JOURNAL
de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Florent JOUVE

The geometry of the third moment of exponential sums

Tome 20, n^o 3 (2008), p. 733-760.

<http://jtnb.cedram.org/item?id=JTNB_2008__20_3_733_0>

Journal de Théorie des Nombres
de Bordeaux **20** (2008), 733-760

The geometry of the third moment of exponential sums

par Florent JOUVE

Résumé. Nous donnons une interprétation géométrique à deux types distincts de sommes d'exponentielles. L'une d'elles correspond au moment d'ordre trois des sommes de Kloosterman sur $\mathbf{F}_q$ de type $K(\nu^2; q)$. Nous commençons par établir un lien entre les sommes considérées et le nombre de points $\mathbf{F}_q$-rationnels sur certaines surfaces projectives lisses : l'une d'entre elles est une surface $K3$ et l'autre est une surface cubique lisse. Appliquant la théorie de Grothendieck-Lefschetz, on retrouve alors en particulier une formule pour le troisième moment des sommes de Kloosterman obtenue par D. H. et E. Lehmer en 1960.

Abstract. We give a geometric interpretation (and we deduce an explicit formula) for two types of exponential sums, one of which is the third moment of Kloosterman sums over $\mathbf{F}_q$ of type $K(\nu^2; q)$. We establish a connection between the sums considered and the number of $\mathbf{F}_q$-rational points on explicit smooth projective surfaces, one of which is a $K3$ surface, whereas the other is a smooth cubic surface. As a consequence, we obtain, applying Grothendieck-Lefschetz theory, a generalized formula for the third moment of Kloosterman sums first investigated by D. H. and E. Lehmer in the 60's .

1. Introduction

The problem of estimating exponential sums over finite fields is a quite standard issue in analytic number theory. Indeed, it arises in classical questions such as determining the Fourier coefficients of cusp forms or resolving the Waring problem via the circle method. As a consequence of Deligne's proof of the Riemann Hypothesis for varieties over finite fields, and, to an even wider extent, of its vast generalization described in [9], a deep and efficient understanding of fairly general types of such sums was derived (see e.g. [17]). That algebro-geometric method has now become the standard way to estimate exponential sums over finite fields.

Manuscrit reçu le 24 novembre 2007.

In our present work, however, instead of investigating the properties of the ℓ-adic sheaves (as the standard attack would suggest) associated to the exponential sum over $\mathbf{F}_q$ (with q not a power of ℓ) we consider, we exhibit an algebraic surface whose number of $\mathbf{F}_q$-rational points is explicitly related to the sum.

Let us first make precise what are the sums involved. Let p be a prime distinct from 2 and 3, q a power of p and φ a nontrivial additive character of $\mathbf{F}_q$:

$$\varphi : \mathbf{F}_q \to \mathbf{C}^\times .$$

For any couple of integers (α, β) such that $\alpha - 1 = 3(\beta - 1)$, we consider the sum

$$S(a^\alpha, a^\beta; q) = \sum_{x \in \mathbf{F}_q} \varphi(a^\alpha x^3 + a^\beta x) ,$$

with parameter $a \in \mathbf{F}_q$.

In [6], Birch was the first to consider moments of those sums (in the case $q = p$). In loc. cit. he conjectured that a modular interpretation should exist for a certain type of such moments. That conjecture was precised by Atkin in [3] and Livné finally proved it in [19]. Our first object of study is what we call the third Birch sum

$$B_3(q) = \sum_{a \in \mathbf{F}_q} S(a^\alpha, a^\beta; q)^3 .$$

That is nothing but the third moment of $S(a^\alpha, a^\beta; q)$ (we point out the fact that a straightforward computation yields the precise value of the first and second moment of the sums $S(a^\alpha, a^\beta; q)$).

To evaluate $B_3(q)$, we establish an explicit relation between the number of $\mathbf{F}_q$-rational points on a certain smooth cubic surface and the value of $B_3(q)$. The arithmetic of such surfaces is well understood notably thanks to the work of Swinnerton-Dyer who showed that the number of $\mathbf{F}_q$-rational points on a smooth projective cubic surface S is entirely determined by the decomposition of the set of 27 lines lying on S into Galois orbits (see [26]). Via that geometric interpretation, we deduce an explicit formula for the value of $B_3(q)$:

Theorem 1.1. *The quantity $B_3(q)/q$ is precisely the number of $\mathbf{F}_q$-rational points on an affine surface, the projective completion of which is a smooth cubic surface. More precisely,*

- *If $p \equiv 1 \pmod 3$, then there exist integers $A_p \equiv 1 \pmod 3$ and B_p satisfying $4p = A_p^2 + 27B_p^2$ and such that, if we let $\varepsilon = 1$ if 4 is a cube modulo p and $\varepsilon = -1$ otherwise, we get*

$$B_3(q)q^{-1} = q^2 + (2 + 2\chi_q(-1) + \zeta_6^{\delta r} + \bar{\zeta}_6^{\delta r})q - \lambda_1^r - \lambda_2^r ,$$

where $q = p^r$, χ_q *denotes the Legendre character of* $\mathbf{F}_q$, ζ_6 *and* $\bar{\zeta_6}$ *are the primitive* 6*th roots of* 1 *in* $\mathbf{C}$, λ_1 *and* λ_2 *are the complex numbers such that* $\lambda_1\lambda_2 = p$, $\lambda_1 + \lambda_2 = -A_p$ *et* $\delta = (3 - \chi_p(-1)(2\varepsilon + 1))/2$.

- *If* $p \equiv 2 \pmod 3$, *then*

$$B_3(q)q^{-1} = q^2 + (3 + (-1)^r + 2\chi_q(-1))q - \lambda_1^r - \lambda_2^r\,,$$

where λ_1 *and* λ_2 *are the complex numbers such that* $\lambda_1\lambda_2 = p$, $\lambda_1 + \lambda_2 = 0$.

We emphasize the fact that the formula obtained gives the *exact* value of the sum $B_3(q)$. We notice here that the investigation of k-th moments for k greater or equal to 4 would surely require other techniques than the study of the variety we would attach to it. Indeed, in the case where $k = 4$, the variety arising, when using orthogonality relations to simplify the expression of $B_4(q)$, is 3-dimensional, and there is no a priori analogue of the result of Swinnerton-Dyer (i.e. a totally explicit way to compute the number of $\mathbf{F}_q$-rational points) in dimension greater than 2.

Nevertheless, the method we describe enables us to evaluate other types of sums as well. Consider, for instance, the famous Kloosterman sums with parameter $\lambda \in \mathbf{F}_q$:

$$K(\lambda; q) = \sum_{x \in \mathbf{F}_q^\times} \varphi(x + \lambda x^{-1})\,,$$

where φ still denotes a nontrivial additive character of $\mathbf{F}_q$. The moments of order 1, 2 and 3 of those sums were computed by Salié in [22]; however, D. H. and E. Lehmer were the first to raise the question of the value of the n-th moment indexed by the squares of $\mathbf{F}_q$:

$$\sigma_n(q) = \sum_{\lambda \in \mathbf{F}_q} K(\lambda^2; q)^n\,.$$

As in the previous case, the computation of the moments $\sigma_1(q)$ and $\sigma_2(q)$ are straightforward. In [18], the authors obtain an explicit formula for the third moment in the special case where $q = p$. Their method, though elementary, requires lots of tricks in the transformations of the sums considered.

Noticing that the formula proved in [18] uses the decomposition $p = a^2 + 3b^2$ for primes $p \equiv 1 \pmod 3$ gives us the intuition that there must exist a geometric interpretation for $\sigma_3(q)$ involving the elliptic curve E with Weierstrass model $y^2 = x^3 + 1$ (or a quadratic twist of that curve). We show that such a link actually exists:

Theorem 1.2. *Assume that* $p \neq 2, 3$. *There exits a* $K3$ *surface defined over* $\mathbf{F}_q$ *and isomorphic, over* $\mathbf{F}_{q^2}$, *to the Kummer surface* $\mathrm{Km}(E \times E)$, *such that the number of* $\mathbf{F}_q$*-rational points on that surface is explicitly related to the* *value of $\sigma_3(q)$. Moreover, we have the exact formula*

$$\sigma_3(q) = \varepsilon^r q^2 + q(2q\chi_q(-1) + \chi_q(-1)(\lambda_1^r + \lambda_2^r) + 2)$$

where

- *if $p \equiv -1 \pmod 6$, then $\varepsilon = -1$ and $\lambda_1 = p$, $\lambda_2 = -p$,*
- *if $p \equiv 1 \pmod 6$, then $\varepsilon = 1$ and there exist integers a and b such that $p = a^2 + 3b^2$. In that case λ_1 and λ_2 are defined as the reciprocal roots of the polynomial $p^2T^2 - (4a^2 - 2p)T + 1$.*

The Kummer surface $\mathrm{Km}(E\times E)$ is the smooth model of the surface $E\times E$ blown up in its 16 points of order 2 (see [4, page 170]). Thus, the number of $\mathbf{F}_q$-rational points on such a surface is explicitly related to $|E(\mathbf{F}_q)|$. In the Theorem above, the surface attached to $\sigma_3(q)$ is isomorphic to $\mathrm{Km}(E \times E)$ only when considered as a surface over a field containing a primitive cube root of 1. That explains why we are naturally led to distinguish the case $p \equiv 1 \pmod 6$ from the case $p \equiv -1 \pmod 6$.

To prove the theorems stated above, we need to compute the number of $\mathbf{F}_q$-rational points on two smooth projective surfaces (the first being a cubic surface and the second being a $K3$ surface). To do so we will need standard facts about zeta functions of varieties over finite fields. We briefly review the terminology and results that will be helpful in what follows.

Recall that the zeta function of a *smooth projective* variety X over $\mathbf{F}_q$ is defined by the formal power series

$$Z(X/\mathbf{F}_q;T) = \exp\Big(\sum_{n\geqslant 1} |X(\mathbf{F}_{q^n})|\frac{T^n}{n}\Big)\,.$$

Thanks to Dwork's theorem, or, more usefully for us, to the Grothendieck-Lefschetz trace formula (see [8]), we know that this function is rational, and, in the case where X is 2-dimensional:

$$Z(X/\mathbf{F}_q;T) = \frac{P_1P_3}{P_0P_2P_4}\,,$$

where $P_i = \det(1 - T\mathrm{Fr}^*|H^i(X\otimes\overline{\mathbf{F}_q}, \mathbf{Q}_\ell))$, $\ell \neq p$ is a prime number and Fr^* is induced on the ℓ-adic cohomology groups by the geometric Frobenius on $X\otimes\overline{\mathbf{F}_q}$ (base change corresponding to the extension of scalars to a separable closure $\overline{\mathbf{F}_q}$ of $\mathbf{F}_q$).

For brevity the ℓ-adic cohomology group $H^i(X\otimes\overline{\mathbf{F}_q}, \mathbf{Q}_\ell)$ will be denoted H^i_X. For each of the two cases we consider, we need to compute the *exact* value of the eigenvalues of Fr^* acting on the spaces H^i_X, for $0 \leqslant i \leqslant 4$. Indeed, to obtain an exact formula for $B_3(q)$ and $\sigma_3(q)$, it is not enough to evaluate both the dimension of the H^i_X and the modulus of the eigenvalues (which we obtain directly by invoking Deligne's Riemann Hypothesis for varieties over finite fields).

The particular structure of the surfaces appearing in our study will be very helpful in order to obtain such a precise information. Let us recall briefly a few facts about surfaces and more specifically about $K3$ surfaces and smooth cubic surfaces.

The classification of algebraic surfaces is much more complex than for algebraic curves. Lots of different invariants are involved and we will not give definitions (but only references) for all of these objects as the precise understanding of what they are is not required for the proof of the theorems above. Let us first state a few facts about smooth cubic surfaces: they are *Del Pezzo surfaces* of degree 3 (see [11, page 401]) and, in the Enriques-Kodaira classification of surfaces (see [4, page 188]), they appear as surfaces with "type 1", that is to say rational minimal surfaces. In particular, the Betti number $b_1 = \dim H^1(X, \mathbf{Z})$ is zero if X is a smooth cubic surface.

Moreover, it is a standard fact that on such a surface lie exactly 27 lines. Computing equations for those lines will be a crucial step in evaluating $B_3(q)$. Indeed, the cycle classes of these lines span the ℓ-adic cohomology space H^2_X, which, concretely, corresponds to the fact that the Galois action on those lines entirely determines $|X(\mathbf{F}_q)|$ (see [26]).

Now we turn to $K3$ surfaces (surfaces of type 7 in the Enriques-Kodaira classification of [4, Table 10 page 188]), an instance of which will appear explicitly when evaluating $\sigma_3(q)$. Such a surface is defined as a geometrically connected surface with trivial canonical sheaf (see [11, page 180]) and Betti number b_1 equal to zero (notice the helpful common point with smooth cubic surfaces). The arithmetic of such varieties is the object of many recent studies, the fact that they can be seen as 2-dimensional analogues of elliptic curves being quite motivating.

The few information we have just given are enough to give an a priori form for the zeta function of $X/\mathbf{F}_q$ if X is either a smooth cubic surface or a $K3$ surface. Indeed, in both cases, $H^1_X = 0$, so, by Poincaré duality (see [8]), we have $H^3_X = 0$ as well. To obtain the expression of the factors P_0 and P_4 of the denominator of $Z(X/\mathbf{F}_q; T)$, we exploit the fact that, X being geometrically irreducible, H^0_X has dimension 1 with a trivial Galois action. In other words $H^0_X \simeq \mathbf{Q}_\ell$ as a Galois module. By Poincaré duality again, we deduce that $H^4_X \simeq \mathbf{Q}_\ell(-4)$: that is the standard notation for the *Tate twist.* More generally, for $d \geqslant 1$, the Galois module $\mathbf{Q}_\ell(-2d)$ denotes a one-dimensional $\mathbf{Q}_\ell$-vector space on which the geometric Frobenius acts by multiplication by q^d. From these standard observations we get, for X a smooth cubic surface or a $K3$ surface,

$$Z(X/\mathbf{F}_q; T) = \frac{1}{(1-T)(1-q^2T)P_2(T)}, \tag{1.1}$$

where the remaining crucial polynomial P_2 satisfies $P_2(T) \in \mathbf{Z}[T]$ and $P_2(0) = 1$.

To evaluate $B_3(q)$ and $\sigma_3(q)$ we will have to compute the action of Frobenius on H^2_X for a suitable surface X. To do so, we need to exhibit, in each case, the surface involved. To begin with, we discuss the case of $B_3(q)$.

2. Evaluation of a Birch sum

Let us recall first the notations defined in the introduction above: p is a prime number distinct from 2 and 3, $q = p^r$ for some integer $r \geqslant 1$ and φ is an additive character of $\mathbf{F}_q$. For simplicity, we consider the sum with parameter $a \in \mathbf{F}_q$:

$$S(a^4, a^2; q) = \sum_{x \in \mathbf{F}_q} \varphi(a^4 x^3 + a^2 x)\,;$$

but we keep in mind the fact that the couple of exponents $(4, 2)$ could be replaced by any (α, β) such that $\alpha - 1 = 3(\beta - 1)$.

The sum we wish to evaluate is the Birch sum

$$B_3(q) = \sum_{a \in \mathbf{F}_q} S(a^4, a^2; q)^3\,.$$

To prove Theorem 1, the first step consists in making explicit the smooth cubic surface related to $B_3(q)$. A straightforward calculation yields

$$B_3(q) = q^3 + \sum_{a \in \mathbf{F}_q^\times} \sum_{x,y,z \in \mathbf{F}_q} \varphi(a(x^3 + y^3 + z^3 + x + y + z))\,.$$

That expression naturally leads us to consider the affine cubic surface S defined by the equation:

$$S : f(x, y, z) = x^3 + y^3 + z^3 + x + y + z = 0\,.$$

Applying orthogonality relations, we deduce

$$B_3(q) = q|S(\mathbf{F}_q)|\,.$$

We are now reduced to determining the number of $\mathbf{F}_q$-rational points on the affine surface S. In order to feel as comfortable as possible with that problem, we prefer to work with a smooth projective model of S. Indeed, such a setting is particularly well-suited to use the properties of the ℓ-adic cohomology groups (where ℓ is a prime different from p) attached to the variety (see the introduction). Also, working with a smooth projective surface enables us to use the beautiful result of [26] in order to count $\mathbf{F}_q$-rational points.

So let $\widetilde{S}$ denote the projective compactification of S. In homogeneous coordinates $(x : y : z : w)$, an equation for $\widetilde{S}$ can be given by:

$$\widetilde{S} : x^3 + y^3 + z^3 + w^2(x + y + z) = 0\,.$$

A direct application of the Jacobi criterion shows that $\widetilde{S}$ is smooth. Hence, it suffices to evaluate the number of $\mathbf{F}_q$-rational points on the smooth projective cubic surface $\widetilde{S}$ to obtain the value of $B_3(q)$. Indeed, the contribution of points at infinity in $\widetilde{S}(\mathbf{F}_q)$ can be explicitly described as follows:

Proposition 2.1. *The $\mathbf{F}_q$-rational points of the complement of the surface S in its projective compactification $\widetilde{S}$ are precisely the $\mathbf{F}_q$-rational points of the projective curve*

$$C :\, x^3 + y^3 + z^3 = 0\,.$$

The curve $C/\mathbf{F}_q$ is an elliptic curve and the number of $\mathbf{F}_q$-rational points of C is given by

$$|C(\mathbf{F}_q)| = q + 1 - \lambda_1^r - \lambda_2^r\,,$$

where $\lambda_1\lambda_2 = p$ and

- *if $p \equiv 1 \pmod 3$, then $A_p = -(\lambda_1 + \lambda_2)$ satisfies $4p = A_p^2 + 27B_p^2$ (for a certain integer B_p) and $A_p \equiv 1 \pmod 3$,*
- *if $p \equiv 2 \pmod 3$, then $A_p = -(\lambda_1 + \lambda_2) = 0$.*

Proof. The curve C is a nonsingular cubic curve defined over $\mathbf{F}_q$; $(0 : -1 : 1)$ being an $\mathbf{F}_q$-rational point on C, we deduce that $C/\mathbf{F}_q$ is an elliptic curve. The number of $\mathbf{F}_q$-rational points on C is therefore given by (see [14, page 302]):

$$|C(\mathbf{F}_q)| = q + 1 - \lambda_1^r - \lambda_2^r\,,$$

where λ_1, λ_2 are the reciprocal roots of the polynomial $P(T) = 1 + A_pT + pT^2$, where $A_p = 0$ if $p \equiv 2 \pmod 3$ and, if $p \equiv 1 \pmod 3$, there exists an integer B_p such that A_p is the unique integer being congruent to 1 modulo 3 and satisfying $4p = A_p^2 + 27B_p^2$ (see [14, Chap. 8.3]). □

2.1. The zeta function of $\widetilde{S}/\mathbf{F}_q$. To begin with, let us recall briefly the link between the set of lines on $\widetilde{S}$ and the cohomology space $H^2_{\widetilde{S}}$. We refer the reader to [20, Chap. 4] for the general theory of cubic surfaces. As mentioned in the introduction, smooth cubic surfaces are del Pezzo surfaces of degree 3. In particular (see [20, Th. 24.4]) any such surface can be realized as the blow up of the projective plane $\mathbb{P}^2$ in 6 points, provided they do not all lie on the same conic and that no three of them lie on the same straight line. The surface we obtain contains 27 so called *exceptional curves* (one for each of the 6 points, one for each of the 15 lines joining two of these points and one for each of the 6 conics passing through 5 of these 6 points). These are precisely the 27 lines on the smooth cubic surface and the cycle classes of these lines generate the Picard group of the surface (see [20, Th. 26.2(i)]). Now, another standard fact about smooth cubic surfaces over finite fields is that their geometric Picard group is isomorphic, as a Galois module, to the ℓ-adic cohomology space H^2 attached to the surface once the scalars are extended to a separable closure of the base field (this can be seen as a way of stating Weil's Theorem [20, Th. 23.1]). Moreover, from a general formula (obtained, e.g. by combining Lemma 24.3.1 and Theorem 24.5 of [20]) valid for any del Pezzo surface we get that the rank of the Picard group for a smooth cubic surface is 7.

In the present context, this implies that

$$|\widetilde{S}(\mathbf{F}_q)| = q^2 + \Big(\sum_{i=1}^{7} \eta_i\Big) q + 1\,,$$

where the η_i are roots of unity. The theorem of Swinnerton-Dyer ([26, Table 1]) gives a correspondence between the value of $\sum_{i=1}^{7} \eta_i$ and the type of decomposition in Galois orbits of the 27 lines lying on $\widetilde{S}$.

2.2. The twenty seven lines on $\widetilde{S}$.

In order to compute the Galois action we need to describe explicitly the 27 lines on $\widetilde{S}$. Some of them are easy to find:

$$\begin{aligned}
&\mathcal{D}_z : (t : -t : 0 : w),\ \mathcal{D}_{z,\pm i} : (t : -t : \pm i : w)\,,\\
&\mathcal{D}_y : (t : 0 : -t : w),\ \mathcal{D}_{y,\pm i} : (t : \pm i : -t : w)\,,\\
&\mathcal{D}_x : (0 : t : -t : w),\ \mathcal{D}_{x,\pm i} : (\pm i : t : -t : w)\,,
\end{aligned}$$

are examples of lines lying on $\widetilde{S}$. However 18 of them remain to be found. To do so, we exploit the method described in [23]. The key observation is that if, by a change of coordinates, we succesively send $\mathcal{D}_x$, $\mathcal{D}_y$ and $\mathcal{D}_z$ on the z-axis and if we consider, after each transformation, the family of planes with parameter λ, $\mathcal{P}_\lambda : y = \lambda x$, then the intersection of $\mathcal{P}_\lambda$ with $\widetilde{S}$ is the union of the z-axis and a conic. That conic degenerates in two lines when the parameter λ takes appropriate values. These values correspond to roots of a polynomial Q with degree less than 5.

Applying that method after sending $\mathcal{D}_x$ on the z-axis, the polynomial we get is

$$Q(\lambda) = (\lambda + 1)(4\lambda^3 + 1)\,.$$

The root $\lambda = -1$ gives us $\mathcal{D}_z$ and $\mathcal{D}_y$; two lines which we have already found. As λ runs over the roots of $Q_x(t) = 4t^3 + 1$, we get six new lines:

$$(\lambda t : \frac{1}{2}(t - \frac{2\sqrt{-3\lambda+3}}{3}w) : \frac{1}{2}(t + \frac{2\sqrt{-3\lambda+3}}{3}w) : w)\,,$$
$$(\lambda t : \frac{1}{2}(t + \frac{2\sqrt{-3\lambda+3}}{3}w) : \frac{1}{2}(t - \frac{2\sqrt{-3\lambda+3}}{3}w) : w)\,.$$

Then sending $\mathcal{D}_y$ on the z-axis, the polynomial $Q(\lambda)$ is given by

$$Q(\lambda) = \lambda(\lambda+1)(\lambda^3+4)\,.$$

For $\lambda = -1$ we recover $\mathcal{D}_x$ and $\mathcal{D}_z$, and, for $\lambda = 0$, the lines $\mathcal{D}_{y,\pm i}$. However for each root λ of $Q_y(t) = t^3 + 4$, we find six new lines:

$$(t(\lambda + \frac{2}{\lambda^2}) - \frac{\sqrt{3}\sqrt{\lambda+1}}{3}w) : t : \frac{2}{\lambda^2}(-t + \frac{\sqrt{3}\sqrt{\lambda+1}}{3}w) : w)\,,$$
$$(t(\lambda + \frac{2}{\lambda^2}) + \frac{\sqrt{3}\sqrt{\lambda+1}}{3}w) : t : \frac{2}{\lambda^2}(-t - \frac{\sqrt{3}\sqrt{\lambda+1}}{3}w) : w)\,.$$

Finally, sending $\mathcal{D}_z$ on the z-axis, we obtain

$$Q(\lambda) = \lambda Q_z(\lambda)\,,$$

where $Q_z(\lambda) = 3\lambda^3 - 12\lambda^2 + 12\lambda - 4$. For $\lambda = 0$, we get the (already found) lines $\mathcal{D}_{z,\pm i}$. If λ runs over the set of roots of Q_z, we obtain the six remaining lines:

$$(t(1 - \frac{1}{k(\lambda)}) + \frac{iw}{k(\lambda)} : (\frac{1}{k(\lambda)} + \lambda - 1)t - \frac{i}{k(\lambda)}w : (1-\lambda)t : w)\,,$$
$$(t(1 - \frac{1}{k(\lambda)}) - \frac{iw}{k(\lambda)} : (\frac{1}{k(\lambda)} + \lambda - 1)t + \frac{i}{k(\lambda)}w : (1-\lambda)t : w)\,,$$

where $k(\lambda) = 3\lambda + (3/2)\lambda^2$.

Remark 2.2. Seeing $\widetilde{S}$ as a surface defined over $\mathbf{Q}$, the computations we have just performed show that the smallest Galois extension of $\mathbf{Q}$ over which the 27 lines on $\widetilde{S}$ are defined is $\mathbf{Q}(i, \omega, 2^{1/3})$, where i, ω, are respectively complex roots of the $\mathbf{Q}$-polynomials $X^2 + 1$ and $X^2 + X + 1$.

We can now compute the Galois action on the set of these 27 lines. We note that it suffices, in the computation of the Galois action, to consider $\widetilde{S}$ as a surface over the prime field $\mathbf{F}_p$ and to determine the eigenvalues of the Frobenius acting on the ℓ-adic cohomology of degree 2 of that surface. The eigenvalues for the second cohomology group of $\widetilde{S}/\mathbf{F}_{p^r}$ are then obtained by raising those corresponding to $\widetilde{S}/\mathbf{F}_p$ to the r-th power.

First, if we denote by σ^* (following [26]) the restriction of the Frobenius morphism to the set of 27 lines on $\widetilde{S}$, then σ^* fixes the three lines $\mathcal{D}_x$, $\mathcal{D}_y$ and $\mathcal{D}_z$. Let us investigate the action of σ^* on the other lines.

If $p \equiv 2 \pmod 3$:

- *either* $p \equiv 1 \pmod 4$ and then the 6 lines $\mathcal{D}_{x,\pm i}$, $\mathcal{D}_{y,\pm i}$ and $\mathcal{D}_{z,\pm i}$ as well as the 6 lines corresponding to the roots of Q_z, are defined over $\mathbf{F}_p$. These 12 lines are exchanged pairwise. We deduce that σ^* is an element of the conjugacy class C16 of [26, Table 1].
- *or* $p \equiv 3 \pmod 4$ and then the 6 lines $\mathcal{D}_{x,\pm i}$, $\mathcal{D}_{y,\pm i}$ and $\mathcal{D}_{z,\pm i}$ form 3 couples of coplanar lines exchanged pairwise. Moreover, as in the previous case, the roots of Q_z give rise to a couple of coplanar lines exchanged pairwise. The 12 remaining lines form 6 couples of skew lines exchanged pairwise. We deduce that σ^* is an element of the conjugacy class denoted C17.

If $p \equiv 1 \pmod 3$: *either* 4 *is a cube modulo* p and

- *either* $p \equiv 1 \pmod 4$ and then the 27 lines are defined over $\mathbf{F}_p$ (and so are all fixed by σ^*). Thus the permutation σ^* is an element of the class C1.
- *or* $p \equiv 3 \pmod 4$ and the lines which are different from $\mathcal{D}_x$, $\mathcal{D}_y$ and $\mathcal{D}_z$ split in 12 couples of coplanar lines exchanged pairwise. Thus σ^* is an element of the class C3.

or 4 *is not a cube modulo* p and

- *either* $p \equiv 1 \pmod 4$ and then the 6 lines $\mathcal{D}_{x,\pm i}$, $\mathcal{D}_{y,\pm i}$ and $\mathcal{D}_{z,\pm i}$ are defined over $\mathbf{F}_p$. Each of the polynomials Q_x, Q_y and Q_z gives rise to 2 triples of cyclicly permuted lines. Thus, the permutation σ^* is an element of the class C6.
- *or* $p \equiv 3 \pmod 4$ and then $\mathcal{D}_{x,\pm i}$, $\mathcal{D}_{y,\pm i}$ and $\mathcal{D}_{z,\pm i}$ form 3 couples of lines permuted pairwise and each of the polynomials Q_x, Q_y and Q_z corresponds to an orbit of 6 lines permuted cyclicly. We deduce that σ^* is an element of the class C7.

Remark 2.3. If X is a smooth cubic surface, it is a standard fact that the 27 lines on X can be described through a unique algebraic equation (see [12, Chap. 4]). Seen over $\mathbf{Q}$, such a polynomial has a splitting field with Galois group isomorphic to $W(E_6)$, the Weyl group of the exceptional algebraic group E_6. In that context the results of Swinnerton-Dyer ([26]) give us precise information about which subgroups of $W(E_6)$ can actually appear as permutation groups of the 27 lines, when working over finite fields.

Notice now (see [14, page 119]) that if $p \equiv 1 \pmod 3$, 4 is a cube modulo p if and only if the coefficient A_p defined in Proposition 2.1 is even. The different cases above can then be partly unified. Indeed the eigenvalues of the morphism induced on $H^2_{\widetilde{S}}$ by the global geometric Frobenius morphism on $\widetilde{S}/\mathbf{F}_q$ are:

- if $p \equiv 2 \pmod 3$: 1 with multiplicity 4, $(-1)^r$ with multiplicity 1, $\chi_q(-1)$ (where χ_q denotes the Legendre character of $\mathbf{F}_q$) with multiplicity 2,
- if $p \equiv 1 \pmod 3$: 1 with multiplicity 3, $\chi_q(-1)$ with multiplicity 2, $\zeta_6^{\delta r}$ with multiplicity 1 and $\bar{\zeta_6}^{\delta r}$ with multiplicity 1 (using the same notations as in Theorem 1.1).

We deduce the number of $\mathbf{F}_q$-rational points on $\widetilde{S}$:

- if $p \equiv 2 \pmod 3$:

$$|\widetilde{S}(\mathbf{F}_q)| = q^2 + (4 + (-1)^r + 2\chi_q(-1))q + 1\,,$$

- if $p \equiv 1 \pmod 3$:

$$|\widetilde{S}(\mathbf{F}_q)| = q^2 + (3 + 2\chi_q(-1) + \zeta_6^{\delta r} + \bar{\zeta_6}^{\delta r})q + 1\,.$$

Combining that formula with Proposition 2.1 and the fact that $B_3(q) = q|S(\mathbf{F}_q)|$, we finally deduce Theorem 1.1.

3. The third moment of Kloosterman sums

We work with the same notations and assumptions on q, p, and φ as in Section 2. In this section, we are interested in the family of Kloosterman sums with parameter λ defined in the introduction:

$$K(\lambda; q) = \sum_{x \in \mathbf{F}_q^\times} \varphi(x + \lambda x^{-1})\,.$$

For $\mu \in \mathbf{F}_q^\times$, we can define the additive character φ_μ via $\varphi_\mu(x) = \varphi(\mu x)$ for $x \in \mathbf{F}_q$. An easy calculation yields

$$K(\lambda\mu^2; q) = \sum_{x \in \mathbf{F}_q^\times} \varphi_\mu(x + \lambda x^{-1})\,,$$

so varying μ (i.e. the character) for fixed λ amounts to varying λ modulo the nonzero squares of $\mathbf{F}_q$. In the case where $q = p$ we can also remark that $K(\lambda; p)$ and $K(\lambda\mu^2; p)$ are Galois conjugate in the cyclotomic field $\mathbf{Q}(e^{2i\pi/p})$. Thus two subfamilies of those sums naturally emerge. Denoting by $\{1, \eta\}$ a set of representatives of $\mathbf{F}_q^\times$ modulo nonzero squares, these subfamilies give rise to the moments (using notations of [18]):

$$\sigma_n(q) = \sum_{\nu \in \mathbf{F}_q} (K(\nu^2; q))^n \quad \text{and} \quad \sigma'_n(q) = \sum_{\nu \in \mathbf{F}_q} (K(\eta\nu^2; q))^n\,.$$

We notice first that $\sigma_n(q) + \sigma'_n(q) = 2\sum_{\lambda\in\mathbf{F}_q} K(\lambda;q)^n$ and, generalizing Salié's formulæ (see [22] and [15, Section 4.4]), we obtain (for $p \neq 2$)

$$\sigma_1(q) = -\sigma'_1(q) = \chi_q(-1)q\,, \quad \sigma_2(q) = q^2 - 2q\,, \sigma'_2(q) = q^2\,,$$
$$\sigma_3(q) + \sigma'_3(q) = 2(\chi_q(-3)q^2 + 2q)$$

where χ_q still denotes the Legendre character of $\mathbf{F}_q$.

D. H. and E. Lehmer (see also [21] for a simplified proof involving the same type of arguments) give, in [18], an explicit formula for $\sigma_3(p)$. Although the elementary (but very clever) arguments they use would surely yield the exact formula of Theorem 1.2 for any $\sigma_3(q)$ (q being a prime power), most interesting in our method is the geometric interpretation we give for the fact that the decomposition $p = a^2 + 3b^2$ (provided $p \equiv 1\,(\mathrm{mod}\,3)$) appears in the formula of [18]. That decompostion is indeed strongly related to the so called a_p coefficient of the CM elliptic curve $E/\mathbf{Q}$ with Weierstrass model $y^2 = x^3 + 1$ (or a quadratic twist of that curve).

Remark 3.1. It is natural to ask for what can be done to evaluate the fourth moment of Kloosterman sums $\sigma_4(q)$. The same easy calculation as the one performed in the next section shows that this problem is equivalent to determining the number of $\mathbf{F}_q$-rational points on the threefold given by

$$\mathscr{Z} : x + x^{-1} + y + y^{-1} + z + z^{-1} + t + t^{-1} = 0\,.$$

In [27], the author, first resolving the singularities of that variety and then using the Faltings-Serre criterion, shows that the number of $\mathbf{F}_p$-rational points on $\mathscr{Z}$ is explicitly related to the coefficient of the expansion of the cusp form $\eta^4(2z)\eta^4(4z)$.

In [1], the authors give an expression relating the number of $\mathbf{F}_p$-rational points of $\mathscr{Z}$ to the sum of the number of $\mathbf{F}_p$-rational points on the Legendre elliptic curves

$$E_{\lambda^2} : y^2 = x(x-1)(x-\lambda^2)\,,$$

where $\lambda \in \mathbf{F}_p \setminus \{0, \pm 1\}$.

Another point of view, in order to try and find the value of $\sigma_n(q)$ for any n greater than 3 would be to apply the standard techniques from algebraic geometry we referred to in the introduction. A theorem of Deligne (see [17, Th. 4.1.1]) asserts that there exists a lisse ℓ-adic sheaf (on $\mathbb{G}_m$) of rank 2 denoted Kl and called *Kloosterman sheaf* such that the action of the local Frobenius (at any $a \in \mathbf{F}_q$) on the fibre of Kl over a geometric point $\bar{a}$ lying over a satisfies

$$\mathrm{Tr}(\mathrm{Fr}_{a,q} \mid \mathrm{Kl}_{\bar{a}}) = -K(a;q)\,.$$

In our case, those sheaves can be seen as Galois representations over the field of ℓ-adic numbers $\mathbf{Q}_\ell$. If we want to use Galois representations to express the moment $\sigma_n(q)$ as well, and if we want those representations to have a dimension that grows as slowly as possible with n, we just need to consider the elevation to the second power $[2] : \mathbb{G}_m \to \mathbb{G}_m$ and the n-th symmetric power (an operation we denote τ_n) of the pullback $[2]^*\mathrm{Kl}$. The sheaf obtained has rank $n+1$ and, from standard properties of such ℓ-adic sheaves (see e.g. [17, 2.3.3]), the value of $\sigma_n(q)$ is explicitly related to the trace of the global Frobenius acting on the cohomology space with compact support $H^1_c(\mathbb{G}_m \times \overline{\mathbf{F}_q}, \tau_n([2]^*\mathrm{Kl}))$. Instead of obtaining a precise value for that trace, which seems very difficult, we only discuss the dimension of the cohomology space involved. Such an information is enough to gain some intuition about the level of difficulty of evaluating $\sigma_n(q)$ as n grows.

In [10, proof of Th. 3.1], the decomposition of $[2]^*\tau_n(\mathrm{Kl})$ as a direct sum of Lang sheaves is given. That enables us to see easily that the sheaves $\tau_n([2]^*\mathrm{Kl})$ and $[2]^*\tau_n(\mathrm{Kl})$ are isomorphic (e.g. via a straightforward computation of the eigenvalues of the local Frobenii acting on those sheaves). The ramification argument given in [10, proof of Th. 3.1] combined with the formula 1.13.1 of [17] yields

$$\dim H^1_c(\mathbb{G}_m \times \overline{\mathbf{F}_q}, \tau_n([2]^*\mathrm{Kl})) = \begin{cases} n - 2\lfloor \frac{n}{2p} \rfloor\,, & \text{if } n \text{ is even}\,, \\ n + 1 - 2\lfloor \frac{n}{2p} + \frac{1}{2} \rfloor & \text{otherwise}\,. \end{cases}$$

so the dimension evaluated increases “almost” linearly with n (at least in the range $1 \leqslant n \leqslant p$).

3.1. A surface related to $\boldsymbol{\sigma_3(q)}$. We start by expanding the formula defining $\sigma_3(q)$

$$\begin{aligned}
\sigma_3(q) &= \sum_{\nu \in \mathbf{F}_q} \Big(\sum_{h \in \mathbf{F}_q^\times} \varphi(h + \nu^2 h^{-1}) \Big)^3 \\
&= \sum_{\nu \in \mathbf{F}_q} \Big(\sum_{x,y,z \in \mathbf{F}_q^\times} \varphi(x + y + z + \nu^2(x^{-1} + y^{-1} + z^{-1})) \Big) \\
&= \sum_{x,y,z \in \mathbf{F}_q^\times} \varphi(x + y + z) \\
&\quad + \sum_{\nu \in \mathbf{F}_q^\times} \Big(\sum_{x,y,z \in \mathbf{F}_q^\times} \varphi(x + y + z + \nu^2(x^{-1} + y^{-1} + z^{-1})) \Big)\,.
\end{aligned}$$

Using orthogonality relations and performing the change of variables $x' = \nu^{-1}x$, $y' = \nu^{-1}y$, $z' = \nu^{-1}z$, we obtain

$$\sigma_3(q) = -1 + \sum_{\nu \in \mathbf{F}_q^\times} \Big(\sum_{x',y',z' \in \mathbf{F}_q^\times} \varphi(\nu(x' + y' + z' + x'^{-1} + y'^{-1} + z'^{-1})) \Big)\,.$$

This leads us to define a surface S_0 in $\mathbb{G}^3_{\mathrm{m}}/\mathbf{F}_q$ in the following way .

$$S_0 :\ f(x,y,z) = x + y + z + x^{-1} + y^{-1} + z^{-1} = 0\,.$$

The link between $\sigma_3(q)$ and the number of $\mathbf{F}_q$-rational points of S_0 is given by

$$\begin{aligned}(3.1)\qquad \sigma_3(q) &= -1 + \sum_{x,y,z\in\mathbf{F}_q^\times}\Big(\sum_{\nu\in\mathbf{F}_q^\times}\varphi(\nu f(x,y,z))\Big)\\ &= -1 + \sum_{\substack{x,y,z\in\mathbf{F}_q^\times\\ f(x,y,z)\neq 0}}(-1) + \sum_{\substack{x,y,z\in\mathbf{F}_q^\times\\ f(x,y,z)=0}}(q-1)\\ &= -1 - ((q-1)^3 - |S_0(\mathbf{F}_q)|) + (q-1)|S_0(\mathbf{F}_q)|\\ &= -(q-1)^3 + q|S_0(\mathbf{F}_q)| - 1\,.\end{aligned}$$

We are now going to see how S_0 is closely related to the $K3$ surface called $\mathscr{C}$ in the paper [5] [1].

First, the equation defining S_0 is obviously equivalent to

$$xyz(x+y+z) + xy + yz + xz = 0 \quad\text{and}\quad xyz \neq 0\,.$$

The surface S_0 is a Zariski open dense subset of the projective surface $S_1 \subset \mathbb{P}^3_{\mathbf{F}_q}$ (i.e. S_1 is defined over $\mathbf{F}_q$) with homogeneous equation in coordinates $(x:y:z:t)$

$$S_1:\ xyz(x+y+z) + t^2(xy+yz+xz) = 0\,.$$

Precisely, S_0 is the open set defined by $xyzt \neq 0$.

Fixing the value $z=1$, we see then that S_0 is isomorphic to the surface $S_2/\mathbf{F}_q$ with equation

$$S_2:\ xy(x+y+1) + t^2(xy+y+x) = 0 \quad\text{and}\quad xyt\neq 0\,.$$

Finally, we define $S_3/\mathbf{F}_q$ by

$$(3.2)\qquad S_3:\ s^2 = -xy(x+y+1)(xy+y+x)\,,$$

and the Zariski open dense subset $S_3^* \subset S_3$ by $xys \neq 0$.

Then the map

$$\begin{aligned} S_3^* &\to S_2\\ (x,y,s) &\mapsto (x,y,t = xy(x+y+1)s^{-1})\end{aligned}$$

establishes an isomorphism between S_3^* and $S_2 \setminus (\mathcal{D}_{\zeta_3}\cup\mathcal{D}_{\zeta_3^2})$, where ζ_3 is a primitive cube root of 1 in $\overline{\mathbf{F}_q}$ and $\mathcal{D} = \mathcal{D}_{\zeta_3}\cup\mathcal{D}_{\zeta_3^2}$ is a degenerate conic in $\mathbf{A}^3_{\mathbf{F}_q}$ with equation

$$x^2+x+1=0\,,\ y=-x-1\,,\ t\neq 0\,,$$

[1] The reference [5] was given by N. Katz via E. Kowalski.

which happens to be, over $\overline{\mathbf{F}_q}$, the union of the two lines (minus a point)

$$\mathcal{D}_{\zeta_3} = \{(\zeta_3;\zeta_3^2;t)|t \in \overline{\mathbf{F}_q} \setminus \{0\}\}\,,$$
$$\mathcal{D}_{\zeta_3^2} = \{(\zeta_3^2;\zeta_3;t)|t \in \overline{\mathbf{F}_q} \setminus \{0\}\}\,.$$

We observe that we have $\mathcal{D}_{\zeta_3}(\mathbf{F}_q) = \mathcal{D}_{\zeta_3^2}(\mathbf{F}_q) = \emptyset$ when $\mathbf{F}_q$ contains no primitive cube root of 1 (for instance if $q = p^r$ with $p \equiv 2 \,(\mathrm{mod}\, 3)$ and r odd).

We have the following lemma relating $\mathbf{F}_q$-rational points on S_0 and S_3^*:

Lemma 3.2.

- *If* $\zeta_3 \in \mathbf{F}_q$ *then*

$$|S_0(\mathbf{F}_q)| = |S_3^*(\mathbf{F}_q)| + 2q - 2\,.$$

- *Otherwise*

$$|S_0(\mathbf{F}_q)| = |S_3^*(\mathbf{F}_q)|\,.$$

Proof. What we have just observed and the fact that, in any case, $\mathcal{D}_{\zeta_3} \cap \mathcal{D}_{\zeta_3^2} = \emptyset$ clearly imply Lemma 3.2 □

We are not going to focus on the computation of $|S_3^*(\mathbf{F}_q)|$ but instead of that we are going to perform one last transformation on the equation defining S_3^*. In so doing the affine equation of the $K3$ surface $\mathscr{C}$ studied by Beukers and Stienstra ([5]) clearly appears. Let us define

$$S_4 :\; s^2 = xy(x+y+1)(xy+y+x)\,. \tag{3.3}$$

From a geometric point of view (i.e. looking at the different varieties as defined over a separable closure $\overline{\mathbf{F}_q}$ of $\mathbf{F}_q$) the surfaces S and S_3 are isomorphic:

$$S_3 \otimes \overline{\mathbf{F}_q} \simeq S_4 \otimes \overline{\mathbf{F}_q}$$
$$(x;y;s) \mapsto (x;y;is)$$

where i denotes a square root of -1 in $\overline{\mathbf{F}_q}$.

The link between the arithmetic properties of S_4 and S_3 can easily be made explicit:

Lemma 3.3. *We have, for all* q,

$$|S_3(\mathbf{F}_q)| - q^2 = \chi_q(-1)(|S(\mathbf{F}_q)| - q^2)\,.$$

Proof. We compute:

$$\begin{aligned}|S_3(\mathbf{F}_q)| &= \sum_{x,y\in\mathbf{F}_q} (1+\chi_q(-xy(x+y+1)(xy+y+x)))\\ &= q^2 + \sum_{x,y\in\mathbf{F}_q} \chi_q(-xy(x+y+1)(xy+y+x))\\ &= q^2 + \chi_q(-1) \sum_{x,y\in\mathbf{F}_q} \chi_q(xy(x+y+1)(xy+y+x))\\ &= q^2 + \chi_q(-1)(|S_4(\mathbf{F}_q)| - q^2)\,.\end{aligned}$$

□

We summarize the connections between the different surfaces involved in the following diagram where all the arrows are defined over $\mathbf{F}_q$:

$$S_0 \hookrightarrow S_1 \simeq S_2 \hookleftarrow S_3^* \hookrightarrow S_3\,.$$

We also have the following isomorphism defined over $\overline{\mathbf{F}_q}$

$$S_3 \otimes \overline{\mathbf{F}_q} \simeq S_4 \otimes \overline{\mathbf{F}_q}\,.$$

We have just explained why the problem of evaluating $\sigma_3(q)$ can be reduced to determining the number of $\mathbf{F}_q$-rational points on S_4. As in the previous case, we construct the smooth projective model of S_4 and study its zeta function.

3.2. Resolving the singularities of S_4. In the following geometric study, all the varieties will implicitly be defined over $\overline{\mathbf{F}_p}$ (for instance the n-projective space $\mathbb{P}^n_{\overline{\mathbf{F}_p}}$ will simply be denoted by $\mathbb{P}^n$). However, for the arithmetic application we have in mind, we will keep track of the fields of definition whenever needed.

We are now going to describe briefly the construction of the minimal smooth projective model of S following [5].

We consider the sextic curve in $\mathbb{P}^2$:

$$C\,:\, XYZ(X+Y+Z)(XY+YZ+XZ) = 0\,.$$

We want to construct the smooth model of the double covering of $\mathbb{P}^2$ ramified over C, an open subset of which will happen to be the surface S_4.

The singularities of C are all double or triple points coming from the intersections between the following rational curves:

$$\mathcal{D}_x\,:\, X=0\,,\, \mathcal{D}_y\,:\, Y=0\,,\, \mathcal{D}_z\,:\, Z=0\,,$$
$$\mathcal{D}_{x,y,z}\,: X+Y+Z=0\,,\, \mathcal{C}\,:\, XY+XZ+YZ=0\,.$$

The set of singular points of C consists in:

- 3 triple points:

$$\begin{aligned}\mathcal{D}_x \cap \mathcal{D}_y \cap \mathcal{C} &= (0:0:1)\,,\\ \mathcal{D}_x \cap \mathcal{D}_z \cap \mathcal{C} &= (0:1:0)\,,\\ \mathcal{D}_y \cap \mathcal{D}_z \cap \mathcal{C} &= (1:0:0)\,.\end{aligned}$$

- 5 double points:

$$\begin{aligned}\mathcal{D}_x \cap \mathcal{D}_{x,y,z} &= (0:1:-1)\,,\\ \mathcal{D}_y \cap \mathcal{D}_{x,y,z} &= (1:0:-1)\,,\\ \mathcal{D}_z \cap \mathcal{D}_{x,y,z} &= (1:-1:0)\,,\\ \mathcal{D}_{x,y,z} \cap \mathcal{C} &= \{(\zeta_3:\zeta_3^2:1);(\zeta_3^2:\zeta_3:1)\}\,.\end{aligned}$$

We notice once more that whenever $\zeta_3 \notin \mathbf{F}_q$, we have $\mathcal{D}_{x,y,z}(\mathbf{F}_q) \cap \mathcal{C}(\mathbf{F}_q) = \emptyset$.

One constructs the smooth model of the double cover of $\mathbb{P}^2$ ramified over C as follows: first we blow up $\mathbb{P}^2$ at the triple points of C. This gives rise to three exceptional curves which are irreducible components of the total transform of the branch locus C in the blown-up $\mathbb{P}^2$ (the other irreducible components being nothing but the strict transform of the irreducible components of C).

The only singularities of the pre-image of the branch locus in the blown-up $\mathbb{P}^2$ are now double points (either coming from the original branch locus C, or from the intersections between the three exceptional curves and the other irreducible components of the pre-image of C). However these double points come from intersections between components of *odd* multiplicity as summand of the divisor attached to the pre-image of the branch locus, so, as explained in [7], we now have to blow up the pre-image of $\mathbb{P}^2$ in the double points of the pre-image of C.

This gives rise to 14 exceptional curves having all even multiplicity. The only remaining singularities are double points coming from intersections between components of odd and even multiplicity of the total transform of the branch locus. Taking the double cover of the pre-image of $\mathbb{P}^2$ ramified over the components of odd multiplicity of the image of C, we then obtain a *smooth* surface.

We denote by $K4$ (adding Kloosterman's name to those of Kähler, Kodaira and Kummer seems fair) the smooth surface we have just constructed (it is the surface called $\mathscr{C}$ in [5]). The resolution graphs corresponding to the resolution of singularities we have performed are the following

On the two dual graphs above, the "full points" represent components of odd multiplicity whereas "empty points" represent components of even

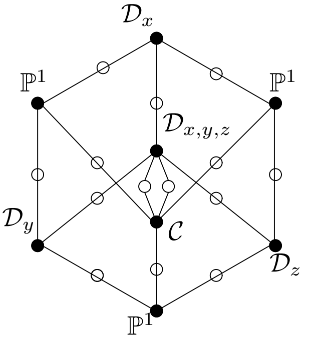

Fig. 1

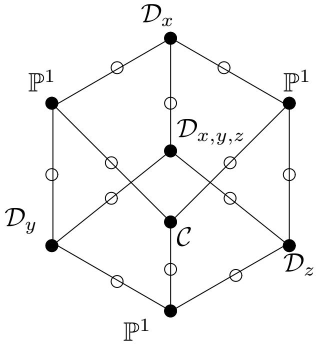

Fig. 2

multiplicity of the total transform of the branch locus (these are all exceptional curves coming from blowing up at the double points of the image of C).

Figure 1 describes the relation existing between the irreducible components of the total transform of the branch locus seen as rational curves over $\overline{\mathbf{F}_p}$. As we mentioned before, it might happen that $\mathcal{D}_{x,y,z}(\mathbf{F}_q) \cap \mathcal{C}(\mathbf{F}_q) = \emptyset$. Figure 2 usefully describes the relations between the irreducible components of the image of the branch locus seen as curves defined over such fields $\mathbf{F}_q$ (that is to say fields containing no primitive cubic root of 1).

The surface $K4$ is smooth and projective. The following criterion tells us that $K4$ is a $K3$ surface (see e.g. [4] page 189 for the proof of a slightly stronger statement):

Proposition 3.4. *A surface constructed as the smooth model of the double cover of $\mathbb{P}^2$ ramified over a sextic curve having only double points or triple points as singularities is a $K3$ surface.*

From what we saw in the introduction the major part of the work consists in determining the polynomial P_2 of (1.1). As $K4$ is a $K3$ surface, we know that P_2 has degree 22 (see [13, (6.7), proof of Th. 6]). The problem of determining P_2 happens to be easier to handle when $\zeta_3 \in \mathbf{F}_q$; as a consequence we are first going to evaluate $|K4(\mathbf{F}_q)|$ when $\zeta_3 \in \mathbf{F}_q$.

3.3. Computing the zeta function of $K4$ over finite fields containing ζ_3.

We fix a finite field $\mathbf{F}$ of characteristic p such that $\zeta_3 \in \mathbf{F}$. We exploit the proof of Theorem 6 in [13]. The morphism of $\mathbb{P}^2$ given by

$$\begin{aligned} U &= \zeta_3 YZ + \zeta_3 XZ - \zeta_3^2 XZ - \zeta_3^2 XY \\ V &= \zeta_3 YZ + \zeta_3 Y^2 - \zeta_3^2 Y^2 - \zeta_3^2 XY \\ W &= -YZ + \zeta_3^2 XY \end{aligned}$$

transforms the curve $C : XYZ(X+Y+Z)(XY+YZ+XZ) = 0$ into the curve of equation $(U^3+W^3)(V^3+W^3) = 0$. As $\zeta_3 \in \mathbf{F}$, the above morphism is defined over $\mathbf{F}$.

As a consequence, $K4$ is, over $\mathbf{F}$, the smooth model of the double cover of $\mathbb{P}^2$ ramified over the curve $(U^3+W^3)(V^3+W^3) = 0$. That is to say, $K4$ is isomorphic over $\mathbf{F}$ to the Kummer surface $\mathrm{Km}(E \times E)$ associated to $E \times E$, where we recall that E has Weierstrass model $y^2 = x^3 + 1$.

We can now exploit the fact that the ℓ-adic cohomology of $K4$ is closely related to that of E. The ℓ-adic cohomology of E is well known and it is proved in [13] that, since $\mathrm{Km}(E \times E)$ is obtained from $E \times E$ by first blowing up its sixteen points of order at most 2 (then quotienting by the involution induced), for some extension $\mathbf{F}_q$ of $\mathbf{F}$, we have

$$P_2(K4/\mathbf{F}_q;T) = (1-qT)^{16}\det(1-T\mathrm{Fr}^*|H^2_{E\times E}) \tag{3.4}$$

The Künneth formula (see [8]) gives

$$H^2_{E\times E} \simeq H^2_E \otimes H^0_E \oplus H^1_E \otimes H^1_E \oplus H^0_E \otimes H^2_E$$

First $H^2_E \otimes H^0_E \simeq H^0_E \otimes H^2_E \simeq H^2_E = \mathbf{Q}_\ell(-2)$ so

$$\det(1-T\mathrm{Fr}^*|H^2_E \otimes H^0_E \oplus H^0_E \otimes H^2_E) = (1-qT)^2\,.$$

What's more, we know (see [14, page 301 and 304]) that the zeta function of E over $\mathbf{F}_q$ is given by

$$Z(E/\mathbf{F}_q;T) = \frac{(1-\pi^r T)(1-\bar{\pi}^r T)}{(1-T)(1-qT)}\,,$$

where r is the integer such that $q = p^r$ and π is an algebraic integer satisfying $\pi\bar{\pi} = p$ and $|\pi| = \sqrt{p}$. An easy calculation then yields

$$\det(1-T\mathrm{Fr}^*|H^1_E \otimes H^1_E) = (1-qT)^2(1-\pi^{2r}T)(1-\bar{\pi}^{2r}T)\,.$$

Gathering these equalities we eventually obtain

$$\det(1-T\mathrm{Fr}^*|H^2_{E\times E}) = (1-qT)^4(1-\pi^{2r}T)(1-\bar{\pi}^{2r}T)\,,$$

thus

$$P_2(K4/\mathbf{F}_q;T) = (1-qT)^{20}(1-\pi^{2r}T)(1-\bar{\pi}^{2r}T)\,. \tag{3.5}$$

Let

$$P_{21}(K4/\mathbf{F}_{p^r};T) = (1-\pi^{2r}T)(1-\bar{\pi}^{2r}T)$$

The reciprocal roots λ_1 and λ_2 of the polynomial $P_{21}(K4/\mathbf{F}_p;T) \in \mathbf{Z}[T]$ satisfy

$$\lambda_1^r = \pi^{2r} \quad \text{and} \quad \lambda_2^r = \bar{\pi}^{2r}\,. \tag{3.6}$$

Exploiting (3.5) and (3.6), we get the following expression for the zeta function of $K4$ over $\mathbf{F}_q = \mathbf{F}_{p^r}$

$$Z(K4/\mathbf{F}_q; T) = \frac{1}{(1-T)(1-q^2T)(1-qT)^{20}(1-\lambda_1^r T)(1-\lambda_2^r T)},$$

which immediately yields

$$|K4(\mathbf{F}_q)| = 1 + q^2 + 20q + \lambda_1^r + \lambda_2^r\,. \tag{3.7}$$

However, the algebraic integer π is not entirely determined by the conditions $\pi\bar{\pi} = p$, $|\pi| = \sqrt{p}$. This means that the expression (3.7), involving λ_1 and λ_2, is not completely satisfactory. We are now going to evaluate precisely λ_1 and λ_2 by computing both $\lambda_1\lambda_2$ and $\lambda_1 + \lambda_2$.

As the elliptic curve $E/\mathbf{Q}$ has complex multiplication by the ring of integers $\mathcal{O}_K$ of the quadratic field $K = \mathbf{Q}(\sqrt{-3})$, we know that $\pi \in \mathcal{O}_K$. Following [5], we focus our attention on whether the prime p splits in $\mathcal{O}_K$ or not. Indeed, writing $\pi = a + b\sqrt{-3}$, $a, b \in \mathbf{Z}$, Beukers and Stienstra show in [5] that, provided $p \neq 2, 3$,

- either p splits in $\mathcal{O}_K$ in which case

$$\begin{cases} \lambda_1\lambda_2 = p^2 \\ \lambda_1 + \lambda_2 \in \{\pm 2(a^2 - 3b^2),\ \pm(a^2 + 6ab - 3b^2),\ \pm(a^2 - 6ab - 3b^2)\} \end{cases}$$

- or

$$\begin{cases} \lambda_1\lambda_2 = \pm p^2 \\ \lambda_1 + \lambda_2 \in \{0,\ \pm 2p\} \end{cases}$$

Remark 3.5. Recall that a prime number p is ramified in $\mathbf{Q}(\sqrt{-3})$ if and only if -3 is a square in $\mathbf{Z}/p\mathbf{Z}$. Using quadratic reciprocity, this is equivalent, for a prime $p \geqslant 5$, to $p \equiv 1 \pmod 3$ (1 is the only nonzero square modulo 3) and thus to $p \equiv 1 \pmod 6$.

Though more precise, the expressions we have obtained for λ_1 and λ_2 remain ambiguous. We are first going to deal with the case $p \equiv 1 \pmod 6$ (i.e. when p splits in $\mathcal{O}_K$). As sketched in [5], we consider the action of a group of order 6 on $K4/\mathbf{F}_q$, q being a power of a prime $p \equiv 1 \pmod 6$.

Let G be the finite group generated by the automorphism γ_1 exchanging the two sheets of the double cover involved in the construction of $\widetilde{S}$ and by the automorphism γ_2 induced on $K4$ by the 3-cycle

$$(X : Y : Z) \in \mathbb{P}^2 \mapsto (Y : Z : X) \in \mathbb{P}^2\,.$$

γ_1 and γ_2 are of respective order 2 and 3, so $|G| = 6$.

The fixed points of γ_1 are the ramification points of $K4$. Figure 1 describes how many of these points are $\mathbf{F}_q$-rational. Indeed, as $\zeta_3 \in \mathbf{F}_q = \mathbf{F}_{p^r}$, all the ramification points of $K4$ have coordinates in $\mathbf{F}_q$. Each vertex of that dual graph represents a rational curve and, as the "empty points" have degree 2 with a distinct couple of "full points" as neighbors, the number of ramification points of $K4$ over $\mathbf{F}_q$ is

$$8(q+1)+14(q-1)\,.$$

Notice that the other $\mathbf{F}_q$-rational points of $K4$ have a trivial stabilizer under the action of G.

The fixed points of γ_2 are the elements of the inverse image of $\{(\xi:\xi^2:1)|\xi^3=1\}$ by the final double cover. If $\xi=\zeta_3$ or $\xi=\zeta_3^2$, we obtain the two branch points of $\mathcal{C}\cap\mathcal{D}_{x,y,z}$ which are also fixed points for γ_1. If $\xi=1$, we obtain the two points $(x,y,s)=(1,1,\pm 3)$ (provided $p\neq 2,3$) on the affine part S_4 of $K4$.

Exploiting (3.7), we finally deduce, in the case where $q=p\equiv 1\,(\mathrm{mod}\,6)$,

$$1+p^2+20p+\lambda_1+\lambda_2\equiv 8(p+1)+14(p-1)+2\,(\mathrm{mod}\,6)$$

thus $\lambda_1+\lambda_2\equiv 2\,(\mathrm{mod}\,6)$. Looking back at the possible values we obtained for the sum and the product of λ_1 and λ_2, this yields

$$\lambda_1+\lambda_2=2(a^2-3b^2)\quad\text{and}\quad\lambda_1\lambda_2=p^2\,.$$

As $p=\pi\bar{\pi}=a^2+3b^2$, we can also write $\lambda_1+\lambda_2=4a^2-2p$. We can now give the explicit form of the polynomial P_{21}:

$$P_{21}(K4/\mathbf{F}_p;T)=p^2T^2-(4a^2-2p)T+1\,.$$

What's more, if $\mathbf{F}_q=\mathbf{F}_{p^r}$ with $p\equiv 1\,(\mathrm{mod}\,6)$, (3.7) is now an entirely satisfactory expression for $|K4(\mathbf{F}_q)|$.

To conclude with the case $\zeta_3\in\mathbf{F}_q$, we must find the value of $|K4(\mathbf{F}_q)|$ when $\mathbf{F}_q$ is an extension of even degree of $\mathbf{F}_p$ with $p\equiv -1\,(\mathrm{mod}\,6)$, say $q=p^{2f}$, $f\geqslant 1$. For that purpose we consider the general situation where X is a smooth projective surface defined over $\mathbf{F}_q$ and we denote by $\mathrm{Div}(X)$ the abelian group of divisors on X. It is well known that the so called *cycle class map* once extended to the $\mathbf{Q}_\ell$-linear *injective* map

$$\mathrm{Div}(X)\otimes_{\mathbf{Z}}\mathbf{Q}_\ell\to H^2(X\otimes\overline{\mathbf{F}_q},\mathbf{Q}_\ell(1))^{\mathrm{Fr}-1\,\mathrm{nilpotent}} \tag{3.8}$$

is of great importance. For instance, if we denote by $m_X(1;q)$ the multiplicity of 1 as eigenvalue of Frobenius acting on $H^2(X\otimes\overline{\mathbf{F}_q},\mathbf{Q}_\ell(1))$ (which can also be seen as the multiplicity of q as eigenvalue of Fr^* acting on H^2_X) and by $\rho(X|\mathbf{F}_q)$ the Picard number of X (i.e. the rank of the Néron-Severi group of X (see [4] page 120), Tate's conjecture, in the case of finite fields (see e.g. [16]), predicts that

$$\rho(X|\mathbf{F}_q)=m_X(1;q)\,. \tag{3.9}$$

Notice that this statement is equivalent to the surjectivity of (3.8) (as it is injective).

However, dealing with the present situation, it is sufficient to exploit the injectivity of (3.8). As assumed earlier, $\mathbf{F}_q$ is an extension of even degree of $\mathbf{F}_p$ with $p \equiv -1 \pmod 6$, so $\zeta_3 \in \mathbf{F}_q$ and the preceding study shows that we have an isomorphism $K4 \simeq \mathrm{Km}(E \times E)$ defined over $\mathbf{F}_q$. As mentioned before, $p \equiv -1 \pmod 6$ implies that p does not split in $\mathcal{O}_K$. Thus (see, e.g. [25, exercice 2.30 page 184]) we conclude that the elliptic curve $E/\mathbf{F}_p$ is supersingular (see [24, page 137]). Moreover we know, by a result of Shioda (see e.g. [2]), that if $\mathrm{char}\,\mathbf{F}_q \neq 2$, the Picard number of $\mathrm{Km}(C \times C)$ is 22 provided the elliptic curve $C/\mathbf{F}_q$ is supersingular. In the present case, we get

$$\rho(K4|\mathbf{F}_q) = \rho(\mathrm{Km}(E \times E)|\mathbf{F}_q) = 22\,.$$

Thus, the injectivity of (3.8) and the fact that $\dim_{\mathbf{Q}_\ell} H^2_{K4} = 22$ enables us to obtain

$$m_{K4}(1; q) = 22\,,$$

hence the following expressions for the polynomial $P_2(K4/\mathbf{F}_{p^{2f}}; T)$ and for the zeta function of $K4$ over $\mathbf{F}_{p^{2f}}$:

$$\begin{aligned} P_2(K4/\mathbf{F}_{p^{2f}}; T) &= (1 - p^{2f}T)^{22}\,,\\ Z(K4/\mathbf{F}_{p^{2f}}; T) &= \frac{1}{(1-T)(1-p^{4f}T)(1-p^{2f}T)^{22}}\,. \end{aligned}$$

This immediately yields

$$|K4(\mathbf{F}_{p^{2f}})| = 1 + p^{4f} + 22p^{2f}\,.$$

3.4. An elliptic pencil on $K4$. Now we turn to the case where $\mathbf{F}_q$ does not necessarily contain any primitive cube root of 1. In that case there is no guarantee that $K4/\mathbf{F}_q$ is a Kummer surface. Following [5], we notice that an elliptic fibration on $K4$ can be made explicit. Indeed, let us consider the family of cubics of $\mathbb{P}^2$ parametrized by τ:

$$E_\tau : XYZ - \tau(X+Y+Z)(XY+YZ+XZ) = 0\,.$$

The discriminant of the generic fibre E_τ is

$$\Delta(\tau) = \frac{1}{16}\tau^9(9\tau - 1)(\tau - 1)^3\,.$$

We deduce that the singular fibres correspond to $\tau \in \{\infty, 0, \frac{1}{9}, 1\}$. With the same notations as in Section 3.2, the base points of the family $\{E_\tau\}_\tau$ are

$$\begin{array}{ll} \mathcal{D}_x \cap \mathcal{D}_y \cap \mathcal{C} = (0:0:1) & \mathcal{D}_x \cap \mathcal{D}_z \cap \mathcal{C} = (0:1:0)\\ \mathcal{D}_y \cap \mathcal{D}_z \cap \mathcal{C} = (1:0:0) & \mathcal{D}_x \cap \mathcal{D}_{x,y,z} = (0:-1:1)\\ \mathcal{D}_y \cap \mathcal{D}_{x,y,z} = (-1:0:1) & \mathcal{D}_z \cap \mathcal{D}_{x,y,z} = (-1:1:0)\,. \end{array}$$

These are all singular points for the sextic curve C. As noticed by the authors in [5], each curve E_τ intersects the branch locus C of $K4$ exactly in the points at which a blowing up is performed for the construction of $K4$ (apart from the elements of $\mathcal{C} \cap \mathcal{D}_{x,y,z}$). So, when blowing up $\mathbb{P}^2$ at the base points of $\{E_\tau\}_\tau$, the strict transform of the generic cubic intersects no components of odd multiplicity of the total transform of the branch locus.

After blowing up $\mathbb{P}^2$ at the base points, we get an elliptic pencil on a rational surface which gives rise, after double cover ramified over the union of the singular cubics E_0 and E_∞ (exactly corresponding to the branch locus C), to the surface $K4$. We denote by φ the corresponding elliptic fibration.

One notices that, taking the final double cover can be interpreted as performing, in the equation defining E_τ the change of variable $\tau = t^2$ so that the generic fibre of the elliptic pencil on $K4$ can be given by

$$XYZ - t^2(X+Y+Z)(XY+YZ+XZ) = 0\,. \tag{3.10}$$

In [5], Beukers and Stienstra, determining the singular fibre combination of the elliptic fibration on $K4$ given by (3.10), prove, using a theorem of Shioda

$$P_2(K4/\mathbf{F}_q;T) = (1-qT)^{19}(1-\varepsilon^r qT)P_{21}(K4/\mathbf{F}_q;T)\,,$$

where $q = p^r$, $\varepsilon = -1$ if $p \equiv -1 \pmod 3$, $\varepsilon = 1$ otherwise. Moreover $P_{21}(K4/\mathbf{F}_q;T) \in \mathbf{Z}[T]$, $P_{21}(K4/\mathbf{F}_q;0) = 1$ and $\deg P_{21}(K4/\mathbf{F}_q) = 2$.

From Section 3.3, for $\mathbf{F}_{q^2} = \mathbf{F}_q(\zeta_3)$, we know that

$$P_{21}(K4/\mathbf{F}_{q^2};T) = P_{21}(\mathrm{Km}(E\times E)/\mathbf{F}_{q^2};T)\,, \tag{3.11}$$

where we recall that E is the CM elliptic curve given by

$$y^2 = x^3 + 1\,.$$

So, there exist conjugate complex numbers λ_1 and λ_2 such that

$$Z(K4/\mathbf{F}_q;T) = \frac{1}{(1-T)(1-q^2T)(1-qT)^{19}(1-\varepsilon^r qT)(1-\lambda_1^r T)(1-\lambda_2^r T)}\,.$$

From that formula we immediately deduce

$$|K4(\mathbf{F}_q)| = 1 + q^2 + 19q + \varepsilon^r q + \lambda_1^r + \lambda_2^r\,, \tag{3.12}$$

where the explicit values of λ_1 and λ_2 are given by the following proposition

Proposition 3.6.

- *If $p \equiv 1 \pmod 6$, there exist $a, b \in \mathbf{Z}$ such that $p = a^2 + 3b^2$ and λ_1, λ_2 are the reciprocal roots of*

$$P_{21}(K4/\mathbf{F}_p;T) = p^2T^2 - (4a^2 - 2p)T + 1\,.$$

- *If $p \equiv -1 \pmod 6$ then λ_1, λ_2 are the reciprocal roots of*

$$P_{21}(K4/\mathbf{F}_p;T) = -p^2T^2 + 1\,,$$

that is to say, $\lambda_1 = p$ and $\lambda_2 = -p$.

Proof. The case $p \equiv 1 \pmod 3$ has been treated in Section 3.3.

If $p \equiv -1 \pmod 6$ we consider, as in Section 3.3, the action of the group $G = \langle \gamma_1, \gamma_2 \rangle$ on $K4$ seen as a surface defined over a field $\mathbf{F}_q$ such that $\zeta_3 \notin \mathbf{F}_q$. Exploiting figure 2, we see that the number of ramification points of $K4/\mathbf{F}_q$ is

$$8(q+1) + 12(q-1)\,.$$

In the case where $q = p \equiv -1 \pmod 6$, we get from (3.12) and the counting of the number of stabilized points on $K4$ under the action of G performed in Section 3.3:

$$1 + p^2 + 18p + \lambda_1 + \lambda_2 \equiv 8(p+1) + 12(p-1) + 2 \pmod 6\,.$$

Hence $\lambda_1 + \lambda_2 \equiv 0 \pmod 6$. As p is inert in $K = \mathbf{Q}(\sqrt{-3})$, Section 3.3 yields

$$\lambda_1 + \lambda_2 = 0 \quad \text{and} \quad \lambda_1 \lambda_2 = \pm p^2\,.$$

Now, as $\zeta_3 \in \mathbf{F}_{p^2}$, the calculation we have just done applied to $K4/\mathbf{F}_{p^2}$ yields

$$|K4(\mathbf{F}_{p^2})| = 1 + p^4 + 20p^2 + \lambda_1^2 + \lambda_2^2 \equiv 8(p^2+1) + 14(p^2-1) + 2 \pmod 6\,.$$

Hence $\lambda_1^2 + \lambda_2^2 \equiv 2 \pmod 6$ so $\lambda_1\lambda_2 \equiv -p^2 \pmod 6$. We conclude that $\lambda_1\lambda_2 = -p^2$ and the proof is complete. □

Remark 3.7. In the context of the Inose-Shioda correspondence (see [13]), equation (3.11) means that the matrix corresponding to the 2-dimensional lattice of transcendental cycles on $K4$ is

$$\begin{pmatrix} 4 & 2 \\ 2 & 4 \end{pmatrix}.$$

By [13, 1.3], this implies that the group of sections of the elliptic fibration on $K4$ is of order 6. Indeed (3.10) can be written in Weierstrass form as follows (see [5]):

$$V^2W + (1-3t)UVW - t^4(t^2-1)VW^2 = U^3\,.$$

We see immediately that $(0:0:1)$ is a point of order 3 on the generic fibre. Moreover, the affine part $Z = 1$ of the generic cubic E_t can be written, after a suitable change of variables (using, for instance, a computer algebra system) $V^2 = f(U)$ where

$$\begin{aligned} f(U) &= U^3 + A(T)U + B(T)\,, \\ A(T) &= \frac{1}{4}(-\frac{3}{4}T^8 + T^6 - \frac{5}{2}T^4 + T^2 - \frac{1}{12})\,, \\ B(T) &= \frac{1}{8}(-\frac{1}{4}T^{12} + \frac{1}{2}T^{10} + \frac{5}{4}T^8 - \frac{5}{3}T^6 + \frac{11}{12}T^4 - \frac{1}{6}T^2 + \frac{1}{108})\,. \end{aligned}$$

In order to find an element of order 2 on each fibre, it is sufficient to find a root of f in the function field $\mathbf{F}_q(t)$. The polynomial

$$r(T) = \frac{1}{2}(-\frac{1}{2}T^4 - T^2 + \frac{1}{6})$$

fulfills this condition.

We are now ready to prove Theorem 1.2; it suffices to recover the number of $\mathbf{F}_q$-rational points on the surface S_0 attached to $\sigma_3(q)$ from the knowledge of the quantity $|K4(\mathbf{F}_q)|$.

3.5. End of the proof of Theorem 1.2. We want to obtain an explicit value for $\sigma_3(q)$; we first determine the number of $\mathbf{F}_q$-rational points on the affine surface S_4 defined by (3.3).

Lemma 3.8. *We have*

$$|S_4(\mathbf{F}_q)| = q^2 + 2q + \lambda_1^r + \lambda_2^r\,,$$

where $q = p^r$ and λ_1, λ_2 are defined by Proposition 3.6.

Proof. From the construction of the surface $K4$ detailed in Section 3.2, we have:

$$|K4(\mathbf{F}_q)| = |S_4(\mathbf{F}_q) \setminus \{(x,y,s)|s=0\}| + |\{\text{ramification points of}\, K4/\mathbf{F}_q\}|$$

Moreover, we claim that

$$|\{(x,y,s) \in S_4(\mathbf{F}_q)|s=0\}| = \begin{cases} 4q-7\,\text{if}\,\zeta_3 \in \mathbf{F}_q\,, \\ 4q-5\,\text{otherwise}\,. \end{cases}$$

Indeed, the cardinality of the left hand side set in the above equality is the number of $\mathbf{F}_q$-rational points on the union of rational affine curves: $\mathcal{D}^x \cup \mathcal{D}^y \cup \mathcal{D}^{x,y} \cup \mathcal{C}^{x,y}$, where

$$\mathcal{D}^x : x = 0 \quad \mathcal{D}^y : y = 0$$
$$\mathcal{D}^{x,y} : x + y + 1 = 0 \quad \mathcal{C}^{x,y} : xy + y + x = 0$$

The number of $\mathbf{F}_q$-rational points of each of the 3 lines $\mathcal{D}^{x,y}$, $\mathcal{D}^x$ and $\mathcal{D}^y$ is q . What's more, we can give the following parametrization: $\mathcal{C}^{x,y}(\mathbf{F}_q) = \{(\lambda; \frac{-\lambda}{\lambda+1})|\lambda \in \mathbf{F}_q \setminus \{-1\}\}$. Hence $|\mathcal{C}^{x,y}(\mathbf{F}_q)| = q - 1$. We also have

$$\mathcal{C}^{x,y}(\mathbf{F}_q) \cap \mathcal{D}^x(\mathbf{F}_q) \cap \mathcal{D}^y(\mathbf{F}_q) = (0;0)$$
$$\mathcal{D}^x(\mathbf{F}_q) \cap \mathcal{D}^{x,y}(\mathbf{F}_q) = (0;-1)\,, \quad \mathcal{D}^y(\mathbf{F}_q) \cap \mathcal{D}^{x,y}(\mathbf{F}_q) = (-1;0)$$
$$\mathcal{D}^{x,y}(\mathbf{F}_q) \cap \mathcal{C}^{x,y}(\mathbf{F}_q) = \begin{cases} \{(\zeta_3;\zeta_3^2),(\zeta_3^2;\zeta_3)\}\ \text{if}\,\zeta_3 \in \mathbf{F}_q\,, \\ \emptyset\,\text{otherwise}\,. \end{cases}$$

The claim follows from putting these pieces of information together.

Thanks to the calculation of the number of ramification points on $K4/\mathbf{F}_q$ performed in the proof of Proposition 3.6 (when $\zeta_3 \notin \mathbf{F}_q$) and in Section 3.3 (when $\zeta_3 \in \mathbf{F}_q$), we deduce

$$|K4(\mathbf{F}_q)| = \begin{cases} |S_4(\mathbf{F}_q)| - (4q-7) + 8(q+1) + 14(q-1) \,\text{if}\, \zeta_3 \in \mathbf{F}_q\,, \\ |S_4(\mathbf{F}_q)| - (4q-5) + 8(q+1) + 12(q-1) \,\text{otherwise}\,. \end{cases}$$
$$= \begin{cases} |S_4(\mathbf{F}_q)| + 18q + 1 \,\text{if}\, \zeta_3 \in \mathbf{F}_q\,, \\ |S_4(\mathbf{F}_q)| + 16q + 1 \,\text{otherwise}\,. \end{cases}$$

Exploiting (3.12) and noticing that $\varepsilon^r = 1$ if and only if $\zeta_3 \in \mathbf{F}_q = \mathbf{F}_{p^r}$, we see that the proof is complete □

Combining Lemmas 3.3 and 3.8, we get

$$\begin{aligned} |S_3(\mathbf{F}_q)| &= q^2 + \chi_q(-1)(|S_4(\mathbf{F}_q)| - q^2) \\ &= q^2 + \chi_q(-1)(2q + \lambda_1^r + \lambda_2^r)\,. \end{aligned}$$

To apply Lemma 3.2 and deduce $|S_0(\mathbf{F}_q)|$ we must exhibit the relation between $|S_3(\mathbf{F}_q)|$ and $|S_3^*(\mathbf{F}_q)|$. Reasoning as in the proof of Lemma 3.8 where we deduced $|S_4(\mathbf{F}_q)|$ from the computation of $|\{(x,y,s) \in S_4(\mathbf{F}_q) | s \neq 0\}|$, we obtain

$$|S_3^*(\mathbf{F}_q)| = \begin{cases} |S_3(\mathbf{F}_q)| - (4q-7) \,\text{if}\, \zeta_3 \in \mathbf{F}_q\,, \\ |S_3(\mathbf{F}_q)| - (4q-5) \,\text{otherwise}\,. \end{cases}$$

Hence

$$|S_3^*(\mathbf{F}_q)| = \begin{cases} q^2 + \chi_q(-1)(2q + \lambda_1^r + \lambda_2^r) - 4q + 7 \,\text{if}\, \zeta_3 \in \mathbf{F}_q\,, \\ q^2 + \chi_q(-1)(2q + \lambda_1^r + \lambda_2^r) - 4q + 5 \,\text{otherwise}\,. \end{cases}$$

We can now apply Lemma 3.2; this yields

$$|S_0(\mathbf{F}_q)| = \begin{cases} q^2 + \chi_q(-1)(2q + \lambda_1^r + \lambda_2^r) - 2q + 5 \,\text{if}\, \zeta_3 \in \mathbf{F}_q\,, \\ q^2 + \chi_q(-1)(2q + \lambda_1^r + \lambda_2^r) - 4q + 5 \,\text{otherwise}\,. \end{cases}$$
$$= \begin{cases} q^2 + 2q(\chi_q(-1) - 1) + \chi_q(-1)(\lambda_1^r + \lambda_2^r) + 5 \,\text{if}\, \zeta_3 \in \mathbf{F}_q\,, \\ q^2 + 2q(\chi_q(-1) - 2) + \chi_q(-1)(\lambda_1^r + \lambda_2^r) + 5 \,\text{otherwise}\,. \end{cases}$$

Moreover, we get from (3.1)

$$\sigma_3(q) = -q^3 + 3q^2 - 3q + q|S_0(\mathbf{F}_q)|\,.$$

We finally obtain the following value for $\sigma_3(q)$, so that the proof of Theorem 1.2 is complete:

$$\sigma_3(q) = \begin{cases} q^2 + q(2q\chi_q(-1) + \chi_q(-1)(\lambda_1^r + \lambda_2^r) + 2) \,\text{if}\, \zeta_3 \in \mathbf{F}_q\,, \\ -q^2 + q(2q\chi_q(-1) + \chi_q(-1)(\lambda_1^r + \lambda_2^r) + 2) \,\text{otherwise}\,. \end{cases}$$

References

[1] S. Ahlgren, K. Ono, *Modularity of a certain Calabi-Yau threefold.* Monatsh. Math. **129** (2000), no. 3, 177–190.

[2] M. Artin, *Supersingular $K3$ surfaces.* Ann. Scient. Éc. Norm. Sup., 4e série, **7** (1974), 543–568.

[3] A. O. L. Atkin, *Note on a paper of Birch.* J. London Math. Soc. **44** (1969).

[4] W. Barth, C. Peters, A. van de Ven, *Compact complex surfaces.* Springer, Berlin-Heidelberg-New York, 1984.

[5] F. Beukers, J. Stienstra, *On the Picard-Fuchs equation and the formal Brauer group of certain elliptic $K3$-surfaces.* Math. Ann. **271** (1985), 269–304.

[6] B. J. Birch, *How the number of points of an elliptic curve over a fixed prime field varies.* J. London Math. Soc. **43** (1968) 57–60.

[7] A. Calabri, R. Ferraro, *Explicit resolutions of double point singularities of surfaces.* Collect. Math. **53** (2002), no. 2, 99–131.

[8] P. Deligne, *Cohomologie étale, SGA* $4\frac{1}{2}$. Lectures Notes in Math. 569, Springer Verlag 1977.

[9] P. Deligne, *La conjecture de Weil. II.* Inst. Hautes Études Sci. Publ. Math. **52** (1980), 137–252.

[10] L. Fu, D. Wan, *L-functions for symmetric products of Kloosterman sums.* J. reine angew. Math. **589** (2005), 79–103.

[11] R. Hartshorne, *Algebraic geometry.* GTM 52, Springer-Verlag, 1977.

[12] B. Hunt, *The geometry of some special arithmetic quotients.* Lecture Notes in Math. **1637**. Springer-Verlag, Berlin, 1996.

[13] H. Inose, T. Shioda, *On singular $K3$ surfaces.* Complex analysis and algebraic geometry (eds Baily, W. and Shioda, T.), Cambridge (1977), 119-136.

[14] K. Ireland, M. Rosen, *A classical introduction to modern number theory*, Second Edition, GTM 84, Springer-Verlag 1990.

[15] H. Iwaniec, *Topics in classical automorphic forms.* Graduate Studies in Mathematics, 17, American Mathematical Society, 1997.

[16] A. J. de Jong, N. M. Katz, *Monodromy and the Tate conjecture: Picard numbers and Mordell-Weil ranks in families.* Israel J. Math. **120** (2000), part A, 47–79.

[17] N. M. Katz, *Gauss sums, Kloosterman sums, and monodromy groups.* Annals of Mathematics Studies **116**. Princeton University Press, Princeton, NJ, 1988

[18] D. H. Lehmer, E. Lehmer, *On the cubes of Kloosterman sums.* Acta Arith. **6** (1960), 15–22.

[19] R. Livné, *Cubic exponential sums and Galois representations* . Current trends in arithmetical algebraic geometry (Arcata, Calif., 1985), 247–261, Contemp. Math. **67**, Amer. Math. Soc., Providence, RI, (1987).

[20] Yu. Manin, *Cubic forms.* Algebra, geometry, arithmetic. Second edition. North-Holland Mathematical Library, 4. North-Holland Publishing Co., Amsterdam, 1986.

[21] L. J. Mordell, *On Lehmer's congruence associated with cubes of Kloosterman's sums.* J. London Math. Soc. **36** (1961), 335–339.

[22] H. Salié, *Über die Kloostermanschen Summen $S(u, v; q)$.* Math. Zeit. **34** (1932), 91–109.

[23] T. W. Sederberg, *Techniques for cubic algebraic surfaces.* IEEE Comp. Graph and Appl., September 1990.

[24] J. Silverman, *The arithmetic of elliptic curves.* GTM 106, Springer-Verlag, 1986.

[25] J. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Second Edition, GTM 151, Springer-Verlag, 1999.

[26] H. P. F. Swinnerton-Dyer, *The zeta function of a cubic surface over a finite field.* Proc. Camb. Phil. Soc. **63** (1967), 55.

[27] H. A. Verril, *The L-series of certain rigid Calabi-Yau threefolds.* J. Number Theory **81** (2000), no. 2, 310–334.

Florent Jouve
Dept. of Mathematics
The University of Texas at Austin
1 University Station C1200
Austin, TX, 78712, USA.
E-mail: jouve@math.utexas.edu
URL: www.math.utexas.edu/~jouve