2-ADIC POINT COUNTING ON $K3$ SURFACES

ANDREAS-STEPHAN ELSENHANS AND JÖRG JAHNEL

Abstract. This article reports on an approach to point counting on algebraic varieties over finite fields that is based on a detailed investigation of the 2-adic orthogonal group. Combining the new approach with a p-adic method, we count the number of points on some $K3$ surfaces over the field $\mathbb{F}_p$, for all primes $p < 10^8$.

1. Introduction

Counting points on algebraic varieties over finite fields is an important problem in algorithmic arithmetic geometry. When the Betti numbers of a variety are known, one has strong estimates on the number of points using étale cohomology. For example, in the case of a $K3$ surface S that is projective over a finite field $\mathbb{F}_q$, the Lefschetz trace formula [SGA4½, Rapport, Théorème 3.2] reads

$$\#S(\mathbb{F}_q) = q^2 + \mathrm{Tr}(\mathrm{Frob}\colon H^2_{\text{ét}}(S_{\overline{\mathbb{F}}_q}, \mathbb{Z}_2(1)) \to H^2_{\text{ét}}(S_{\overline{\mathbb{F}}_q}, \mathbb{Z}_2(1)))q + 1\,. \tag{1}$$

Moreover, according to the Weil conjectures proven by P. Deligne [De74, Théorème 1.6], all eigenvalues of Frobenius are algebraic numbers of absolute value 1. As $K3$ surfaces have $\mathrm{rk}\, H^2_{\text{ét}}(S_{\overline{\mathbb{F}}_q}, \mathbb{Z}_2(1)) = 22$ and the hyperplane section causes one eigenvalue to be 1, the inequality

$$|\#S(\mathbb{F}_q) - (q^2 + q + 1)| \leq 21q \tag{2}$$

results, which is of exactly the same form as the one formulated by P. Deligne for hypersurfaces [De74, Théorème 8.1]. In particular, one sees that it is sufficient to determine $\#S(\mathbb{F}_q)$ modulo some auxiliary integer that is larger than $42q$.

Nowadays, the p-adic methods, as developed by K. Kedlaya, D. Harvey, and others, are frequently used for point counting, cf. [Ke, Ha, HS, EJ16]. They determine the number $\#S(\mathbb{F}_q)$, for q a power of the prime number p, by actually computing $(\#S(\mathbb{F}_q) \bmod p^j)$, for a suitable value of the exponent j.

In this note, we are interested only in the number $\#S(\mathbb{F}_p)$ of points over the prime field $\mathbb{F}_p$. Then the estimate (2) shows that, in most cases, $(\#S(\mathbb{F}_p) \bmod p^2)$ carries enough information. However, for most of the primes, even the modulus p^2 is by far larger than necessary. Moreover, the p-adic methods are faster, at least by a factor of 10, when working only modulo p and not modulo p^2, cf. Remark 5.9. It is thus

Date: June 28, 2022.

2010 *Mathematics Subject Classification.* Primary 14J28; Secondary 20G25, 14F20, 11G25.

Key words and phrases. $K3$ surface, point counting, 2-adic orthogonal group, 2-adic overdetermination.

worth trying to use a p-adic method just for counting modulo p and to combine the result with the point count modulo some other small integer, which has to be obtained in a different way.

l-adic point counting in general – Explicitisation of étale cohomology. Let l be a prime that is not the characteristic of the base field. Then, the essence of an l-adic point counting algorithm is to make the l-adic cohomology $\mathbb{Z}_l$-module $H^i_{\text{ét}}(S_{\overline{\mathbb{F}}_p}, \mathbb{Z}_l)$ explicit, including the action of Frob, for the varieties of type considered.

A famous example is R. Schoof's algorithm [Sch] for elliptic curves and its generalisation to abelian varieties [Pi]. Here, the l-adic cohomology may be explicitly described using torsion points. Another well-known example works for del Pezzo surfaces. Here, formula (1) holds, as well. Moreover, one has $\mathrm{T}(S_{\overline{\mathbb{F}}_p}, \mathbb{Z}_l) = 0$. In other words, $H^2_{\text{ét}}(S_{\overline{\mathbb{F}}_p}, \mathbb{Z}_l(1))$ and the action of Frob upon it can be made explicit in terms of the geometric Picard group, cf. formula (7). This essentially breaks down to the computation of the exceptional curves, cf. [EJ20b, §2.5].

A 2-adic point counting method for $K3$ surfaces. Following these ideas, the algorithm we describe below relies on an explicitisation of $\mathrm{T}(S_{\overline{\mathbb{F}}_p}, \mathbb{Z}_2)/4\,\mathrm{T}(S_{\overline{\mathbb{F}}_p}, \mathbb{Z}_2)$ for a particular family of $K3$ surfaces. This turns out to suffice for point counting modulo 16.

We assume that we are given a $K3$ surface that is presented as a double cover of $\mathbf{P}^2_{\mathbb{F}_p}$, branched over six $\mathbb{F}_p$-rational lines. This assumption is certainly more restrictive than necessary, but coincides with the generality, for which the algorithm is currently implemented. It coincides, too, with the generality, in which we describe the algorithm in Section 5. We indicate in Section 6 how to treat a slightly more general case and discuss the possibility of further generalisations in Section 7.

The very first step is to choose a lift to a flat $\mathbb{Z}$-scheme S containing the given surface as the special fibre $S_{\mathbb{F}_p}$. Such a lift exists for any $K3$ surface, at least as long as $p \geq 5$, as follows from [Og, Corollary 2.3], together with [Ch, Theorem 1], cf. [De81, Remarque 1.9]. In our situation, one simply needs to lift the coefficients of the linear forms defining the lines from $\mathbb{F}_p$ to $\mathbb{Z}$. One then finds a double cover S of $\mathbf{P}^2_{\mathbb{Z}}$, branched over the union of six lines, each of which is defined over $\operatorname{Spec}\mathbb{Z}$. Then, for every good prime $l \neq 2$ of S, in particular for $l = p$, one has an isomorphism of $\mathbb{Z}_2$-modules

$$H^2_{\text{ét}}(S_{\overline{\mathbb{F}}_l}, \mathbb{Z}_2(1)) \cong H^2_{\text{ét}}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2(1))\,,$$

the action of Frob on the left agreeing with that of Frob_l on the right [SGA4, Exposé XVI, Corollaire 2.3].

The assumptions and preparations made up to here have two consequences, as explained in i) and ii), below.

i) One has that $\operatorname{rk}\operatorname{Pic}(S_{\overline{\mathbb{Q}}}) \geq 16$. In fact, a sublattice of $\operatorname{Pic}(S_{\overline{\mathbb{Q}}})$ of rank 16 is explicitly known, which is a trivial $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module. Thus, there is an improvement over (2) implying that it is sufficient to count $(\#S(\mathbb{F}_p) \bmod 16p)$, cf. Paragraph 2.5. Assuming that $(\#S(\mathbb{F}_p) \bmod p)$ is known, only the information about $(\#S(\mathbb{F}_p) \bmod 16)$ is missing.

We assume that $\operatorname{Pic}(S_{\overline{\mathbb{Q}}})$ is a trivial $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module in the case $\operatorname{rk}\operatorname{Pic}(S_{\overline{\mathbb{Q}}}) > 16$, as well. Then in order to count $(\#S(\mathbb{F}_p) \bmod 16)$, it suffices to determine

$$(\operatorname{Tr}(\operatorname{Frob}_p\colon \operatorname{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2) \to \operatorname{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)) \bmod 16)\,,$$

for $\operatorname{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2) \subset H^2_{\text{ét}}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2(1))$ the transcendental lattice. Cf. Definition 3.1 and formula (8).

ii) The $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module $\operatorname{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)/2\operatorname{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)$ is trivial. Indeed, one has a canonical $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-equivariant isomorphism $\operatorname{Br}(S_{\overline{\mathbb{Q}}})_2 \cong \operatorname{Hom}(\operatorname{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2), \mathbb{Z}/2\mathbb{Z})$, cf. Theorem 3.5. Moreover, the 2-torsion of the geometric Brauer group is well understood for double covers, thanks to the work of A. N. Skorobogatov [Sk, Theorem 1.1].

Here, an important observation comes into play. The action of $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $\operatorname{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)$ takes place via maps being orthogonal with respect to the cup product pairing (Cf. Section 3). And for the orthogonal group, a remarkable phenomenon of 2-adic overdetermination occurs. We discuss this in detail in Section 4, which is, from the technical point of view, the main part of this article. In fact, the following is true.

Theorem. *Let $n \in \mathbb{N}$. With respect to a non-degenerate, symmetric bilinear form on $\mathbb{Q}_2^n$, let $U_1, U_2 \in \operatorname{M}_{n\times n}(\mathbb{Z}_2)$ be orthogonal matrices such that $U_1 \equiv U_2 \pmod 4$. If $U_1 \equiv E_n \pmod 2$ then $\operatorname{Tr}(U_1) \equiv \operatorname{Tr}(U_2) \pmod{16}$.*

In particular, for an orthogonal endomorphism a of $\operatorname{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)$ such that $a \equiv \mathrm{id} \pmod 2$, the reduction $(a \bmod 4) \in \operatorname{End}(\operatorname{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)/4\operatorname{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2))$ completely determines $(\operatorname{Tr}(a\colon \operatorname{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2) \to \operatorname{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)) \bmod 16)$.

Moreover, $\{A \in \operatorname{GL}_n(\mathbb{Z}/4\mathbb{Z}) \mid A \equiv E_n \,(\mathrm{mod}\ 2)\}$ is an elementary abelian 2-group. Therefore, the splitting field K of the $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action on $\operatorname{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)/4\operatorname{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)$ is an abelian extension of $\mathbb{Q}$ of exponent 2. Furthermore, K is unramified at every good prime $l \neq 2$ of S, so that one has $K \subseteq \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{d} \mid d \text{ bad prime of } S)$. Thus, in order to determine $(\operatorname{Tr}(\operatorname{Frob}_p\colon \operatorname{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2) \to \operatorname{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)) \bmod 16)$, it suffices

i) to look for a small good prime l such that the action of Frob_l agrees with that of Frob_p on $K = \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{d} \mid d \text{ bad prime of } S)$ and

ii) to count $\#S(\mathbb{F}_l)$ by another method, either naive or p-adic, and to deduce $\operatorname{Tr}(\operatorname{Frob}\colon \operatorname{T}(S_{\overline{\mathbb{F}}_l}, \mathbb{Z}_2) \to \operatorname{T}(S_{\overline{\mathbb{F}}_l}, \mathbb{Z}_2))$ from that value.

A situation, where this approach is particularly efficient, is when a $\mathbb{Z}$-scheme S is given, the points on many special fibres $S_{\mathbb{F}_p}$ of which are to be counted.

Practical experiments. We applied the 2-adic method, as described in combination with a p-adic method, to count the $\mathbb{F}_p$-rational points on some $K3$ surfaces, for all primes p up to 10^8. All computations were done using `magma` [BCP].

Checks for correctness of the implementation. For each of the surfaces, we compared the output with the result of a completely naive algorithm, for all primes $p < 1000$, and with that of a p-adic method, counting modulo p^2, for all primes $p < 100\,000$.

There is a further check as follows. The estimate (4) allows for $\#S(\mathbb{F}_p)$ an interval of length $12p$. Thus, knowing $(\#S(\mathbb{F}_p) \bmod p)$, there are only twelve (or perhaps 13) options for $\#S(\mathbb{F}_p)$, which means that not all residues modulo 16 are permissible. At least a "random" bug would certainly produce such residue classes from time to time.

Code. On the web pages of either author, related to the project described in this article, the following code is publicly available.

i) Naive point counting, as used for initialisation and checks.

ii) A Harvey style p-adic point counting method in p-adic precision 1 with remainder tree, for surfaces of the shape $w^2 = xyzf_3$. It runs through all prime numbers $p \leq 10^6$ in a few minutes.

iii) The initialisation following the more efficient approach, as described in Algorithm 5.1.A') and A").

iv) Point counting modulo $16p$, as described in Algorithm 5.1.B).

Terminology and Notation. i) For $\mathscr{O}$ a commutative ring with 1 and $n \in \mathbb{N}$, we write $\mathrm{GL}_n(\mathscr{O}) := \{A \in \mathrm{M}_{n\times n}(\mathscr{O}) \mid \det A \text{ is a unit in } \mathscr{O}\}$.

We let E_n be the $n \times n$ identity matrix. For any matrix A, we denote by $A^\top$ the transpose in the usual sense. Note that $A^\top$ is usually *not* the adjoint matrix in situations when the latter is defined.

When $\varphi\colon \Gamma \to \Gamma'$ is an $\mathscr{O}$-linear map between free $\mathscr{O}$-modules of finite rank with bases $\mathscr{B}$ and $\mathscr{B}'$, respectively, then we denote by $\mathrm{M}_{\mathscr{B}}^{\mathscr{B}'}(\varphi)$ the matrix of φ with respect to $\mathscr{B}$ and $\mathscr{B}'$.

ii) By an *$\mathscr{O}$-lattice,* we mean a free $\mathscr{O}$-module Γ of finite rank equipped with a non-degenerate, symmetric $\mathscr{O}$-bilinear form $b\colon \Gamma \times \Gamma \to \mathscr{O}$. When there seems to be no danger of confusion, we simply write Γ instead of (Γ, b).

An $\mathscr{O}$-lattice (Γ, b) is called *regular* if b provides an isomorphism $\Gamma \to \mathrm{Hom}_{\mathscr{O}}(\Gamma, \mathscr{O})$.

iii) An $\mathscr{O}$-linear map between $\mathscr{O}$-lattices $\varphi\colon (\Gamma, b) \to (\Gamma', b')$ is called *orthogonal* if $b'(\varphi(x), \varphi(y)) = b(x, y)$ holds for all $x, y \in \Gamma$. And similarly for $m \times n$-matrices if $\Gamma = \mathscr{O}^n$ and $\Gamma' = \mathscr{O}^m$.

iv) We let $\mathbb{P}$ denote the set of all prime numbers.

v) For $a \in \mathbb{Q}_2$, we let $\nu_2(a) \in \mathbb{Z} \cup \{\infty\}$ be the 2-*adic exponential valuation* of a. I.e. the exponent of 2 in the unique factorisation $a = u2^{\nu_2(a)}$, for $u \in \mathbb{Z}_2$ a unit.

Putting $\nu_2(A) := \min\{\nu_2(a_{ij}) \mid i = 1, \dots, m,\ j = 1, \dots, n\}$, we extend the 2-adic valuation from $\mathbb{Q}_2$ to matrices $A = (a_{ij}) \in \mathrm{M}_{m\times n}(\mathbb{Q}_2)$.

vi) A generic line on the projective plane $\mathbf{P}^2$ is denoted by l.

2. The surfaces studied

2.1. Let k be a field of characteristic $\neq 2$ and $l_1, \ldots, l_6 \in \Gamma(\mathbf{P}^2_{\overline{k}}, \mathscr{O}(1))$ six linear forms, such that the vanishing loci of any three of them do not have a geometric point in common. Suppose that $\{l_1, \ldots, l_6\}$ is a $\mathrm{Gal}(\overline{k}/k)$-invariant set. Then the double cover S' of $\mathbf{P}^2_k$, given by

$$W^2 = l_1 \cdots l_6\,, \tag{3}$$

geometrically has 15 isolated singularities, which are ordinary double points. The minimal resolution of singularities is a surface S of type $K3$. This is, in fact, one of the most classical families of $K3$ surfaces, cf. [GH, Chapter 6, Section 2].

Examples 2.2. We actually work over $\mathbb{Z}$ and consider the double covers of $\mathbf{P}^2_{\mathbb{Z}}$, given by the equations below,

i) $S'_1\colon W^2 = T_1T_2T_3(T_1 + T_2 + T_3)(3T_1 + 5T_2 + 7T_3)(-5T_1 + 11T_2 - 2T_3)$,

ii) $S'_2\colon W^2 = T_1T_2T_3(2T_1 + 4T_2 - 3T_3)(T_1 - 5T_2 - 3T_3)(T_1 + 3T_2 + 3T_3)$,

iii) $S'_3\colon W^2 = T_1T_2T_3(4T_1 + 9T_2 + T_3)(-T_1 - T_2 - 4T_3)(16T_1 + 25T_2 + T_3)$,

iv) $S'_4\colon W^2 = T_1T_2T_3(T_1 + T_2 + T_3)(T_1 + 2T_2 + 3T_3)(5T_1 + 8T_2 + 20T_3)$.

v) $S'_5\colon W^2 = T_1T_2(T_1^4 - 7T_1^3T_2 - T_1^3T_3 + 19T_1^2T_2^2 + 4T_1^2T_2T_3 + T_1^2T_3^2 - 23T_1T_2^3 - 7T_1T_2^2T_3 - 6T_1T_2T_3^2 - T_1T_3^3 + 11T_2^4 + 7T_2^3T_3 + 9T_2^2T_3^2 + 3T_2T_3^3 + T_3^4)$.

Note that, in the equation for S'_5, the homogeneous degree four factor on the right hand side completely splits over the integer ring of the fifth cyclotomic field $\mathbb{Q}(\zeta_5)$, the irreducible factors being $(T_1 - (\zeta_5 + 2)T_2 + \zeta_5^2T_3)$ and its conjugates.

In each case, we let S_i be the blowing-up of S'_i in the Zariski closure, equipped with the induced reduced scheme structure, of the singular locus of the generic fibre $S'_{i,\mathbb{Q}}$. In particular, $S_{i,\mathbb{Q}}$ is the minimal resolution of singularities of $S'_{i,\mathbb{Q}}$.

Remark 2.3. The surfaces above were investigated in detail in a project concerning the Frobenius trace distributions and the Sato–Tate conjecture for $K3$ surfaces. The efficient point counting algorithm described here was used in order to speed up the computations that led to the histograms presented there [EJ21].

Remarks 2.4. Let us recall from [EJ21, Section 5] the main properties of the surfaces S_i, for $i = 1, \ldots, 5$.

a) (Geometric Picard ranks) In each case, the pull back of a general line on $\mathbf{P}^2_{\overline{\mathbb{Q}}}$, together with the exceptional curves resulting from the resolution of singularities, generates a rank-16 sublattice in the geometric Picard group. The geometric Picard rank of each of the surfaces $S_{1,\mathbb{Q}}$, $S_{2,\mathbb{Q}}$, and $S_{4,\mathbb{Q}}$ is indeed equal to 16, while the surface $S_{3,\mathbb{Q}}$ is of geometric Picard rank 17.

b) (Bad primes) Aside from the prime 2, these are exactly the primes p such that, modulo p, some combination of three of the branch lines has at least one point in common. Thus, the bad primes could be determined by factoring the determinants $\det(l_i\ l_{i'}\ l_{i''})$, for $\{i, i', i''\} \subset \{1, \ldots, 6\}$ any subset of size three. The computation results in the sets $\{2, 3, 5, 7, 11, 13, 29\}$, $\{2, 3, 5, 7\}$, $\{2, 3, 5, 7, 11\}$, $\{2, 3, 5\}$, and $\{2, 5\}$ of bad primes, for S_1, S_2, S_3, S_4 and S_5, respectively.

c) (Special properties) The surface S_1 is a generic surface with a branch locus of six lines, while S_2 has a trivial jump character [CEJ]. The surface S_3 has trivial jump character, too, but higher Picard rank. Finally, the surface $S_4(\mathbb{C})$ has complex multiplication by $\mathbb{Q}(\sqrt{-1})$ and $S_5(\mathbb{C})$ is known to have real multiplication by $\mathbb{Q}(\sqrt{5})$.

2.5 (An improvement of Deligne's general bound)**.** As the $K3$ surfaces S_i, for $i = 1, 2, 3, 4$, are of geometric Picard rank ≥ 16 and $\mathrm{Pic}(S_{i,\overline{\mathbb{Q}}})$ is a trivial $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module, the action of Frob on $H^2_{\text{ét}}(S_{\overline{\mathbb{F}}_q}, \mathbb{Z}_2(1))$ is bound to have the eigenvalue 1 at least of multiplicity 16. Formula (1) therefore actually yields the sharper estimate

$$|\#S_i(\mathbb{F}_p) - (p^2 + 16p + 1)| \leq 6p\,. \tag{4}$$

Thus, in each of these cases, it suffices to determine $(\#S_i(\mathbb{F}_p) \bmod 16p)$.

2.6. We explain the 2-adic method in Sections 3, 4, and 5 below, for $K3$ surfaces of type (3), of the kind that the linear forms $l_1, \ldots, l_6$ are defined over $\mathbb{Z}$. This covers Examples 2.2.i), ii), iii), and iv), but not v), which is more advanced. We report on the modifications necessary in order to deal with S_5 in Section 6.

3. Étale cohomology and the Brauer group

General $K3$ surfaces. Let S be a $K3$ surface over a field k. Then $H^2_{\text{ét}}(S_{\overline{k}}, \mathbb{Z}_2(1))$ is a free $\mathbb{Z}_2$-module of rank 22. Since $H^3_{\text{ét}}(S_{\overline{k}}, \mathbb{Z}_2(1)) = 0$, the change of coefficients map $H^2_{\text{ét}}(S_{\overline{k}}, \mathbb{Z}_2(1)) \otimes_{\mathbb{Z}_2} \mathbb{Z}/2^i\mathbb{Z} \xrightarrow{\cong} H^2_{\text{ét}}(S_{\overline{k}}, \mu_{2^i})$ is an isomorphism, for any $i \in \mathbb{N}$.

Let us recall that there is the natural cup product pairing

$$\langle.,.\rangle\colon H^2_{\text{ét}}(S_{\overline{k}}, \mathbb{Z}_2(1)) \times H^2_{\text{ét}}(S_{\overline{k}}, \mathbb{Z}_2(1)) \to \mathbb{Z}_2 \tag{5}$$

that is non-degenerate and even perfect, by Poincaré duality [SGA4, Exposé XVIII, Théorème 3.2.5]. Moreover, we have at our disposal the Chern class homomorphism $c_1\colon \mathrm{Pic}(S_{\overline{k}}) \to H^2_{\text{ét}}(S_{\overline{k}}, \mathbb{Z}_2(1))$ [SGA5, Exposé VII, Section 3], under which the intersection pairing agrees with the cup product pairing.

Definition 3.1. Let S be a $K3$ surface over a field k.

a) Then, we write $\mathrm{P}(S_{\overline{k}}, \mathbb{Z}_2) := c_1(\mathrm{Pic}(S_{\overline{k}}))$.

b) The orthogonal complement $\mathrm{T}(S_{\overline{k}}, \mathbb{Z}_2) := \mathrm{P}(S_{\overline{k}}, \mathbb{Z}_2)^\perp \subset H^2_{\text{ét}}(S_{\overline{k}}, \mathbb{Z}_2(1))$ is called the *transcendental lattice* of S. Note that $\mathrm{T}(S_{\overline{k}}, \mathbb{Z}_2)$, as well as $\mathrm{P}(S_{\overline{k}}, \mathbb{Z}_2)$, is a $\mathbb{Z}_2$-lattice.

According to this definition, $\mathrm{T}(S_{\overline{k}}, \mathbb{Z}_2) \subset H^2_{\text{ét}}(S_{\overline{k}}, \mathbb{Z}_2(1))$ clearly has no cotorsion. Let us note that $\mathrm{P}(S_{\overline{k}}, \mathbb{Z}_2) \subset H^2_{\text{ét}}(S_{\overline{k}}, \mathbb{Z}_2(1))$ has no cotorsion either. Indeed, suppose, for a certain $\mathscr{L} \in \mathrm{Pic}(S_{\overline{k}})$, that the Chern class $c_1(\mathscr{L}) \in H^2_{\text{ét}}(S_{\overline{k}}, \mathbb{Z}_2(1))$ is divisible by 2. Then $(c_1 \otimes_{\mathbb{Z}_2} \mathbb{Z}/2\mathbb{Z})(\mathscr{L}) = 0 \in H^2_{\text{ét}}(S_{\overline{k}}, \mu_2)$ and the exactness of the cohomology sequence $\mathrm{Pic}(S_{\overline{k}}) \xrightarrow{\cdot 2} \mathrm{Pic}(S_{\overline{k}}) \to H^2_{\text{ét}}(S_{\overline{k}}, \mu_2)$, induced by the Kummer sequence, shows that $\mathscr{L}$ is divisible by 2 itself.

Consequently, one has

$$\mathrm{P}(S_{\overline{k}}, \mathbb{Z}_2) := \mathrm{T}(S_{\overline{k}}, \mathbb{Z}_2)^\perp \,, \tag{6}$$

too. Indeed, the cup product pairing (5) is non-degenerate.

3.2. Let k be the finite field $\mathbb{F}_q$. Then, in terms of the geometric Picard group and the transcendental lattice, the Lefschetz trace formula (1) takes the form

$$\begin{aligned}\#S(\mathbb{F}_q) = q^2 + \mathrm{Tr}(\mathrm{Frob}\colon\ &\mathrm{Pic}(S_{\overline{\mathbb{F}}_q}) \otimes_{\mathbb{Z}} \mathbb{Q} \to \mathrm{Pic}(S_{\overline{\mathbb{F}}_q}) \otimes_{\mathbb{Z}} \mathbb{Q})q \\ &+ \mathrm{Tr}(\mathrm{Frob}\colon\ \mathrm{T}(S_{\overline{\mathbb{F}}_q}, \mathbb{Z}_2) \to \mathrm{T}(S_{\overline{\mathbb{F}}_q}, \mathbb{Z}_2))q + 1\,.\end{aligned} \tag{7}$$

Similarly, for S a flat $\mathbb{Z}$-scheme such that $S_\mathbb{Q}$ is a $K3$ surface and a prime p of good reduction, one has

$$\begin{aligned}\#S(\mathbb{F}_p) = p^2 + \mathrm{Tr}(\mathrm{Frob}_p\colon\ &\mathrm{Pic}(S_{\overline{\mathbb{Q}}}) \otimes_{\mathbb{Z}} \mathbb{Q} \to \mathrm{Pic}(S_{\overline{\mathbb{Q}}}) \otimes_{\mathbb{Z}} \mathbb{Q})p \\ &+ \mathrm{Tr}(\mathrm{Frob}_p\colon\ \mathrm{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2) \to \mathrm{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2))p + 1\,.\end{aligned} \tag{8}$$

In particular, this means $\#S(\mathbb{F}_p) = p^2 + rp + \mathrm{Tr}(\mathrm{Frob}_p\colon\ \mathrm{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2) \to \mathrm{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2))p + 1$ in the case that $\mathrm{rk}\,\mathrm{Pic}(S_\mathbb{Q}) = \mathrm{rk}\,\mathrm{Pic}(S_{\overline{\mathbb{Q}}}) = r$.

3.3. On cohomology with 2-torsion coefficients, the cup product pairing induces a canonical $\mathrm{Gal}(\overline{k}/k)$-equivariant isomorphism

$$\begin{aligned}H^2_{\text{ét}}(S_{\overline{k}}, \mu_2) &\xrightarrow{\cong} \mathrm{Hom}(H^2_{\text{ét}}(S_{\overline{k}}, \mu_2), \mathbb{Z}/2\mathbb{Z}) \\ &= \ \mathrm{Hom}(H^2_{\text{ét}}(S_{\overline{k}}, \mathbb{Z}_2(1)), \mathbb{Z}/2\mathbb{Z})\,.\end{aligned}$$

Restricting the domain on the right hand side from $H^2_{\text{ét}}(S_{\overline{k}}, \mathbb{Z}_2(1))$ to the transcendental lattice, one obtains a canonical homomorphism

$$H^2_{\text{ét}}(S_{\overline{k}}, \mu_2) \longrightarrow \mathrm{Hom}(\mathrm{T}(S_{\overline{k}}, \mathbb{Z}_2), \mathbb{Z}/2\mathbb{Z})\,, \tag{9}$$

which is surjective, since $\mathrm{T}(S_{\overline{k}}, \mathbb{Z}_2) \subset H^2_{\text{ét}}(S_{\overline{k}}, \mathbb{Z}_2(1))$ has no cotorsion.

Lemma 3.4. *Let S be a $K3$ surface over a field k. Then the kernel of the homomorphism (9) coincides with the image of $c_1 \otimes_{\mathbb{Z}_2} \mathbb{Z}/2\mathbb{Z}\colon\ \mathrm{Pic}(S_{\overline{k}}) \to H^2_{\text{ét}}(S_{\overline{k}}, \mu_2)$.*

Proof. "$\supseteq$" is clear. "$\subseteq$": Let $\gamma \in H^2_{\text{ét}}(S_{\overline{k}}, \mu_2)$ be in the kernel of (9). Lift γ to a class $\widetilde{\gamma} \in H^2_{\text{ét}}(S_{\overline{k}}, \mathbb{Z}_2(1))$. Then, for every $\chi \in \mathrm{T}(S_{\overline{k}}, \mathbb{Z}_2)$, one has that $\langle \widetilde{\gamma}, \chi \rangle \in \mathbb{Z}_2$ is divisible by 2. Since $\mathrm{T}(S_{\overline{k}}, \mathbb{Z}_2)$ has no cotorsion and the pairing (5) is perfect, there exists a class $\kappa \in H^2_{\text{ét}}(S_{\overline{k}}, \mathbb{Z}_2(1))$ of the kind that $\langle \widetilde{\gamma}, \chi \rangle = 2\langle \kappa, \chi \rangle$, for any $\chi \in \mathrm{T}(S_{\overline{k}}, \mathbb{Z}_2)$. In other words, $\widetilde{\gamma} - 2\kappa \in \mathrm{T}(S_{\overline{k}}, \mathbb{Z}_2)^\perp = \mathrm{P}(S_{\overline{k}}, \mathbb{Z}_2)$, according to (6), which identifies γ as an element in the image of $c_1 \otimes_{\mathbb{Z}_2} \mathbb{Z}/2\mathbb{Z}$. $\square$

We denote by $\mathrm{Br}(S_{\overline{k}}) := H^2_{\text{ét}}(S_{\overline{k}}, \mathbb{G}_m)$ the geometric Brauer group of S. A standard application of the Kummer sequence shows that the 2-torsion part is given by $\mathrm{Br}(S_{\overline{k}})_2 = H^2_{\text{ét}}(S_{\overline{k}}, \mu_2)/\operatorname{im}(c_1 \otimes_{\mathbb{Z}_2} \mathbb{Z}/2\mathbb{Z})$.

Theorem 3.5. *Let S be a $K3$ surface over a field k. Then the homomorphism (9) induces a canonical $\mathrm{Gal}(\overline{k}/k)$-equivariant isomorphism*

$$\mathrm{Br}(S_{\overline{k}})_2 \xrightarrow{\cong} \mathrm{Hom}(\mathrm{T}(S_{\overline{k}}, \mathbb{Z}_2), \mathbb{Z}/2\mathbb{Z})\,. \tag{10}$$

Remark 3.6. In other words, the transcendental lattice modulo 2 is dual to the 2-torsion of the Brauer group. This has been known before, at least in the context of complex analytic $K3$ surfaces, cf. [vG, Paragraph 2.1].

Double covers of $\mathbf{P}^2$ *branched over six lines.* Let S be a $K3$ surface over a field k of the kind described in paragraph 2.1. Then S may be obtained as a double cover of B, the projective plane, blown up in the singular locus of $V(l_1 \cdots l_6)$, which forms a reduced k-scheme of length 15. The branch locus of the double cover $\pi\colon S \to B$ is the strict transform of $V(l_1 \cdots l_6)$. This is a disjoint union of six projective lines.

Theorem 3.7 (A. N. Skorobogatov)**.** *Let k be a field of characteristic not 2 and let S be a $K3$ surface over k as in 2.1. Then there is a* $\mathrm{Gal}(\overline{k}/k)$*-equivariant isomorphism*

$$\mathrm{Br}(S_{\overline{k}})_2 \stackrel{\cong}{\longrightarrow} \mathrm{Pic}(B_{\overline{k}})^{\mathrm{even}}/\pi_* \,\mathrm{Pic}(S_{\overline{k}})\,,$$

for $\mathrm{Pic}(B_{\overline{k}})^{\mathrm{even}} \subseteq \mathrm{Pic}(B_{\overline{k}})$ *the subgroup formed by the classes having an even intersection number with each connected component of the branch locus.*

Proof. This is a particular case of A. N. Skorobogatov's explicit description of $\mathrm{Br}(S_{\overline{k}})_2$ for double covers [Sk, Theorem 1.1]. Note that the geometric Picard group of the branch locus has no torsion. □

The case of six k-rational lines.

Corollary 3.8. *Let k be a field of characteristic not 2 and S a $K3$ surface over k as in 2.1. Suppose that $l_1, \ldots, l_6$ are defined over k.*

a) *Then the natural* $\mathrm{Gal}(\overline{k}/k)$*-action on* $\mathrm{Br}(S_{\overline{k}})_2$ *is trivial.*

b) *The natural* $\mathrm{Gal}(\overline{k}/k)$*-action on* $\mathrm{T}(S_{\overline{k}}, \mathbb{Z}_2)/2\,\mathrm{T}(S_{\overline{k}}, \mathbb{Z}_2)$ *is trivial, too.*

Proof. a) Since $l_1, \ldots, l_6$ are defined over k, B is the blowing-up of $\mathbf{P}^2_k$ in 15 k-rational points. Therefore, the $\mathrm{Gal}(\overline{k}/k)$-action on the whole of $\mathrm{Pic}(B_{\overline{k}})$ is trivial.

b) follows from a), together with Theorem 3.5. □

Corollary 3.9 (The splitting field of $\mathrm{T}(S_{\overline{k}}, \mathbb{Z}_2)/4\,\mathrm{T}(S_{\overline{k}}, \mathbb{Z}_2)$)**.** *Let k be a field of characteristic not 2 and S a $K3$ surface over k as in 2.1. Suppose that $l_1, \ldots, l_6$ are defined over k. Denote by $K \supseteq k$ the splitting field of* $\mathrm{T}(S_{\overline{k}}, \mathbb{Z}_2)/4\,\mathrm{T}(S_{\overline{k}}, \mathbb{Z}_2)$.

a) *Then K is an abelian extension of k of exponent at most 2.*

b) *Suppose that k is a number field. Then K is unramified over k at all primes of good reduction and odd residue characteristic.*

Proof. a) By definition, one has a natural injection

$$\mathrm{Gal}(K/k) \hookrightarrow \mathrm{Aut}(\mathrm{T}(S_{\overline{k}}, \mathbb{Z}_2)/4\,\mathrm{T}(S_{\overline{k}}, \mathbb{Z}_2))\,.$$

But $\{A \in \mathrm{GL}_n(\mathbb{Z}/4\mathbb{Z}) \mid A \equiv E_n \pmod 2\}$ is an elementary abelian 2-group, for any $n \in \mathbb{N}$.

b) As $\mathrm{T}(S_{\overline{k}}, \mathbb{Z}_2) \subset H^2_{\mathrm{\acute{e}t}}(S_{\overline{k}}, \mathbb{Z}_2(1))$ has no cotorsion, the natural homomorphism $\mathrm{T}(S_{\overline{k}}, \mathbb{Z}_2)/4\,\mathrm{T}(S_{\overline{k}}, \mathbb{Z}_2) \hookrightarrow H^2_{\mathrm{\acute{e}t}}(S_{\overline{k}}, \mu_4)$ is injective. Moreover, by virtue of the smooth specialisation theorem [SGA4, Exposé XVI, Corollaire 2.3], the splitting field of

$H^2_{\text{ét}}(S_{\overline{k}}, \mu_4)$ is known to be unramified at any prime of k of odd residue characteristic, at which S has good reduction. $\square$

Corollary 3.10. *Let S be a $K3$ surface as in 2.1, over $k = \mathbb{Q}$. Suppose that $l_1, \ldots, l_6$ are defined over $\mathbb{Q}$. Then, for an odd prime p of good reduction, the action of the Frobenius* Frob_p *on* $\mathrm{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)/4\,\mathrm{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)$ *is completely determined by the class of* Frob_p *in the Galois group of the number field*

$$K = \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{d} \mid d \text{ a bad prime for } S)\,.$$

Proof. This is the particular case of Corollary 3.9, for $k = \mathbb{Q}$. $\square$

The action of $\mathrm{Sym}(6)$ *on* $\mathrm{T}(S_{\overline{k}}, \mathbb{Z}_2)/2\,\mathrm{T}(S_{\overline{k}}, \mathbb{Z}_2)$ *in the case that* $\mathrm{rk}\,\mathrm{Pic}(S_{\overline{k}}) = 16$.

Notation. In the remainder of this section, a double index is meant to be an unordered pair. E.g., $a_{ij} = a_{ji}$. In particular, we write e_{ij}, but also e_{ji}, for the exceptional curve on $B_{\overline{k}}$ that lies over the point of intersection $\mathrm{V}(l_i) \cap \mathrm{V}(l_j)$, for $i \neq j$, $1 \leq i, j \leq 6$.

Lemma 3.11. *Let k be a field of characteristic not 2 and S a $K3$ surface over k as in 2.1. Suppose that* $\mathrm{rk}\,\mathrm{Pic}(S_{\overline{k}}) = 16$.

a.i) *Then* $\mathrm{Pic}(S_{\overline{k}}) \supset \mathbb{Z}\pi^*[l] \oplus \mathbb{Z}\pi^*[e_{12}] \oplus \cdots \oplus \mathbb{Z}\pi^*[e_{56}]$ *is a sublattice of full rank.*

ii) *There are further divisor classes* $[D_1], \ldots, [D_6] \in \mathrm{Pic}(S_{\overline{k}})$ *such that*

$$2[D_i] = \pi^*[l] + \sum_{\substack{j=1,\ldots,6,\\ j \neq i}} \pi^*[e_{ij}]\,. \tag{11}$$

The classes $[D_1], \ldots, [D_6]$ *generate* $\mathrm{Pic}(S_{\overline{k}})$*, together with* $\pi^*[l], \pi^*[e_{12}], \ldots, \pi^*[e_{56}]$.

b) *Put*

$$M := \{a\pi^*[l] + a_{12}\pi^*[e_{12}] + \cdots + a_{56}\pi^*[e_{56}] \in \mathbb{F}_2\pi^*[l] \oplus \mathbb{F}_2\pi^*[e_{12}] \oplus \cdots \oplus \mathbb{F}_2\pi^*[e_{56}] \mid a + \sum_{\substack{j=1,\ldots,6,\\ j \neq i}} a_{ij} = 0, \text{ for } i = 1, \ldots, 6\}\,.$$

Then there is a natural isomorphism

$$\mathrm{Br}(S_{\overline{k}})_2 \cong M/\langle \pi^*[l] + \sum_{\substack{j=1,\ldots,6,\\ j \neq i}} \pi^*[e_{ij}] \mid i = 1, \ldots, 6\rangle\,. \tag{12}$$

Proof. One has $\mathrm{Pic}(B_{\overline{k}}) = \mathbb{Z}[l] \oplus \mathbb{Z}[e_{12}] \oplus \cdots \oplus \mathbb{Z}[e_{56}]$, the direct sum being orthogonal. Moreover, $[l]\cdot[l] = 1$ and $[e_{ij}]\cdot[e_{ij}] = -1$, for $1 \leq i < j \leq 6$. As $\pi_{\overline{k}}\colon S_{\overline{k}} \to B_{\overline{k}}$ is finite of degree 2, this yields that $\pi^*[l], \pi^*[e_{12}], \ldots, \pi^*[e_{56}] \in \mathrm{Pic}(S_{\overline{k}})$ are mutually perpendicular, with $\pi^*[l]\cdot\pi^*[l] = 2$ and $\pi^*[e_{ij}]\cdot\pi^*[e_{ij}] = -2$. From this, a.i) immediately follows. Consequently, one has $\mathbb{Q}\pi^*[l] \oplus \mathbb{Q}\pi^*[e_{12}] \oplus \cdots \oplus \mathbb{Q}\pi^*[e_{56}] \supset \mathrm{Pic}(S_{\overline{k}})$. As the intersection numbers with the base elements have to be integers, the coefficients are in fact half integral, at most.

Furthermore, over the strict transform of the quintic $\mathrm{V}(l_2 \cdots l_6 - l_1^5) \subset \mathbf{P}^2_{\overline{k}}$, the double cover $\pi_{\overline{k}}\colon S_{\overline{k}} \to B_{\overline{k}}$ splits, since the equation of the surface goes over into $w^2 = l_1^6$ [EJ18, Remark 4.6]. This yields a divisor $D \in \mathrm{Div}(S_{\overline{k}})$ such that

$\pi_*[D] = 5[l] + [e_{12}] + [e_{13}] + [e_{14}] + [e_{15}] + [e_{16}]$. One may put $[D_1] := [D] - 2\pi^*[l]$ in order to fulfil (11). The divisor classes $[D_2], \dots, [D_6]$ are constructed analogously. Thus, there is an inclusion

$$\operatorname{Pic}(B_{\overline{k}}) \supseteq (\mathbb{Z}[l] \oplus \mathbb{Z}[e_{12}] \oplus \dots \oplus \mathbb{Z}[e_{56}]) + [D_1] + \dots + [D_6]\,, \tag{13}$$

and in order to complete the proof of a), it needs to be shown that equality holds.

On the other hand, one has $M = \operatorname{Pic}(B_{\overline{k}})^{\text{even}}/\pi_*(\mathbb{Z}\pi^*[l] \oplus \mathbb{Z}\pi^*[e_{12}] \oplus \dots \oplus \mathbb{Z}\pi^*[e_{56}])$. Hence, by Theorem 3.7, there is actually a natural surjection

$$\operatorname{Br}(S_{\overline{k}})_2 \twoheadrightarrow M/\langle \pi^*[l] + \sum_{\substack{j=1,\dots,6,\\ j\neq i}} \pi^*[e_{ij}] \mid i = 1, \dots, 6\rangle \tag{14}$$

that is a bijection if and only if equality holds in (13). But an explicit calculation reveals that the right hand side of (14) is of order 64, M being of order 2048. As, by Theorem 3.5, $\operatorname{Br}(S_{\overline{k}})_2$ is of order 64, too, this proves both, a) and b). □

Theorem 3.12. *Let k be a field of characteristic not 2 and S a $K3$ surface over k as in 2.1. Suppose that* $\operatorname{rk}\operatorname{Pic}(S_{\overline{k}}) = 16$.

a.i) *Then the group* $\operatorname{Sym}(6)$ *permuting the six branch lines naturally acts on the sublattice of* $\operatorname{Pic}(S_{\overline{k}})$ *described in Lemma 3.11.a.i) by*

$$\sigma(\pi^*[l]) = \pi^*[l] \qquad \textit{and} \qquad \sigma(\pi^*[e_{ij}]) = \pi^*[e_{\sigma(i)\sigma(j)}]\,.$$

ii) *The action on* $\operatorname{Br}(S_{\overline{k}})_2$ *is as follows. There is an* $\mathbb{F}_2$*-basis* $(b_1, \dots, b_6)$ *of* $\operatorname{Br}(S_{\overline{k}})_2$ *such that*

$$\sigma(b_i) = \begin{cases} b_{\widetilde{\sigma}(i)}\,, & \text{if } \sigma \in \operatorname{Alt}(6)\,,\\ b_{\widetilde{\sigma}(i)} + c\,, & \text{if } \sigma \notin \operatorname{Alt}(6)\,, \end{cases}$$

for $c := b_1 + \dots + b_6$. *Here,* $\operatorname{Sym}(6) \to \operatorname{Sym}(6)$, $\sigma \mapsto \widetilde{\sigma}$, *is an outer automorphism.*

b) *The natural* $\operatorname{Gal}(\overline{k}/k)$*-actions on* $\operatorname{Pic}(S_{\overline{k}})$ *and* $\operatorname{Br}(S_{\overline{k}})_2$ *are the compositions of the natural* $\operatorname{Gal}(\overline{k}/k)$*-action on the six branch lines with the actions described in a).*

Proof. a.i) and b) are clear.

a.ii) One puts $b_6 := \overline{\pi^*[e_{12}] + \pi^*[e_{23}] + \pi^*[e_{34}] + \pi^*[e_{45}] + \pi^*[e_{15}]} \in \operatorname{Br}(S_{\overline{k}})_2$. Note that indeed $\pi^*[e_{12}] + \pi^*[e_{23}] + \pi^*[e_{34}] + \pi^*[e_{45}] + \pi^*[e_{15}] \in M$, so that this is a correct definition.

It is clear that b_6 is stabilised by a dihedral group of order ten, permuting only $\{1, \dots, 5\}$. Moreover, applying the relations in (12), for $i = 1$ and 4, one finds that $b_6 = \overline{\pi^*[e_{13}] + \pi^*[e_{23}] + \pi^*[e_{24}] + \pi^*[e_{46}] + \pi^*[e_{16}]}$, too. Hence, the stabiliser of b_6 is a 2-transitive subgroup of $\operatorname{Sym}(6)$, of order a multiple of 60.

A machine calculation shows that the orbit of b_6 under $\operatorname{Sym}(6)$ is indeed of size twelve, so that the stabiliser of b_6 is $\operatorname{Alt}(5)$, transitively embedded into $\operatorname{Sym}(6)$ [DM, Table 2.1]. Furthermore, the orbit $\{b_1, \dots, b_6\}$ of b_6 under $\operatorname{Alt}(6) \subset \operatorname{Sym}(6)$ turns out to be $\mathbb{F}_2$-linearly independent.

The orbit under $\operatorname{Sym}(6)$ is, in fact, $\{b_1, \dots, b_6, b_1 + c, \dots, b_6 + c\}$. Moreover, $c \in \operatorname{Br}(S_{\overline{k}})_2 \backslash \{0\}$ is the unique $\operatorname{Alt}(6)$-invariant element, and hence $\operatorname{Sym}(6)$-invariant. Consequently, the stabiliser of the class $\overline{b}_6 \in \operatorname{Br}(S_{\overline{k}})_2/\langle c\rangle$ is 2-transitive of order 120, and thus Sym(5), transitively embedded into Sym(6). This shows that indeed the classes $\overline{b}_1, \ldots, \overline{b}_6 \in \mathrm{Br}(S_{\overline{k}})_2/\langle c \rangle$ are permuted according to an outer automorphism of the group Sym(6) [Wi, Subsection 2.4.2], which completes the proof. □

4. A theorem on the 2-adic orthogonal group

The main theorem. 2-adic overdetermination of the trace.

Theorem 4.1. *Let $n \in \mathbb{N}$. With respect to a non-degenerate, symmetric bilinear form on $\mathbb{Q}_2^n$, let $U_1, U_2 \in \mathrm{M}_{n\times n}(\mathbb{Z}_2)$ be orthogonal matrices such that*

$$U_1 \equiv U_2 \pmod 4 .$$

a) *If* $U_1 \equiv E_n \pmod 2$ *then* $\mathrm{Tr}(U_1) \equiv \mathrm{Tr}(U_2) \pmod{16}$.

b) *If* $U_1^2 \equiv E_n \pmod 2$ *then* $\mathrm{Tr}(U_1) \equiv \mathrm{Tr}(U_2) \pmod 8$.

Proof. One has $\det(U_1) = \pm 1$, since U_1 is orthogonal. Hence, $U_1^{-1} \in \mathrm{M}_{n\times n}(\mathbb{Z}_2)$. The congruence $U_1 \equiv U_2 \pmod 4$ therefore implies that $U_1^{-1}U_2 \equiv E_n \pmod 4$. I.e., there exists a matrix $B \in \mathrm{M}_{n\times n}(\mathbb{Z}_2)$ such that

$$U_2 = U_1(E_n + 4B) .$$

Moreover, $\det(E_n + 4B) = \det(U_1^{-1}U_2) = 1$, hence the linear approximation of det near the unit matrix yields $1 = \det(E_n + 4B) \equiv \det(E_n) + 4\,\mathrm{Tr}(B) \pmod{16}$. I.e.,

$$\mathrm{Tr}(B) \equiv 0 \pmod 4 . \tag{15}$$

a) Writing $U_1 = E_n + 2A$, one finds

$$\begin{aligned}\mathrm{Tr}(U_2) = \mathrm{Tr}((E_n + 2A)\cdot(E_n + 4B)) &= \mathrm{Tr}(E_n + 2A) + 4\,\mathrm{Tr}(B) + 8\,\mathrm{Tr}(AB)\\ &\equiv \mathrm{Tr}(U_1) + 8\,\mathrm{Tr}(AB) \pmod{16} .\end{aligned}$$

Finally, one has $\mathrm{Tr}(AB) \equiv 0 \pmod 2$, due to Theorem 4.2.a), below.

b) Analogously, writing $U_1 = E_n + A$, one sees

$$\mathrm{Tr}(U_2) = \mathrm{Tr}((E_n + A)\cdot(E_n + 4B)) = \mathrm{Tr}(U_1) + 4\,\mathrm{Tr}(B) + 4\,\mathrm{Tr}(AB) ,$$

so that the assertion follows from (15) and Theorem 4.2.b). □

2-*adic divisibility of traces.*

Theorem 4.2. *For $n \in \mathbb{N}$, let b be a non-degenerate, symmetric bilinear form on $\mathbb{Q}_2^n$.*

a) *Let $A, B \in \mathrm{M}_{n\times n}(\mathbb{Z}_2)$ be such that $E_n + 2A$ and $E_n + 4B$ are orthogonal with respect to b. Then* $\mathrm{Tr}(AB) \equiv 0 \pmod 2$.

b) *Let $A, B \in \mathrm{M}_{n\times n}(\mathbb{Z}_2)$ be such that $E_n + A$ and $E_n + 4B$ are orthogonal with respect to b and $(E_n + A)^2 \equiv E_n \pmod 2$. Then* $\mathrm{Tr}(AB) \equiv 0 \pmod 2$.

A more natural formulation, not explicitly considering matrices, goes as follows.

Theorem 4.3. *Let Γ be a $\mathbb{Z}_2$-lattice and $\varphi, \psi \colon \Gamma \to \Gamma$ orthogonal endomorphisms.*

a) *If* $(\varphi \bmod 2)$ *acts trivially on* $\Gamma/2\Gamma$ *and* $(\psi \bmod 4)$ *acts trivially on* $\Gamma/4\Gamma$ *then* $\mathrm{Tr}((\varphi-\mathrm{id})\circ(\psi-\mathrm{id})) \equiv 0 \pmod{16}$.

b) *If* $(\varphi\circ\varphi \bmod 2)$ *acts trivially on* $\Gamma/2\Gamma$ *and* $(\psi \bmod 4)$ *acts trivially on* $\Gamma/4\Gamma$ *then* $\mathrm{Tr}((\varphi-\mathrm{id})\circ(\psi-\mathrm{id})) \equiv 0 \pmod{8}$.

4.4 (Structure of the proof)**.** The proof of Theorem 4.3 is organised as follows.

i) We directly check the analogue of Theorem 4.3 for regular $\mathbb{Z}_2[\sqrt{2}]$-lattices.

ii) We show Theorem 4.3 in a particular case, in which the discriminant of b has a small 2-adic valuation. The idea is to construct a $\mathbb{Z}_2[\sqrt{2}]$-lattice $\widetilde{\Gamma} \supseteq \Gamma\otimes_{\mathbb{Z}_2}\mathbb{Z}_2[\sqrt{2}]$ such that b is regular on $\widetilde{\Gamma}$. We check that all relevant properties of the endomorphisms φ and ψ are preserved under this change of lattices.

iii) For the general case, the idea is as follows. By inspection of the dual lattice $\Gamma^\vee$, we show that the endomorphisms φ and ψ respect various other lattices, as well. We choose one rather particular such lattice $\Gamma' \subset \Gamma\otimes_{\mathbb{Z}_2}\mathbb{Q}_2$, thereby making sure that the discriminant of b on Γ' has a 2-adic valuation sufficiently small, so that ii) applies.

Remarks 4.5. a) For the concept of an $\mathscr{O}$-lattice, in general, recall the terminology and notation fixed in the introduction.

b) The ring $\mathscr{O} = \mathbb{Z}_2[\sqrt{2}]$ is a principal ideal domain, in fact a discrete valuation ring. In particular, every finitely generated $\mathscr{O} = \mathbb{Z}_2[\sqrt{2}]$-module that is projective or only torsion-free is automatically free.

c) There is a more elementary proof for Theorem 4.3 that avoids $\mathbb{Z}_2[\sqrt{2}]$-lattices at the cost of a more complicated case distinction.

First step of the proof – A variant for regular lattices over discrete valuation rings.

Proposition 4.6. *Let* $\mathscr{O}$ *be a discrete valuation ring, in which* $2 \neq 0$ *is not a unit,* Γ *a regular* $\mathscr{O}$*-lattice, and* $\varphi, \psi\colon \Gamma \to \Gamma$ *orthogonal endomorphisms.*

a) *If* $(\varphi \bmod 2)$ *acts trivially on* $\Gamma/2\Gamma$ *and* $(\psi \bmod 4)$ *acts trivially on* $\Gamma/4\Gamma$ *then* $\mathrm{Tr}((\varphi-\mathrm{id})\circ(\psi-\mathrm{id})) \equiv 0 \pmod{16}$.

b) *If* $(\varphi\circ\varphi \bmod 2)$ *acts trivially on* $\Gamma/2\Gamma$ *and* $(\psi \bmod 4)$ *acts trivially on* $\Gamma/4\Gamma$ *then* $\mathrm{Tr}((\varphi-\mathrm{id})\circ(\psi-\mathrm{id})) \equiv 0 \pmod{8}$.

Proof. Choose a basis for Γ and denote the rank of Γ by n. The bilinear form on Γ is then given by a symmetric $n\times n$ matrix M. Thanks to the regularity assumption, one has $M \in \mathrm{GL}_n(\mathscr{O})$. Moreover, the matrix representing ψ can be written as $E_n + 4B$, for some $B \in \mathrm{M}_{n\times n}(\mathscr{O})$. By Lemma 4.7.b), MB is symmetric modulo 2 all diagonal coefficients being divisible by 2.

a) Here, the matrix representing φ is E_n+2A, for a certain $A \in \mathrm{M}_{n\times n}(\mathscr{O})$. Thus, the assertion follows from Lemmas 4.7.a) and 4.8, below.

b) Let $A \in \mathrm{M}_{n\times n}(\mathscr{O})$ be the matrix representing $\varphi-\mathrm{id}$. The fact that φ is orthogonal is then equivalent to

$$A^\top M + MA + A^\top MA = 0\,, \tag{16}$$

which implies
$$A^\top MA + MA^2 + A^\top MA^2 = 0\,.$$
On the other hand, the assumption $(E_n+A)^2 \equiv E_n \pmod 2$ yields $A^2 \equiv 0 \pmod 2$, so that one has $A^\top MA \equiv 0 \pmod 2$. Therefore, formula (16), together with the fact that M is symmetric, yields that MA is symmetric modulo 2. To summarise, it is proved that Lemma 4.8 is applicable, which shows that $\mathrm{Tr}(AB)$ is divisible by 2. □

Lemma 4.7. *Let $\mathscr{O}$ be a discrete valuation ring, in which $2 \neq 0$ is not a unit, and $M \in \mathrm{GL}_n(\mathscr{O})$ a symmetric matrix.*

a) *Let $C \in \mathrm{M}_{n\times n}(\mathscr{O})$ be such that E_n+2C is orthogonal with respect to M. Then the reduction modulo 2 of MC is symmetric.*

b) *Let $C \in \mathrm{M}_{n\times n}(\mathscr{O})$ be such that E_n+4C is orthogonal with respect to M. Then the reduction modulo 2 of MC is symmetric. Furthermore, every diagonal coefficient of MC is divisible by 2.*

Proof. a) The orthogonality condition explicitly reads
$$C^\top M + MC + 2C^\top MC = 0\,. \tag{17}$$
Moreover, as M is symmetric, we have $C^\top M = (MC)^\top$. Thus, (17) implies that $MC \equiv (MC)^\top \pmod 2$, which shows a).

b) Here, orthogonality means $C^\top M + MC + 4C^\top MC = 0$. Moreover, once again, we have $C^\top M = (MC)^\top$, so that $MC \equiv -(MC)^\top \pmod 4$ follows. This proves both conclusions of b). □

Lemma 4.8. *Let $\mathscr{O}$ be a discrete valuation ring, in which $2 \neq 0$ is not a unit, $M \in \mathrm{GL}_n(\mathscr{O})$ symmetric, and $A, B \in \mathrm{M}_{n\times n}(\mathscr{O})$ such that $MA \equiv (MA)^\top \pmod 2$, $MB \equiv (MB)^\top \pmod 2$, and all diagonal coefficients of MB are divisible by 2. Then $\mathrm{Tr}(AB)$ is divisible by 2.*

Proof. Writing $U := AM^{-1}$ and $V := MB$, one has
$$\mathrm{Tr}(AB) = \mathrm{Tr}(AM^{-1}MB) = \mathrm{Tr}(UV) = \sum_{i,j} u_{ij}v_{ji}\,. \tag{18}$$
Here, $U = M^{-1}MAM^{-1}$ is symmetric modulo 2, since both, MA and M^{-1}, are. Furthermore, $V = MB$ is symmetric modulo 2, by assumption.

Therefore, in (18), the summands for the indices (i,j) and (j,i) coincide modulo 2, so that the sum of each pair is divisible by 2. Finally, the summands for $i = j$ are divisible by 2, as the diagonal coefficients v_{ii} of V are. □

Second step of the proof – Generalities on $\mathbb{Z}_2$-lattices.

Proposition 4.9 (Decomposition of $\mathbb{Z}_2$-lattices)**.** *Let (Γ, b) be a $\mathbb{Z}_2$-lattice. Then there is a decomposition $\Gamma = \bigoplus_{i=0}^N \Gamma_i$ into an orthogonal direct sum of the kind that*
$$b = \bigoplus_{i=0}^N 2^i b_i\,, \tag{19}$$

for regular symmetric bilinear forms $b_0, \ldots, b_N$ on $\Gamma_0, \ldots, \Gamma_N$, respectively.

Proof. See [CS, Chapter 15, Theorem 2] or [Kn, Satz 15.1]. It is, in fact, shown that, for each i, the lattice Γ_i may be decomposed further into an orthogonal direct sum of only 1- and 2-dimensional lattices. $\square$

Definition 4.10. Let (Γ, b) be a $\mathbb{Z}_2$-lattice. Then, by the *dual lattice,* we mean

$$\Gamma^\vee := \{x \in \Gamma \otimes_{\mathbb{Z}_2} \mathbb{Q}_2 \mid b(x, \Gamma) \subseteq \mathbb{Z}_2\}\,.$$

Here, the $\mathbb{Q}_2$-bilinear extension of $b\colon \Gamma \times \Gamma \to \mathbb{Z}_2$ to $\Gamma \otimes_{\mathbb{Z}_2} \mathbb{Q}_2$ is again denoted by b.

Example 4.11. A decomposition $\Gamma = \bigoplus\limits_{i=0}^{N} \Gamma_i$ as above, with $b = \bigoplus\limits_{i=0}^{N} 2^i b_i$, yields

$$\Gamma^\vee = \bigoplus_{i=0}^{N} 2^{-i} \Gamma_i\,.$$

Indeed, for each i, the lattice (Γ_i, b_i) is regular.

Lemma 4.12. *Let Γ be a $\mathbb{Z}_2$-lattice and $\varphi\colon \Gamma \to \Gamma$ an orthogonal map. Denote the $\mathbb{Q}_2$-linear extension of φ to $\Gamma \otimes_{\mathbb{Z}_2} \mathbb{Q}_2$ again by φ. Then $\varphi(\Gamma^\vee) = \Gamma^\vee$.*

Proof. We have

$$x \in \Gamma^\vee \Leftrightarrow b(x, \Gamma) \subseteq \mathbb{Z}_2 \Leftrightarrow b(\varphi(x), \varphi(\Gamma)) \subseteq \mathbb{Z}_2 \Leftrightarrow b(\varphi(x), \Gamma) \subseteq \mathbb{Z}_2 \Leftrightarrow \varphi(x) \in \Gamma^\vee\,. \ \square$$

Lemma 4.13. *Let Γ be a $\mathbb{Z}_2$-lattice and $\varphi\colon \Gamma \to \Gamma$ an orthogonal endomorphism. Moreover, let $\Gamma = \bigoplus_{i=0}^{N} \Gamma_i$, with $b = \bigoplus_{i=0}^{N} 2^i b_i$, be a decomposition as above and let $\mathscr{B}$ be a basis of Γ obtained by concatenating bases of $\Gamma_0, \ldots, \Gamma_N$. Finally, put*

$$D = (D_{ij})_{i,j=0,\ldots,N} := \mathrm{M}_{\mathscr{B}}^{\mathscr{B}}(\varphi)\,,$$

so that, for $i, j = 0, \ldots, N$, the block D_{ij} represents an element of $\mathrm{Hom}(\Gamma_j, \Gamma_i)$*.*

a) *Then, for $i, j = 0, \ldots, N$, one has $\nu_2(D_{ij}) \geq j - i$.*

b) *Let $e \in \mathbb{N}$ and suppose, in addition, that φ acts trivially on the quotient $\Gamma/2^e\Gamma$. Then $\nu_2(D_{ij}) \geq j - i + e$, for $i \neq j$, $i, j = 0, \ldots, N$.*

Proof. a) As φ maps Γ onto itself, by Lemma 4.12, it does the same to the dual lattice $\Gamma^\vee = \bigoplus_{i=0}^{N} 2^{-i} \Gamma_i$. This shows that $\nu_2(D_{ij}) \geq j - i$, for $j > i$. Note that the assertion is trivial in the case that $j \leq i$.

b) By assumption, φ maps the lattices Γ and $2^e\Gamma$ onto themselves. Furthermore, the action induced on the quotient $\Gamma/2^e\Gamma$ is assumed to be trivial. Consequently, φ maps every lattice Δ of the kind that $2^e\Gamma \subseteq \Delta \subseteq \Gamma$ onto itself.

We apply this observation to the lattices, given by

$$\Delta_j := \Bigg(\bigoplus_{\substack{i=0,\ldots,N \\ i \neq j}} \Gamma_i \Bigg) \oplus 2^e \Gamma_j\,,$$

for $j = 0, \dots, N$. As φ maps Δ_j onto itself, the same is true for $\Delta_j^\vee$. Noticing that

$$\Delta_j^\vee = \left(\bigoplus_{\substack{i=0,\dots,N \\ i \neq j}} 2^{-i}\Gamma_i \right) \oplus 2^{-j-e}\Gamma_j \,,$$

this yields $\nu_2(D_{ij}) \geq j - i + e$, for $j \neq i$. Indeed, one has that $\varphi(2^{-j-e}\Gamma_j) \subseteq \Delta_j^\vee$. $\square$

Remark 4.14. An alternative proof for b) may be given as follows. As φ acts trivially on $\Gamma/2^e\Gamma$, the adjoint map acts trivially on $\Gamma^\vee/2^e\Gamma^\vee$. As the adjoint coincides with the inverse of φ, the map being orthogonal, one may conclude that φ acts trivially on $\Gamma^\vee/2^e\Gamma^\vee$, as well. This implies the divisibility $\nu_2(D_{ij}) \geq j - i + e$, for $i \neq j$.

Third step of the proof – A particular case.

Proposition 4.15. *Let (Γ_0, b_0) and (Γ_1, b_1) be regular $\mathbb{Z}_2$-lattices. Equip the direct sum $\Gamma := \Gamma_0 \oplus \Gamma_1$ with the symmetric bilinear form $b := b_0 \oplus 2b_1$. Then Theorem 4.3 holds for Γ.*

Proof. Let us first note that the $\mathbb{Z}_2[\sqrt{2}]$-lattice

$$\begin{aligned} \widetilde{\Gamma} &:= \left(\Gamma_0 \otimes_{\mathbb{Z}_2} \mathbb{Z}_2[\sqrt{2}]\right) \oplus \tfrac{1}{2}\sqrt{2}\left(\Gamma_1 \otimes_{\mathbb{Z}_2} \mathbb{Z}_2[\sqrt{2}]\right) \\ &\subset \Gamma \otimes_{\mathbb{Z}_2} \mathbb{Q}_2[\sqrt{2}] \,, \end{aligned} \tag{20}$$

equipped with the bilinear form induced by b, is regular.

a) By assumption, $\varphi, \psi \colon \Gamma \to \Gamma$ are orthogonal maps acting trivially on $\Gamma/2\Gamma$ and $\Gamma/4\Gamma$, respectively. Then Lemma 4.16 shows that the induced maps $\widetilde{\varphi}, \widetilde{\psi} \colon \widetilde{\Gamma} \to \widetilde{\Gamma}$ are again orthogonal, that $(\widetilde{\varphi} \bmod 2)$ acts trivially on $\widetilde{\Gamma}/2\widetilde{\Gamma}$, and that $(\widetilde{\psi} \bmod 2)$ acts trivially on $\widetilde{\Gamma}/4\widetilde{\Gamma}$. By Proposition 4.6.a), this implies that

$$\mathrm{Tr}((\widetilde{\varphi} - \mathrm{id}) \circ (\widetilde{\psi} - \mathrm{id})) \in 16\mathbb{Z}_2[\sqrt{2}] \,.$$

Since $\widetilde{\varphi}$ and $\widetilde{\psi}$ are obtained from φ and ψ only by base extension, one has $\mathrm{Tr}((\varphi - \mathrm{id}) \circ (\psi - \mathrm{id})) \in 16\mathbb{Z}_2[\sqrt{2}]$, too. But the latter trace is automatically in $\mathbb{Z}_2$, so that the assertion follows.

The proof of b) works along the same lines. $\square$

Lemma 4.16. *Let (Γ_0, b_0) and (Γ_1, b_1) be regular $\mathbb{Z}_2$-lattices. Equip $\Gamma := \Gamma_0 \oplus \Gamma_1$ with the bilinear form $b := b_0 \oplus 2b_1$ and let $\widetilde{\Gamma}$ be the $\mathbb{Z}_2[\sqrt{2}]$-lattice, defined by (20). Moreover, let $\varphi \colon \Gamma \to \Gamma$ be an orthogonal map, and write $\widetilde{\varphi} \colon \widetilde{\Gamma} \to \Gamma \otimes_{\mathbb{Z}_2} \mathbb{Q}_2[\sqrt{2}]$ for the map induced by φ.*

a) *Then $\widetilde{\varphi}$ actually sends $\widetilde{\Gamma}$ onto itself.*

b) *Moreover, $\widetilde{\varphi} \colon \widetilde{\Gamma} \to \widetilde{\Gamma}$ is an orthogonal map.*

c) *Let $e \in \mathbb{N}$. If $(\varphi \bmod 2^e)$ acts trivially on $\Gamma/2^e\Gamma$ then $(\widetilde{\varphi} \bmod 2^e)$ acts trivially on $\widetilde{\Gamma}/2^e\widetilde{\Gamma}$.*

Proof. b) is clear from the construction of $\widetilde{\varphi}$, once the assertion of a) is established.

a) and c) Let $\mathscr{B}$ be a basis of Γ as in Lemma 4.13 and put $\left(\begin{smallmatrix} C_{00} & C_{01} \\ C_{10} & C_{11} \end{smallmatrix}\right) := \mathrm{M}^{\mathscr{B}}_{\mathscr{B}}(\varphi - \mathrm{id})$. The blocks C_{ij} are then matrices with coefficients in $\mathbb{Z}_2$. One even has $\nu_2(C_{ij}) \geq e$, for $0 \leq i,j \leq 1$, under the assumption of c).

Multiplying the basis vectors of Γ_1 by $\frac{1}{2}\sqrt{2}$, one finds a basis $\widetilde{\mathscr{B}}$ of $\widetilde{\Gamma}$, for which

$$\mathrm{M}^{\widetilde{\mathscr{B}}}_{\widetilde{\mathscr{B}}}(\widetilde{\varphi} - \mathrm{id}) = \begin{pmatrix} C_{00} & \frac{1}{2}\sqrt{2}C_{01} \\ \sqrt{2}C_{10} & C_{11} \end{pmatrix} .$$

Thus, in order to prove the assertions, only $\nu_2(C_{01}) \geq 1$ and $\nu_2(C_{01}) \geq e+1$, respectively, need to be verified. Both claims are true, due to Lemma 4.13. $\square$

Completion of the proof.

Lemma 4.17 (Change of lattice)**.** *Let Γ be an arbitrary $\mathbb{Z}_2$-lattice and $\Gamma = \bigoplus\limits_{i=0}^{N} \Gamma_i$ a decomposition as above. Furthermore, let $\varphi\colon \Gamma \to \Gamma$ be an orthogonal map.*

a) *Then φ maps the lattice $\Gamma' := \bigoplus\limits_{i=0}^{N} \Gamma'_i$, for*

$$\Gamma'_i := 2^{-\lfloor \frac{i}{2} \rfloor}\Gamma_i \,,$$

onto itself, as well.

b) *Let $e \in \mathbb{N}$ and suppose that φ acts trivially on $\Gamma/2^e\Gamma$. Then φ acts trivially on the quotient $\Gamma'/2^e\Gamma'$.*

Proof. Let $\mathscr{B}$ be a basis of Γ as in Lemma 4.13. Then there is a basis $\mathscr{B}'$ of Γ' given by scaling the basis vectors of Γ_i by $2^{-\lfloor \frac{i}{2} \rfloor}$, for $i = 0, \ldots, N$. The matrix

$$C' = (C'_{ij})_{i,j=0,\ldots,N} := \mathrm{M}^{\mathscr{B}'}_{\mathscr{B}'}(\varphi - \mathrm{id})$$

is then constructed out of the matrix $(C_{ij})_{i,j=0,\ldots,N} = \mathrm{M}^{\mathscr{B}}_{\mathscr{B}}(\varphi - \mathrm{id})$ by putting $C'_{ij} := 2^{\lfloor \frac{i}{2} \rfloor - \lfloor \frac{j}{2} \rfloor}C_{ij}$, for $i,j = 0, \ldots, N$. This translates the claims into certain inequalities for $\nu_2(C_{ij})$.

a) The assertion means that $\nu_2(C'_{ij}) \geq 0$, for $i,j = 0, \ldots, N$, which is equivalent to $\nu_2(C_{ij}) \geq \lfloor \frac{j}{2} \rfloor - \lfloor \frac{i}{2} \rfloor$. By assumption, one has $\nu_2(C_{ij}) \geq 0$, so that, for $i \geq j$, there is nothing left to be shown. For $i < j$, the inequality $\nu_2(C_{ij}) \geq \lfloor \frac{j}{2} \rfloor - \lfloor \frac{i}{2} \rfloor$ indeed holds, due to Lemma 4.13.a).

b) Here, the assertion means $\nu_2(C'_{ij}) \geq e$, for $i,j = 0, \ldots, N$, and is equivalent to $\nu_2(C_{ij}) \geq e + \lfloor \frac{j}{2} \rfloor - \lfloor \frac{i}{2} \rfloor$. As $\nu_2(C_{ij}) \geq e$ holds by assumption, the case that $i \geq j$ does not need any further consideration. Moreover, for $i < j$, the assertion follows from Lemma 4.13.b). $\square$

Proof of **Theorem 4.3.** Let Γ be any $\mathbb{Z}_2$-lattice. In order to prove that Theorem 4.3 holds for Γ, by Lemma 4.17, it suffices to show that exactly the same statement holds for the $\mathbb{Z}_2$-lattice Γ'. To actually treat Γ', note that, by construction, the bilinear form b' on Γ' is of the form $b'_0 \oplus 2b'_1 \oplus b'_2 \oplus 2b'_2 \oplus \cdots \oplus 2^{N-2\lfloor \frac{N}{2} \rfloor}b'_N$, for regular $\mathbb{Z}_2$-lattices (Γ'_0, b'_0), $\ldots$, (Γ'_N, b'_N). Thus, Γ' allows a decomposition $\Gamma' = \Gamma''_0 \oplus \Gamma''_1$ with $b' = b''_0 \oplus 2b''_1$, for regular lattices (Γ''_0, b''_0) and (Γ''_1, b''_1). But for exactly this particular case, the assertion of Theorem 4.3 is established by Proposition 4.15. $\square$

5. The point counting algorithm

Input. i) Let a scheme S' be given that is presented as a double cover of $\mathbf{P}^2_\mathbb{Z}$ branched over the union of six lines, each of which is defined over $\operatorname{Spec}\mathbb{Z}$. Suppose that no three of these lines have a $\mathbb{Q}$-rational point in common, and let S be the blowing-up of S' in the Zariski closure, equipped with the induced reduced scheme structure, of the singular locus of the generic fibre $S'_\mathbb{Q}$.

Suppose that $\operatorname{Pic}(S_{\overline{\mathbb{Q}}})$ is a trivial $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module in the case that $\operatorname{rk}\operatorname{Pic}(S_{\overline{\mathbb{Q}}}) \geq 16$, as well.

ii) Moreover, let a bound B be given.

Then the algorithm below computes $\#S(\mathbb{F}_p)$, for all good primes $p < B$ of S.

Algorithm 5.1. A) *Initialisation.*

i) Calculate the odd primes $p_1, \ldots, p_b$, at which S has bad reduction. In terms of these, declare the map

$$\varrho\colon \mathbb{P}\backslash\{2, p_1, \ldots, p_b\} \to \{\pm 1\}^{b+2}, \quad p \mapsto ((\tfrac{-1}{p}), (\tfrac{2}{p}), (\tfrac{p_1}{p}), \ldots, (\tfrac{p_b}{p}))\,.$$

ii) For each $\sigma \in \{\pm 1\}^{b+2}$, run through $\mathbb{P}\backslash\{2, p_1, \ldots, p_b\}$ from below, until a prime l_σ is found of the kind that $\varrho(l_\sigma) = \sigma$. Then count $\#S(\mathbb{F}_{l_\sigma})$ by a naive method. From the point count, derive $(\operatorname{Tr}(\operatorname{Frob}_{l_\sigma}\colon \operatorname{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2) \to \operatorname{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)) \bmod 16)$ using the Lefschetz trace formula (8) and store this value in a table.

Remark 5.2. As the action of $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $\operatorname{Pic}(S_{\overline{\mathbb{Q}}}) \otimes_\mathbb{Z} \mathbb{Q}$ is known to be trivial, formula (8) allows, of course, to calculate $\operatorname{Tr}(\operatorname{Frob}_{l_\sigma}\colon \operatorname{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2) \to \operatorname{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2))$ from $\#S(\mathbb{F}_{l_\sigma})$ exactly. But only the residue class modulo 16 is of importance. Which is exactly the information that is stored.

Indeed, let p be a possibly large prime. Then, the value $\sigma = \varrho(p) \in \{\pm 1\}^{b+2}$ completely determines the action of Frob_p on $\operatorname{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)/4\operatorname{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)$, according to Corollary 3.10. I.e., the action of Frob_p coincides with that of $\operatorname{Frob}_{l_\sigma}$. Furthermore, by Theorem 4.1.a), this is enough to fix the trace modulo 16 on $\operatorname{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)$. I.e.,

$$\operatorname{Tr}(\operatorname{Frob}_p\colon \operatorname{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2) \to \operatorname{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)) \equiv \operatorname{Tr}(\operatorname{Frob}_{l_\sigma}\colon \operatorname{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2) \to \operatorname{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)) \pmod{16}\,,$$

the residue class on the right hand side being the one that was stored. Cf. part B) of the algorithm.

Remark 5.3. The calculation of the bad primes in step A.i) involves the factorisation of a discriminant. A failure in this step would prevent the algorithm from proceeding. In our present implementation, this does not present any difficulty, as the discriminant for the family of double covers of $\mathbf{P}^2$ branched over six lines is highly reducible [Yo, Def. 7.7 and Lemma 7.8], cf. Remark 2.4.b). Step A.i) might, however, become an issue when trying to carry over the algorithm to other types of surfaces. This may concern other families of $K3$ surfaces, already.

5.4. The initialisation as described above ignores the group structure. It determines $(\operatorname{Tr}(\sigma\colon \operatorname{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2) \to \operatorname{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)) \bmod 16)$ individually, for every element of

$\mathrm{Gal}(K/\mathbb{Q})$, where $K := \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{p_1}, \ldots, \sqrt{p_b})$. The number of these elements is exponential in the number b of odd bad primes.

A more efficient approach is as follows. To simplify notation, put $p_{-1} := -1$ and $p_0 := 2$. Moreover, let $\sigma_{-1}, \sigma_0, \sigma_1, \ldots, \sigma_b \in \mathrm{Gal}(K/\mathbb{Q})$ be the standard generators. I.e.,

$$\sigma_i(\sqrt{p_j}) = \begin{cases} \sqrt{p_j}\,, & \text{if } j \neq i,\ j \in \{-1, 0, 1, \ldots, b\}\,, \\ -\sqrt{p_j}\,, & \text{if } j = i\,, \end{cases}$$

for $i \in \{-1, 0, 1, \ldots, b\}$. Every element $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ may then uniquely be described by some sequence $s \in \{0,1\}^{b+2}$, indexed from (-1) to b,

$$\sigma = \sigma_{-1}^{s_{-1}} \sigma_0^{s_0} \sigma_1^{s_1} \cdots \sigma_b^{s_b}\,.$$

Or, $\sigma = \prod_{i \in M_s} \sigma_i$, for $M_s := \{i \in \{-1, \ldots, b\} \mid s_i = 1\}$.

With respect to a basis of $\mathrm{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)$, each generator $\sigma_i \in \mathrm{Gal}(K/\mathbb{Q})$ yields a matrix $E_n + 2A_i$, with $A_i \in \mathrm{M}_{n \times n}(\mathbb{Z}_2)$, encoding the action on $\mathrm{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)$. A product $\sigma_{-1}^{s_{-1}} \cdots \sigma_b^{s_b}$ then corresponds to the matrix

$$(E_n + 2A_{-1})^{s_{-1}} \cdots (E_n + 2A_b)^{s_b}\,,$$

the trace of which modulo 16 is given by

$$\begin{aligned} \mathrm{Tr}((E_n + 2A_{-1})^{s_{-1}} \cdots (E_n + 2A_b)^{s_b}) \equiv n + 2 \sum_{i \in M_s} \mathrm{Tr}(A_i) + 4 \sum_{\substack{i,j \in M_s, \\ i < i'}} \mathrm{Tr}(A_i A_{i'}) \\ + 8 \sum_{\substack{i,i',i'' \in M_s, \\ i < i' < i''}} \mathrm{Tr}(A_i A_{i'} A_{i''}) \pmod{16}\,. \quad (21) \end{aligned}$$

Based on (21), the traces modulo 8 of all matrices A_i, together with the traces modulo 4 of all products $A_i A_{i'}$ and the traces modulo 2 of all triple products $A_i A_{i'} A_{i''}$, can be determined efficiently by solving a system of linear congruences. This can be described as an algorithm as follows.

Algorithm (continued)**.** A') *Initialisation. A more efficient approach – First step.* Let l run through $\mathbb{P} \backslash \{2, p_1, \ldots, p_b\}$ from below. Each time, do the following.

i) Compute $\varrho(l)$. I.e., determine a presentation of $\mathrm{Frob}_l \in \mathrm{Gal}(K/\mathbb{Q})$ as a product $\sigma_{-1}^{s_{-1}} \cdots \sigma_b^{s_b}$ of some of the standard generators.

ii) Count $\#S(\mathbb{F}_l)$ by a naive method. Derive

$$\begin{aligned} (\mathrm{Tr}((E_n + 2A_{-1})^{s_{-1}} \cdots (E_n + 2A_b))^{s_b} \bmod 16) = \\ (\mathrm{Tr}(\mathrm{Frob}_l \colon \mathrm{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2) \to \mathrm{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)) \bmod 16) \end{aligned}$$

from this value using the Lefschetz trace formula (8).

iii) According to formula (21) above, write down a linear congruence involving all $\mathrm{Tr}(A_i)$, $\mathrm{Tr}(A_i A_{i'})$, and $\mathrm{Tr}(A_i A_{i'} A_{i''})$, for $-1 \leq i \leq b$, $-1 \leq i < i' \leq b$, and $-1 \leq i < i' < i'' \leq b$, respectively. Add this congruence to the system of congruences already obtained.

iv) Check whether the system of linear congruences obtained for $(\mathrm{Tr}(A_i) \bmod 8)$, $(\mathrm{Tr}(A_iA_{i'}) \bmod 4)$, and $(\mathrm{Tr}(A_iA_{i'}A_{i''}) \bmod 2)$, for $-1 \leq i \leq b$, $-1 \leq i < i' \leq b$, and $-1 \leq i < i' < i'' \leq b$, respectively, is uniquely solvable. If this is the case then compute the solution, store it, and terminate Step A').

A") *Initialisation. A more efficient approach – Second step.*

Let s run through the elements of $\{0,1\}^{b+2}$. Each time, determine

$$\mathrm{T}(s) := (\mathrm{Tr}((E_n + 2A_{-1})^{s_{-1}} \cdots (E_n + 2A_b)^{s_b}) \bmod 16)$$

using formula (21) and the stored values of $(\mathrm{Tr}(A_i) \bmod 8)$, $(\mathrm{Tr}(A_iA_{i'}) \bmod 4)$, and $(\mathrm{Tr}(A_iA_{i'}A_{i''}) \bmod 2)$. Store the value in a table.

B) *Point counting.*

Let p run through $\mathbb{P}\backslash\{2, p_1, \dots, p_b\}$ from below up to B. Each time, do the following.

i) Compute $s := \varrho(p)$, which means to the determine $\mathrm{Frob}_p \in \mathrm{Gal}(K/\mathbb{Q})$.

ii) Look up the corresponding value $\mathrm{T}(s)$ in the precomputed table. This is just $(\mathrm{Tr}(\mathrm{Frob}_p\colon\ \mathrm{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2) \to \mathrm{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)) \bmod 16)$.

Applying the Lefschetz trace formula (8), calculate $(\#S(\mathbb{F}_p) \bmod 16)$ from this value.

iii) Use a p-adic Harvey style algorithm [Ha] to compute $(\#S(\mathbb{F}_p) \bmod p)$.

iv) Use the Chinese remainder theorem to calculate the class $(\#S(\mathbb{F}_p) \bmod 16p)$ from $(\#S(\mathbb{F}_p) \bmod 16)$ and $(\#S(\mathbb{F}_p) \bmod p)$.

v) Determine the unique representative of this residue class modulo $16p$ that is compatible with Deligne's bound (4) for $\#S(\mathbb{F}_p)$ and output this number.

Remarks 5.5 (On the assumptions made on S). i) The assumptions made on the intersection points of the six lines imply that the generic fibre $S_{\mathbb{Q}}$ of S is nonsingular, i.e. a $K3$ surface. Moreover, as the lines are assumed to be defined over $\mathbb{Z}$, Corollary 3.8.a) shows that the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $\mathrm{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)/2\,\mathrm{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)$ is trivial. The assumption on $\mathrm{Pic}(S_{\overline{\mathbb{Q}}})$ is automatically fulfilled if $\mathrm{rk}\,\mathrm{Pic}(S_{\overline{\mathbb{Q}}}) = 16$.

ii) The algorithm as described immediately carries over to other types of $K3$ surfaces, as soon as the actions of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $\mathrm{Pic}(S_{\overline{\mathbb{Q}}})$ and $\mathrm{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)/2\,\mathrm{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)$ are trivial.

iii) A further generalisation is possible to $K3$ surfaces, for which the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $\mathrm{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)/2\,\mathrm{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)$ is trivial and that on $\mathrm{Pic}(S_{\overline{\mathbb{Q}}})$ is explicitly known. Indeed, the triviality of $\mathrm{Pic}(S_{\overline{\mathbb{Q}}})$ is only used in the references to the Lefschetz trace formula (8).

iv) Finally, one might want to consider the case when both $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-actions, that on $\mathrm{Pic}(S_{\overline{\mathbb{Q}}})$ and that on $\mathrm{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)/2\,\mathrm{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)$, are nontrivial, but explicitly known. At least when the action on $\mathrm{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)/2\,\mathrm{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)$ is of exponent 2, a modification of Algorithm 5.1 is possible, which is based on Theorem 4.1.b). It may determine $\mathrm{Tr}(\mathrm{Frob}_p\colon\ \mathrm{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2) \to \mathrm{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)$ only modulo 8.

The idea is as follows. Let the number field F be the known splitting field of $\mathrm{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)/2\,\mathrm{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)$. Then the Galois action on $\mathrm{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)/4\,\mathrm{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)$ factors via $\mathrm{Gal}(K/\mathbb{Q})$, for K the maximal abelian extension of F of exponent 2, ramified only at the primes above 2 and the bad primes of S. This is a ray class field over F and thus, in principle, accessible to computation. Cf. Section 6 for an example.

Remark 5.6 (Initialisation). Among $S_1, \dots, S_4$, the surface S_1 is the one having the most bad primes. There are actually six bad primes $p \neq 2$. Thus, the direct initialisation requires to count the points for 256 primes. As all elements of $\{\pm 1\}^8$ have to be hit, the largest prime to be used would be 21 121.

The more efficient approach needs to solve a system of linear congruences in 92 variables. Thus, it requires the point count only for 92 primes. As the elements of $\{\pm 1\}^8$ to be hit by Frob_p are otherwise arbitrary, we could get by working with the primes up to 593.

Remark 5.7. Note that, in our examples, we always have $2^{b+2} \leq 256$ in comparison to $B = 10^8$. For other samples with many more bad primes, so that $2^b \gg B$, one might want to optimise by reversing steps A") and B). I.e., to calculate the values $\mathrm{T}(\varrho(p))$ separately for each prime.

Remark 5.8 (Practical performance). i) For each of the surfaces $S_1, \dots, S_4$, running up to $B = 10^8$, our implementation used about 20 GB of memory and between 8 and 12 hours of CPU time on one core of an Intel i7-7700 processor running at 3.6 GHz.

This running time is completely dominated by the modulo p point count, for which we ran a variant of a Harvey style algorithm in p-adic precision 1 with remainder tree implemented for this particular project. Note that our implementation is in `magma`, not in a compiled language. And that, presumably, some of the possible optimisations are still missing. Cf. [EJ16, Sections 3 and 4] for a description of an earlier implementation.

ii) The initialisation, as described in A') and A"), took less than one minute per surface. More precisely, for the surface S_1, the naive point counting had to be done for 92 primes, which took around 49 seconds. For all other steps of the initialisation together, including the linear algebra calculations, the `magma` profiler reports a running time of 2.5 seconds. For the surfaces S_2, S_3, and S_4, the initialisation runs faster by a factor of at least 10, because there are fewer bad primes.

The actual modulo 16 point counting mainly required Legendre symbol computations for the slightly more than 5.7 million primes up to $B = 10^8$, which took only 23 seconds per surface. Finally, the determination of the point counts modulo $16p$ took 5 seconds, which are essentially accounted for the computations related to the Chinese remainder theorem.

Remark 5.9 (Point counting modulo p^2 versus modulo p). i) p-adic point counting for a surface of the shape $w^2 = xyzf_3(x,y,z)$ requires to do the following: In order to count modulo p, one has to compute the coefficient at $(xyz)^{(p-1)/2}$ in $f_3^{(p-1)/2}$ with p-adic precision 1. In all our examples, the moving simplex approach (cf. [EJ16, Remark 4.8]) never resulted in a loss of p-adic precison. Thus, we were able to work with p-adic precision 1 during all the intermediate steps.

On the other hand, for point counting modulo p^2, one has to compute the coefficient at $(xyz)^{(p-1)/2}$ in $f_3^{(p-1)/2}$ with p-adic precision 2 and, furthermore, the coefficient at $x^{i(p-1)/2}y^{j(p-1)/2}z^{k(p-1)/2}$ in $f_3^{3(p-1)/2}$, for every triple $(i,j,k) \in \mathbb{N}^3$ of odd numbers such that $i+j+k=9$. Thus, instead of computing one coefficient, one has to compute eleven. Assuming that this can be done without p-adic precision loss, one can work with p-adic precision 2 during all the intermediate steps. This indicates that one has to expect an increase of the run time by at least a factor of 22.

As the exponent in $f_3^{3(p-1)/2}$ is increased by a factor of 3 compared to $f_3^{(p-1)/2}$, a naive implementation would slow down the process even more, in the worst case by another factor of 3. However, a better implementation using multipoint evaluation techniques [vGG, Section 10.1] might reduce this factor significantly.

ii) For checking correctness, we implemented a simple p-adic point counting with p-adic precision 2 that does not use advanced techniques such as the remainder tree. This implementation took about one day of CPU time per surface, running only to $B = 10^5$. It is important to note, however, that this is not a fair comparison, since too many optimisations were missing.

Remarks 5.10 (Results). a) The main outcome of our computations are the histograms presented in [EJ21, Section 5].

b) The distribution of the traces modulo 16 relative to the elements in $\{\pm1\}^{b+2}$, as indicated in the table below, appears to be rather erratic.

Residue mod 16	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S_1	46	0	44	0	32	0	26	0	18	0	36	0	32	0	22	0
S_2	0	0	7	0	0	0	7	0	0	0	9	0	0	0	9	0
S_3	0	20	0	0	0	28	0	0	0	4	0	0	0	12	0	0
S_4	8	0	2	0	0	0	4	0	0	0	2	0	0	0	0	0

TABLE 1. Number of elements of $\{\pm1\}^{b+2}$ for each residue mod16

Nevertheless, there are a few more observations that should perhaps be noticed.

i) For instance, for S_3, it happens that $(\mathrm{Tr}(\mathrm{Frob}_p\colon \mathrm{T}(S_{\overline{\mathbb{Q}}},\mathbb{Z}_2) \to \mathrm{T}(S_{\overline{\mathbb{Q}}},\mathbb{Z}_2)) \bmod 16)$ is independent of the Legendre symbol $(\frac{2}{p})$. For S_4, it suffices to consider $(\frac{6}{p})$, instead of $(\frac{2}{p})$ and $(\frac{3}{p})$ individually. These, however, are the only regularities that occurred above those predicted by Corollary 3.10.

ii) (Explanation of the zeroes in Table 1) For p odd, a double cover of $\mathbf{P}^2_{\mathbb{F}_p}$, branched over six $\mathbb{F}_p$-rational lines in general position, has an odd number of points, since the branch locus has. This yields that $\mathrm{Tr}(\mathrm{Frob}_p\colon \mathrm{T}(S_{\overline{\mathbb{Q}}},\mathbb{Z}_2) \to \mathrm{T}(S_{\overline{\mathbb{Q}}},\mathbb{Z}_2))$ is always even in the case of geometric Picard rank 16, and odd, for geometric Picard rank 17.

But more is true. One has that $\det(E_n+2A) = \pm1$ implies $1+2\,\mathrm{Tr}(A) \equiv \pm1 \pmod 4$ and therefore $\mathrm{Tr}(E_n+2A) \equiv n-1\pm1 \pmod 4$. This explains why, for S_1

and S_4, there are equally many elements of $\{\pm 1\}^{b+2}$ leading to traces $(0 \bmod 4)$ and $(2 \bmod 4)$.

The surfaces S_2 and S_3, however, have trivial jump characters [CEJ], so that $\det(\mathrm{Frob}_p\colon \mathrm{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2) \to \mathrm{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)) = +1$, for every prime p. This explains why only traces $(2 \bmod 4)$ occur for S_2 and only traces $(1 \bmod 4)$ for S_3.

Finally, for every $p \equiv 3 \pmod 4$, $\mathrm{Tr}(\mathrm{Frob}_p\colon \mathrm{T}(S_{4,\overline{\mathbb{Q}}}, \mathbb{Z}_2) \to \mathrm{T}(S_{4,\overline{\mathbb{Q}}}, \mathbb{Z}_2)) = 0$ holds exactly. This is the spike in [EJ21, Figure 3]. On the other hand, for $p \equiv 1 \pmod 4$, one has $\det(\mathrm{Frob}_p\colon \mathrm{T}(S_{4,\overline{\mathbb{Q}}}, \mathbb{Z}_2) \to \mathrm{T}(S_{4,\overline{\mathbb{Q}}}, \mathbb{Z}_2)) = +1$, so that only traces $(2 \bmod 4)$ are allowed. The non-occurrence of traces $(14 \bmod 16)$ seems to be explained only by the fact that $b = 2$ is very small.

6. A more advanced example – A surface with real multiplication

This section is devoted to the surface S_5 from Example 2.2.v).

6.1 (Properties of the surface)**.** i) This surface is [EJ21, Example 5.8]. Also, S_5 is isomorphic to the specialisation to $t = 0$ of the family described in [EJ20a, Example 1.5]. In particular, $\mathrm{rk}\,\mathrm{Pic}(S_{5,\overline{\mathbb{Q}}}) = 16$ and $S_5(\mathbb{C})$ has real multiplication by $\mathbb{Q}(\sqrt{5})$.

ii) The surface $S'_{5,\mathbb{Q}}$ is a double cover of $\mathbf{P}^2_{\mathbb{Q}}$, branched geometrically over six lines, any three of which do not have a geometric point in common. Two of these lines are defined over $\mathbb{Q}$, while the other four are defined over $\mathbb{Q}(\zeta_5)$ and permuted cyclically by $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$.

By Theorem 3.12.a.i) and b), $\mathrm{Pic}(S_{5,\overline{\mathbb{Q}}})$ contains a sublattice of full rank that is a linear permutation representation of $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$. The underlying permutation representation has one fixed point and is otherwise the action on pairs of six objects, two of which are fixed while the others form a 4-cycle. Thus, in total, there are three orbits of size four each, one orbit of size two, and two fixed points. I.e.,

$$\mathrm{Tr}(\sigma\colon \mathrm{Pic}(S_{5,\overline{\mathbb{Q}}})\otimes_{\mathbb{Z}}\mathbb{Q} \to \mathrm{Pic}(S_{5,\overline{\mathbb{Q}}})\otimes_{\mathbb{Z}}\mathbb{Q}) = \begin{cases} 16\,, & \text{if } \mathrm{ord}(\sigma) = 1\,, \\ 4\,, & \text{if } \mathrm{ord}(\sigma) = 2\,, \\ 2\,, & \text{if } \mathrm{ord}(\sigma) = 4\,. \end{cases} \qquad (22)$$

iii) For every good prime $p \equiv 2, 3 \pmod 5$, one has

$$\#S_5(\mathbb{F}_p) = p^2 + 2p + 1$$

by [EJ20a, Lemma 6.7]. This means that $\mathrm{Tr}(\mathrm{Frob}_p\colon \mathrm{T}(S_{5,\overline{\mathbb{Q}}}, \mathbb{Z}_2) \to \mathrm{T}(S_{5,\overline{\mathbb{Q}}}, \mathbb{Z}_2)) = 0$.

iv) In other words, only the good primes $p \equiv 1, 4 \pmod 5$ need consideration in this example. For these, according to (22) and (8), one has

$$\#S_5(\mathbb{F}_p) = p^2 + T_{\mathrm{alg}}p + \mathrm{Tr}(\mathrm{Frob}_p\colon \mathrm{T}(S_{5,\overline{\mathbb{Q}}}, \mathbb{Z}_2) \to \mathrm{T}(S_{5,\overline{\mathbb{Q}}}, \mathbb{Z}_2))p + 1\,, \qquad (23)$$

for

$$T_{\mathrm{alg}} := \begin{cases} 16\,, & \text{if } p \equiv 1 \pmod 5\,, \\ 4\,, & \text{if } p \equiv 4 \pmod 5\,. \end{cases}$$

6.2 (The $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action on $\mathrm{T}(S_{5,\overline{\mathbb{Q}}},\mathbb{Z}_2)/2\,\mathrm{T}(S_{5,\overline{\mathbb{Q}}},\mathbb{Z}_2)$)**.**
Theorem 3.12.a.i) and b), together with Theorem 3.5, provides an explicit description of $\mathrm{T}(S_{\overline{\mathbb{Q}}},\mathbb{Z}_2)/2\,\mathrm{T}(S_{\overline{\mathbb{Q}}},\mathbb{Z}_2)$ as a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module. The results are as follows.

i) The $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action on $\mathrm{Br}(S_{\overline{\mathbb{Q}}})_2$ factors via $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$, which is cyclic of order four.

ii) With respect to a suitable basis, the action of a generator of $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ on $\mathrm{Br}(S_{\overline{\mathbb{Q}}})_2$ is given by the matrix

$$\begin{pmatrix} 1&1&1&0&1&1\\ 0&1&1&1&1&1\\ 1&0&1&1&1&1\\ 1&1&0&1&1&1\\ 1&1&1&1&0&1\\ 1&1&1&1&1&0 \end{pmatrix}.$$

Thus, the action of the element of order two is given by

$$\begin{pmatrix} 0&1&0&0&0&0\\ 1&0&0&0&0&0\\ 0&0&0&1&0&0\\ 0&0&1&0&0&0\\ 0&0&0&0&1&0\\ 0&0&0&0&0&1 \end{pmatrix}. \tag{24}$$

iii) By Theorem 3.5, one has $\mathrm{T}(S_{\overline{\mathbb{Q}}},\mathbb{Z}_2)/2\,\mathrm{T}(S_{\overline{\mathbb{Q}}},\mathbb{Z}_2)\cong(\mathrm{Br}(S_{\overline{\mathbb{Q}}})_2)^\vee$. The action on $\mathrm{T}(S_{\overline{\mathbb{Q}}},\mathbb{Z}_2)/2\,\mathrm{T}(S_{\overline{\mathbb{Q}}},\mathbb{Z}_2)$ is therefore provided by the transposed inverses of the matrices given.

6.3 (The $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action on $\mathrm{T}(S_{\overline{\mathbb{Q}}},\mathbb{Z}_2)/4\,\mathrm{T}(S_{\overline{\mathbb{Q}}},\mathbb{Z}_2)$)**.**
As the Galois action on $\mathrm{T}(S_{\overline{\mathbb{Q}}},\mathbb{Z}_2)/2\,\mathrm{T}(S_{\overline{\mathbb{Q}}},\mathbb{Z}_2)$ factors via $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$, the action on $\mathrm{T}(S_{\overline{\mathbb{Q}}},\mathbb{Z}_2)/4\,\mathrm{T}(S_{\overline{\mathbb{Q}}},\mathbb{Z}_2)$ factors via $\mathrm{Gal}(K/\mathbb{Q})$, for K the maximal abelian extension of $\mathbb{Q}(\zeta_5)$ of exponent 2, ramified only at 2 and the prime above 5. It is not hard to see that

$$K=\mathbb{Q}(\sqrt{-1},\sqrt{2},\zeta_5,\sqrt{\zeta_5-1},\sqrt{\zeta_5^2-1}). \tag{25}$$

Note here that the prime above 5 is (ζ_5-1). Moreover, the unit group $\mathbb{Z}[\zeta_5]^*$ is generated by the cyclotomic unit $\frac{\zeta_5^2-1}{\zeta_5-1}=\zeta_5+1$, together with $(-\zeta_5)$.

6.4 (Adaptation of the point counting algorithm)**.**
Suppose a good prime $p\equiv 1,4 \pmod 5$ to be given. Then one determines the conjugacy class Frob_p in $\mathrm{Gal}(K/\mathbb{Q})$. As before, there is a small prime l such that Frob_l is the same class. By the construction of K, this means that the action of Frob_p on $\mathrm{T}(S_{5,\overline{\mathbb{Q}}},\mathbb{Z}_2)/4\,\mathrm{T}(S_{5,\overline{\mathbb{Q}}},\mathbb{Z}_2)$ agrees with that of Frob_l. Moreover, one may look up the value $(\mathrm{Tr}(\mathrm{Frob}_l\colon \mathrm{T}(S_{5,\overline{\mathbb{Q}}},\mathbb{Z}_2)\to\mathrm{T}(S_{5,\overline{\mathbb{Q}}},\mathbb{Z}_2)) \bmod 16)$ in a precomputed table. Let us now distinguish between the two cases.

Case 1: $p\equiv 4\pmod 5$. Then $\mathrm{Frob}_p\in\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ is the element of order two. Correspondingly, the action of Frob_p on $\mathrm{T}(S_{5,\overline{\mathbb{Q}}},\mathbb{Z}_2)/2\,\mathrm{T}(S_{5,\overline{\mathbb{Q}}},\mathbb{Z}_2)$ is not trivial, cf. (24), but that of Frob_p^2 is. Hence, Theorem 4.1.b) applies and shows that

$$\begin{aligned}&\mathrm{Tr}(\mathrm{Frob}_p\colon \mathrm{T}(S_{5,\overline{\mathbb{Q}}},\mathbb{Z}_2)\to\mathrm{T}(S_{5,\overline{\mathbb{Q}}},\mathbb{Z}_2))\equiv\\ &\qquad\qquad\mathrm{Tr}(\mathrm{Frob}_l\colon \mathrm{T}(S_{5,\overline{\mathbb{Q}}},\mathbb{Z}_2)\to\mathrm{T}(S_{5,\overline{\mathbb{Q}}},\mathbb{Z}_2)) \pmod 8.\end{aligned}$$

Thus, the precomputation determines $(\mathrm{Tr}(\mathrm{Frob}_p\colon \mathrm{T}(S_{5,\overline{\mathbb{Q}}}, \mathbb{Z}_2) \to \mathrm{T}(S_{5,\overline{\mathbb{Q}}}, \mathbb{Z}_2)) \bmod 8)$, and therefore $(\#S_5(\mathbb{F}_p) \bmod 8)$, when taking (23) into consideration. Combining this with a point count modulo p, one may easily compute $(\#S_5(\mathbb{F}_p) \bmod 8p)$.

Recall at this point that $S_5(\mathbb{C})$ has real multiplication by a quadratic number field. This causes the algebraic monodromy group to be significantly smaller than usual. Concretely, the Zariski closure of the image of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ in $\mathrm{Aut}(\mathrm{T}(S_{\overline{\mathbb{Q}}}, \overline{\mathbb{Q}}_2))$ is isomorphic to $[\mathrm{O}_3(\overline{\mathbb{Q}}_2)]^2$, and not to $\mathrm{O}_6(\overline{\mathbb{Q}}_2)$. Moreover, as $p \equiv 4 \pmod 5$, the action of Frob_p lies in $[\mathrm{O}_3^-(\overline{\mathbb{Q}}_2)]^2$ [EJ21, Theorem 5.9]. In particular, two of the six eigenvalues are bound to be (-1).

Denoting the other eigenvalues by $\lambda_1, \ldots, \lambda_4$, formula (23) takes the form

$$\#S_5(\mathbb{F}_p) = p^2 + (2 + \lambda_1 + \lambda_2 + \lambda_3 + \lambda_4)p + 1\,.$$

As $|\lambda_i| = 1$, for $i = 1, \ldots, 4$, this shows that $(\#S_5(\mathbb{F}_p) \bmod 8p)$ uniquely determines $\#S_5(\mathbb{F}_p)$, except for the two edge cases $\lambda_1 = \cdots = \lambda_4 = 1$ and $\lambda_1 = \cdots = \lambda_4 = -1$, which seem indistinguishable. However, the second of these does not occur, due to the Lemma below.

Lemma 6.5. *Let p be an odd prime number and S a $K3$ surface over $\mathbb{F}_p$ as in 2.1. Suppose that Frob_p acts on the six lines as a permutation of order at most two. Then, among the six eigenvalues of Frob_p on the orthogonal complement of $\pi^*[l]$, $\pi^*[e_{12}]$, …, $\pi^*[e_{56}]$ in $H^2_{\text{ét}}(S_{\overline{\mathbb{F}}_p}, \mathbb{Z}_2(1))$, at least one is not equal to (-1).*

Proof. Assume the contrary. Then, for the arithmetic Picard group of S, one has $\mathrm{Pic}(S) \otimes_{\mathbb{Z}} \mathbb{Q} \subseteq \mathbb{Q}\pi^*[l] \oplus \mathbb{Q}\pi^*[e_{12}] \oplus \cdots \oplus \mathbb{Q}\pi^*[e_{56}]$. An orthogonal basis is provided by the class $\pi^*[l]$, the classes $\pi^*[e_{ij}]$ being invariant under Frob_p, and the classes $\pi^*[e_{ij}] + \pi^*[e_{i'j'}]$ formed by an orbit of size two. The self-intersection numbers of these are equal to 2, (-2), and (-4), respectively, so that the discriminant of $\mathrm{Pic}(S)$ as a quadratic space is $(\pm\overline{1})$ or $(\pm\overline{2}) \in \mathbb{Q}^*/\mathbb{Q}^{*2}$.

On the other hand, according to the Artin–Tate formula [Mi, Theorem 6.1], the value of this discriminant may be calculated as $\overline{\pm p \cdot \prod_{\lambda \neq 1}(1-\lambda)}$, the product being taken over all eigenvalues $\lambda \neq 1$ of Frob_p on $H^2_{\text{ét}}(S_{\overline{\mathbb{F}}_p}, \mathbb{Z}_2(1))$, counted with multiplicities. However, according to our assumptions, every eigenvalue $\neq 1$ of Frob_p is (-1), which enforces the discriminant of $\mathrm{Pic}(S)$ to be $(\pm\overline{p})$ or $(\pm\overline{2p})$. A contradiction. $\square$

Case 2: $p \equiv 1 \pmod 5$. This case is easier. One has that $\mathrm{Frob}_p \in \mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ is the neutral element. Consequently, the action of Frob_p on $\mathrm{T}(S_{5,\overline{\mathbb{Q}}}, \mathbb{Z}_2)/2\,\mathrm{T}(S_{5,\overline{\mathbb{Q}}}, \mathbb{Z}_2)$ is trivial, so that Theorem 4.1.a) applies and shows

$$\begin{aligned}\mathrm{Tr}(\mathrm{Frob}_p\colon\ &\mathrm{T}(S_{5,\overline{\mathbb{Q}}}, \mathbb{Z}_2) \to \mathrm{T}(S_{5,\overline{\mathbb{Q}}}, \mathbb{Z}_2)) \equiv \\ &\mathrm{Tr}(\mathrm{Frob}_l\colon\ \mathrm{T}(S_{5,\overline{\mathbb{Q}}}, \mathbb{Z}_2) \to \mathrm{T}(5, S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)) \pmod{16}\,.\end{aligned}$$

I.e., the precomputed value fixes $(\mathrm{Tr}(\mathrm{Frob}_p\colon\ \mathrm{T}(S_{5,\overline{\mathbb{Q}}}, \mathbb{Z}_2) \to \mathrm{T}(S_{5,\overline{\mathbb{Q}}}, \mathbb{Z}_2)) \bmod 16)$ and therefore $(\#S_5(\mathbb{F}_p) \bmod 16)$. Combining this with a modulo p point count, one may compute $(\#S_5(\mathbb{F}_p) \bmod 16p)$. And, similarly to (4), this is enough to completely determine $\#S_5(\mathbb{F}_p)$. Note that, in formula (23), the trace of Frob_p is bounded by 6 in absolute value.

Remark 6.6. The information on $(\#S_5(\mathbb{F}_p) \bmod 8p)$ suffices to determine $\#S_5(\mathbb{F}_p)$ in Case 2, as well. Indeed, real multiplication causes two further eigenvalues $(+1)$, so that one has $\#S_5(\mathbb{F}_p) = p^2 + (18 + \lambda_1 + \lambda_2 + \lambda_3 + \lambda_4)p + 1$. This shows that, again, only the two edge cases seem indistinguishable. But 22 eigenvalues $(+1)$ are impossible for a $K3$ surface over the prime field $\mathbb{F}_p$, for $p \neq 2$, [Ar, (6.8)].

Remark 6.7 (Practical performance). The total running time for S_5 was around 58 hours, which is a lot more than for the other examples. Cf. Remark 5.8.

The difference comes mainly from the p-adic algorithm. In fact, for a surface given by $W^2 = f_6(T_1, T_2, T_3)$ as a double cover of $\mathbf{P}^2_{\mathbb{F}_p}$, the number of $\mathbb{F}_p$-rational points modulo p depends only on the coefficient at $T_1^{p-1}T_2^{p-1}T_3^{p-1}$ of $f_6^{(p-1)/2}$. Therefore, for $f_6 = T_1T_2T_3f_3$, one only needs to compute the coefficient at $T_1^{(p-1)/2}T_2^{(p-1)/2}T_3^{(p-1)/2}$ of $f_3^{(p-1)/2}$. Our implementation makes systematic use of this simplification, which applies to S_1, S_2, S_3, and S_4.

However, the equation of S_5 only has the form $f_6 = T_1T_2f_4$, so that the coefficient at $T_1^{(p-1)/2}T_2^{(p-1)/2}T_3^{p-1}$ of $f_4^{(p-1)/2}$ is asked for. This computation is more elaborate, so the last example took about five times longer.

Remarks 6.8 (Results). a) The main purpose of our computations for this example was to generate the histogram in [EJ21, Figure 4] to the left.

b) Moreover, our computations show that, in this particular example, the trace $\mathrm{Tr}(\mathrm{Frob}_p\colon \mathrm{T}(S_{5,\overline{\mathbb{Q}}}, \mathbb{Z}_2) \to \mathrm{T}(S_{5,\overline{\mathbb{Q}}}, \mathbb{Z}_2))$ modulo 8 or 16, respectively, is determined by the conjugacy class Frob_p in a field a lot smaller than the field K deduced from the general theory, cf. formula (25). In fact, the following holds.

i) If $p \equiv 4 \pmod 5$ then

$$\mathrm{Tr}(\mathrm{Frob}_p\colon \mathrm{T}(S_{5,\overline{\mathbb{Q}}}, \mathbb{Z}_2) \to \mathrm{T}(S_{5,\overline{\mathbb{Q}}}, \mathbb{Z}_2)) \equiv \begin{cases} 6 \pmod 8\,, & \text{if } (-1) \text{ is a square in } \mathbb{F}_p\,, \\ 2 \pmod 8\,, & \text{otherwise}\,. \end{cases}$$

ii) If $p \equiv 1 \pmod 5$ then

$$\mathrm{Tr}(\mathrm{Frob}_p\colon \mathrm{T}(S_{5,\overline{\mathbb{Q}}}, \mathbb{Z}_2) \to \mathrm{T}(S_{5,\overline{\mathbb{Q}}}, \mathbb{Z}_2)) \equiv$$
$$\begin{cases} 6 \pmod{16}\,, & \text{if } (-1),\ (\zeta_5 - 1), \text{ and } (\zeta_5^2 - 1) \text{ are squares in } \mathbb{F}_p\,, \\ 2 \pmod{16}\,, & \text{if } (-1) \text{ is a square, but } \frac{\zeta_5^2-1}{\zeta_5-1} = \zeta_5 + 1 \text{ is a non-square in } \mathbb{F}_p\,, \\ 14 \pmod{16}\,, & \text{otherwise}\,. \end{cases}$$

Note that these conditions are independent of the choice of the fifth root of unity $\zeta_5 \in \mathbb{F}_p$. Indeed, replacing ζ_5 by ζ_5^2, one finds that only $\frac{\zeta_5^4-1}{\zeta_5-1} = -\zeta^4 = -(\zeta^2)^2$ needs to be identified as being a square.

7. The very general picture

Consider the class of all $K3$ surfaces over $\mathbb{Q}$, or even a different kind of surfaces, but suppose that $H^1_{\text{ét}}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2) = 0$ and that $\operatorname{Pic}(S_{\overline{\mathbb{Q}}})$ is computable as a $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module. Is it then, at least in principle, possible to devise a 2-adic point counting algorithm for such a class of surfaces? This, in essence, means to make the $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module $\mathrm{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)/2^m\,\mathrm{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)$ explicit, for a suitable value of m.

A major portion of the information on the $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module structure is encoded in the splitting field F_m of $\mathrm{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)/2^m\,\mathrm{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)$. This is, by definition, the smallest field allowing a commutative diagram

$$\begin{tikzcd} \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \arrow[r, "\varrho"] \arrow[d] & \operatorname{Aut}(\mathrm{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)/2^m\,\mathrm{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)) \\ \operatorname{Gal}(F_m/\mathbb{Q}) \arrow[ur, "\varrho_{F_m}"] & \end{tikzcd},$$

for ϱ the natural action. One has that F_m is an algebraic number field, for every $n \in \mathbb{N}$.

7.1. One might want to determine the splitting fields F_m inductively. The induction step from m to $m+1$ should work as follows.

One has that $\{A \in \mathrm{GL}_n(\mathbb{Z}/2^{m+1}\mathbb{Z}) \mid A \equiv E_n \pmod{2^m}\}$ is an elementary abelian 2-group, hence F_{m+1}/F_m is always an abelian field extension of exponent 2. Moreover, the smooth specialisation theorem [SGA4, Exposé XVI, Corollaire 2.3] implies that F_{m+1}/F_m is unramified at any prime of odd residue characteristic, except possibly those lying above the prime numbers at which S has bad reduction. In other words, an upper bound for F_{m+1} is provided by a certain ray class field of F_m, which is, at least in principle, amenable to computation.

7.2. On the other hand, the splitting field F_2 of $\mathrm{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)/2\,\mathrm{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)$ is a number field of degree $\leq \#\,\mathrm{GL}_t(\mathbb{F}_2) = 2^{t(t-1)/2}(2^t-1)\cdots(2^1-1)$, for $t := \dim T$, unramified at every odd prime of good reduction of S. There are only finitely many such number fields, according to Minkowski's Theorem [Ne, Theorem III.2.13], and to determine all of them is, in theory, effective. Thus, the composite of all these fields is an upper bound for F_2.

Such an approach, however, appears practically unfeasable under virtually all circumstances. Thus, it seems that, generally speaking, the base case is more complex than the induction step.

Remark 7.3. In order to settle this issue with the base case for the particular family of $K3$ surfaces considered in this article, we decided to apply the isomorphism from Theorem 3.5. This requires to make $\operatorname{Br}(S_{\overline{\mathbb{Q}}})_2$ explicit, for which there is no obvious general approach either. The work of A. N. Skorobogatov [Sk, Theorem 1.1] we use is limited to double covers. Furthermore, it provides, in general, only an exact sequence, which might be non-split in certain cases.

Remark 7.4. Only a subfield of F_m, the *trace field,* is relevant for the algorithm. This is a minimal field K, for which there is a commutative diagram

$$\begin{tikzcd}
\mathrm{Gal}(F_m/\mathbb{Q}) \arrow[r, "\varrho_{F_m}"] \arrow[d] & \mathrm{Aut}(\mathrm{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)/2^m\,\mathrm{T}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_2)) \arrow[d, "\mathrm{Tr}"] \\
\mathrm{Gal}(K/\mathbb{Q}) \arrow[r] & \mathbb{Z}/2^m\mathbb{Z}
\end{tikzcd}.$$

The 2-adic overdetermination phenomenon established in Section 4 indicates that $[K:\mathbb{Q}]$ may be significantly smaller than $[F_m:\mathbb{Q}]$.

References

[Ar] Artin, M.: *Supersingular $K3$ surfaces,* Ann. Sci. École Norm. Sup. **7** (1974), 543–567

[BCP] Bosma, W., Cannon, J., and Playoust, C.: *The Magma algebra system I. The user language,* J. Symbolic Comput. **24** (1997), 235–265

[Ch] Charles, F.: *The Tate conjecture for $K3$ surfaces over finite fields,* Invent. Math. **194** (2013), 119–145

[CS] Conway, J. H. and Sloane, N. J. A.: Sphere packings, lattices and groups, Third edition, Grundlehren der Mathematischen Wissenschaften 290, *Springer,* New York 1999

[CEJ] Costa, E., Elsenhans, A.-S., and Jahnel, J.: *On the distribution of the Picard ranks of the reductions of a $K3$ surface*, Research in Number Theory **6** (2020)art.27

[De74] Deligne, P.: *La conjecture de Weil I,* Publ. Math. IHES **43** (1974), 273–307

[De81] Deligne, P.: *Relèvement des surfaces $K3$ en caractéristique nulle,* Prepared for publication by Luc Illusie, in: Algebraic surfaces (Orsay 1976–78), Lecture Notes in Math. 868, *Springer,* Berlin–New York 1981, 58–79

[DM] Dixon, J. D. and Mortimer, B.: Permutation groups, Graduate Texts in Mathematics 163, *Springer,* New York 1996

[EJ16] Elsenhans, A.-S. and Jahnel, J.: *Point counting on $K3$ surfaces and an application concerning real and complex multiplication,* in: Proceedings of the ANTS XII conference (Kaiserslautern 2016), LMS Journal of Computation and Mathematics **19** (2016), 12–28

[EJ18] Elsenhans, A.-S. and Jahnel, J.: *Real and complex multiplication on $K3$ surfaces via period integration*, To appear in: Experimental Mathematics, `doi: 10.1080/10586458.2022.2061649`

[EJ20a] Elsenhans, A.-S. and Jahnel, J.: *Explicit families of $K3$ surfaces having real multiplication,* To appear in: Michigan Mathematical Journal, `doi: 10.1307/mmj/20205878`

[EJ20b] Elsenhans, A.-S. and Jahnel, J.: *Computations with algebraic surfaces,* in: Mathematical software–ICMS 2020, Lecture Notes in Comput. Sci. 12097, *Springer,* Cham 2020, 87–93

[EJ21] Elsenhans, A.-S. and Jahnel, J.: *Frobenius trace distributions for $K3$ surfaces,* `arXiv: 2102.10620`

[vGG] von zur Gathen, J. and Gerhard, J.: Modern computer algebra, *Cambridge University Press,* New York 1999

[vG] van Geemen, B.: *Some remarks on Brauer groups of $K3$ surfaces,* Adv. Math. **197** (2005), 222–247

[GH] Griffiths, P. and Harris, J.: Principles of algebraic geometry, *Wiley-Interscience,* New York 1978

[Ha] Harvey, D.: *Computing zeta functions of arithmetic schemes,* Proc. Lond. Math. Soc. **111** (2015), 1379–1401

[HS] Harvey, D. and Sutherland, A.: *Computing Hasse-Witt matrices of hyperelliptic curves in average polynomial time, II. Frobenius distributions: Lang-Trotter and Sato-Tate conjectures,* in: Contemp. Math. 663, *AMS,* Providence 2016, 127–147

[Ke] Kedlaya, K.: *Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology,* Journal of the Ramanujan Mathematical Society **16** (2001), 323–338

[Kn] Kneser, M.: Quadratische Formen, *Springer,* Berlin 2002

[Mi] Milne, J. S.: *On a conjecture of Artin and Tate,* Ann. of Math. **102** (1975), 517–533

[Ne] Neukirch, J.: Algebraic number theory, Grundlehren der Mathematischen Wissenschaften 322, *Springer,* Berlin 1999

[Og] Ogus, A.: *Supersingular $K3$ crystals,* in: Journées de Géométrie Algébrique de Rennes (Rennes 1978) II, Astérisque 64, *SMF,* Paris 1979, 3-86

[Pi] Pila, J.: *Frobenius maps of abelian varieties and finding roots of unity in finite fields,* Math. Comp. **55** (1990), 745–763

[Sch] Schoof, R.: *Counting points on elliptic curves over finite fields,* J. Théor. Nombres Bordeaux **7** (1995), 219–254

[SGA4] Artin, M., Grothendieck, A. et Verdier, J.-L. (avec la collaboration de Deligne, P. et Saint-Donat, B.): Théorie des topos et cohomologie étale des schémas, Séminaire de Géométrie Algébrique du Bois Marie 1963–1964 (SGA 4), Lecture Notes in Math. 269, 270, 305, *Springer,* Berlin, Heidelberg, New York 1972–1973

[SGA4½] Deligne, P. (avec la collaboration de Boutot, J. F., Grothendieck, A., Illusie, L. et Verdier, J.-L.): Cohomologie Étale, Séminaire de Géométrie Algébrique du Bois Marie (SGA4½), Lecture Notes in Math. 569, *Springer,* Berlin, Heidelberg, New York 1977

[SGA5] Grothendieck, A. (avec la collaboration de Bucur, I., Houzel, C., Illusie, L. et Serre, J.-P.): Cohomologie l-adique et Fonctions L, Séminaire de Géométrie Algébrique du Bois Marie 1965–1966 (SGA 5), Lecture Notes in Math. 589, *Springer,* Berlin, Heidelberg, New York 1977

[Sk] Skorobogatov, A. N.: *Cohomology and the Brauer group of double covers,* in: Brauer groups and obstruction problems: moduli spaces and arithmetic (A. Auel, B. Hassett, A. Várilly-Alvarado, and B. Viray eds.), *Springer,* Cham 2017

[Wi] Wilson, R. A.: The finite simple groups, Graduate Texts in Mathematics 251, *Springer,* London 2009

[Yo] Yoshikawa, K.-I.: *Discriminant of certain $K3$ surfaces,* in: Representation theory and automorphic forms, Progr. Math. 255, *Birkhäuser,* Boston 2008, 175–210

Institut für Mathematik, Universität Würzburg, Emil-Fischer-Strasse 30, D-97074 Würzburg, Germany

Email address: `stephan.elsenhans@mathematik.uni-wuerzburg.de`

URL: `https://www.mathematik.uni-wuerzburg.de/computeralgebra/team/elsenhans-stephan-prof-dr/`

Department Mathematik, Univ. Siegen, Walter-Flex-Str. 3, D-57068 Siegen, Germany

Email address: `jjahnel@mathematik.uni-siegen.de`

URL: `http://www.uni-math.gwdg.de/jahnel`