Crelle 328 (1981), 208-220.

Some estimates from étale cohomology

By *J. S. Milne**) at Ann Arbor

The primary purpose of this paper is to prove the inequality used in § 13 of the preceding paper (see especially Lemma 17 of that paper). The elegant argument used in C to complete the proof is largely due to P. Deligne (for the author's original approach, see Remark 3 below). A secondary purpose is to illustrate how the methods developed by Deligne in [1] and [2] can be used to derive certain types of estimates. For this reason, some of the arguments have been given in greater generality than is strictly necessary to prove the main result, and some proofs have been given in more detail than is the (author's) custom. I would like to thank N. Katz for many helpful conversations.

The notations concerning étale cohomology will be the same as in [6]. All cohomology groups will be with respect to the étale topology; F will denote the Frobenius endomorphism (relative to $\mathbb{F}_p$), and $\operatorname{Tr}(F|H^*)$ abbreviates $\sum(-1)^r \operatorname{Tr}(F|H^r)$. The numbers p, q, l, and r are related by $l \neq p$, $q = p^r$. Other notations are similar to, but not identical with, those used in the preceding paper. The symbols $\mathbb{A}^1$ and $\mathbb{P}^1$ denote the affine and projective lines, and $\mathbb{F}_q$ and $\bar{\mathbb{F}}_q$ denote the field of q elements and its algebraic closure.

A. Pencils of elliptic curves

Let V^* be a projective smooth surface over $\bar{\mathbb{F}}_p$ and let $\pi\colon V^* \longrightarrow \mathbb{P}^1$ be a morphism whose fibres, except for a finite number, are elliptic curves. We assume that a model for (V^*, π) is given over $\mathbb{F}_q$ so that it makes sense, for example, to speak of the points of a fibre V_t^*, $t \in \mathbb{P}^1(\mathbb{F}_q)$, with coordinates in $\mathbb{F}_q$. Write $q - e_r(t) + 1$ for the number of such points; the Riemann hypothesis shows that $|e_r(t)| \leqq 2\sqrt{q}$. Let $\mathscr{E} = R^1\pi_* \mathbb{Q}_l$, and let $S \subset \mathbb{P}^1(\bar{\mathbb{F}}_p)$ be the set of t for which V_t^* is singular. There is a morphism $j\colon \mathbb{P}^1 - S \longrightarrow \mathbb{P}^1$ sending each point t to the j-invariant of the fibre V_t^*. Let $\eta = \operatorname{spec} K$ be the generic point of $\mathbb{P}^1$, and let $M = \mathscr{E}_{\bar{\eta}}$ be the generic stalk of $\mathscr{E}$, so that $M = T_l \otimes \mathbb{Q}$ where T_l is the Tate module of the generic member V_η^* of our family of elliptic curves.

Lemma 1. *If j is not constant, then M is an absolutely irreducible* $\operatorname{Gal}(\bar{K}/K)$*-module.*

Proof. Assume $p \neq 2$; then there is a finite extension K' of K and a $\lambda \in K'$ such that V_η^* is isomorphic over K' to

$$Y^2Z = X(X-Z)(X-\lambda Z).$$

*) partially supported by N.S.F.

0075-4102/81/0328-0013$02.00

Theorem 1 of [4] shows that the image of $\mathrm{Gal}(\bar{K}/K')$ in $\mathrm{End}(M)$ generates $\mathrm{End}(M)$ as a $\mathbb{Q}_l$-algebra. Thus M is absolutely irreducible as a $\mathrm{Gal}(\bar{K}/K')$-module and, a fortiori, as a $\mathrm{Gal}(\bar{K}/K)$-module. If $p=2$, the argument can be repeated with Theorem 2 of [4] substituted for Theorem 1. (If π arises from a Lefschetz pencil, one can also use the fact that the action of $\mathrm{Gal}(\bar{K}/K)$ on $E/E \cap E^{\perp}$ is absolutely irreducible, where E denotes the vanishing cycles (see [1], 5. 5); in our case $E^{\perp} = M^{\mathrm{Gal}} = 0$ and $E = M$.)

Proposition 1. (a) $\mathrm{Tr}(F^r|H^*(\mathbb{P}^1, \mathcal{E})) = \sum_t e_r(t)$, *where the sum is over all* $t \in \mathbb{P}^1(\mathbb{F}_q)$.

(b) *If j is not constant, then* $|\sum e_r(t)| \leqq (\beta_2(V^*)-2)q$, *where* $\beta_2(V^*)$ *is the second l-adic Betti number of* V^*.

Proof. (a) According to the Lefschetz trace formula [6], VI 13. 4,

$$\mathrm{Tr}(F^r|H^*(\mathbb{P}^1, \mathcal{E})) = \sum_t \mathrm{Tr}(F^r|\mathcal{E}_{\bar{t}})$$

where $\mathcal{E}_{\bar{t}}$ is the stalk of $\mathcal{E}$ at a geometric point $\bar{t}$ lying over $t \in \mathbb{P}^1(\mathbb{F}_q)$. The proper base change theorem shows that $\mathcal{E}_{\bar{t}} = H^1(V^*_{\bar{t}}, \mathbb{Q}_l)$, and the trace formula shows that $\mathrm{Tr}(F^r|H^1(V_{\bar{t}}, \mathbb{Q}_l)) = e_r(t)$.

(b) Let $U = \mathbb{P}^1 - S$; we have $H^2(\mathbb{P}^1, \mathcal{E}) = H^2_c(U, \mathcal{E})$ and, because $\mathcal{E}$ has no sections with support on a finite set, $H^0(\mathbb{P}^1, \mathcal{E}) \hookrightarrow H^0(U, \mathcal{E})$. The action of $\mathrm{Gal}(\bar{K}/K)$ on M factors through $\pi_1 \overset{df}{=} \pi_1(U, \bar{\eta})$, and $H^0(U, \mathcal{E}) = M^{\pi_1}$ and $H^2_c(U, \mathcal{E}) = M_{\pi_1}(-1)$ (see [6], V 2. 4b). Lemma 1 therefore shows that $H^0(\mathbb{P}^1, \mathcal{E}) = 0 = H^2(\mathbb{P}^1, \mathcal{E})$, and the Leray spectral sequence $H^r(\mathbb{P}^1, R^s\pi_* \mathbb{Q}_l) \Rightarrow H^{r+s}(V^*, \mathbb{Q}_l)$ consequently degenerates. As $R^r\pi_*\mathbb{Q}_l = \mathbb{Q}_l, \mathcal{E}, \mathbb{Q}_l(-1)$ for $r = 0, 1, 2$, this shows that

$$H^2(V^*, \mathbb{Q}_l) = \mathbb{Q}_l(-1) \oplus H^1(\mathbb{P}^1, \mathcal{E}) \oplus \mathbb{Q}_l(-1).$$

Hence $\dim H^1(\mathbb{P}^1, \mathcal{E}) = \beta_2(V^*) - 2$, and (b) of the proposition follows from part (a) because the Riemann hypothesis for V^* shows that the eigenvalues of F^r on $H^1(\mathbb{P}^1, \mathcal{E})$ have absolute value q.

Remark 1. It is usually possible to compute the dimension of $H^1(\mathbb{P}^1, \mathcal{E})$ from a knowledge of the singularities of the fibres V^*_t, $t \in S$ (see [3], XVI 2. 4). For example, if π arises from a Lefschetz pencil, then

$$\dim H^1(\mathbb{P}^1, \mathcal{E}) = -\chi(\mathbb{P}^1, \mathcal{E}) = s - 4$$

where s is the order of S, and so $|\sum e_r(t)| \leqq (s-4)\, q^{1/2}$ (see [6], V 2. 12).

Proposition 2. *If j is not constant, then*

$$\sum_{t \in \mathbb{F}_q} e_r(t)^2 = q^2 + O(q^{3/2}).$$

Proof. The Lefschetz trace formula shows that

$$\mathrm{Tr}(F^r|H^*_c(\mathbb{A}^1, \mathcal{E} \otimes \mathcal{E})) = \sum e_r(t)^2.$$

Let $U = \mathbb{A}^1 - S$. Then $\mathcal{E}|U$ is locally constant and self-dual, and so

$$H^2_c(\mathbb{A}^1, \mathcal{E} \otimes \mathcal{E}) = H^2_c(U, \mathcal{E} \otimes \mathcal{E})$$

is, up to a Tate twist, the dual of

$$H^0(U, \mathcal{E} \otimes \mathcal{E}) = (M \otimes M)^{\pi_1} = \mathrm{Hom}(M, M)^{\pi_1} = \mathrm{Hom}(M, M)^{\mathrm{Gal}(\bar{K}/K)}.$$

Lemma 1 shows that this last vector space is $\mathbb{Q}_l$, and so $H_c^2(\mathbb{A}^1, \mathscr{E} \otimes \mathscr{E}) = \mathbb{Q}_l(-2)$. Therefore

$$\operatorname{Tr}(F^r | H_c^*(\mathbb{A}^1, \mathscr{E} \otimes \mathscr{E})) = q^2 - \operatorname{Tr}(F^r | H_c^1) + \operatorname{Tr}(F^r | H_c^0) = q^2 + O(q^{3/2})$$

by [2].

Remark 2. (a) The constant implicit in the O can be calculated from $\mathscr{E}$. For example, if π arises from a Lefschetz pencil, then the conductor $c_t(\mathscr{E}) = 1$ and $c_t(\mathscr{E} \otimes \mathscr{E}) \leqq 3$ for $t \in S$. Therefore [6], V 2. 12 shows that

$$\chi_c(\mathbb{A}^1, \mathscr{E} \otimes \mathscr{E}) \geqq 2 \cdot 4 - 3s - 4 = 4 - 3s.$$

As $H_c^0(\mathbb{A}^1, \mathscr{E} \otimes \mathscr{E}) = 0$, we see that $\dim H_c^1(\mathbb{A}^1, \mathscr{E} \otimes \mathscr{E}) \leqq 3s - 3$, and so

$$\Big| \sum_{t \in \mathbb{F}_q} e_r(t)^2 - q^2 \Big| \leqq (3s-3)\, q^{3/2}.$$

(b) An argument similar to that in the proposition shows that

$$\sum_{t \in \mathbb{F}_q} e_r(t)\, e_r(t+u) = O(q^{3/2})$$

provided the sets S and $\{s - u | s \in S\}$ are disjoint.

Let $\phi: \mathbb{A}^2 \to \mathbb{A}^1$ be the map $(t_1, t_2) \mapsto t_1 + t_2$, and let pr_1 and pr_2 be the projection maps $\mathbb{A}^2 \rightrightarrows \mathbb{A}^1$. Denote $\mathbf{R}\phi_!(\mathrm{pr}_1^* \mathscr{E} \otimes \mathrm{pr}_2^* \mathscr{E})$ (an object of the derived category of $\mathbb{Q}_l$-sheaves on $\mathbb{A}^1$) by $\mathscr{E} * \mathscr{E}$.

Lemma 2. $$\operatorname{Tr}(F^r | \mathbb{H}_c^*(\mathbb{A}^1, (\mathscr{E} * \mathscr{E}) \otimes (\mathscr{E} * \mathscr{E}))) = \sum_{u \in \mathbb{F}_q} \Big(\sum_{t \in \mathbb{F}_q} e_r(t)\, e_r(u-t) \Big)^2 = \sum_{u \in \mathbb{F}_q} \Big(\sum_{t \in \mathbb{F}_q} e_r(t)\, e_r(t+u) \Big)^2.$$

Proof. The first equality is an immediate consequence of the Lefschetz trace formula, and the second is trivial, both sums being equal to $\sum_{t_1 + t_2 = t_3 + t_4} e_r(t_1)\, e_r(t_2)\, e_r(t_3)\, e_r(t_4)$.

Proposition 3. *If π arises from a Lefschetz pencil then there exists a constant $A(s)$, depending only on s, such that*

$$\dim(H_c^i(\mathbb{A}^1, (\mathscr{E} * \mathscr{E}) \otimes (\mathscr{E} * \mathscr{E}))) \leqq A(s)$$

for all i.

Proof. We first need a lemma.

Lemma 3. *Let $\mathscr{F}$ be a sheaf on $\mathbb{P}^1$ that is locally constant off a finite set S with s' elements, has stalks of dimension $\leqq d$, and is tamely ramified at all points of S. Then the dimensions of the spaces $H^i(\mathbb{P}^1, \mathscr{F})$ are bounded in terms of s' and d.*

Proof. Let $U = \mathbb{P}^1 - S$. From the exact sequence

$$\cdots \to H_c^i(U, \mathscr{F}) \to H^i(\mathbb{P}^1, \mathscr{F}) \to \bigoplus_{t \in S} H^i(t, \mathscr{F}) \to \cdots$$

we see that it suffices to bound the dimensions of the spaces $H_c^i(U, \mathscr{F})$. But $H_c^0(U, \mathscr{F}) = 0$, and $H_c^2(U, \mathscr{F}) = (\mathscr{F}_{\bar\eta})_{\pi_1}(-1)$ has dimension $\leqq d$. The conductor of $j_!\mathscr{F}$, where j denotes the inclusion $U \hookrightarrow \mathbb{P}^1$, is ds' and so $\chi_c(U, \mathscr{F}) = 2d - ds'$; therefore $\dim H_c^1(U, \mathscr{F}) \leqq d(s'-1)$.

Let $a\colon \mathbb{A}^1 \hookrightarrow \mathbb{P}^1$ be the usual inclusion; we have to show that $a_!((\mathscr{E} * \mathscr{E}) \otimes (\mathscr{E} * \mathscr{E}))$ (or rather its homology groups—recall that $\mathscr{E} * \mathscr{E}$ is a complex) satisfies the conditions of the lemma with s' and d bounded in terms of s. Clearly it suffices to prove the same result for $a_!(\mathscr{E} * \mathscr{E})$.

The existence of d is easy: for any $u \in \mathbb{A}^1(\bar{\mathbb{F}}_p)$

$$H^i(a_!(\mathscr{E} * \mathscr{E}))_u = H^i(\mathscr{E} * \mathscr{E})_u = H^i_c(\mathbb{A}^1, \mathscr{E} \otimes \mathscr{E}(u))$$

where $\mathscr{E}(u)$ is the pull-back of $\mathscr{E}$ relative to $t \mapsto (u-t)$; since $a_!(\mathscr{E} \otimes \mathscr{E}(u))$ is locally constant off a set with at most (s^2+1) elements, has stalks of dimension $\leqq 4$, and is tamely ramified, the lemma provides a bound for the dimensions of its cohomology groups.

For the other two conditions, we need the following general result.

Lemma 4. *Consider a diagram*

$$\begin{tikzcd}
X \arrow[d, "\pi"'] & & D \arrow[ll, hook', "i"'] \arrow[dll] \\
T & &
\end{tikzcd}$$

in which T is a smooth curve, π is proper and smooth with fibres of dimension 1, *and D is a divisor on X with normal crossings relative to π. Let $\mathscr{F}$ be a constructible sheaf of $\mathbb{Q}_l$ vector spaces on X which is locally constant off D and tamely ramified on D, and let D' be an open subscheme of D which is finite and étale over T and such that $i^*\mathscr{F}$ is locally constant on D'. Then $R^i\pi_*\mathscr{F}$ is locally constant off $\pi(D-D')$ and is tamely ramified for all r.*

Proof. First suppose that $\mathscr{F} = j_!(\mathscr{F}|U)$, where $U = X - D$ and j is the immersion $U \hookrightarrow X$. As π is proper, there is an exact sequence

$$\cdots \longrightarrow H^i(X_{\bar t}, \mathscr{F}) \longrightarrow H^i(X_{\bar\eta}, \mathscr{F}) \longrightarrow H^i(X_{\bar t}, \mathbf{R}\Phi(\mathscr{F})) \longrightarrow \cdots$$

in which t and η are respectively closed and generic points of T and $\mathbf{R}\Phi(\mathscr{F})$ is the complex of vanishing cycles (see [3], XIII 2. 18. 9). It follows from [3], XIII 2. 1. 11 that $\mathbf{R}\Phi\mathscr{F} = 0$, and so $H^i(X_{\bar t}, \mathscr{F}) \xrightarrow{\approx} H^i(X_{\bar\eta}, \mathscr{F})$, i.e. $(R^i\pi_*\mathscr{F})_{\bar t} \xrightarrow{\approx} (R^i\pi_*\mathscr{F})_{\bar\eta}$. Because $R^i\pi_*\mathscr{F}$ is constructible, this implies ([6], V. 1. 10a) that $R^i\pi_*\mathscr{F}$ is locally constant on the whole of T in this case.

The lemma is obvious if $\mathscr{F}$ has support on D, and the general case now follows from considering the cohomology sequence of

$$0 \longrightarrow j_!(j^*\mathscr{F}) \longrightarrow \mathscr{F} \longrightarrow i_*i^*\mathscr{F} \longrightarrow 0.$$

We apply this with $X = \mathbb{A}^1 \times \mathbb{P}^1$ and π the projection map $\mathbb{A}^1 \times \mathbb{P}^1 \longrightarrow \mathbb{A}^1$. Let $a\colon \mathbb{A}^1 \times \mathbb{A}^1 \hookrightarrow \mathbb{A}^1 \times \mathbb{A}^1 \subset \mathbb{A}^1 \times \mathbb{P}^1$ be the map $(x, y) \mapsto (x+y, y)$, and let $\mathscr{F} = a_!(\mathrm{pr}_1^*\mathscr{E} \otimes \mathrm{pr}_2^*\mathscr{E})$. As $\pi \circ a = \phi$, $\mathbf{R}\pi_*\mathscr{F} = \mathscr{E} * \mathscr{E}$. Let $D = \{(x, y) | x - y \in S \text{ or } y \in S \cup \{\infty\}\}$. The lemma shows that $\mathscr{E} * \mathscr{E}$ is locally constant off a set with at most s^2+2 elements and that it is tamely ramified there.

We come now to the example that will be of particular interest to us. Fix a prime p and elements α, β, γ, and N of $\mathbb{F}_p$. We assume:

(1) $$p > 3,\ N \neq 0,\ \alpha\beta\gamma \neq 0.$$

Let V be the projective smooth surface defined by

$$X^3+Y^3+Z^3=NW^3.$$

For $t=(t_0:t_1)\in \mathbb{P}^1(\bar{\mathbb{F}}_p)$, let H_t be the plane defined by

$$t_0(\alpha X+\beta Y+\gamma Z)=t_1 W,$$

and let $V_t=V\cap H_t$. We denote $(0:1)$ by ∞.

Let α', β', γ' be square roots of α, β, γ. The curve V_t is singular if and only if $t^3=N(\alpha'^3\pm\beta'^3\pm\gamma'^3)^2$ for some choice of signs. The family (H_t) is a Lefschetz pencil for V if and only if V_t is singular for exactly twelve $t\in\bar{\mathbb{F}}_p$ and $V_0\cap V_\infty$ has exactly three points in $\bar{\mathbb{F}}_p$. These conditions are satisfied if

$$\text{(2)}\qquad \left.\begin{array}{l}\alpha'^3\pm\beta'^3\pm\gamma'^3\neq 0\\ \alpha'^3\pm\beta'^3\neq 0,\ \ \beta'^3\pm\gamma'^3\neq 0,\ \ \gamma'^3\pm\alpha'^3\neq 0\end{array}\right\}\ \text{(all choices of signs).}$$

For the rest of this section we assume both (1) and (2) hold. Let $\pi\colon V^*\longrightarrow\mathbb{P}^1$ be the map defined by the pencil (H_t). Thus V^* is obtained from V by blowing up the three points of $V_0\cap V_\infty$, and for any $t\in\mathbb{P}^1$, $\pi^{-1}(t)=V_t$. The set S contains twelve values of t. For each $t\notin S$, V_t is an elliptic curve, and for $t\in S$, V_t has a single node as singularity. Note that, as V and the pencil are defined over $\mathbb{F}_p$, so also are V^* and π.

Let $q-e_r(t)+1$ denote the number of points on V_t with coordinates in $\mathbb{F}_q$, $q=p^r$. Then remarks 1 and 2 show that

$$\text{(3)}\qquad \Big|\sum_{t\in\mathbb{F}_q\cup\{\infty\}} e_r(t)\Big|\leqq 8q,$$

$$\text{(4)}\qquad \Big|\sum_{t\in\mathbb{F}_q} e_r(t)^2-q^2\Big|\leqq 33q^{3/2}.$$

Equation (3) can be made more precise. For example, if $p\equiv 2\pmod 3$, then $(x:y:z:w)\mapsto(x^3:y^3:z^3:w^3)$ is a bijection between the set of $\mathbb{F}_p$-rational points on the hyperplane $X+Y+Z=N^{1/3}W$ and $V(\mathbb{F}_p)$. Thus

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

$$\#(V^*(\mathbb{F}_p))=p^2+(1+f)\,p+1$$

where f is the number of $\mathbb{F}_p$-rational points on $V_0\cap V_\infty$ (note that f is 0, 1, or 3). Therefore $\sum(p-e(t)+1)=p^2+(1+f)\,p+1$, and $\sum e(t)=(1-f)\,p$ in this case. (We drop the subscript r when it is 1.)

In the preceding paper, $e(t)$ is written $E(t,p)$; thus, in the present notation, formulas (116) and (117) of that paper become

$$\Delta(\lambda)=\sum_{t\in\mathbb{F}_p} e(t)\,e(t+\lambda),$$

$$\square=\sum_{\lambda\in\mathbb{F}_p}\Delta(\lambda)^2.$$

We now state the main result of the paper, whose proof will be completed in C.

Theorem. *There exist constants B and C with the following property: for any α, β, γ, N, and p such that*

(a) *conditions* (1) *and* (2) *are satisfied,*

(b) $p > C$, *and*

(c) $p \equiv 1 \,(\mathrm{mod}\, 3)$ *or* $p \equiv 2 \,(\mathrm{mod}\, 3)$ *and* $f \neq 0$,

the inequality

$$\square \geqq 2\,p^4 - Bp^{7/2}$$

holds.

Remark 3. According to Lemma 2, in order to prove the theorem we have to show that

$$\mathrm{Tr}\left(F|\mathbb{H}_c^*(\mathbb{A}^1, (\mathscr{E} * \mathscr{E}) \otimes (\mathscr{E} * \mathscr{E}))\right) \geqq 2\,p^4 + O(p^{7/2}).$$

It is not difficult to show that p^4 occurs at least twice as an eigenvalue of F on this space, but I do not know how to prove in general that cancellation does not occur. My original approach was to find conditions on α, β, γ, N, and p sufficient to ensure that all eigenvalues of F on this space equalled p^4.

B. Exponential sums

For the rest of the paper, we assume $\mathbb{Q}_l$ contains a primitive p^{th} root ζ of 1, and we fix an embedding $\mathbb{Q}_l \hookrightarrow \mathbb{C}$ under which ζ maps to $\exp(2\pi i/p)$. Let U be the Galois covering of $\mathbb{A}^1_{\mathbb{F}_p}$ defined by $X^p - X = T$, and let Ψ be the locally constant sheaf on $\mathbb{A}^1$ associated with the representation $\mathrm{Gal}(U/\mathbb{A}^1) \longrightarrow \mathrm{Aut}(\mathbb{Q}_l)$ sending the canonical generator $\sigma\colon (t, x) \longmapsto (t, x+1)$ of $\mathrm{Gal}(U/\mathbb{A}^1)$ to multiplication by ζ. For $x \in \mathbb{F}_q$, we let

$$\psi(x) = \exp\left(2\pi i\, \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x)/q\right).$$

Lemma 5. (a) *For any* $t \in \mathbb{F}_q$, $\mathrm{Tr}(F^r|\Psi_{\bar{t}}) = \psi(t)$.

(b) *The wild conductor of* Ψ *at* ∞ *is* 1.

(c) *For all* i, $H_c^i(\mathbb{A}^1, \Psi) = 0$.

Proof. (a) Consider $x \in \bar{\mathbb{F}}_p$ such that $x^p - x = t$; then

$$x^q = x + \sum_{i=1}^{r} x^{p^i} - x^{p^{i-1}} = x + \mathrm{Tr}(t) = \sigma^{\mathrm{Tr}(t)}(x).$$

This shows that the Frobenius automorphism acts on U, and $\Psi_{\bar{t}}$, as

$$\zeta^{\mathrm{Tr}(t)} = \exp\left(2\pi i\, \mathrm{Tr}(t)/p\right) = \psi(t).$$

(b) Consider the extension K of $\bar{\mathbb{F}}_p((T^{-1}))$ defined by the equation $X^p - X = T$. If $\pi^{-1} \in K$ satisfies this equation, then π is a uniformizing parameter for K and $\sigma(\pi) = \sigma(\pi^{-1})^{-1} = \pi/1 - \pi$. The ramification groups of $K/\bar{\mathbb{F}}_p((T^{-1}))$ are

$$G_{-1} = G_0 = G_1 = \mathbb{Z}/p\mathbb{Z} \quad \text{and} \quad G_2 = \{0\}.$$

It is now easy to compute the conductor using [6], p. 188, Formula (d).

(c) It is obvious that $H_c^0(\mathbb{A}^1, \Psi)=0=H_c^2(\mathbb{A}^1, \Psi)$, and [6], V 2. 12 and (b) show that $\chi_c(\mathbb{A}^1, \Psi)=0$.

Let V be a smooth surface of degree d in $\mathbb{P}^3$, defined over $\bar{\mathbb{F}}_p$, but having a given model over $\mathbb{F}_q$. For $t=(t_0:t_1)\in\mathbb{P}^1(\bar{\mathbb{F}}_p)$, let $V_t=V\cap H_t$ where H_t is the hyperplane defined by

$$t_0(\alpha X+\beta Y+\gamma Z)=t_1 W$$

some $\alpha, \beta, \gamma\in\mathbb{F}_q$, $\alpha\beta\gamma\neq 0$. Assume that V_∞ is smooth and that $V_0\cap V_\infty$ has exactly d points in $\bar{\mathbb{F}}_p$. On blowing up these d points we obtain a surface V^* and a map $\pi\colon V^*\longrightarrow\mathbb{P}^1$ such that the fibre $\pi^{-1}(t)$, for $t\in\mathbb{P}^1(\bar{\mathbb{F}}_p)$, is V_t. Let $\mathscr{E}=R^1\pi_*\mathbb{Q}_l$ and let $c(\mathscr{E})$ be the sum $\sum c_t(\mathscr{E})$ of the conductors of $\mathscr{E}$ at the closed points t of $\mathbb{P}^1_{\mathbb{F}_p}$.

Lemma 6. *The conductor $c(\mathscr{E})$ of $\mathscr{E}$ is $d(d-1)^2$.*

Proof. A standard formula [6], VI. 5. 6 shows that the Betti numbers of V are 1, 0, d^3-4d^2+6d-2, 0, 1, and therefore the Betti numbers of V^* are 1, 0, d^3-4d^2+7d-2, 0, 1. From the Leray spectral sequence for π, we find that $\chi(V^*)=4-\chi(\mathscr{E})$. For η a generic point of $\mathbb{P}^1$, $\mathscr{E}_{\bar\eta}$ has dimension 2 genus$(V_{\bar\eta})=(d-1)(d-2)$. Thus [6], V. 2. 12 shows that $\chi(\mathscr{E})=2(d-1)(d-2)-c(\mathscr{E})$. On combining these statements, we find $c(\mathscr{E})=d(d-1)^2$.

For $\lambda\in\mathbb{F}_q^\times$, let Ψ^λ be the translate of Ψ by λ, so that $\Psi^\lambda_{\bar t}=\Psi_{\lambda\bar t}$. We write $e_r(t)=\mathrm{Tr}(F^r|\mathscr{E}_{\bar t})$ when $t\in\mathbb{F}_q$.

Proposition 4. (a) *If $i\neq 1$, then $H_c^i(\mathbb{A}^1, \Psi^\lambda\otimes\mathscr{E})=0$.*

(b) *The vector space $H_c^1(\mathbb{A}^1, \Psi^\lambda\otimes\mathscr{E})$ has dimension $d(d-1)^2$ and weight* $\leqq 2$ (in the sense of [2]).

(c) $\Big|\sum\limits_{t\in\mathbb{F}_q}\psi(\lambda t)\, e_r(t)\Big|\leqq d(d-1)^2 q$.

Proof. (a) is obvious.

(b) An easy calculation shows that

$$c_t(\Psi^\lambda\otimes\mathscr{E})=c_t(\mathscr{E}),\quad t\in\mathbb{A}^1,$$
$$c_\infty(\Psi^\lambda\otimes\mathscr{E})=c_\infty(\Psi^\lambda)\dim(\mathscr{E}_\infty)=2(d-1)(d-2),$$

and so $c(\Psi^\lambda\otimes\mathscr{E})=c(\mathscr{E})+2\dim(\mathscr{E}_\infty)$. Therefore

$$\dim H_c^1(\mathbb{A}^1, \Psi^\lambda\otimes\mathscr{E})=-\chi_c(\mathbb{A}^1, \Psi^\lambda\otimes\mathscr{E})=c(\mathscr{E})=d(d-1)^2$$

by [6], V. 2. 12. As $\Psi^\lambda\otimes\mathscr{E}$ has weight 1, [2], Théorème 1 shows that $H_c^1(\mathbb{A}^1, \Psi^\lambda\otimes\mathscr{E})$ has weight $\leqq 2$.

(c) From the Lefschetz trace formula, we find that

$$\mathrm{Tr}(F^r|H_c^1(\mathbb{A}^1, \Psi^\lambda\otimes\mathscr{E}))=\sum_{t\in\mathbb{F}_q}\mathrm{Tr}(F^r|(\Psi^\lambda\otimes\mathscr{E})_{\bar t})=\sum\psi(\lambda t)\, e_r(t),$$

and so (c) follows from (b).

Remark 4. (a) If (H_t) is a Lefschetz pencil for V, then $\mathscr{E}\xrightarrow{\approx}j_*j^*\mathscr{E}$ where j is the inclusion into $\mathbb{P}^1$ of any open subset U on which $\mathscr{E}$ is constant. Let a be the inclusion $\mathbb{A}^1\hookrightarrow\mathbb{P}^1$; then $a_!(\Psi^\lambda\otimes\mathscr{E})\xrightarrow{\approx}j_*((\Psi^\lambda\otimes\mathscr{E})|U)$, and so [2], Théorème 2 shows that $H_c^1(\mathbb{A}^1, \Psi^\lambda\otimes\mathscr{E})$ is pure of weight 2.

(b) Part (c) of the proposition was first proved, using an adaptation of the proof of [1], 8. 4, by N. Katz who also showed that $H_c^1(\mathbb{A}^1, \Psi^\lambda \otimes \mathscr{E})$ is always pure of weight 2. (See also the comments at the end of § 11 of the preceding paper.)

We now assume that V is the cubic surface introduced in A and that (1) and (2) hold. For $\lambda \in \mathbb{F}_q$, we write

$$S_r'(\lambda) = \sum_{t \in \mathbb{F}_q} e_r(t)\, \psi(\lambda t),$$

which is the same as the sum $S_r'(\lambda;\, \alpha, \beta, \gamma; p)$ defined in (93) of the preceding article. We also write

$$\Delta_r(\lambda) = \sum_{t \in \mathbb{F}_q} e_r(t)\, e_r(t+\lambda),$$

$$\square_r = \sum_{t \in \mathbb{F}_q} (\Delta_r(\lambda))^2.$$

When $r=1$, we omit the subscript.

Proposition 5. (a) $|S_r'(\lambda)| \leqq 12q$.

(b) $\sum_{\lambda \in \mathbb{F}_q} |S_r'(\lambda)|^2 = q \sum e_r(t)^2 = q^3 + O(q^{5/2})$.

(c) $\sum_{\lambda \in \mathbb{F}_q} |S_r'(\lambda)|^4 = q \square_r$.

Proof. (a) This is the special case $d=3$ of (a) of Proposition 4.

(b), (c). Elementary calculations, starting from the definition of $S_r'(\lambda)$, show that

$$|S_r'(\lambda)|^2 = \sum_u \Delta_r(u)\, \psi(\lambda u),$$

$$\sum_\lambda |S_r'(\lambda)|^2 = q\Delta_r(0) = q \sum e_r(t)^2,$$

$$\sum_\lambda |S_r'(\lambda)|^4 = q \sum \Delta_r(u)^2 = q \square_r.$$

The estimate in (b) follows from (4).

C. Proof of the main inequality

Throughout this section $\mathscr{E}$ will be the sheaf on $\mathbb{A}^1$ corresponding to the cubic surface considered at the end of section A; conditions (1) and (2) of A will be assumed to hold. We define Ψ' to be the locally constant sheaf on $\mathbb{A}^2$ corresponding to the covering $X^p - X = T_1 T_2$ of $\mathbb{A}^2$ in the same way that Ψ corresponds to the covering $X^p - X = T$ of $\mathbb{A}^1$; thus $\mathrm{Tr}(F^r | \Psi'_{\bar{t}}) = \psi(t_1 t_2)$ for $t = (t_1, t_2) \in \mathbb{F}_q^2$. Let $\mathscr{F} = R_c^1\, \mathrm{pr}_{1*}(\Psi' \otimes \mathrm{pr}_2^* \mathscr{E})$. The stalk of $\mathscr{F}$ at $\bar{\lambda}$, where $\lambda \in \mathbb{F}_q$, is $H_c^1(\mathbb{A}^1, \Psi^\lambda \otimes \mathscr{E})$ (we set $\Psi^0 = \mathbb{Q}_l$). Consequently,

$$\mathrm{Tr}(F^r | \mathscr{F}_{\bar{\lambda}}) = \sum_{t \in \mathbb{F}_q} e_r(t)\, \psi(\lambda t) = S_r'(\lambda), \quad \lambda \in \mathbb{F}_q,$$

$$\mathrm{Tr}(F^r | H_c^*(\mathbb{A}^1, \mathscr{F})) = \sum_{\lambda \in \mathbb{F}_q} S'(\lambda).$$

It follows from Proposition 4 that $\mathcal{F}$ is locally constant with stalks of dimension 12 on $\mathbb{A}^1-\{0\}$, and it follows from Remark 4(a) that $\mathcal{F}$ is (punctually) pure of weight 2. Therefore $\mathcal{F}^\vee = \mathcal{H}om\,(\mathcal{F}, \mathbb{Q}_l(-2))$ is also locally constant and pure of weight 2 on $\mathbb{A}^1-\{0\}$, and the eigenvalues of F^r on $\mathcal{F}^\vee_\lambda$ are the complex conjugates of the eigenvalues of F^r on $\mathcal{F}_\lambda$. This implies the following equalities (the estimates result from Proposition 5(a) and equation (3)):

$$(5)\qquad \mathrm{Tr}\big(F^r|H^*_c(\mathbb{A}^1-\{0\}, \mathcal{F}\otimes\mathcal{F}^\vee\big) = \sum_{\lambda\neq 0,\,\lambda\in\mathbb{F}_q} |S'_r(\lambda)|^2 = q^3 + O(q^{5/2});$$

$$(6)\qquad \mathrm{Tr}\big(F^r|H^*_c(\mathbb{A}^1-\{0\}, \mathcal{F}\otimes\mathcal{F}\otimes\mathcal{F}^\vee\otimes\mathcal{F}^\vee)\big) = \sum_{\lambda\neq 0,\,\lambda\in\mathbb{F}_q} |S'_r(\lambda)|^4 = q\,\square_r + O(q^4).$$

Let M be the generic stalk $\mathcal{F}_{\bar\eta}$ of $\mathcal{F}$, and let π_1 and $\bar\pi_1$ respectively be the arithmetic and geometric fundamental groups, $\pi_1(\mathbb{A}^1_{\mathbb{F}_p}-\{0\}, \bar\eta)$ and $\pi_1(\mathbb{A}^1_{\mathbb{F}_p}-\{0\}, \bar\eta)$; thus

$$\bar\pi_1 = \mathrm{Ker}\big(\pi_1 \xrightarrow{\deg} \hat{\mathbb{Z}} = \mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)\big).$$

Lemma 7. *The $\bar\pi_1$-module M is irreducible.*

Proof. If M has a composition series with n nonzero quotients, then $\dim\big(\mathrm{End}(M)_{\bar\pi_1}\big) \geqq n$. As

$$H^2_c(\mathbb{A}^1-\{0\}, \mathcal{F}\otimes\mathcal{F}^\vee) = \mathrm{Hom}\big(M, M(-2)\big)_{\bar\pi_1}(-1) = \mathrm{End}(M)_{\bar\pi_1}(-3)$$

we see that then

$$\mathrm{Tr}\big(F^r|H^*_c(\mathbb{A}^1-\{0\}, \mathcal{F}\otimes\mathcal{F}^\vee) \geqq nq^3 + O(q^{5/2})$$

for q sufficiently large. Equation (5) now shows that n is at most one: M is irreducible as a $\bar\pi_1$-module.

Let G° be the algebraic envelope of the image of $\bar\pi_1$ in $\mathrm{Aut}(M)$, and let $G^{\circ\circ}$ be the identity connected component of G°. A theorem of Grothendieck, together with Lemma 7, shows that G° is semisimple (see [2], 1.3.9). Therefore

$$\begin{aligned}\mathrm{End}(M\otimes M)^{G^\circ} &= \mathrm{End}(M\otimes M)_{G^\circ} = \mathrm{End}(M\otimes M)_{\bar\pi_1}\\ &= H^2_c(\mathbb{A}^1-\{0\}, \mathcal{F}\otimes\mathcal{F}\otimes\mathcal{F}^\vee\otimes\mathcal{F}^\vee)\,(5).\end{aligned}$$

Equation (6) now shows that

$$(7)\qquad \square_r = q^4\big(\mathrm{Tr}(F^r|\mathrm{End}(M\otimes M)^{G^\circ}\big) + O(q^{7/2}).$$

Lemma 8. *The eigenvalues of F acting on* $\mathrm{End}(M\otimes M)^{G^\circ}$ *are roots of* 1.

Proof. Let $W = \{g\in\pi_1|\deg(g)\in\mathbb{Z}\}$ and let G be the extension of $\mathbb{Z}$ by G° defined by the following diagram

$$\begin{tikzcd}
1 \arrow[r] & \bar\pi_1 \arrow[r] \arrow[d, hook] & W \arrow[r] \arrow[d] & \mathbb{Z} \arrow[r] \arrow[d, equal] & 0 \\
1 \arrow[r] & G^\circ \arrow[r] & G \arrow[r] & \mathbb{Z} \arrow[r] & 0.
\end{tikzcd}$$

As $G^{\circ\circ}$ is semisimple, the group of outer automorphisms of G° (modulo $(G^\circ)^{ad}$) is finite. Let $\tilde{F}\in G$ lift the generator F of $\mathbb{Z}$. There is a $g\in G^\circ$ and an $n\geqq 1$ such that $\tilde{F}^n g$ centralizes G° and therefore acts as a scalar on M (and also $M\otimes M$). Then F^n acts as 1 on $\operatorname{End}(M\otimes M)^{G^\circ}$ since it acts as $\tilde{F}^n g$.

Lemma 9. *There exist constants B and C such that if $p>C$ and* $\operatorname{Tr}(F|\operatorname{End}(M\otimes M)^{G^\circ})>1$, *then*

$$\Box \geqq 2p^4 - Bp^{7/2}.$$

Proof. From Lemma 2 and the definition of $\Box_r$ we see that the L-series of $(\mathscr{E}*\mathscr{E})\otimes(\mathscr{E}*\mathscr{E})$ is

$$L(t)\overset{df}{=}\exp\Big(\sum_{r>0}\operatorname{Tr}(F^r|\mathbb{H}^*_c(\mathbb{A}^1,(\mathscr{E}*\mathscr{E})\otimes(\mathscr{E}*\mathscr{E}))t^r/r\Big)=\exp(\sum\Box_r t^r/r).$$

Equation (7) shows that

$$L(t)=\big(\det(1-Ft|\operatorname{End}(M\otimes M)^{G^\circ}(-4))\big)^{-1}L_1(t)$$

where $L_1(t)$ has no zeros or poles with $|t|<p^{-7/2}$. Let $a_1,\ldots,a_{m_1}$ be the eigenvalues of F on $\mathbb{H}^*_c(\mathbb{A}^1,(\mathscr{E}*\mathscr{E})\otimes(\mathscr{E}*\mathscr{E}))$ having absolute value equal to p^4; then $a_1^{-1},\ldots,a_{m_1}^{-1}$ are the only poles of $L(p^{-s})$ with absolute value $<p^{-7/2}$, and so $\{a_1/p^4,\ldots,a_{m_1}/p^4\}$ is the set of eigenvalues of F on $\operatorname{End}(M\otimes M)^{G^\circ}$. In particular, each a_i/p^4 is a root of 1.

Let $b_1,\ldots,b_{m_2}$ be the remaining eigenvalues of F on $\mathbb{H}^*_c(\mathbb{A}^1,(\mathscr{E}*\mathscr{E})\otimes(\mathscr{E}*\mathscr{E}))$. The main theorem of [2] shows that the b_i, and all their conjugates, have absolute value $\leqq p^{7/2}$. We have

$$(8_r)\qquad \Box_r=\sum_{i=1}^{m_1}a_i^r+\sum_{i=1}^{m_2}b_i^r.$$

According to Proposition 3, there exists a constant m (independent of α, β, γ, N, and p) such that $m_1, m_2\leqq m$. Moreover there exists a constant n such that $(a_i/p^4)^n=1$, all i; to see this note that a_i is a root of a polynomial of degree $\leqq m$ with coefficients in $\mathbb{Q}_l$, and therefore lies in an extension of $\mathbb{Q}_l$ of degree $\leqq m$.

Let $\varepsilon>0$ be such that any nonzero sum of n^{th} roots of 1 with at most $2m$ terms has absolute value $\geqq\varepsilon$, and let $C=(2m/\varepsilon)^2$. If $p>C$, then $\Box$ can be written in only one way as a sum

$$\Box=ap^4+b$$

in which a is a sum of at most m n^{th} roots of 1 and $|b|\leqq mp^{7/2}$; for if we also have

$$\Box=a'p^4+b'$$

then

$$|a-a'|=|b-b'|p^{-4}\leqq 2mp^{7/2}p^{-4}=2mp^{-1/2}<\varepsilon$$

and so $a=a'$.

We apply this to equation (8_1); for any $\sigma \in \mathrm{Aut}(\mathbb{C})$,

$$\square = \sum a_i + \sum b_i = \sigma\,\square = \sum \sigma(a_i) + \sum \sigma(b_i),$$

and so $\sum a_i = \sum \sigma(a_i)$: $\sum a_i$ is in $\mathbb{Q}$. As $p^{-4}\sum a_i$ is a sum of roots of 1, it lies in $\mathbb{Z}$. Now the equation $p^{-4}\sum a_i = \mathrm{Tr}(F|\mathrm{End}(M \otimes M)^{G^\circ})$ shows that, under the hypothesis of the lemma, $p^{-4}\sum a_i \geqq 2$. We conclude that

$$\square = \sum a_i + \sum b_i \geqq 2p^4 - mp^{7/2}.$$

Lemma 10. $\mathrm{Tr}(F|\mathrm{End}(M \otimes M)^{G^\circ}) \geqq 1$, *and equals* 1 *only if* $\mathrm{Tr}(\tilde{F}|M) = p$ *for all* $\tilde{F} \in G$ *mapping to* F.

Proof. Replace G by

$$1 \to K^\circ \to K \to \mathbb{Z} \to 0$$

where K° is a maximal compact subgroup of G°. The action of K on $M(1)$ factors through a compact quotient $\bar{K}$:

$$1 \to K^\circ \to \bar{K} \to \mathbb{Z}/n\mathbb{Z} \to 0.$$

Let χ be the character of $M(1)$, and let $\tilde{F}$ be a lifting of F. We have

$$\mathrm{Tr}(F|M(1)^{G^\circ}) = \mathrm{Tr}(F|M(1)^{K^\circ}) = \int_{K^\circ} \chi(\tilde{F}g)\,dg.$$

Similarly,

$$\int_{K^\circ} |\chi(\tilde{F}g)|^2\,dg = \mathrm{Tr}(F|\mathrm{End}(M(1))^{G^\circ}) = \mathrm{Tr}(F|\mathrm{End}(M)^{G^\circ}) = 1$$

because $\mathrm{End}(M)^{G^\circ} = \mathbb{Q}_l$. Moreover,

$$\begin{aligned}\mathrm{Tr}(F|\mathrm{End}(M \otimes M)^{G^\circ}) &= \int_{K^\circ} |\chi(\tilde{F}g)|^4\,dg \\ &\geqq \Big(\int_{K^\circ} |\chi(\tilde{F}g)|^2\,dg\Big)^2 \quad \text{(Cauchy-Schwarz)} \\ &= 1.\end{aligned}$$

If equality holds, then

$$\int_{K^\circ} (|\chi(\tilde{F}g)|^2 - 1)^2\,dg = \int_{K^\circ} |\chi(\tilde{F}g)|^4\,dg - 2\int_{K^\circ} |\chi(\tilde{F}g)|^2\,dg + \int_{K^\circ} l\,dg = 0,$$

and so $|\chi(\tilde{F}g)| = 1$ for all $g \in K^\circ$.

Thus we have to find conditions, as general as possible, that ensure that we cannot have $|\mathrm{Tr}(\tilde{F}|M)| = p$ for all $\tilde{F} \in G$ mapping to F. We do this by analyzing the local monodromy of $\mathscr{F}$ at 0. Let D be the decomposition group at $0 \in \mathbb{A}^1_{\mathbb{F}_p}$, and let $I \subset D$ be the inertia group. Choose an embedding $D \hookrightarrow \pi_1$. Recall that $V_\infty = V \cap H_\infty$ is the curve $X^3 + Y^3 + Z^3 = 0$.

Lemma 11. *There exists a D-stable filtration* $M=M_0\supset M_1\supset M_2\supset M_3=\{0\}$ *of* M *such that*:

(a) *I acts trivially on each quotient* M_i/M_{i+1};

(b) *there are isomorphisms of* $D/I=\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$*-modules*

$$\begin{aligned} M/M_1 &\approx H^1\big(V_\infty,\ \mathbb{Q}_l(-1)\big),\\ M_1/M_2 &\approx H^1(\mathbb{P}^1,\mathscr{E}),\\ M_2 &\approx H^1(V_\infty,\ \mathbb{Q}_l). \end{aligned}$$

Proof. Let $\mathscr{G}$ be the sheaf on $\mathbb{A}^1\times\mathbb{P}^1$ obtained by extending $\Psi'\otimes\mathrm{pr}_2^*\mathscr{E}$ by zero from $\mathbb{A}^1\times\mathbb{A}^1$. On the fibre over $\lambda\neq 0$, $\mathscr{G}$ is $\Psi^\lambda\otimes\mathscr{E}$ extended by zero to $\mathbb{P}^1$, and on the fibre over 0, $\mathscr{G}$ is $\mathscr{E}$ extended by zero. By definition, $\mathscr{F}=R^1\,\mathrm{pr}_{1*}\mathscr{G}$.

It follows from [3], XIII (especially 2. 1. 11) that the vanishing cycle complex $\mathbf{R}\Phi(\mathscr{E})=0$, and the complex $\mathbf{R}\Phi(\Psi')$ has support on $(0,\ \infty)$. Consequently $\mathbf{R}\Phi(\mathscr{G})$ has support on $(0,\ \infty)$ and if we write $\Phi^i(-)$ for $H^i\big(\mathbf{R}\Phi(-)\big)_{\overline{(0,\ \infty)}}$, then $\Phi^i(\mathscr{G})=\mathscr{E}_{\bar\infty}\otimes\Phi^i(\Psi')$. Moreover there are exact sequences,

$$\begin{array}{l} \cdots\to\Phi^0(\Psi')\to H_c^1(\mathbb{A}^1,\ \Psi')\to H_c^1(\mathbb{A}^1_{\bar\eta},\ \Psi')\to\Phi^1(\Psi')\to\cdots\\ \cdots\to\Phi^0(\mathscr{G})\longrightarrow\mathscr{F}_{\bar o}\longrightarrow\mathscr{F}_{\bar\eta}\longrightarrow\Phi^1(\mathscr{G})\to\cdots. \end{array}$$

As $H_c^i(\mathbb{A}^1_{\bar\eta},\ \Psi')=0$ (see Lemma 5) and $H_c^i(\mathbb{A}^1,\ \Psi')=H_c^i(\mathbb{A}^1,\ \mathbb{Q}_l)=0$ for $i\neq 2$, and $=\mathbb{Q}_l(-1)$ for $i=2$, we see that $\Phi^i(\Psi')=0$ for $i\neq 1$ and $\Phi^1(\Psi')=\mathbb{Q}_l(-1)$. The second sequence therefore is

$$0\to M^I\to M\to\mathscr{E}_{\bar\infty}(-1)\to 0$$

where $\mathscr{E}_{\bar\infty}(-1)=H^1\big(V_\infty,\ \mathbb{Q}_l(-1)\big)$. We define $M_1=M^I$. Then M_1 also equals $H_c^1(\mathbb{A}^1,\ \mathscr{E})$, and there is an exact sequence,

$$0\to\mathscr{E}_{\bar\infty}\to H_c^1(\mathbb{A}^1,\ \mathscr{E})\to H^1(\mathbb{P}^1,\mathscr{E})\to 0.$$

We define $M_2=\mathrm{Ker}\big(H_c^1(\mathbb{A}^1,\ \mathscr{E})\to H^1(\mathbb{P}^1,\ \mathscr{E})\big)=\mathscr{E}_{\bar\infty}$.

The lemma shows that, if $\tilde F\in D$ lifts F, then

$$\mathrm{Tr}(\tilde F|M)=\big(e(\infty)+e'+pe(\infty)\big)$$

where $-e'=\mathrm{Tr}\big(F|H^1(\mathbb{P}^1,\ \mathscr{E})\big)=\#\big(V^*(\mathbb{F}_p)\big)-(p^2+2p+1)$ (cf. the proof of Proposition 1). Lemma 10 therefore shows that, if $\mathrm{Tr}\big(F|\mathrm{End}(M\otimes M)^{G^\circ}\big)=1$, then

$$e(\infty)+e'+pe(\infty)=\pm p. \tag{9}$$

If $p\equiv 2$, then $\#\big(V_\infty(\mathbb{F}_p)\big)=p+1$ (obviously) and so $e(\infty)=0$, and the discussion preceding Theorem 1 shows that $e'=(1-f)\,p$. Thus equation (9) is impossible unless $f=0$. If $p\equiv 1$, then $e(\infty)$ is an integer such that $0<|e(\infty)|<2\sqrt{p}$ (see for example [5], p. 140); as e' is an integer divisible by p ($e'/p+2$ is the trace of F on the Néron-Severi group of V^*, which is a $\mathbb{Z}$-module), equation (9) is always impossible in this case. This completes the proof of the theorem.

Remark 5. The preceding arguments indicate that "in general"

$$\square \overset{df}{=} \sum_{u} \Big(\sum_{t} e(t)\, e(t+u)\Big)^2 \geqq 2\, p^4 + O(p^{7/2})$$

for a Lefschetz pencil of curves over $\mathbb{F}_p$ provided the corresponding family of Jacobians has no constant part. The example considered above should be regarded as being rather special in that the curve at infinity, $X^3 + Y^3 + Z^3 = 0$, has complex multiplication.

Bibliography

[1] *P. Deligne*, La conjecture de Weil. I, Inst. Hautes Etudes Sci. Publ. Math. **43** (1974), 273—307.

[2] *P. Deligne*, La conjecture de Weil. II, Inst. Hautes Etudes Sci. Publ. Math. **52** (1980), 137—252.

[3] *P. Deligne* and *N. Katz*, Groupes de monodromie en Géométrie Algébrique, SGA7 II, Lecture Notes in Math. **340**, Berlin-Heidelberg-New York 1973.

[4] *I. Igusa*, Fibre systems of Jacobian varieties. III, Amer. J. Math. **81** (1959), 453—476.

[5] *S. Lang*, Elliptic functions, Reading, Mass. 1973.

[6] *J. Milne*, Etale cohomology, Princeton 1980.

Mathematics Department, University of Michigan, Ann Arbor, MI 48109, USA

Eingegangen 23. März 1981