{\zeta} \mathfrak{l}_i(\zeta, \eta) \tag{10}$$

$$= \sum_{\eta} \mathfrak{l}_j(\zeta, \eta) \tag{11}$$

for any fixed η resp. ζ and independent of the index. Taking the sum of the lines $\mathfrak{l}_1(\cdot, 1)$, we see that H is in the span of $\mathcal{B}$. In consequence, all $\mathfrak{l}_i(m-1, l)$ for $1 < l < m-1$ can be expressed by $\mathcal{B}$ as well. It remains to write the lines $\mathfrak{l}_i(\cdot, 0), \mathfrak{l}_j(\cdot, m-1)$ in terms of the previous lines.

A second set of relations is derived for all those $\alpha \in \mathfrak{D}_m^i \cap \mathfrak{D}_m^j$ for some $i \neq j$. Since $V(\alpha)$ is always one-dimensional, we have

$$V(\alpha) = \mathbb{C} w_i(\alpha) = \mathbb{C} w_j(\alpha),$$

so the two eigendivisors are multiples of each other. Recall that each eigendivisor $w_j(\alpha)$ intersects its complex conjugate $w_j(-\alpha)$ with intersection multiplicity $-m^3$.

Claim. *Let $i \neq j$ and $\alpha \in \mathfrak{D}_m^i \cap \mathfrak{D}_m^j$. Then*

$$w_i(\alpha) = -w_j(\alpha). \tag{12}$$

Recall the orthogonality for eigendivisors with character from (5). To see the claim, it thus suffices to compute the intersection number

$$w_i(\alpha).w_j(-\alpha) = m^3.$$

This is easily verified thanks to the intersection behaviour of the lines in (6).

The coefficients of the lines in the relations (12) involve m-th roots of unity. In order to derive relations over $\mathbb{Q}$, we shall now simplify the above relations by multiplying with fixed powers of a varying root $\varepsilon \in \mu_m$.

For any pair (i, j) with $i \neq j$, we define the map

$$\alpha_{i,j} : \mathbb{Z}/m\mathbb{Z} - \{0\} \to \mathfrak{D}_m^i \cap \mathfrak{D}_m^j$$
$$r \mapsto \alpha_{i,j}(r)$$

by setting $a_0 = r$. Then $a_i = a_j = -r$ and $a_k = r$ with $\{i, j, k\} = \{1, 2, 3\}$. For any $\varepsilon \in \mu_m$ and (i, j) with $i \neq j$, we then consider the relations of divisors obtained from (12)

$$\sum_{r \in \mathbb{Z}/mZ - \{0\}} \varepsilon^r w_i\big(\alpha_{i,j}(r)\big) = -\sum_{r \in \mathbb{Z}/mZ - \{0\}} \varepsilon^r w_j\big(\alpha_{i,j}(r)\big).$$

Both sums simplify greatly. For instance,

$$\begin{aligned}
\sum_{r \in \mathbb{Z}/mZ - \{0\}} \varepsilon^r w_1\big(\alpha_{1,2}(r)\big) &= \sum_{\zeta,\eta} \sum_{r} \left(\frac{\varepsilon\eta}{\zeta}\right)^r \mathfrak{l}_1(\zeta, \eta) \\
&= (m-1) \sum_{\zeta = \varepsilon\eta} \mathfrak{l}_1(\zeta, \eta) - \sum_{\zeta \neq \varepsilon\eta} \mathfrak{l}_1(\zeta, \eta) \\
&\overset{(10)}{=} m\left(\sum_{\zeta = \varepsilon\eta} \mathfrak{l}_1(\zeta, \eta) - H \right).
\end{aligned}$$

Analogous sums for the other indices result in the following $3m$ relations (depending on the choice of $\varepsilon \in \mu_m$):

$$\sum_{\zeta=\varepsilon\eta} \mathfrak{l}_1(\zeta,\eta) = -\sum_{\zeta=\varepsilon\eta} \mathfrak{l}_2(\zeta,\eta) \tag{13}$$

$$\sum_{\zeta\eta=\varepsilon} \mathfrak{l}_1(\zeta,\eta) = -\sum_{\zeta=\varepsilon\eta} \mathfrak{l}_3(\zeta,\eta) \tag{14}$$

$$\sum_{\zeta\eta=\varepsilon} \mathfrak{l}_2(\zeta,\eta) = -\sum_{\zeta\eta=\varepsilon} \mathfrak{l}_3(\zeta,\eta) \tag{15}$$

We are now ready to start the proof of Proposition 4.1. It states that the lines $\mathfrak{l}_j(\cdot,0), \mathfrak{l}_j(\cdot,m-1)$ are superfluous in the sense that the remaining lines already generate the span of *all* lines, including these superfluous ones. In other words, Proposition 4.1 claims that these superfluous lines can be expressed as linear combinations of the remaining lines in $\mathrm{NS}(S)\otimes\mathbb{Q}$. To prove this, we work with the $6m\times 6m$-matrix M whose entries are the coefficients of the superfluous lines in the relations (11) and (13)–(15).

The entries of the matrix M are ordered as follows:

columns	lines	$\mathfrak{l}_1(0,0),\dots,\mathfrak{l}_1(m-1,0),\mathfrak{l}_1(0,m-1),\dots,\mathfrak{l}_1(m-1,m-1),$ $\mathfrak{l}_2(0,0),\dots,\mathfrak{l}_3(m-1,m-1)$
rows	relations	(11) for $\eta=\gamma^l, l=0,\dots,m-1$ and $j=1,2,3$ (13)–(15) for $\varepsilon=\gamma^i, i=0,\dots,m-1$.

That is to say, the matrix M encodes the following system of relations on $\mathrm{NS}(S)$

$$M\cdot\mathfrak{l}=\boldsymbol{r} \tag{16}$$

where the vector $\mathfrak{l}$ has entries the superfluous lines (ordered as above) and the right-hand side vector $\boldsymbol{r}$ comprises the remaining terms of the chosen relation with the appropriate signs.

By the relations, all entries of M are either 0 or 1. It will be convenient to write M as a block matrix whose entries are 36 matrices of type $m\times m$. In fact, the blocks arising from relation (11) are just the identity Matrix I. For the other relations, we need two permutation matrices of order m which are transposes of each other:

$$D=\begin{pmatrix} 0 & 1 & 0 & \cdots & & 0\\ 0 & 0 & 1 & 0 & \cdots & 0\\ & & \cdots & & & \\ & & & \cdots & & \\ 0 & & \cdots & & 0 & 1\\ 1 & 0 & & \cdots & & 0 \end{pmatrix}, \qquad B=D^{\mathrm{t}}=D^{-1}.$$

Then M is given as follows:

$$M=\begin{pmatrix} I & I & 0 & 0 & 0 & 0\\ 0 & 0 & I & I & 0 & 0\\ 0 & 0 & 0 & 0 & I & I\\ I & B & I & B & 0 & 0\\ I & D & 0 & 0 & I & B\\ 0 & 0 & I & D & I & D \end{pmatrix}.$$

We claim that there is a solution to the system of relations (16) in $\mathrm{NS}(S)\otimes\mathbb{Q}$. If the matrix M were invertible, then this would follow immediately. However, M is not invertible, so we have to find a way to circumvent this problem.

Recall that we are looking for a solution in $\mathrm{NS}(S)\otimes\mathbb{Q}$. Hence we can still modify any relation in $\mathrm{NS}(S)$ by adding multiples of relations (10) for any index i and $\eta=1$ or $\eta=\gamma^{m-1}=\gamma^{-1}$. On the system of relations (16), this has the effect of adding a constant row to any of the six blocks associated to the invariants i and η of the chosen relation (10). We will refer to this as adding constant rows. Of course, this modification changes the vector $\boldsymbol{r}$ on the right-hand side of (16) by adding a multiple of H, but we will not need to consider this expression at all.

We will achieve a proof of Proposition 4.1 by making the matrix M invertible by adding constant rows. First we shall simplify the matrix. Note that elementary operations of linear algebra, if performed blockwise, are compatible with the modifications by adding constant rows. This simplifies the problem of invertibility greatly:

$$M=\begin{pmatrix} I & I & 0 & 0 & 0 & 0\\ 0 & 0 & I & I & 0 & 0\\ 0 & 0 & 0 & 0 & I & I\\ I & B & I & B & 0 & 0\\ I & D & 0 & 0 & I & B\\ 0 & 0 & I & D & I & D\end{pmatrix}\to\begin{pmatrix} I & I & 0 & 0 & 0 & 0\\ 0 & 0 & I & I & 0 & 0\\ 0 & 0 & 0 & 0 & I & I\\ 0 & B-I & 0 & B-I & 0 & 0\\ 0 & D-I & 0 & 0 & 0 & B-I\\ 0 & 0 & 0 & D-I & 0 & D-I\end{pmatrix}$$
$$\to\begin{pmatrix} B-I & B-I & 0\\ D-I & 0 & B-I\\ 0 & D-I & D-I\end{pmatrix}\to\begin{pmatrix} B-I & 0 & 0\\ D-I & 2I-B-D & B-I\\ 0 & 0 & D-I\end{pmatrix}.$$

To show that each of the superfluous lines can be expressed in terms of the other lines in $\mathrm{NS}(S)\otimes\mathbb{Q}$, it thus suffices to modify the following block matrices by adding constant rows such that they become invertible:

$$B-I,\qquad D-I,\qquad 2I-B-D.$$

Lemma 4.2. *Let $U(r)$ denote the $m\times m$ matrix with entries 1 in the r-th row and 0 elsewhere.*

(i) *The determinants of $B-I+U(r)$ and $D-I+U(r)$ equal $(-1)^{m-1}m$ for any $r=1,\dots,m$.*
(ii) *The determinant of $2I-B-D+U(2)$ equals m^2.*

Proof. (i) We calculate the determinants by computing all eigenvalues of the given matrices. We claim that the eigenvalues are exactly

$$\left\{\varepsilon-1;\ \varepsilon^m=1,\ \varepsilon\neq 1\right\}\cup\{1\}. \tag{17}$$

Then the determinant equals the product of the eigenvalues which can be written as

$$\prod_{\varepsilon\neq 1}(\varepsilon-1)=\prod_{\varepsilon\neq 1}(\varepsilon-t)|_{t=1}=(-1)^{m-1}\left[\frac{t^m-1}{t-1}\right]_{t=1}=(-1)^{m-1}m.$$

To prove the claim about the eigenvalues, we exhibit simultaneous eigenvectors for all matrices $D,B,I,U(r)$. This is easily accomplished by working with both multiplication from left and right.

For multiplication from the left, we have the common eigenvectors

$$\mathbf{v}_\varepsilon=\left(\varepsilon^i\right)_{0<i\leqslant m}\quad\forall\varepsilon\in\mu_m\setminus\{1\}.$$

These eigenvectors have eigenvalues $\varepsilon, \varepsilon^{-1}, 1, 0$, respectively. Hence we obtain all eigenvalues from (17) except for 1. The remaining eigenvalue is easily computed for multiplication from the right. Here we have the eigenvector

$$\mathbf{v}_1 = (1, \ldots, 1)$$

with eigenvalue 1 for each matrix $D, B, I, U(r)$. Thus the given matrices have the eigenvalue 1. This completes the proof of (i).

For (ii), note that

$$B \cdot U(1) = U(2) \quad \text{and} \quad U(1) \cdot D = U(1) \cdot U(1) = U(1).$$

Together with the equality $DB = I$, this implies that

$$\big(B - I + U(1)\big) \cdot \big(D - I + U(1)\big) = 2I - B - D + U(2).$$

By (i), this matrix has determinant m^2. □

By Lemma 4.2 the matrix M can be modified by adding constant rows to its blocks in such a way that it becomes invertible over $\mathbb{Q}$. Thus we can express all superfluous lines rationally in terms of the lines in $\mathcal{B}$. Since lines generate $\mathrm{NS}(S)$ rationally by Theorem 3.1 and $\#\mathcal{B} = \rho(S)$, this completes the proof of Proposition 4.1. □

Remark 4.3.

(i) The result of Proposition 4.1 stays valid in positive characteristic if the Picard number does not increase upon reduction (for instance for characteristics $p \equiv 1 \bmod m$).
(ii) The method of proof does not require that $(m, 6) = 1$, but only that m is odd. For arbitrary odd degree m, we deduce that the lines in $\mathcal{B}$ generate the span of all lines L rationally.
(iii) For even degrees m, the matrix M takes a different shape, as we cannot choose $\omega = -1$. Hence the relations for $\alpha \in \mathfrak{D}_m^1 \cap \mathfrak{D}_m^3$ change to

$$w_1(\alpha) = -\omega^{2a_0} w_3(\alpha).$$

Summing up as for odd m, we obtain

$$\sum_{\zeta\eta=\varepsilon} \mathfrak{l}_1(\zeta, \eta) = -\sum_{\omega^2\zeta=\varepsilon\eta} \mathfrak{l}_3(\zeta, \eta)$$

yielding a different relation matrix.

Corollary 4.4. *Let m be any odd integer. Let $\Lambda \subset \mathrm{NS}(S)$ be the lattice generated by all lines and Λ' the sublattice generated by those in $\mathcal{B}$ of Proposition 4.1. Then the index $[\Lambda : \Lambda']$ is only divisible by primes dividing m. In particular, Λ' has discriminant dividing some power of m.*

Proof. The second claim follows from the first in conjunction with Corollary 3.2. For the first claim, it suffices to deduce from Lemma 4.2 that the matrix M can be modified in such a way that it becomes invertible over $\mathbb{Z}[\frac{1}{m}]$. □

Remark 4.5. The modified matrices in Lemma 4.2 have determinant of absolute value m or m^2. There is no obvious way to make the matrix M invertible over $\mathbb{Z}$. Note, however, that we may still have $\Lambda' = \Lambda$ and even $\Lambda' = \mathrm{NS}(S)$, since the expression on the right-hand side of (16) might be divisible

in $\mathrm{NS}(S)$. In the cases of this paper with $(m,6)=1$, these equalities do indeed hold. This will be checked as part of the proof of Theorem 1.1.

For all odd degrees $m \leqslant 81$, we calculated the determinant of the intersection form of the lines in $\mathcal{B}$. In each case, the determinant turned out to be a perfect power of m, with exponent as conjectured in [18]:

$$\det\left(\mathfrak{l}.\mathfrak{l}'\right)_{\mathfrak{l},\mathfrak{l}'\in\mathcal{B}} = m^{3(m-3)^2}. \tag{18}$$

5. Supersingular reduction technique

Consider the reduction of the integral model (1) of a Fermat surface S modulo p. Denote the resulting surface by S_p. Then S_p is smooth for any $p \nmid m$. For any such p, reduction induces a specialisation embedding (see [4, X], and note that $\mathrm{NS}(S)$ and $\mathrm{NS}(S_p)$ are torsion-free)

$$\mathrm{NS}(S) \hookrightarrow \mathrm{NS}(S_p). \tag{19}$$

We call a surface X supersingular if its Picard number is maximal: $\rho(X) = b_2(X)$. For Fermat surfaces, we have the following result of Katsura and Shioda:

Theorem 5.1. *(See Katsura and Shioda [8].) The reduction S_p is supersingular if and only if there is some $r \in \mathbb{N}$ such that*

$$p^r \equiv -1 \mod m.$$

One advantage of working with supersingular surfaces is that we have good knowledge about the discriminant of their Néron–Severi groups. The following result is a generalisation of Artin's classification of supersingular K3 surfaces [2].

Theorem 5.2. *(See Ekedahl [6], Schütt and Schweizer [16].) Let X be a smooth projective surface over a finite field k of characteristic p. Assume that X is supersingular. Then*

$$\left|\mathrm{disc}\left(\mathrm{Num}(X)\right)\right| = p^{2\sigma} \quad (\sigma \in \mathbb{N}_0).$$

The proof in [16] uses exactly the same techniques as Artin's original paper, mainly the Artin–Tate conjecture. The proof in [6] is based on cohomological results by Illusie and even allows to compute the (Artin) invariant σ.

We now explain the method by which we will prove Theorem 1.1. For this we recall the second Betti number of S:

$$b = b_2(S) = m^3 - 4m^2 + 6m - 2.$$

We shall also use the Lefschetz number $\lambda(S) = b_2(S) - \rho(S)$.

Supersingular reduction technique. *Fix the degree m. Let p be a prime of supersingular reduction for S.*

(1) *Compute a basis of $\mathrm{NS}(S) \otimes \mathbb{Q}$ consisting of lines $\mathfrak{l}_j$.*
(2) *Let $N = \langle \mathfrak{l}_j;\ j = 1,\dots,\rho\rangle \subseteq \mathrm{NS}(S)$. Compute $\mathrm{disc}(N)$ in terms of the Gram matrix of the intersection numbers of the lines. Then $\mathrm{disc}(N) = \nu^2\,\mathrm{disc}(\mathrm{NS}(S))$ where ν denotes the index of N in $\mathrm{NS}(S)$.*
(3) *Complement the reductions of the lines $\mathfrak{l}_j (j = 1,\dots,\rho)$ by $\lambda(S)$ divisor classes d_k on the supersingular reduction S_p for a basis of $\mathrm{NS}(S_p) \otimes \mathbb{Q}$.*
(4) *Let $N_p = \langle \mathfrak{l}_j, d_k;\ j = 1,\dots,\rho;\ k = 1,\dots,b-\rho\rangle \subseteq \mathrm{NS}(S_p)$. Compute $\mathrm{disc}(N_p)$.*

If $(m, 6) = 1$, then we will work with the rational basis $\mathcal{B}$ from Proposition 4.1 in step 1. At the end of the previous section, we computed the discriminants of the lattice N generated by these lines for several m. Recall that this discriminant was always a power of m (and in general it is a divisor of some power of m by Corollary 4.4).

Criterion 5.3. *Assume that the discriminants N and N_p have squarefree greatest common divisor. Then $N = \mathrm{NS}(S)$ (i.e. $\nu = 1$).*

Proof. Let $D \in \mathrm{NS}(S)$. Consider the lattices

$$N' = \langle N, D\rangle, \qquad N'_p = \langle N_p, D\rangle.$$

Let $r = [N' : N]$, i.e. r is the minimal positive integer such that $rD \in N$, and we can write in N

$$rD = \sum a_i \mathfrak{l}_i \quad (a_i \in \mathbb{Z}). \tag{20}$$

We claim that this implies $r = [N'_p : N_p]$. Assume on the contrary that there is a positive integer $s < r$ with $sD \in N_p$. By assumption, we can write in N_p

$$sD = \sum b_i \mathfrak{l}_i + \sum c_k d_k \quad (b_i, c_k \in \mathbb{Z}). \tag{21}$$

Necessarily there is some index k with $d_k \neq 0$, for otherwise (21) would be a relation in N, thus contradicting the minimality of r. As not all d_k are zero, Eqs. (20) and (21) combine to a non-trivial relation between the basis elements $\mathfrak{l}_i, d_k$ of N_p. This is impossible, hence the index of N_p in N'_p is r as claimed.

We conclude that the lattices N', N'_p have discriminants

$$\mathrm{disc}\big(N'\big) = \mathrm{disc}(N)/r^2, \qquad \mathrm{disc}\big(N'_p\big) = \mathrm{disc}(N_p)/r^2.$$

As the discriminants are integers, r^2 divides the greatest common divisor of the discriminants of N and N_p. By assumption, $r = 1$ and hence $D \in N$. $\square$

In Sections 6.1–6.5, we will apply the supersingular reduction technique to the Fermat surfaces of degree $4, 5, 7, 11$ and 13. For a generalisation of Criterion 5.3, one should note that the above proof does not actually require that N_p has finite index in $\mathrm{NS}(S_p)$. Hence we can also apply the same technique to sublattices of positive corank in $\mathrm{NS}(S_p)$ (which is computationally preferable as we can work with lattices of substantially smaller rank). This approach will be extended in Section 7 before we apply it to the degrees $m \geqslant 17$ in order to complete the proof of Theorem 1.1.

5.1. Additional lines mod p. The supersingular reduction technique requires to complement the lines from characteristic zero by divisors which only appear after reduction modulo a supersingular prime p. In this section, we will show how one can exhibit such divisors. We concentrate on the case where the degree equals $q + 1$ for some prime power $q = p^r$. In general, this situation can be achieved by replacing the degree m by a suitable multiple mk. Then one can map down the divisors on the Fermat surface $\hat{S}_p$ of degree mk to S_p by the k-th power map

$$\begin{aligned} \hat{S}_p &\to S_p \\ x_i &\mapsto x_i^k. \end{aligned}$$

Throughout this section, we let p be a prime, $r \in \mathbb{N}$ and $q = p^r$. We fix the degree $m = q + 1$ of the Fermat surface S_p and perform our calculations over $\mathbb{F}_q$. In this situation, Tate and Thompson realised that the unitary group over $\mathbb{F}_{q^2}$ acts irreducibly on the primitive part of $H^2(S_p)$ (cf. [19]). This provided the first proof for the if-part in Theorem 5.1. In consequence, the images of any line on S_p under the action of the unitary group generate $\mathrm{NS}(S_p)$ rationally together with the hyperplane section.

In the sequel, we shall exhibit very specific lines for different choices of $m > 3$. In each case, we shall only give one line. Many further lines are obtained by applying the automorphisms of the surface to this line. For our purposes, it will suffice to consider the images under the abelian group μ_m^4/μ_m studied before.

5.2. General *m*. Let $\alpha \in \mathbb{F}_q^*$ with $\alpha^2 \neq -1$. Then consider the solutions $\beta \in \mathbb{F}_{q^2}$ of

$$\beta^2 = 1 + \alpha^2. \tag{22}$$

Since $m - 2 = q - 1$, we have $\alpha^{m-2} = 1$. As $\beta^2 \in \mathbb{F}_q^*$, we also have

$$\beta^{2(m-2)} = 1.$$

There are at least two $\alpha \in \mathbb{F}_q^*$ such that each solution β of (22) satisfies

$$\beta^{m-2} = -1.$$

For each such pair (α, β), we obtain the following line on S_p:

$$\mathfrak{l}_p = \left\{[\lambda, \alpha\lambda + \beta\mu, \beta\lambda + \alpha\mu, \mu];\ [\lambda, \mu] \in \mathbb{P}^1\right\}.$$

For many $m = q + 1$, we can find simpler lines on S_p. We consider two cases:

5.3. $m \equiv 2 \bmod 3$. If $m \equiv 2 \bmod 3$, i.e. $q \equiv 1 \bmod 3$, then let $\alpha \in \mathbb{F}_q$ be a primitive third root of unity: $\alpha^2 + \alpha + 1 = 0$. Then S_p contains the following line:

$$\mathfrak{l}_p = \left\{\left[\lambda, \alpha(\lambda + \alpha\mu), \alpha(\alpha\lambda - \mu), \mu\right];\ [\lambda, \mu] \in \mathbb{P}^1\right\}.$$

5.4. $p = 3$. Let $p = 3$. For any $q = p^r$ and $m = q + 1$, S_p contains the following line:

$$\mathfrak{l}_p = \left\{\left[\lambda, (\lambda + \mu), (\lambda - \mu), \mu\right];\ [\lambda, \mu] \in \mathbb{P}^1\right\}.$$

5.5. Notation. In the sequel, we shall always fix one line $\mathfrak{l}_p$ as above. Then we let the subgroup μ_m^4/μ_m of $\mathrm{Aut}(S)$ act on $\mathfrak{l}_p$. For convenience, we normalise the action of $\mu_m^4/\mu_m \cong \mu_m^3$ corresponding to the choice $\zeta_3 = 1$:

$$g = (\zeta, \eta, \xi) \in \mu_m^3 : [x_0, x_1, x_2, x_3] \mapsto [\zeta x_0, \eta x_1, \xi x_2, x_3].$$

As before, we denote the resulting m^3 lines by

$$\mathfrak{l}_p(\zeta, \eta, \xi) = g(\mathfrak{l}_p) \quad \text{or} \quad \mathfrak{l}_p(j, k, l) \quad \text{if } \zeta = \gamma^j,\ \eta = \gamma^k,\ \xi = \gamma^l.$$

To identify the latter lines, we shall always consider the reduction of the primitive root of unity $\gamma \in \mu_m$ that was used to enumerate the lines $\mathfrak{l}_j(k, l)$ on S in characteristic zero.

Remark 5.4. In the supersingular case, $V(\alpha) \subset H^2(S_p)$ is algebraic for any character $\alpha \in \mathfrak{A}_m$. Given a line $\mathfrak{l}_p$ as above, we can mimic the construction from Section 3 to produce an eigendivisor with character $\alpha = (a_0, a_1, a_2, a_3)$:

$$w_p(\alpha) = \sum_{\zeta,\eta,\xi} \zeta^{a_0} \eta^{a_1} \xi^{a_2} \mathfrak{l}_p(\zeta, \eta, \xi).$$

However, it is non-trivial to decide whether $w_p(\alpha)$ is non-zero in $\mathrm{NS}(S_p)$ (cf. Remark 6.5).

6. Fermat surfaces of low degree

In this section, we give a proof of Theorem 1.1 for degrees $m = 4, 5, 7, 11, 13$ that is based on the supersingular reduction technique. For $m = 4$, this result has been known since the mid 70's. We will review the historical development and give an alternative proof. For $m > 4$, the result is new.

6.1. The Fermat quartic revisited. In this section, we let $m = 4$. Thus S is a singular K3 surface (in the sense that $\rho(S) = 20$, the maximum possible over $\mathbb{C}$). It was shown by Pjateckiĭ-Šapiro and Šafarevič [15] that $\mathrm{NS}(S)$ has discriminant $d = -16$ or -64. The latter is the case if the Néron–Severi group is generated by lines. Depending on a claim by Demjanenko, Pjateckiĭ-Šapiro and Šafarevič deduced $d = -64$. However, Demjanenko's argument contained a mistake. A correction was given by Cassels in 1978 [5].

In the meantime, Mizukami had investigated the following family of K3 surfaces:

$$X_\lambda\colon \quad \left\{x^4 + y^4 + z^4 + w^4 = 2\lambda\left(x^2y^2 + z^2w^2\right)\right\} \subset \mathbb{P}^3.$$

The following result was part of his Master's thesis in 1975 [12]:

Proposition 6.1 *(Mizukami). Let X_λ as above. Then $\rho(X_\lambda) \geqslant 19$, and*

$$\operatorname{disc}\left(\mathrm{NS}(X_\lambda)\right) = \begin{cases} -64, & \text{if } \lambda = 0, \\ 128, & \text{if } \rho(X_\lambda) = 19. \end{cases}$$

For the Fermat quartic, this result implied $d = -64$. Thus it follows that lines generate $\mathrm{NS}(S)$ integrally (Proposition 6.2). An alternative proof can be based on another result about certain Kummer surfaces by Inose [7].

Here we present an alternative argument using the supersingular reduction technique from Section 5 at the prime $p = 3$. Note that by Theorem 5.1 a prime p is supersingular if and only if $p \equiv 3 \bmod 4$. Since m is even, the situation differs from the cases considered in Section 4. In particular, we cannot use $\omega = -1$; instead we need ω with $\omega^4 = -1$, so that we can use $\gamma = \omega^2$.

(1) A rational basis $\mathcal{B}'$ of $\mathrm{NS}(S)$ can be expressed in terms of $\mathcal{B}$ as in Proposition 4.1 by switching $l \mapsto l - 1$ and adding $\mathfrak{l}_2(0, m-2)$:

$$\mathcal{B}' = \left\{\mathfrak{l}_j(k, l);\ \mathfrak{l}_j(k, l+1) \in \mathcal{B}\right\} \cup \left\{\mathfrak{l}_2(0, m-2)\right\}.$$

(2) Let $N = \langle \mathfrak{l};\ \mathfrak{l} \in \mathcal{B}' \rangle$. Then $\operatorname{discr}(N) = -64$.

(3) On the supersingular reduction S_3, we have the additional line

$$\mathfrak{l}_3 = \left\{\left[\lambda, (\lambda + \mu), (\lambda - \mu), \mu\right];\ [\lambda, \mu] \in \mathbb{P}^1\right\}$$

from Section 5.4. Recall γ, the fixed square root of -1. Let

$$\mathfrak{l}_3' = \left\{\left[\lambda, \gamma(\lambda + \mu), (\lambda - \mu), \mu\right];\ [\lambda, \mu] \in \mathbb{P}^1\right\}.$$

Then we compute that the lines $\mathfrak{l} \in \mathcal{B}'$ together with $\mathfrak{l}_3, \mathfrak{l}'_3$ constitute a rational basis $\mathcal{B}_3$ of $\mathrm{NS}(S_3)$:

(4) Let $N_3 = \langle \mathfrak{l}; \mathfrak{l} \in \mathcal{B}_3 \rangle$. Then $\mathrm{discr}(N_3) = -9$.

By Criterion 5.3, we deduce that $N = \mathrm{NS}(S)$. In other words we have reproven the following result:

Proposition 6.2 *(Mizukami, Inose). The complex Fermat quartic surface has Néron–Severi group generated by lines. Its discriminant is* -64.

The next result was first pointed out to the second author by Mizukami in the 1970's (unpublished report). Mizukami's proof was based on the computation of the intersection matrix for a suitable collection of lines on S_3.

Lemma 6.3 *(Mizukami). The reduction S_3 of the Fermat quartic mod 3 has Néron–Severi group generated by lines over $\mathbb{F}_9$.*

Proof. Since S_3 is a supersingular K3 surface, the exponent σ from Theorem 5.2 is the Artin invariant of S_3. By Artin's stratification [2], $\sigma \in \{1, \ldots, 10\}$. Since the sublattice N_3 of $\mathrm{NS}(S_3)$ has discriminant -9, we deduce $N_3 = \mathrm{NS}(S_3)$. $\square$

6.2. Fermat quintic. In this section we shall prove Theorem 1.1 for the complex Fermat quintic surface S. Note that $\rho(S) = 37, b_2(S) = 53$. It follows from Theorem 5.1 that $p = 2$ is a supersingular prime. We now apply the supersingular reduction technique from Section 5.

(1) Take the rational basis $\mathcal{B}$ of $\mathrm{NS}(S)$ from Proposition 4.1.
(2) Then $N = \langle \mathfrak{l}; \mathfrak{l} \in \mathcal{B} \rangle$ has discriminant 5^{12}.

On the supersingular reduction S_2 mod 2, Section 5.3 gives 125 additional lines $\mathfrak{l}_2(j,k,l)$ (plus their conjugates with respect to $\alpha \mapsto \alpha^2$). Here we write the third root of unity α in terms of a primitive fifth root of unity γ as $\alpha = \gamma^3 + \gamma^2 + 1$.

We express the 125 lines relative to γ and α through one parameter $\nu = 1, \ldots, 125$ as $\mathfrak{l}_p(j,k,l) = \mathfrak{l}_p(\nu)$ where

$$\nu = \nu(j,k,l) = 25j + 5k + l + 1.$$

(3) Let $\mathcal{N} = \{32, 33, 34, 35, 36, 37, 38, 39, 44, 80, 81, 82, 83, 84, 93, 95\}$ and $\mathcal{B}_2 = \{\mathfrak{l}_p(\nu);\ \ \nu \in \mathcal{N}\}$. Then $\mathcal{B} \cup \mathcal{B}_2$ constitutes a rational basis of $\mathrm{NS}(S_2)$.
(4) Let $N_2 = \langle \mathfrak{l}; \mathfrak{l} \in \mathcal{B} \cup \mathcal{B}_2 \rangle$. Then $\mathrm{discr}(N_2) = 2^{16}$.

By Criterion 5.3, we deduce that $N = \mathrm{NS}(S)$ with discriminant 5^{12}. In other words we have proven Theorem 1.1 for the Fermat quintic surface.

By [6, p. 12], $\mathrm{NS}(S_p)$ has discriminant p^{16} for all primes $p \equiv 2, 3 \bmod 5$. Hence we deduce

Lemma 6.4. *The Néron–Severi group of the reduction of the Fermat quintic modulo 2 is generated by lines over $\mathbb{F}_{16}$.*

6.3. Fermat septic. The Fermat septic surface S has $\rho(S) = 91$, $b_2(S) = 187$. In characteristic zero, we have

(1) rational basis $\mathcal{B}$ of $\mathrm{NS}(S)$ from Proposition 4.1,
(2) lattice $N = \langle \mathfrak{l}; \mathfrak{l} \in \mathcal{B} \rangle$ of discriminant 7^{48}.

Since Section 5.1 only applies to $m = q + 1$ for some prime power q, the Fermat septic S does not admit any supersingular reduction with apparent additional lines. Instead we consider a suitable covering Fermat surface and push down the additional lines on a supersingular reduction.

Here we can work with the Fermat surface $\hat{S}$ of degree 14 and consider the reduction $\hat{S}_p \bmod p = 13$. In order to define a line mod p, we fix a primitive root $\gamma \in \mu_7$ as a zero of x^2+5x+1. Let $\mathfrak{l}_p$ denote the line from 5.2 for $\alpha = 2, \beta = 3\gamma + 1$. Denote the push-down to S by D_p. Then $D_p^2 = -8$ by the adjunction formula. The action of μ_7^4/μ_7 as in Section 5.5 gives divisors $D_p(j,k,l)$. We compute the following rational basis of $\mathrm{NS}(S_p)$:

$$\mathcal{B}_p = \left\{D_p(j,k,l);\ (j,k,l) \in I\right\}$$

where

$$I = I_1 \cup I_2,$$
$$I_1 = \left\{(j,k,l);\ 0 \leqslant j,k < m-1,\ 0 < l < m-1\right\},$$
$$I_2 = \left\{(j,0,0);\ 0 \leqslant j < m-1\right\} \cup \left\{(m-1, m-2, m-2)\right\}.$$

The discriminant of the intersection form of the divisors in $\mathcal{B}_p$ is $2^{38}7^2 13^{48}$.

In order to combine the above divisors with the original lines from characteristic zero, we number them as follows:

$$I_1 \ni (j,k,l) \mapsto \nu(j,k,l) = 1 + j + (m-1)k + (m-1)^2(l-1),$$
$$I_2 \ni (j,k,l) \mapsto \nu(j,k,l) = b_2(S) - (m-1) + j.$$

With this notation, we can refer to $D_p(\nu)$ for $1 \leqslant \nu \leqslant b_2(S)$. We then find a mixed basis using certain multiples of all ν in the range $1, \ldots, \lambda(S)$ modulo $b_2(S)$:

(3) Let $\mathcal{N} = \{[31\nu \bmod b_2(S)];\ 1 \leqslant \nu \leqslant \lambda(S)\}$ and $\mathcal{B}'_p = \{D_p(\nu);\ \nu \in \mathcal{N}\}$. Then $\mathcal{B} \cup \mathcal{B}'_p$ constitutes a rational basis of $\mathrm{NS}(S_p)$.
(4) Let $N_p = \langle C; C \in \mathcal{B} \cup \mathcal{B}'_p\rangle$. Then $\mathrm{discr}(N_p) = 13^{40}$.

By Criterion 5.3, we deduce that $N = \mathrm{NS}(S)$ with discriminant 7^{48}. Thus we have proven Theorem 1.1 for the Fermat septic surface.

By [6, p. 12], the geometric genus $p_g(S)$ equals the Artin invariant σ of S_p for all $p \equiv -1 \bmod m$ (m being the degree of the Fermat surface S). For $m = 7$ and $p = 13$, the latter condition is fulfilled, and $p_g(S) = 20$. Hence we deduce $N_p = \mathrm{NS}(S_p)$. In particular, it follows that $\mathrm{NS}(S_p)$ can be generated by divisors defined over $\mathbb{F}_{p^2}$.

Remark 6.5. The choice $\alpha = 1$ and $\beta = \sqrt{2}$ would yield another set of m^3 divisors on S. It is easily verified that the divisors from $\mathcal{B}_p$, even combined with the original lines from $\mathcal{B}$, only generate a sublattice of rank 133 inside $\mathrm{NS}(S_p)$. This indicates that non-trivial linear combinations as in Remark 5.4 might return zero for particular choices of α, β.

6.4. Fermat surface of degree 11. The Fermat surface S of degree $m = 11$ has $\rho(S) = 271$, $b_2(S) = 911$. In characteristic zero, we have

(1) rational basis $\mathcal{B}$ of $\mathrm{NS}(S)$ from Proposition 4.1,
(2) lattice $N = \langle \mathfrak{l}; \mathfrak{l} \in \mathcal{B}\rangle$ of discriminant 11^{192}.

Consider the supersingular reduction S_p mod $p=2$. In order to exhibit additional divisors on S_p, we consider the Fermat surface $\hat{S}$ of degree 33. The covering map $\hat{S} \to S$ has degree 27. By Section 5.1, the reduction $\hat{S}_p$ admits many additional lines. These will be pushed down to S_p.

The primitive roots $\gamma \in \mu_m$ are given as zeroes of the irreducible polynomial $(x^m-1)/(x-1)$. Fix such a $\gamma \in \mathbb{F}_{p^{10}}$. Let $\mathfrak{l}_p$ denote the line from 5.2 for

$$\alpha = \gamma^8+\gamma^7+\gamma^6+\gamma^5+\gamma^4+\gamma^3, \qquad \beta = \alpha+1.$$

Denote the push-down to S by D_p. By the adjunction formula, as mentioned in Section 2, we have $D_p^2=-23$. The action of μ_m^4/μ_m as in Section 5.5 gives divisors $D_p(j,k,l)$. We compute the same rational basis $\mathcal{B}_p=\mathcal{B}_p(m)$ of $\mathrm{NS}(S_p)$ as in Section 6.3. The lattice generated by the divisors in $\mathcal{B}_p$ has discriminant

$$2^{1200}3^2 11^2 23^{64} 43^{24} 67^8 131^{16} 197^4 307^8 331^8 463^{12} 593^8 3541^8.$$

With m and p replaced, we employ the same numbering of $D_p(\nu)$ for $1 \leqslant \nu \leqslant b_2(S)$ as in the previous section. As before we determine a mixed basis by using appropriate multiples of all ν in the range $1,\dots,\lambda(S)$ modulo $b_2(S)$:

(3) Let $\mathcal{N}=\{[253\nu \bmod b_2(S)];\ 1 \leqslant \nu \leqslant \lambda(S)\}$ and $\mathcal{B}'_p=\{D_p(\nu);\ \nu \in \mathcal{N}\}$. Then $\mathcal{B}\cup\mathcal{B}'_p$ constitutes a rational basis of $\mathrm{NS}(S_p)$.
(4) Let $N_p=\langle C; C \in \mathcal{B}\cup\mathcal{B}'_p\rangle$. Then N_p has discriminant

$$2^{1202}5^4 7^4 23^{48} 43^{16} 131^{16} 439^2.$$

By Criterion 5.3, we deduce that $N=\mathrm{NS}(S)$ with discriminant 11^{192}. This completes the proof of Theorem 1.1 for the Fermat surface of degree 11.

6.5. Fermat surface of degree 13. The Fermat surface S of degree $m=13$ has $\rho(S)=397$, $b_2(S)=1597$. In characteristic zero, we have

(1) rational basis $\mathcal{B}$ of $\mathrm{NS}(S)$ from Proposition 4.1,
(2) lattice $N=\langle \mathfrak{l}; \mathfrak{l} \in \mathcal{B}\rangle$ of discriminant 13^{300}.

Consider the supersingular reduction S_p mod $p=5$. In order to derive additional divisors on S_p, we consider the Fermat surface $\hat{S}$ of degree 26 which is a degree 8-covering of S. The reduction $\hat{S}_p$ admits many additional lines by Section 5.1.

Here, we fix a primitive root $\gamma \in \mu_m$ as a zero of $x^4+2x^3+x^2+2x+1$. Let $\mathfrak{l}_p$ denote the line from 5.2 for

$$\alpha = 2\gamma^3+2\gamma^2+\gamma, \qquad \beta = -\gamma^2-\gamma+3.$$

Denote the push-down to S by D_p. The action of μ_m^4/μ_m as in Section 5.5 gives divisors $D_p(j,k,l)$. We compute the same rational basis $\mathcal{B}_p=\mathcal{B}_p(m)$ of $\mathrm{NS}(S_p)$ as in Sections 6.3 and 6.4. The determinant of the intersection form of the divisors in $\mathcal{B}_p$ is

$$2^{26}3^{192}5^{912}13^2 53^{24} 79^{24} 103^{32} 181^8 233^8 313^8 677^{16} 883^4 2003^8 2729^8 3847^8.$$

Employ the same numbering of $D_p(\nu)$ for $1 \leqslant \nu \leqslant b_2(S)$. Again we find a mixed basis using appropriate multiples of all ν in the range $1,\dots,\lambda(S)$ modulo $b_2(S)$:

(3) Let $\mathcal{N}=\{[5\nu \bmod b_2(S)];\ 1 \leqslant \nu \leqslant \lambda(S)\}$ and $\mathcal{B}'_p=\{D_p(\nu);\ \nu \in \mathcal{N}\}$. Then $\mathcal{B}\cup\mathcal{B}'_p$ constitutes a rational basis of $\mathrm{NS}(S_p)$.

(4) Let $N_p = \langle C; C \in \mathcal{B} \cup \mathcal{B}'_p \rangle$. Then N_p has discriminant

$$2^4 3^{144} 5^{912} 53^{16} 103^{32} 677^{16} 1151^2 40627^2 42702482453593^2 247634616308749^2.$$

By Criterion 5.3, we deduce that $N = \mathrm{NS}(S)$ with discriminant 13^{300}. This completes the proof of Theorem 1.1 for the Fermat surface of degree 13.

7. Generalisations and extensions

For Fermat surfaces of degrees up to $m = 13$, we exhibited an explicit rational basis of $\mathrm{NS}(S_p)$ for some supersingular prime p, thus enabling us to apply the supersingular reduction technique. This approach has two advantages: first we can double-check the compatibility with the discriminant of $\mathrm{NS}(S_p)$ from Theorem 5.2; secondly we obtained additional information on generators of $\mathrm{NS}(S_p)$ in some cases.

For higher degrees, however, the matrices get too large for an explicit computation of the determinant. In this section we develop an extension of Criterion 5.3. This will allow us to treat much higher degrees and eventually give a full proof of Theorem 1.1. First we rephrase the old criterion in a more general setting.

Lemma 7.1. *Suppose*

$$\begin{tikzcd} M \arrow[r, "\varphi"] \arrow[d, "\psi"'] & L \arrow[d, "\chi"] \\ M' \arrow[r, "\varrho"'] & L' \end{tikzcd}$$

is a commutative diagram of homomorphisms of abelian groups with χ and ϱ injective. Suppose that $L/\varphi(M)$ is torsion-free and that $M'/\psi(M)$ is torsion. Then ϱ induces an injective homomorphism $M'/\psi(M) \to L'/\chi(L)$. If the group $L'/\chi(L)$ is finite, then the index $[M' : \psi(M)]$ divides the index $[L' : \chi(L)]$.

Proof. Set $\sigma = \varrho \circ \psi = \chi \circ \varphi$. As χ is injective, it induces an injection $\chi : L/\varphi(M) \to L'/\sigma(M)$. The quotient $(\chi(L) \cap \varrho(M'))/\sigma(M)$ is contained in $\chi(L/\varphi(M))$, which by injectivity of χ is torsion-free. The same quotient is also contained in $\varrho(M'/\psi(M))$, which is torsion. We conclude that the quotient is trivial, i.e., $\chi(L) \cap \varrho(M') = \sigma(M)$. The kernel of the map $M' \to L'/\chi(L)$ induced by ϱ is

$$\varrho^{-1}\big(\chi(L)\big) = \varrho^{-1}\big(\chi(L) \cap \varrho(M')\big) = \varrho^{-1}\big(\sigma(M)\big) = \psi(M),$$

where the last equality follows from the injectivity of ϱ. The first statement of the lemma follows. Assuming finiteness of $L'/\chi(L)$, the divisibility of indices follows immediately. □

Recall that we only consider integral non-degenerate lattices. The following proposition gives a method to show that a given lattice M equals an a priori unknown superlattice M' that contains M as a sublattice of finite index.

Proposition 7.2. *Suppose $\varrho : M' \to L'$ is an injective homomorphism of lattices. Let M be a finite-index sublattice of M' and L a sublattice of L' that contains $\varrho(M)$ primitively. If the greatest common divisor* $(\mathrm{disc}(M), \mathrm{disc}(L))$ *is squarefree, then M equals M'.*

Proof. Let L'' be the saturation of L in L', i.e., $L'' = L_{\mathbb{Q}} \cap L'$, where the intersection is taken inside $L'_{\mathbb{Q}}$. From $M_{\mathbb{Q}} = M'_{\mathbb{Q}}$ we find

$$\varrho(M') \subset \varrho(M'_{\mathbb{Q}}) = \varrho(M_{\mathbb{Q}}) \subset L_{\mathbb{Q}}$$

and conclude $\varrho(M') \subset L''$. After replacing L' by L'', we may assume that L has finite index in L'. By Lemma 7.1, with $\varphi = \varrho$ and ψ and χ being inclusions, we find that $[M' : M]$ divides $[L' : L]$. From $\operatorname{disc}(M) = [M' : M]^2 \operatorname{disc}(M')$ we conclude that $[M' : M]^2$ divides $\operatorname{disc}(M)$ and similarly $[L' : L]^2$ divides $\operatorname{disc}(L)$. Therefore $[M' : M]^2$ divides $(\operatorname{disc}(M), \operatorname{disc}(L))$. If $(\operatorname{disc}(M), \operatorname{disc}(L))$ is squarefree, then it follows that M equals M'. $\square$

Criterion 5.3 is exactly Proposition 7.2 applied to $M' = \mathrm{NS}(S)$ and $L' = \mathrm{NS}(S_p)$; the primitivity was ensured by complementing a basis of $M'_{\mathbb{Q}}$ to a basis of $L'_{\mathbb{Q}}$ (cf. the proof of Criterion 5.3). As mentioned at the end of Section 5, the sublattice in L' does not need to have finite index in L'. In practice, Proposition 7.2 will often be applied when we have $(\operatorname{disc}(M), \operatorname{disc}(L)) = 1$. Suppose $\varrho : M' \to L'$ is an injective homomorphism of lattices whose discriminants we do not know. Assume we have a finite-index sublattice M of M' with discriminant $\Delta = \operatorname{disc}(M)$ that we do know and we wish to show that M equals M'. By Proposition 7.2 it suffices to find a sublattice L of L' that contains $\varrho(M)$ primitively with $(\Delta, \operatorname{disc}(L)) = 1$ or more generally squarefree greatest common divisor.

7.1. Alternative approach. In the previous section, we suggested to use an intermediate lattice $\Lambda \subset L \subset \mathrm{NS}(S_p)$ for the supersingular reduction technique. While this does decrease the size of the matrices considered, we still had to compute their determinants which may be infeasible. Instead we shall pursue an alternative approach that decreases the size of the matrix drastically and has further computational advantages. Before an abstract treatment of the method, we sketch the general idea for the Fermat surfaces.

Consider the Fermat surface S of degree m with $(m, 6) = 1$. Let Λ denote the sublattice of $\mathrm{NS}(S)$ generated by the lines in $\mathcal{B}$ as in Proposition 4.1. Suppose that $\Lambda \neq \mathrm{NS}(S)$, so there is a prime ℓ and a divisor $D_0 \in \Lambda$ that is ℓ-divisible in $\mathrm{NS}(S)$, but not in Λ. Clearly this implies $\ell \mid (D_0.C)$ for any curve C on S – and on S_p for any prime p of good reduction.

Now let $\mathcal{C}$ denote any finite subset of $\operatorname{Div}(S)$ or $\operatorname{Div}(S_p)$. Then we build the matrix of intersection numbers

$$Q = (D.C)_{D \in \mathcal{B},\, C \in \mathcal{C}}.$$

This matrix has integer entries, so we can also consider it over $\mathbb{F}_\ell$.

Claim. *The rank of Q over $\mathbb{F}_\ell$ does not exceed $\#\mathcal{B} - 1 = \rho(S) - 1$.*

Proof. To see this, consider the map

$$\varphi : \Lambda_{\mathbb{F}_\ell} \to \operatorname{Hom}(\mathbb{F}_\ell^{\mathcal{C}}, \mathbb{F}_\ell)$$

that sends $D \in \Lambda_{\mathbb{F}_\ell}$ to the map that sends $C \in \mathcal{C}$ to $(C \cdot D \bmod \ell)$ (and is extended linearly to $\mathbb{F}_\ell^{\mathcal{C}}$). Then multiplication by $(Q \bmod \ell)$ from the right describes the linear map φ with respect to the basis $\mathcal{B}$ of $\Lambda_{\mathbb{F}_\ell}$ and the basis of $\operatorname{Hom}(\mathbb{F}_\ell^{\mathcal{C}}, \mathbb{F}_\ell)$ that is dual to $\mathcal{C}$. Since D_0 is not ℓ-divisible in Λ, its image in $\Lambda_{\mathbb{F}_\ell}$ is non-trivial. From $\varphi(D_0) = 0$ we conclude that φ is not injective, so Q does not have maximal rank over $\mathbb{F}_\ell$.

Alternatively, pick a basis containing the primitive closure D' of D in Λ. Since D' is still ℓ-divisible in $\mathrm{NS}(S)$, all entries in the row of Q corresponding to D' are zero mod ℓ. Hence the rank of Q over $\mathbb{F}_\ell$ cannot exceed $\#\mathcal{B} - 1$. $\square$

In order to show that $\Lambda = \mathrm{NS}(S)$, we find a suitable set $\mathcal{C}$ of divisors on S or any good reduction S_p such that the matrix Q has maximal rank $\rho(S)$ over $\mathbb{F}_\ell$. Since the index of Λ in $\mathrm{NS}(S)$ divides an m-power by Corollary 4.4, it suffices to carry out the above procedure for all prime divisors $\ell \mid m$. This approach has several computational advantages:

(1) We can work with a relatively small matrix Q of size $\rho(S) \times \#\mathcal{C}$.
(2) We can work with the matrix Q mod ℓ.
(3) The elements of $\mathcal{C}$ do not have to be independent in $\mathrm{NS}(S_p)$.
(4) We can add divisors to $\mathcal{C}$ successively until the kernel of multiplication by Q (from the right) on $\mathbb{F}_\ell^{\rho(S)}$ is zero.

We shall now give an abstract formulation of this approach. In 7.4, we will apply the method to Fermat surfaces of degrees up to $m = 97$ to complete the proof of Theorem 1.1.

7.2. Abstract formulation. Suppose for this paragraph that the conditions of Proposition 7.2 are met, so L is a lattice containing $\varrho(M)$ primitively. Let ℓ be a prime divisor of Δ, the discriminant of M. The quotient $L/\varrho(M)$ is free, and it follows that the induced map $M_{\mathbb{F}_\ell} \to L_{\mathbb{F}_\ell}$ is injective. Since ℓ does not divide $\mathrm{disc}(L)$, the pairing $L_{\mathbb{F}_\ell} \times L_{\mathbb{F}_\ell} \to \mathbb{F}_\ell$ is non-degenerate in the sense that the induced map $L_{\mathbb{F}_\ell} \to L^*_{\mathbb{F}_\ell}$ is injective. In particular, the restriction $M_{\mathbb{F}_\ell} \to L^*_{\mathbb{F}_\ell}$ is injective. We will see that this is in fact sufficient to conclude $M = M'$.

Proposition 7.3. *Let $\varrho : M \to L'$ be an injective homomorphism of lattices. Suppose that for every prime ℓ dividing* $\mathrm{disc}(M)$*, there is a sublattice $L(\ell)$ of L' containing $\varrho(M)$ such that the composition $M_{\mathbb{F}_\ell} \to L(\ell)^*_{\mathbb{F}_\ell}$ of the reduction $M_{\mathbb{F}_\ell} \to L(\ell)_{\mathbb{F}_\ell}$ of ϱ with the map $L(\ell)_{\mathbb{F}_\ell} \to L(\ell)^*_{\mathbb{F}_\ell}$ induced by the pairing on $L(\ell)$, is injective. Then $\varrho(M)$ is primitively contained in L'.*

Proof. Let M' denote the saturation $\varrho(M)_{\mathbb{Q}} \cap L'$ of $\varrho(M)$ in L', where the intersection is taken in $L'_{\mathbb{Q}}$. Then the inclusion $M' \to L'$ induces an isomorphism

$$M'/\varrho(M) \to \big(L'/\varrho(M)\big)_{\mathrm{torsion}}.$$

Let ℓ be a prime with $\ell \nmid \mathrm{disc}(M)$. From $[M' : \varrho(M)] \mid \mathrm{disc}(\varrho(M)) = \mathrm{disc}(M)$ we find

$$\ell \nmid \big[M' : \varrho(M)\big] = \#M'/\varrho(M) = \#\big(L'/\varrho(M)\big)_{\mathrm{torsion}},$$

so the quotient $L'/\varrho(M)$ has no non-trivial ℓ-torsion. Now let ℓ be a prime with $\ell \mid \mathrm{disc}(M)$ and consider the composition

$$M_{\mathbb{F}_\ell} \xrightarrow{\varrho_\ell} L(\ell)_{\mathbb{F}_\ell} \to L'_{\mathbb{F}_\ell} \to L'^*_{\mathbb{F}_\ell} \to L(\ell)^*_{\mathbb{F}_\ell}.$$

Here ϱ_ℓ is the reduction of ϱ mentioned in the proposition, the second map is the reduction of the inclusion $L(\ell) \subset L'$, the third is induced by the pairing on L', and the last is the dual of the second. Then the composition of the last three maps is induced by the pairing on $L(\ell)$, so the full composition is injective by assumption. This implies that the composition

$$\tau : M_{\mathbb{F}_\ell} \to L'_{\mathbb{F}_\ell}$$

of the first two maps is injective. Suppose $y \in L'/\varrho(M)$ satisfies $\ell y = 0$. Let $x \in L'$ be a lift of y, so that there is an $m \in M$ with $\varrho(m) = \ell x$. The reduction $\bar{m} \in M_{\mathbb{F}_\ell}$ satisfies $\tau(\bar{m}) = 0$, so by injectivity of τ, we obtain $\bar{m} = 0$, i.e. there is an $m' \in M$ with $\ell m' = m$. Then we have

$$\ell\varrho\big(m'\big) = \varrho(m) = \ell x, \quad \text{so } \ell\big(\varrho\big(m'\big) - x\big) = 0.$$

As L' is torsion-free, we conclude $\varrho(m') = x$ and thus $y = 0$. We deduce that again $L'/\varrho(M)$ has no non-trivial ℓ-torsion, and therefore that $L'/\varrho(M)$ is torsion-free, i.e., $\varrho(M)$ is contained primitively in L'. $\square$

Corollary 7.4. *Suppose $\varrho : M' \to L'$ is an injective homomorphism of lattices. Let M be a finite-index sublattice of M'. Suppose that for each prime ℓ dividing* $\operatorname{disc}(M)$*, there is a sublattice $L(\ell)$ of L' containing $\varrho(M)$ such that the induced map $M_{\mathbb{F}_\ell} \to L(\ell)^*_{\mathbb{F}_\ell}$ is injective. Then M equals M'.*

Proof. We have inclusions $\varrho(M) \subset \varrho(M') \subset L'$. By Proposition 7.3, the lattice $\varrho(M)$ is primitively contained in L', so also primitively in $\varrho(M')$. As $\varrho(M)$ has finite index in $\varrho(M')$, we find $\varrho(M) = \varrho(M')$ and thus $M = M'$ by injectivity of ϱ. $\square$

Corollary 7.4 is weaker than Proposition 7.2 in the sense that it implicitly assumes that the map $M_{\mathbb{F}_\ell} \to L^{\prime *}_{\mathbb{F}_\ell}$ is injective. For instance, Corollary 7.4 cannot be applied in the case $M = M' = L' = \langle e_\ell \rangle$, where $\langle e_\ell \rangle$ denotes a one-dimensional lattice whose generator e_ℓ has norm ℓ for some prime number ℓ; Proposition 7.2 does apply, as $\operatorname{disc}(M) = \ell$ is squarefree.

However, Corollary 7.4 has several advantages over Proposition 7.2, especially computationally. First of all, we only need to know the pairing between elements in a basis A for M and those in a set B of generators for $L = L(\ell)$, as opposed to the pairing among all elements of B, which saves a lot of work when the rank of L is much larger than that of M. Furthermore, we do not need to compute the discriminant of the larger lattice L. This also means that we do not even need to find a basis among the elements of B. Also, all computations can be done over $\mathbb{F}_\ell$ instead of $\mathbb{Z}$, which for finding (large) ranks makes quite a difference. Finally, Proposition 7.3 and Corollary 7.4 can easily be modified in such a way that it is possible to work with different lattices L' and embeddings $\varrho : M \to L'$ for each prime $\ell \mid \operatorname{disc}(M)$. In the framework of the supersingular reduction technique, one could then take different supersingular primes of the Fermat surface S for each prime divisor ℓ of the degree m.

7.3. Application to surfaces. Now suppose $\mathcal{X}$ is a nice surface over $\mathbb{Z}[1/N]$ (so smooth, projective, and every geometric fiber is integral) for some integer N and denote $X = \mathcal{X} \otimes \bar{\mathbb{Q}}$. Let $p \nmid N$ be a prime, so that p is a prime of good reduction of $\mathcal{X}$ and denote $X_p = \mathcal{X} \otimes \bar{\mathbb{F}}_p$. Then there is an injective homomorphism

$$\mathrm{NS}(X)/(p\text{-torsion}) \hookrightarrow \mathrm{NS}(X_p)/(p\text{-torsion})$$

of lattices (see [4, X]). We can therefore apply Proposition 7.2 or Corollary 7.4 with

$$M' = \mathrm{NS}(X)/\text{torsion} \cong \mathrm{Num}(X) \quad \text{and} \quad L' = \mathrm{NS}(X_p)/\text{torsion} \cong \mathrm{Num}(X_p),$$

while M is a finite-index sublattice of M'. This means, that if a priori we do not yet know the lattice $\mathrm{Num}(X)$, but we do know its rank $\rho = \operatorname{rk}\mathrm{Num}(X) = \operatorname{rk}\mathrm{NS}(X)$ and a sublattice $M \subset \mathrm{Num}(X)$ of rank ρ, then this gives a method to prove that $\mathrm{Num}(X)$ equals M; it suffices to find a lattice L as in Proposition 7.2 (as we have done in the previous sections) or lattices $L(\ell)$ as in Corollary 7.4. Note that L and $L(\ell)$ do not need to have the same rank as L'. If they do have the same rank, and thus finite index in $\mathrm{Num}(X_p)$, then this may also give extra information about $\mathrm{Num}(X_p)$, such as an upper bound for its discriminant.

7.4. Fermat surfaces. In order to complete the proof of Theorem 1.1, we continue to consider the Fermat surfaces $\mathcal{S} = \mathcal{S}_m \subset \mathbb{P}^3$ over $\mathbb{Z}[\frac{1}{m}]$ given by

$$x^m + y^m + z^m + w^m = 0$$

for any integer $m > 4$ with $\gcd(m, 6) = 1$. As in 7.3, we let $S = \mathcal{S} \otimes \bar{\mathbb{Q}}$ and $S_p = \mathcal{S} \otimes \bar{\mathbb{F}}_p$ for any prime $p \nmid m$. Sometimes we will also indicate the degree m as a subscript and write S_m and $(S_m)_p$, but

whenever the degree is clear, it will be omitted. Then as before, $\mathrm{NS}(S)$ and $\mathrm{NS}(S_p)$ are torsion-free for any prime $p \nmid m$ (see Section 2).

Table 1 contains for each m with $4 < m < 100$ and $\gcd(m, 6) = 1$ an integer r such that $q = rm - 1$ is a prime power, namely $q = p^n$ with p prime, a prime $\ell \mid m$, an irreducible polynomial of degree $2n$ over $\mathbb{F}_p$, and one or two pairs $(\alpha, \beta) \in \mathbb{F}_q \times \mathbb{F}_{q^2}$. A dash indicates the same as the entry above it.

Before elaborating on how the contents of Table 1 was computed, let us explain its meaning. Suppose $m, r, p^n = q = rm - 1$, ℓ, f, and the s pairs $(\alpha_1, \beta_1), \ldots, (\alpha_s, \beta_s)$ are the elements contained in one row of Table 1.

- Let γ denote a root of f in $\mathbb{F}_p[x]/(f) \cong \mathbb{F}_{q^2}$. By choice of f, γ is a primitive m-th root of unity.
- Let $M \subset \mathrm{NS}(S)$ denote the lattice generated by those lines on the Fermat surface S of degree m that are contained in the set $\mathcal{B}$ of Proposition 4.1, associated to a root of unity in $\bar{\mathbb{Q}}$ that reduces to γ. In Section 4 we have verified for $m \leqslant 81$ that M has discriminant $\mathrm{disc}(M) = m^{3(m-3)^2}$. For $m > 81$ the discriminant of M is a divisor of a power of m by Corollary 4.4.
- For each i with $1 \leqslant i \leqslant s$ we have $\alpha_i \in \mathbb{F}_q$, while $\alpha_i^2 + 1 = \beta_i^2$ and $\beta_i^q = -\beta_i$. In characteristic $p = 2$ this implies $\beta_i = \alpha_i + 1$, while in odd characteristic it means that $-\beta_i$ is the quadratic conjugate of β_i over $\mathbb{F}_q$. In all cases we have $\beta_i^{q-1} = -1$. As in Section 5.2, the line $\mathfrak{l}(\alpha_i, \beta_i)$ given by $y = \alpha_i x + \beta_i w$ and $z = \beta_i x + \alpha_i w$ is contained in $(S_{rm})_p$.
- Let $\phi : \mathcal{S}_{rm} \to \mathcal{S}_m$ be the morphism given by $[x : y : z : w] \mapsto [x^r : y^r : z^r : w^r]$ and set $D_i = \phi(\mathfrak{l}(\alpha_i, \beta_i)) \subset (S_m)_p$. Let $L \subset \mathrm{NS}(S_p)$ denote the lattice generated by the image of M and the elements $\sigma(D_i)$ for all $\sigma \in \mu_m^4/\mu_m$ and all i with $1 \leqslant i \leqslant s$.

Result 7.5. *In the above set-up, we have verified with the help of a machine that the induced map $M_{\mathbb{F}_\ell} \to L^*_{\mathbb{F}_\ell}$ is injective. We will comment in* 7.5 *on some aspects of the implementation.*

Note that there are two independent reductions involved: the lattice L is contained in the Néron–Severi group $\mathrm{NS}(S_p)$ of the reduction of S modulo p, while $L_{\mathbb{F}_\ell}$ is the base change of the lattice L over $\mathbb{Z}$ to $\mathbb{F}_\ell$ for a divisor ℓ of m.

Proof of Theorem 1.1. Let m be an integer with $0 < m < 100$. If $m > 4$ and $(m, 6) \neq 1$, then $\mathrm{NS}(S) \otimes \mathbb{Q}$ is not generated by lines by Theorem 3.1, so certainly $\mathrm{NS}(S)$ is not either. As seen before, for $m \leqslant 3$ the statement is classical, while for $m = 4$ we refer to Section 6.1. We now assume $4 < m < 100$ and $(m, 6) = 1$. For $5 \leqslant m \leqslant 13$ we could refer to Sections 6.2, 6.3, 6.4, and 6.5, but in any case we can refer to the big table. By Corollary 4.4, the discriminant of the lattice M, generated by the lines in $\mathcal{B}$ of Proposition 4.1, is divisible only by primes dividing m.

Now we fix the set-up of the table corresponding to the degree m. This involves the supersingular prime p for $\mathcal{S}$. Corollary 7.4, applied to $M' = \mathrm{NS}(S)$ and $L' = \mathrm{NS}(S_p)$, shows that M equals $\mathrm{NS}(S)$ thanks to Result 7.5. We conclude that the Néron–Severi lattice $\mathrm{NS}(S)$ is generated by the well-known $3m^2$ lines on S over the m-th cyclotomic field, and in fact by those in $\mathcal{B}$. $\square$

7.5. Remarks on the implementation. The polynomial f in the table was randomly chosen among the factors of the m-th cyclotomic polynomial over $\mathbb{F}_p$. The pairs (α_i, β_i) were chosen randomly among all pairs $(\alpha, \beta) \in \mathbb{F}_q \times \mathbb{F}_{q^2}$ satisfying $\alpha^2 + 1 = \beta^2$ and $\beta^{q-1} = -1$. First one pair would be chosen, giving a divisor D_1. It was then checked whether the induced map $M_{\mathbb{F}_\ell} \to (L_1)^*_{\mathbb{F}_\ell}$ is injective, where L_1 is generated by the image of M in $\mathrm{NS}(S_p)$ and the elements in the orbit of D_1 under μ_m^4/μ_m. In order to save memory, this was not done by writing the entire matrix of intersection numbers between elements of $\mathcal{B}$ on one hand and *all* elements of $\mathcal{B}$ and those in the orbit of D_1 on the other hand, as there are as many as m^3 elements in this orbit. Instead, the kernel of the map $M_{\mathbb{F}_\ell} \to (L_1)^*_{\mathbb{F}_\ell}$ was computed by intersecting the kernel of the map $M_{\mathbb{F}_\ell} \to M^*_{\mathbb{F}_\ell}$ with those of the maps $M_{\mathbb{F}_\ell} \to \langle \sigma(D_1) \colon \sigma \in C \rangle^*_{\mathbb{F}_\ell}$, where C runs through some subsets of μ_m^4/μ_m until either the intersection of all kernels was trivial or the union of all subsets C was μ_m^4/μ_4. In order to avoid accidental dependencies, the elements of C were chosen randomly.

Table 1

m	r	p^n	ℓ	f	(α, β)
5	1	2^2	5	$(x^5-1)/(x-1)$	$(\gamma^3+\gamma^2+1, \alpha+1)$
7	2	13	7	x^2+3x+1	$(11, 11\gamma+10)$
11	3	2^5	11	$(x^{11}-1)/(x-1)$	$(\gamma^9+\gamma^8+\gamma^3+\gamma^2+1, \alpha+1)$
13	2	5^2	13	$x^4+x^3-x^2+x+1$	$(-\gamma^3-\gamma^2+2\gamma+1, 3\gamma^3+\gamma^2+3\gamma-1)$
17	1	2^4	17	$x^8+x^5+x^4+x^3+1$	$(\gamma^7+\gamma^5+\gamma^4+1, \alpha+1)$
19	2	37	19	x^2+3x+1	$(13, 5\gamma+26)$
23	6	137	23	$x^2+11x+1$	$(67, 91\gamma+21)$
25	2	7^2	5	$x^4+2x^3+4x^2+2x+1$	$(\gamma^3+2\gamma^2+3\gamma, 5\gamma^3+\gamma^2-1)$
29	6	173	29	$x^2+18x+1$	$(137, 127\gamma+105)$
31	2	61	31	x^2+5x+1	$(-3, 11\gamma-3)$
35	4	139	5	x^2+4x+1	$(-15, 86\gamma+33)$
–	–	–	7	–	–
37	2	73	37	x^2+3x+1	$(31, 5\gamma+44)$
41	2	3^4	41	$x^8+x^6+x^5-x^4$ $+x^3+x^2+1$	$(\gamma^7+\gamma^6+2\gamma^4+\gamma^2+2, \gamma^7+2\gamma^6+2\gamma^3+\gamma+1)$
43	3	2^7	43	$x^{14}+x^{11}+x^{10}+x^9+x^8$ $+x^7+x^6+x^5+x^4+x^3+1$	$(\gamma^{12}+\gamma^{11}+\gamma^9+\gamma^8+\gamma^6+\gamma^5+$ $+\gamma^4+\gamma^3+\gamma^2, \alpha+1)$
47	6	281	47	$x^2+10x+1$	$(-18, 158\gamma+228)$
49	2	97	7	x^2+3x+1	$(-6, 7\gamma+59)$
53	4	211	53	x^2+4x+1	$(34, 33\gamma+66)$
55	2	109	5	x^2+6x+1	$(72, 12\gamma+36)$
–	–	–	11	–	$(53, 18\gamma+54), (73, 51\gamma+44)$
59	6	353	59	x^2+3x+1	$(-28, 236\gamma+1)$
61	2	11^2	61	$x^4+x^3+3x^2+x+1$	$(\gamma^3+\gamma^2+2\gamma+8, -\gamma^3+6\gamma^2+3\gamma+4)$
65	1	2^6	5	$x^{12}+x^8+x^7+x^6$ $+x^5+x^4+1$	$(\gamma^{11}+\gamma^9+\gamma^7+\gamma^6+\gamma^3+\gamma^2, \alpha+1)$, $(\gamma^9+\gamma^5+\gamma^4+\gamma^2+\gamma, \alpha+1)$
–	–	–	13	–	$(\gamma^{10}+\gamma^9+\gamma^7+\gamma^6+\gamma^5+\gamma+1, \alpha+1)$
67	6	401	67	$x^2+24x+1$	$(222, 229\gamma+342)$
71	4	283	71	x^2+4x+1	$(-39, 160\gamma+37)$
73	10	3^6	73	$x^{12}+x^{10}+x^7-x^6$ $+x^5+x^2+1$	$(-\gamma^{11}+\gamma^{10}-\gamma^8-\gamma^5+\gamma^4+\gamma^3+\gamma+1,$ $\gamma^{11}+\gamma^9+\gamma^8+\gamma^7+\gamma^6+\gamma^5+\gamma^4-\gamma^3+\gamma^2+\gamma)$
77	4	307	7	x^2+4x+1	$(29, 136\gamma-35), (-73, 61\gamma+122)$
–	–	–	11	–	$(197, -51\gamma+205), (91, -10\gamma-20)$
79	2	157	79	x^2+3x+1	$(-5, 127\gamma+112)$
83	4	331	83	x^2+4x+1	$(163, 19\gamma+38)$
85	2	13^2	5	$x^4+x^3+4x^2+x+1$	$(8\gamma^3+8\gamma^2-2\gamma-1, 7\gamma^3-\gamma^2+\gamma+4)$, $(6\gamma^3+6\gamma^2+5\gamma, 10\gamma^3-\gamma^2+1)$
–	–	–	17	–	–
89	16	1423	89	$x^2+14x+1$	$(536, 184\gamma+49)$
91	2	181	7	x^2+5x+1	$(145, 139\gamma+76), (80, 109\gamma+1)$
–	–	–	13	–	–
95	4	379	5	$x^2+59x+1$	$(35, 243\gamma+157), (200, \gamma+219)$
–	–	–	19	–	$(45, 89\gamma+162), (26, 8\gamma+236)$
97	2	193	97	x^2+3x+1	$(6, 50\gamma+75)$

If the computed kernel was not trivial, then a second pair (α_2, β_2) was chosen, yielding a divisor D_2. The lattice L_1 would then be augmented to L_2 by also including D_2 and the elements in its orbit. The kernel of the new map $M_{\mathbb{F}_\ell} \to (L_2)^*_{\mathbb{F}_\ell}$ would be computed by intersecting the previously computed kernel of $M_{\mathbb{F}_\ell} \to (L_1)^*_{\mathbb{F}_\ell}$ with the kernels of maps $M_{\mathbb{F}_\ell} \to \langle \sigma(D_2)\colon \sigma \in C\rangle^*_{\mathbb{F}_\ell}$ for some subsets C of μ_m^4/μ_m. In all cases this was enough to find a lattice L (namely $L = L_1$ or $L = L_2$) for which $M_{\mathbb{F}_\ell} \to L^*_{\mathbb{F}_\ell}$ is injective.

References

[1] N. Aoki, T. Shioda, Generators of the Néron–Severi group of a Fermat surface, in: Arithmetic and Geometry, vol. I, in: Progr. Math., vol. 35, 1983, pp. 1–12.
[2] M. Artin, Supersingular $K3$ surfaces, Ann. Sci. Éc. Norm. Super. (4) 7 (1974) 543–568.
[3] W. Barth, K. Hulek, C. Peters, A. van de Ven, Compact Complex Surfaces, second ed., Ergeb. Math. Grenzgeb. (3), vol. 4, Springer, Berlin, 2004.
[4] P. Berthelot, A. Grothendieck, L. Illusie (Eds.), Séminaire de Géométrie Algébrique du Bois–Marie 1966–1967 (SGA 6): Théorie des Intersections et Théorème de Riemann–Roch, Lecture Notes in Math., vol. 225, Springer, Berlin, 1971.
[5] J.W.S. Cassels, A Diophantine equation over a function field, J. Aust. Math. Soc. Ser. A 25 (4) (1978) 489–496.
[6] T. Ekedahl, Varieties of CM-type, preprint, arXiv:alg-geom/9512004v2, 1995.
[7] H. Inose, On certain Kummer surfaces which can be realized as non-singular quartic surfaces in P^3, J. Fac. Sci. Univ. Tokyo Sect. IA Math. 23 (3) (1976) 545–560.
[8] T. Katsura, T. Shioda, On Fermat varieties, Tohoku Math. J. (2) 31 (1) (1979) 97–115.
[9] N.M. Katz, On the intersection matrix of a hypersurface, Ann. Sci. Éc. Norm. Super. (4) 2 (1969) 583–598.
[10] R. Kloosterman, Elliptic K3 surfaces with geometric Mordell–Weil rank 15, Canad. Math. Bull. 50 (2) (2007) 215–226.
[11] J. Milne, On a conjecture of Artin and Tate, Ann. of Math. 102 (1975) 517–533.
[12] M. Mizukami, Birational mappings from quartic surfaces to Kummer surfaces, Master's thesis at University of Tokyo, 1975 (in Japanese).
[13] D. Mumford, Lectures on Curves on an Algebraic Surface, Princeton Univ. Press, 1966.
[14] A. Ogus, Griffiths transversality in crystalline cohomology, Ann. of Math. (2) 108 (2) (1978) 395–419.
[15] I.I. Pjateckiĭ-Šapiro, I.R. Šafarevič, Torelli's theorem for algebraic surfaces of type $K3$, Izv. Akad. Nauk SSSR Ser. Mat. 35 (1971) 530–572.
[16] M. Schütt, A. Schweizer, Davenport–Stothers inequalities and elliptic surfaces in positive characteristic, Q. J. Math. 59 (2008) 499–522.
[17] T. Shioda, On the Picard number of a Fermat surface, J. Fac. Sci. Univ. Tokyo Sect. IA Math. 28 (3) (1982) 725–734.
[18] T. Shioda, Some observations on Jacobi sums, in: Galois Representations and Arithmetic Algebraic Geometry, Kyoto 1985/Tokyo 1986, in: Adv. Stud. Pure Math., vol. 12, 1987, pp. 119–135.
[19] J.T. Tate, Algebraic cycles and poles of zeta functions, in: Arithmetical Algebraic Geometry, Proc. Conf. Purdue Univ., 1963, Harper & Row, 1965, pp. 93–110.
[20] R. van Luijk, K3 surfaces with Picard number one and infinitely many rational points, Algebra Number Theory 1 (1) (2007) 1–15.
[21] A. Weil, Numbers of solutions of equations in finite fields, Bull. Amer. Math. Soc. 55 (1949) 497–508.
[22] A. Weil, Jacobi sums as "Grössencharaktere", Trans. Amer. Math. Soc. 73 (1952) 487–495.