J. reine angew. Math. **540** (2001), 115—166

Journal für die reine und
angewandte Mathematik
© Walter de Gruyter
Berlin · New York 2001

A general stratification theorem for exponential sums, and applications

By *E. Fouvry* at Orsay and *N. Katz* at Princeton

1. Introduction

The use of exponential sum techniques is one of the cornerstones of modern analytic number theory. The proof of the Riemann hypothesis by Weil for curves, by Deligne for general varieties, provides fantastic tools to solve problems from number theory. However controlling the size of exponential sums in a large number of variables remains very difficult, since certain geometric conditions are almost impossible to check before applying the corresponding theorem. The work of Katz and Laumon [K-L] is very illuminating, since it describes how a natural exponential sum over a given variety (even very complicated) behaves generically. In the applications to number theory, the effect of large values of the exponential sums can be well controlled this way. The aim of this paper is to give more general and more precise results than [K-L] and [Fo2] (which gave an improvement already implicitly contained in [K-L]). As applications we have given statements which can be easily applied by number theorists (Theorems 1.1 and 1.2), and we have given three applications (Corollaries 1.3, 1.4 and 1.5) which concern divisibility properties of class numbers of real quadratic fields, the equidistribution of values of polynomials in intervals and equidistribution of points of varieties in small boxes.

The following theorem is a less general statement than Corollary 3.2, from which it is easily deduced (see the proof after the statement of that corollary). It is written in a way more adapted to applications to number theory. As usual, we reserve the letter p for prime numbers.

Theorem 1.1. *Let d and n be integers $(n \geqq 1, d \geqq 1)$. Let V be a locally closed subscheme of $\mathbb{A}^n_{\mathbb{Z}}$, such that* $\dim(V_{\mathbb{C}}) \leqq d$. *Let $f(X)$ be a polynomial in $\mathbb{Z}[X_1, \dots, X_n]$.*

Then there exists a constant C, depending only on $(n, d, V$, and $f)$, closed subschemes of $\mathbb{A}^n_{\mathbb{Z}}$ called X_j $(j = 1, \dots, n)$ of relative dimension $\leqq n - j$, $\mathbb{A}^n_{\mathbb{Z}} \supset X_1 \supset X_2 \supset \cdots \supset X_n$, such that for any invertible function g on V, any prime p, any $h \in \mathbb{A}^n(\mathbb{F}_p) - X_j(\mathbb{F}_p)$, we have

$$\Big| \sum_{x \in V(\mathbb{F}_p)} \chi\big(g(x)\big)\psi\big(f(x_1, \dots, x_n) + (h_1x_1 + \cdots + h_nx_n)\big)\Big| \leqq Cp^{\frac{d}{2}+\frac{j-1}{2}},$$

for every non trivial additive character ψ of $\mathbb{F}_p$, and for every multiplicative character (possibly trivial) χ of $\mathbb{F}_p^\times$.

(Notice here the trivial inequality $\Bigl|\sum_{x\in V(\mathbb{F}_p)}\dots\Bigr| \leqq \#V(\mathbb{F}_p) \leqq C'p^d$, so the above statement has only interest for $j \leqq d$.) The interest of this theorem is that it requires almost no assumption on V. For $f \equiv 0$ and $j = 1$, we recover the result of [K-L], and for $f \equiv 0$, $g \equiv 1$ and any j the result of [Fo], Prop. 1.0. The purpose of the next theorem is to decrease by one the dimension of the set of the $(h_1, \dots, h_n)$ where the exponential sum in question has given size. It requires an extra condition on V (smoothness) and the nonvanishing of the "A-number" associated to the situation. This number will be defined precisely in section 4; roughly speaking, the A-number is zero if and only if the exponential sum is generically 0 (see Lemma 4.3). Theorem 1.2 is an easy consequence of Corollary 4.6. We have

Theorem 1.2. *Let d, n and D be integers $\geqq 1$. Let V be a closed subscheme of $\mathbb{A}^n_{\mathbb{Z}[1/D]}$, such that $V_{\mathbb{C}}$ is irreducible and smooth of dimension d. Suppose also that $A(V,k,\psi) \geqq 1$ for all finite fields k of sufficiently large characteristic and for all $\bar{\mathbb{Q}}_\ell^\times$-valued non-trivial additive characters ψ of k.*

Then:

1) *There exists a constant C, depending only on V, closed subschemes of $\mathbb{A}^n_{\mathbb{Z}[1/D]}$ called X_j $(j = 1, \dots, n)$, $\mathbb{A}^n_{\mathbb{Z}[1/D]} \supset X_1 \supset X_2 \supset \cdots \supset X_n$, of relative dimension $\leqq n - j$, such that for $h \in \mathbb{A}^n(\mathbb{F}_p) - X_j(\mathbb{F}_p)$ we have*

$$\Bigl|\sum_{x\in V(\mathbb{F}_p)} \psi(h_1x_1 + \cdots + h_nx_n)\Bigr| \leqq Cp^{\sup(\frac{d}{2},\frac{d+j-2}{2})},$$

for every $p \nmid D$ and for every non trivial additive character ψ of $\mathbb{F}_p$.

2) *Moreover, we may choose the closed subschemes X_j to be homogeneous, i.e. defined by the vanishing of homogeneous forms.*

(Again, this is trivial for $j \geqq d + 2$, since $\Bigl|\sum_{x\in V(\mathbb{F}_p)}\dots\Bigr| \leqq \#V(\mathbb{F}_p) \leqq C'p^d$.) It remains to give criteria to ensure that the A-number is non-zero, in order to apply Theorem 1.2. This question has been already partly treated in [KA-PES] and [KA-PESII]. In sections 5, 6, 7 and 8, we give new situations where $A \geqq 1$. This is done by comparison with another invariant, the "B-number", and establishing links between these two numbers for hypersurfaces defined by $F(x) = \alpha$, where F is a homogeneous polynomial. We give very simple criteria for the non vanishing of these numbers.

For the polynomial $\Delta_3(x)$ defined in section 6, as the discriminant of a binary cubic form, the A-number attached to the hypersurface defined by $\Delta_3(x) = \alpha$, $\alpha \neq 0$, is non-zero. We can then apply Theorem 1.2, from which we deduce, via the theory of Davenport-Heilbronn and sieve techniques, the following result concerning divisibility properties of class numbers of real quadratic fields. If Δ is a discriminant of a quadratic field, we denote by $h(\Delta)$ the cardinality of the ideal class group of the ring of the integers of the field $\mathbb{Q}(\sqrt{\Delta})$.

Corollary 1.3. *There exists $c_0 > 0$ and x_0, such that, for $x > x_0$ we have*

$$\#\{p \leqq x; p \equiv 1 \ (\mathrm{mod}\, 4), p+4 \ \textit{squarefree},\ 3 \nmid h(p+4)\} \geqq c_0 \frac{x}{\log x}.$$

This result improves [Fo1], Théorème, where the lower bound of Corollary 1.3 was proved to be true, but with the prime variable p replaced by positive fundamental discriminants Δ such that $h(\Delta)$ is odd. Recall that this last condition is equivalent, for positive Δ, to the fact that Δ has either one prime divisor or two prime divisors, one of which is congruent to 3 modulo 4. The fact that we gain 1 in the dimension of the X_j is crucial to getting Corollary 1.3 (see Lemma 9.3 below). We do not see how to use sieve techniques alone to affect this passage from products of at most two primes to primes themselves.

Our second application concerns the equidistribution of the values of quite general polynomials. In section 10, we will deduce from Theorem 1.1

Corollary 1.4. *Let $n \geqq 1$ and $r \geqq 1$ be integers. Let $P_1(X), \dots, P_r(X)$ be r polynomials in $\mathbb{Z}[X_1, \dots, X_n]$, such that the total degree of any linear combination $a_1P_1 + \cdots + a_rP_r$ (with coefficients $(a_1, \dots, a_r) \in \mathbb{Z}^r - \{0\}$) is at least two. Let $P(X)$ be the vector $P(X) = \big(P_1(X), \dots, P_r(X)\big)$.*

Let w: $\mathbb{R}^+ \to \mathbb{R}$ be any function of the form $w(x) = \sqrt{x} \cdot \log x \cdot \phi(x)$, with $\phi(x) \to \infty$ as $x \to \infty$.

Then, for p tending to infinity, the sequence of vectors

$$\left\{\frac{P(x_1, \dots, x_n)}{p}; 0 \leqq x_1, \dots, x_n \leqq w(p)\right\}$$

is equidistributed modulo 1. In other words, if we denote by $\{t\}$ the fractional part of the real number t, we have, for every $\alpha = (\alpha_1, \dots, \alpha_r) \in \mathbb{R}^r$ and every $\beta = (\beta_1, \dots, \beta_r) \in \mathbb{R}^r$ satisfying $0 \leqq \alpha_j < \beta_j \leqq 1$ $(1 \leqq j \leqq r)$,

$$\#\Bigg\{(x_1, \dots, x_n) \in \mathbb{Z}^n; 0 \leqq x_i \leqq w(p) \ (1 \leqq i \leqq n)$$
$$\text{and } \alpha_j \leqq \left\{\frac{P_j(x_1, \dots, x_n)}{p}\right\} \leqq \beta_j \ (1 \leqq j \leqq r)\Bigg\} \sim \prod_{i=1}^{r} (\beta_i - \alpha_i) w(p)^n$$

for p tending to infinity.

We wish to emphasize that no geometric hypothesis is imposed on the P_i, or on their linear combinations, except the degree $\geqq 2$ hypothesis. Corollary 1.4 is quite standard for $n = 1$: it is an easy consequence of Weyl's criterion (see section 7) and of Weil's bound for exponential sums of a polynomial in one variable. In the same order of ideas, it is now not difficult to prove Corollary 1.4, if one makes the extra assumption that the projective variety defined by the vanishing of the homogeneous part of highest degree of $a_1P_1 + \cdots + a_rP_r$, is non singular for $(a_1, \dots, a_r) \neq (0, \dots, 0)$, because we can use [De-WI], Théorème 8.4, p. 302. Finally, note that the condition concerning the degree of

$a_1P_1 + \cdots + a_rP_r$ cannot be avoided and that the lower bound for the growth of $w(x)$ is almost optimal (think of the polynomial $P_1(X_1) = X_1^2$).

Our last application deals with another problem of equidistribution. We are concerned with the equidistribution on points of $V(\mathbb{F}_p)$ in small boxes, where V is a closed subscheme of $\mathbb{A}_{\mathbb{Z}}^s$. We identify $\mathbb{F}_p$ with the set of the integers of the interval $[0, p[$, choose an integer x satisfying $1 \leqq x \leqq p$ and want to have a precise evaluation of $\# V(\mathbb{F}_p, x)$ where $V(\mathbb{F}_p, x)$ is the set of points of $V(\mathbb{F}_p)$ with all their coordinates x_i $(1 \leqq i \leqq s)$ satisfying $0 \leqq x_i < x$. If some natural hypotheses concerning V are satisfied, heuristic considerations lead to the estimation

$$\#V(\mathbb{F}_p, x) \sim \#V(\mathbb{F}_p) \cdot \left(\frac{x}{p}\right)^s, \tag{1.1}$$

for p and $x \to \infty$. The question is to find an inequality between p and x to ensure the uniformity of (1.1). In [Fo2], Theorem, for a quite general V, (1.1) was proved to be true uniformly for

$$x \geqq p^{1-\frac{1}{2(s-d+1)}} \cdot \log p \cdot \phi(p), \tag{1.2}$$

where d is the dimension of V and where ϕ is any function tending to infinity. This result was deduced from a theorem similar to Theorem 1.1.

Here we improve the lower bound (1.2), by adding extra hypotheses on V in order to apply Theorem 1.2.

Corollary 1.5. *Let d and s be integers $(s \geqq d \geqq 2)$. Let V be a closed subscheme of $\mathbb{A}_{\mathbb{Z}}^s$. Suppose that $V_{\mathbb{C}}$ is smooth and irreducible of dimension d and suppose further that $V_{\mathbb{C}}$ does not lie in a hyperplane of $\mathbb{A}_{\mathbb{C}}^s$. Suppose also that $A(V, k, \psi) \geqq 1$ for all finite fields k of sufficiently large characteristic and for all $\bar{\mathbb{Q}}_\ell^\times$-valued non-trivial additive characters ψ over k. Then for every x satisfying $1 \leqq x \leqq p$, we have*

$$\#V(\mathbb{F}_p, x) = \#V(\mathbb{F}_p) \cdot \left(\frac{x}{p}\right)^s + O\big(p^{\frac{d}{2}}(\log p)^s\{1 + x^d p^{-\frac{d+1}{2}}(\log p)^{-d}\}\big).$$

The proof of this corollary is given in section 11. In sections 7 and 8 we give examples of V satisfying the hypotheses of this corollary. For example, we can take the hypersurface defined by the equation

$$x_1^{a_1} \ldots x_s^{a_s} = 1,$$

with $a_1, \ldots, a_s$ positive, relatively prime integers. (See also [Ka-SE], section 5.5 for a direct approach of this particular case.) In [Ka-PES], Corollary 6.5, one finds other examples of smooth V such that $A \geqq 1$, for which this corollary applies. These examples are built with weighted homogeneous polynomials. All these examples deal with hypersurfaces. Also in section 8, we give a less obvious example of a V satisfying the hypotheses of Corollary 1.5, but with codimension 2.

Let V be as in Corollary 1.5. By Lang-Weil we know that $\#V(\mathbb{F}_p) = p^d\bigl(1 + o(1)\bigr)$. Corollary 1.5 implies that (1.1) holds as soon as we have

$$x \geqq \max(p^{1-\frac{d}{2s}}, p^{1-\frac{1}{2(s-d)}}) \cdot \log p \cdot \phi(p) \tag{1.3}$$

with $\phi(t)$ tending to ∞ as t tends to ∞. This improves (1.1) in a very interesting manner particularly for hypersurfaces ($s - d = 1$). For hypersurfaces, (1.3) reduces to

$$x \geqq p^{\frac{1}{2}+\frac{1}{2s}} \cdot \log p \cdot \phi(p), \tag{1.4}$$

instead of $x \geqq p^{\frac{3}{4}} \cdot \log p \cdot \phi(p)$ as given by (1.2). By the technique described in section 11, we would not get a better result if all the sums $S(V; h, p)$ satisfied the optimal inequality $S(V; h, p) = O(p^{\frac{d}{2}})$ ($h \neq 0$). To give another illustration, we consider the variety V defined by

$$x_1 \dots x_s = 1.$$

The sums $S(V; h, p)$ are then Kloosterman sums, for which purity is well known. However, for the moment, nothing better than (1.4) can be proved even in this case. In conclusion, Theorem 1.2 is strong enough to annihilate the effect of large values of $S(V; h, p)$ in the particular case of hypersurfaces.

Acknowledgement. This work was done when both authors were at the Institute for Advanced Study (Princeton). They thank the Institute for its hospitality and for providing a marvelous venue for collaboration. They also thank Cécile Dartyge for pointing out an error in an earlier version of this paper, cf. the paragraph following (9.12).

2. The general stratification theorem

We first consider the following general situation. We are given

1) an affine scheme $T = \mathrm{Spec}(R)$ with R a finitely generated $\mathbb{Z}$-algebra,

2) a T-scheme π: $X \to T$ which is separated and of finite type,

3) a function f on X, i.e. a T-morphism f: $X \to \mathbb{A}^1_T$,

4) a prime number ℓ, and an object K in $\mathrm{D}^b_c(X[1/\ell], \bar{\mathbb{Q}}_\ell)$.

For each finite field k of characteristic $p \neq \ell$, we can make the base change $\mathbb{Z} \to k$ and form the k-schemes

$$X \otimes k := X \otimes_{\mathbb{Z}} k, \quad T \otimes k := T \otimes_{\mathbb{Z}} k,$$

and the k-morphisms

$$\pi \otimes k \colon X \otimes k \to T \otimes k, \quad f \otimes k \colon X \otimes k \to \mathbb{A}^1_{T \otimes k}.$$

We denote by $K \otimes k$ in $\mathrm{D}_c^b(X \otimes k, \bar{\mathbb{Q}}_\ell)$ the restriction of K to $X \otimes k$.

For each non trivial $\bar{\mathbb{Q}}_\ell^\times$-valued character ψ of k, we have the Artin-Schreier sheaf $\mathscr{L}_{\psi(f \otimes k)}$ on $X \otimes k$.

The exponential sums we have in mind depend on auxiliary data (k, ψ, t):

k: a finite field of characteristic not ℓ,

ψ, a non trivial $\bar{\mathbb{Q}}_\ell^\times$-valued additive character of k,

t in $T(k) = (T \otimes k)(k)$ i.e. a ring homomorphism φ: $R \to k$.

Given such auxiliary data, we form the scheme $X_t/k := (f \otimes k)^{-1}(t)$. On X_t, we have the pullback K_t of K, and the function f_t. We denote by $S(X/T, f, K, k, \psi, t)$ the exponential sum

$$S(X/T, f, K, k, \psi, t) = \sum_{x \in X_t(k)} \psi\bigl(f_t(x)\bigr) \operatorname{Trace}(\mathrm{Frob}_{k,X} | K_t).$$

The cohomological genesis of this sum is this. On $X \otimes k$, we have the object $(K \otimes k) \otimes_{\bar{\mathbb{Q}}_\ell} \mathscr{L}_{\psi(f \otimes k)}$ in $\mathrm{D}_c^b(X \otimes k, \bar{\mathbb{Q}}_\ell)$. We form the object

$$R(\pi \otimes k)_!\bigl((K \otimes k) \otimes_{\bar{\mathbb{Q}}_\ell} \mathscr{L}_{\psi(f \otimes k)}\bigr)$$

in $\mathrm{D}_c^b(T \otimes k, \bar{\mathbb{Q}}_\ell)$. We have

$$\begin{aligned} S(X/T, f, K, k, \psi, t) &= \operatorname{Trace}\bigl(\mathrm{Frob}_{k,t} | R(\pi \otimes k)_!\bigl((K \otimes k) \otimes_{\bar{\mathbb{Q}}_\ell} \mathscr{L}_{\psi(f \otimes k)}\bigr)\bigr) \\ &:= \sum_i (-1)^i \operatorname{Trace}\bigl(\mathrm{Frob}_{k,t} | R^i(\pi \otimes k)_!\bigl((K \otimes k) \otimes_{\bar{\mathbb{Q}}_\ell} \mathscr{L}_{\psi(f \otimes k)}\bigr)\bigr). \end{aligned}$$

In order to state the first result, we need to recall the notion of a stratification $\mathscr{Y}$ of a scheme Y. It is simply a set-theoretic partition of Y^{red} into finitely many reduced, locally closed subschemes Y_j of Y. Given any morphism ρ: $Z \to Y$, the stratification $\rho^*\mathscr{Y}$ of Z is defined as $\{\rho^{-1}(Y_j)^{\mathrm{red}}\}$.

If Y is a $\mathbb{Z}$-scheme of finite type (or more generally a "good" scheme, cf. [K-L], 1.0), we say that an object L in $\mathrm{D}_c^b(Y[1/\ell], \bar{\mathbb{Q}}_\ell)$ is adapted to $\mathscr{Y}$ if each of its cohomology sheaves $\mathscr{H}^i(L)$ is lisse on each $Y_j[1/\ell]$. We say that L is χ-adapted to $\mathscr{Y}$ if it is adapted to $\mathscr{Y}$ and if, in addition, the function $y \mapsto \sum_i (-1)^i \dim \mathscr{H}^i(L)_y$ is constant on each $Y_j[1/\ell]$. We denote by $\|L\|$ the $\mathbb{Z}$-valued function on the geometric points of Y defined by

$$\|L\|(y) := \sum_i \dim \mathscr{H}^i(L)_y.$$

We now have the general stratification theorem:

Theorem 2.1. *Hypotheses and notations as above, suppose given a stratification $\mathscr{X}$ of X. There exists an integer $N \geqq 1$, an integer $C \geqq 1$, a stratification $\mathscr{T} = \{T_i\}$ of $T[1/N] := \operatorname{Spec}(R[1/N])$ and a map*

$$(\pi, f)_!\colon \{\textit{functions } f\colon X \to \mathbb{Z},\ \textit{constant on } \mathscr{X}\}$$
$$\to \{\textit{functions } f\colon T[1/N] \to \mathbb{Z},\ \textit{constant on } \mathscr{T}\}$$

with the following properties:

1) *Each strat T_i is smooth and surjective over $\mathbb{Z}[1/N]$, and all the geometric fibres of $T_i/\mathbb{Z}[1/N]$ are equidimensional of some common dimension δ_i.*

2) *For any flat morphism $\varphi\colon S \to T$ of finite type, put $X_S := X \times_T S$, $\pi_S\colon X_S \to S$ the structural morphism, $f_S\colon X_S \to \mathbb{A}^1_S$ the function deduced from f on X. For any prime ℓ, any object K in $\mathrm{D}^b_c(X_S[1/\ell], \bar{\mathbb{Q}}_\ell)$ which is adapted to the inverse image stratification $\mathscr{X}_S$ of X_S, any finite field k of characteristic p not dividing ℓN, any direct factor L of $K \otimes k$ in $\mathrm{D}^b_c(X_S \otimes k, \bar{\mathbb{Q}}_\ell)$ and any choice of $\bar{\mathbb{Q}}_\ell^\times$-valued non-trivial additive character ψ of k, the object $R(\pi_S \otimes k)_!(L \otimes_{\bar{\mathbb{Q}}_\ell} \mathscr{L}_{\psi(f_S \otimes k)})$ on $S \otimes k$ is adapted to the stratification*

$$\varphi^*(\mathscr{T} \otimes k) := \{\varphi^{-1}(T_i \otimes k)\}.$$

For any geometric point s of $S \otimes k$, with image $t = \varphi(s)$ in $T \otimes k$, we have

$$\|R(\pi_S \otimes k)_!(L \otimes_{\bar{\mathbb{Q}}_\ell} \mathscr{L}_{\psi(f_S \otimes k)})\|(s) \leqq \sup_{x \in X_t} \|L\|(x),$$

the sup *taken over all geometric points x of the fibre X_t. Moreover, if L is χ-adapted to $\mathscr{X}_S \otimes k$ on $X_S \otimes k$, then $R(\pi_S \otimes k)_!\big(L \otimes_{\bar{\mathbb{Q}}_\ell} \mathscr{L}_{\psi(f_S \otimes k)}\big)$ is χ-adapted to $\mathscr{T} \otimes k$ on $T \otimes k$, and their locally constant χ-functions are related by*

$$\chi\big(R(\pi_S \otimes k)_!(L \otimes_{\bar{\mathbb{Q}}_\ell} \mathscr{L}_{\psi(f_S \otimes k)})\big) = (\pi, f)_!\big(\chi(L)\big).$$

Proof. Factor $\pi\colon X \to T$ as $f\colon X \to \mathbb{A}^1_T$ followed by the projection pr_2 of $\mathbb{A}^1_T$ onto T. Then $R(\pi_S \otimes k)_!(L \otimes_{\bar{\mathbb{Q}}_\ell} \mathscr{L}_{\psi(f_S \otimes k)})$ is

$$R(\mathrm{pr}_2 \otimes k)_!\big(\mathscr{L}_\psi \otimes_{\bar{\mathbb{Q}}_\ell} \big(R(f_S \otimes k)_! L\big)\big).$$

One first applies [K-L], 3.1.2 to the morphism $f\colon X \to \mathbb{A}^1_T$ and the stratification $\mathscr{X}$. This produces an integer $N_1 \geqq 1$ and a stratification $\mathscr{A}$ of $\mathbb{A}^1_{T[1/N_1]}$ such that $Rf_! K$ is adapted to $\mathscr{A}_S$. Then $R(f_S \otimes k)_! L$ is a direct factor $R(f_S \otimes k)_!(K \otimes k) = (Rf_{S!}K) \otimes k$. So we are reduced to the case when X is $\mathbb{A}^1_{T[1/N_1]}$, with stratification $\mathscr{A}$, and function the identity. In this case, we first apply [K-L], 3.4.1.1 and then [K-L], 4.3.2 to produce an integer $N_2 \geqq 2$ and a stratification $\mathscr{T}_1 = \{T_{i,1}\}$ of $T[1/N_1 N_2]$ which satisfies 2), in which each strat $T_{i,1}$ is normal, connected, and flat over $\mathbb{Z}$. We then apply [Ka-PES], 1.4.4 to produce an integer $N_3 \geqq 1$ and a stratification $\mathscr{T}$ of $T[1/N_1 N_2 N_3]$ which refines $\mathscr{T}_1[1/N_3]$ and which satisfies 1), with $N := N_1 N_2 N_3$. (Since $\mathscr{T}$ refines a stratification which already satisfies 2), $\mathscr{T}$ satisfies 2) automatically.) QED

Remark. In the application of this theorem in the next section, the only flat base changes $\varphi: S \to T$ occuring will be the inclusions of open sets $T[1/M] \subset T$ for various integers $M \geqq 1$.

3. First application to estimates for exponential sums

We fix an integer $n \geqq 1$, and work in affine n-space $\mathbb{A}^n_{\mathbb{Z}}$ over $\mathrm{Spec}(\mathbb{Z})$, with coordinates $x_1, \dots, x_n$. We give ourselves a locally closed subscheme V of $\mathbb{A}^n_{\mathbb{Z}}$, (i.e. V is a Zariski open set of a closed subscheme of $\mathbb{A}^n_{\mathbb{Z}}$), and an integer d such that all geometric fibres of $V/\mathbb{Z}$ have dimension $\leqq d$. We also give ourselves a function f on V, i.e. a morphism $f: V \to \mathbb{A}^1_{\mathbb{Z}}$. We further give ourselves a stratification $\mathscr{V}$ of V, a prime number ℓ, and an object K in $\mathrm{D}^b_c(V[1/\ell], \bar{\mathbb{Q}}_\ell)$ which is adapted to $\mathscr{V}[1/\ell]$. We make two further assumptions:

1) The object K on $V[1/\ell]$ is fibrewise semiperverse: for each finite field k of characteristic $p \neq \ell$, and each integer i, the cohomology sheaf $\mathscr{H}^i(K \otimes k)$ on $V \otimes k$ satisfies

$$\dim \mathrm{Supp}\big(\mathscr{H}^i(K \otimes k)\big) \leqq -i.$$

2) The object K on $V[1/\ell]$ is fibrewise mixed of weight $\leqq d$: for each finite field k of characteristic $p \neq \ell$, and each integer i, the cohomology sheaf $\mathscr{H}^i(K \otimes k)$ on $V \otimes k$ is mixed of weight $\leqq d + i$.

We are interested in the following exponential sums, which depend on auxiliary data (k, ψ, h):

k: a finite field of characteristic $p \neq \ell$,

ψ: a non trivial $\bar{\mathbb{Q}}_\ell^\times$-valued additive character of k,

h: an n-tuple $(h_1, \dots, h_n)$ in k^n.

Given such data, we consider the exponential sum

$$S(V, f, K, k, \psi, h) := \sum_{v \in V(k)} \mathrm{Trace}(\mathrm{Frob}_{k,v}|K)\psi\Big(f(v) + \sum_i h_i x_i(v)\Big).$$

Before going on, let us give the basic example we have in mind. We take for $\mathscr{V}$ the stratification $\{V\}$. We take $K := \bar{\mathbb{Q}}_\ell[d]$, the constant sheaf on V, placed in degree $-d$. (This object K is adapted to $\mathscr{V}$, because the only non vanishing $\mathscr{H}^i(K)$ is $\mathscr{H}^{-d}(K)$, which is the constant sheaf on V. It is fibrewise semiperverse and mixed of weight $\leqq d$, because the only non vanishing $\mathscr{H}^i(K \otimes k)$ is $\mathscr{H}^{-d}(K \otimes k)$, which is the constant sheaf on $V \otimes k$. Thus $\mathscr{H}^{-d}(K \otimes k)$ has support $V \otimes k$, whose dimension is $\leqq d$ by hypothesis, and $\mathscr{H}^{-d}(K \otimes k)$ is trivially mixed of weight $\leqq -d + d = 0$.) In this case, the sum we are considering is

$$S(V, f, \bar{\mathbb{Q}}_\ell[d], k, \psi, h) := (-1)^d \sum_{v \in V(k)} \psi\Big(f(v) + \sum_i h_i x_i(v)\Big).$$

Theorem 3.1. *Denote by H the n-dimensional affine space over $\mathbb{Z}$ with coordinates $h_1, \dots, h_n$. Given data $(n, V \subset \mathbb{A}^n_{\mathbb{Z}}, f, \mathscr{V})$ as above, there exists an integer $N \geqq 1$, an integer $C \geqq 1$, a stratification $\mathscr{H}$ of $H[1/N]$ and a map*

$$(V,f)_!\colon \{\textit{functions } f\colon V \to \mathbb{Z},\ \textit{constant on } \mathscr{V}\}$$

$$\to \{\textit{functions } f\colon H[1/N] \to \mathbb{Z},\ \textit{constant on } \mathscr{H}\}$$

with the following properties:

1) *Each strat H_i is smooth and surjective over $\mathbb{Z}[1/N]$ and all the geometric fibres of $H_i/\mathbb{Z}[1/N]$ are equidimensional of some common dimension η_i.*

2) *For any integer $M \geqq 1$, any prime number ℓ, any object K in $\mathrm{D}^b_c(V[1/M\ell], \bar{\mathbb{Q}}_\ell)$ which is adapted to $\mathscr{V}[1/M\ell]$, fibrewise semiperverse and fibrewise mixed of weight $\leqq d$, any finite field k of characteristic p not dividing ℓNM, any direct factor L of $K \otimes k$ in $\mathrm{D}^b_c(V \otimes k, \bar{\mathbb{Q}}_\ell)$, any choice of $\bar{\mathbb{Q}}^\times_\ell$-valued nontrivial additive character ψ of k, the Fourier Transform $\mathrm{FT}_\psi\big(i_!(L \otimes \mathscr{L}_{\psi(f)})\big)$ is adapted to the stratification $\mathscr{H} \otimes k$. If L is χ-adapted to the stratification $\mathscr{V} \otimes k$, then $\mathrm{FT}_\psi\big(i_!(L \otimes \mathscr{L}_{\psi(f)})\big)$ is χ-adapted to the stratification $\mathscr{H} \otimes k$, and their locally constant χ-functions are related by*

$$\chi\big(\mathrm{FT}_\psi\big(i_!(L \otimes \mathscr{L}_{\psi(f)})\big)\big) = (V,f)_!\big(\chi(L)\big).$$

For any point h in $H(k)$, we have the following estimate. Suppose that h lies in the strat H_i. Then after any field embedding of $\bar{\mathbb{Q}}_\ell$ into $\mathbb{C}$, we have the estimate

$$\Big|\sum_{v \in V(k)} \mathrm{Trace}(\mathrm{Frob}_{k,v}|L)\psi\Big(f(v) + \sum_i h_i x_i(v)\Big)\Big| \leqq C \times \Big(\sup_{v \in V \otimes k} \|L\|(v)\Big) \times (\sqrt{\#k})^{d+n-\eta_i}.$$

Proof. We wish to apply Theorem 2.1 to produce $(N, C, \mathscr{H})$. In that theorem, take the input as follows: T is H, X is the product $V \times H := V \times_{\mathrm{Spec}(\mathbb{Z})} H$, $\mathscr{X}$ is the stratification $\mathscr{V} \times H = \{V_i \times H\}$ of $V \times H$, π is the projection of $V \times H$ onto H, and f is the function on $V \times H$ given by $F(v,h) := f(v) + \sum_i h_i x_i(v)$. We must explain why the output $(N, C, \mathscr{H})$ of that theorem works in the theorem being proven.

The key point is this. Fix data (ℓ, K, k, L, ψ, h) as in the assertion 1). Then the sum

$$\sum_{v \in V(k)} \mathrm{Trace}(\mathrm{Frob}_{k,v}|L)\psi\Big(f(v) + \sum_i h_i x_i(v)\Big)$$

has a simple interpretation in terms of Fourier transform on $\mathbb{A}^n_k$, as follows.

On $V \otimes k$, we have the object L, which is semiperverse and mixed of weight $\leqq d$. Form the tensor product $L \otimes \mathscr{L}_{\psi(f)} := L \otimes_{\bar{\mathbb{Q}}_\ell} \mathscr{L}_{\psi(f)}$ on $V \otimes k$. It is still semiperverse of weight $\leqq d$ (because $\mathscr{L}_{\psi(f)}$ is lisse on $V \otimes k$, and pure of weight zero). Denote by

$$i\colon V \otimes k \to \mathbb{A}^n_k$$

the inclusion. Then $i_!(L \otimes \mathscr{L}_{\psi(F)})$ is semiperverse on $\mathbb{A}^n_k$ and mixed of weight $\leqq d$. Its

Fourier Transform $\mathrm{FT}_\psi\big(i_!(L \otimes \mathscr{L}_{\psi(f)})\big)$ on $\mathscr{H} \otimes k$ is semiperverse, and mixed of weight $\leqq n + d$. (That FT_ψ preserves semiperversity results from the equality $\mathrm{FT}_{!,\psi} = \mathrm{FT}_{*,\psi}$ and the τ-left-exactness of Rg_* for an affine morphism g, cf. [SGA 4], XIV, 3.1.) The effect of $\mathrm{FT}_\psi = \mathrm{FT}_{!,\psi}$ on weights is immediate from Deligne's main theorem in Weil II [De-WII], 3.3.1.) By the Lefschetz trace formula, we have

$$\begin{aligned}
&\mathrm{Trace}\big(\mathrm{Frob}_{k,h}|\mathrm{FT}_\psi\big(i_!(L \otimes \mathscr{L}_{\psi(f)})\big)\big)\\
&\quad = (-1)^n \sum_{x \in \mathbb{A}^n(k)} \mathrm{Trace}\Big(\mathrm{Frob}_{k,x}|i_!(L \otimes \mathscr{L}_{\psi(f)}) \otimes \mathscr{L}_\psi\Big(\sum_i h_i x_i\Big)\Big)\\
&\quad = (-1)^n \sum_{v \in V(k)} \mathrm{Trace}\Big(\mathrm{Frob}_{k,v}|L \otimes \mathscr{L}_{\psi(f)} \otimes \mathscr{L}_\psi\Big(\sum_i h_i x_i\Big)\Big)\\
&\quad = (-1)^n \sum_{v \in V(k)} \mathrm{Trace}\big(\mathrm{Frob}_{k,v}|L \otimes \mathscr{L}_{\psi(f+\sum_i h_i x_i)}\big)\\
&\quad = (-1)^n \sum_{v \in V(k)} \mathrm{Trace}(\mathrm{Frob}_{k,v}|L)\psi\Big(f(v) + \sum_i h_i x_i(v)\Big).
\end{aligned}$$

How is the Fourier transform related to the function F on $V \times H$ and the projection π of $V \times H$ onto H? We can describe $\mathrm{FT}_\psi\big(i_!(L \otimes \mathscr{L}_{\psi(f)})\big)$ as follows. On $(V \times H) \otimes k$, we have the object $\mathrm{pr}_1^*(L \otimes \mathscr{L}_{\psi(f)})$, and it is tautological that

$$\begin{aligned}
\mathrm{FT}_\psi\big(i_!(L \otimes \mathscr{L}_{\psi(f)})\big) &= R(\pi \otimes k)_!\Big(\mathrm{pr}_1^*(L \otimes \mathscr{L}_{\psi(f)}) \otimes \mathscr{L}_\psi\Big(\sum_i h_i x_i\Big)\Big)[n]\\
&= R(\pi \otimes k)_!\big(\mathrm{pr}_1^*(L) \otimes \mathscr{L}_{\psi(F)}\big)[n].
\end{aligned}$$

Now consider what we know about $R(\pi \otimes k)_!\big(\mathrm{pr}_1^*(L) \otimes \mathscr{L}_{\psi(F)}\big)[n]$ on $H \otimes k$. Its trace function at h in $H(k)$ is the sum we are trying to estimate. It is adapted to the stratification $\mathscr{H} \otimes k$ on $H \otimes k$. (These results come from Theorem 2.1, applicable because $\mathrm{pr}_1^*(L)$ is a direct factor of $\big(\mathrm{pr}_1^*(K)\big) \otimes k$ and $\mathrm{pr}_1^*(K)$ on $(V \otimes H)[1/M\ell]$ is adapted to the stratification $(\mathscr{V} \otimes H)[1/M\ell]$.) Being equal to $\mathrm{FT}_\psi\big(i_!(L \otimes \mathscr{L}_{\psi(f)})\big)$, it is semiperverse, and mixed of weight $\leqq d + n$.

Let us denote by $\mathscr{H}^a := \mathscr{H}^a\big(R(\pi \otimes k)_!\big(\mathrm{pr}_1^*(L) \otimes \mathscr{L}_{\psi(F)}\big)[n]\big)$ the a'th cohomology sheaf of $R(\pi \otimes k)_!\big(\mathrm{pr}_1^*(L) \otimes \mathscr{L}_{\psi(F)}\big)[n]$. We know that $\mathscr{H}^a$ is mixed of weight $\leqq d + n + a$, and that the dimension of its support is at most $-a$. What about the restriction of $\mathscr{H}^a$ to a strat $H_i \otimes k$ of $\mathscr{H} \otimes k$? Well, this restriction is a lisse sheaf on $H_i \otimes k$, and $H_i \otimes k$ is equidimensional and smooth of dimension η_i. So if this restriction is non-zero, then $\mathscr{H}^a$ has support of dimension $\geqq \eta_i$. But $\mathscr{H}^a$ has its support of dimension at most $-a$. Therefore

$$\mathscr{H}^a|H_i \otimes k = 0 \quad \text{if } \eta_i > -a,$$

i.e.

$$\mathscr{H}^a|H_i \otimes k \neq 0 \Rightarrow a \leqq -\eta_i.$$

On the other hand, $\mathscr{H}^a$ is mixed of weight $\leqq d + n + a$. So

$$\mathscr{H}^a|H_i \otimes k \neq 0 \Rightarrow \mathscr{H}^a \quad \text{is mixed of weight} \leqq d+n-\eta_i.$$

So for h in $H_i(k)$, we have

$$\begin{aligned}
&\Big|\sum_{v \in V(k)} \mathrm{Trace}(\mathrm{Frob}_{k,v}|L)\psi\Big(f(v)+\sum_i h_i x_i(v)\Big)\Big| \\
&\qquad = \Big|\sum_a (-1)^a \mathrm{Trace}(\mathrm{Frob}_{k,h}|\mathscr{H}^a)\Big| \\
&\qquad = \Big|\sum_{a \leqq -\eta_i} (-1)^a \mathrm{Trace}(\mathrm{Frob}_{k,h}|\mathscr{H}^a)\Big| \\
&\qquad \leqq \sum_{a \leqq -\eta_i} |\mathrm{Trace}(\mathrm{Frob}_{k,h}|\mathscr{H}^a)|
\end{aligned}$$

(since $\mathscr{H}^a$ is mixed of weight $\leqq d+n+a$)

$$\begin{aligned}
&\leqq \sum_{a \leqq -\eta_i} \dim\,(\mathscr{H}^a)_h \times (\sqrt{\#k})^{d+n+a} \\
&\leqq \Big(\sum_a \dim\,(\mathscr{H}^a)_h\Big) \times (\sqrt{\#k})^{d+n-\eta_i} \\
&= \big\|R(\pi \otimes k)_!\big(\mathrm{pr}_1^*(L) \otimes \mathscr{L}_{\psi(F)}\big)[n]\big\|(h) \times (\sqrt{\#k})^{d+n-\eta_i} \\
&\leqq C \times \Big(\sup_{v \in V \otimes k} \|L\|(v)\Big) \times (\sqrt{\#k})^{d+n-\eta_i}. \quad \text{QED}
\end{aligned}$$

Corollary 3.2. *Hypotheses and notations as in Theorem* 3.1, *suppose we are given also an invertible function g on V. For any finite field k of characteristic p not dividing* ℓN, *any* (*possibly trivial*) $\bar{\mathbb{Q}}_\ell^\times$*-valued multiplicative character* χ *of* $k^\times$, *any choice of* $\bar{\mathbb{Q}}_\ell^\times$*-valued non-trivial additive character* ψ *of k, and any point h in* $H(k)$, *we have the following estimate. Suppose that h lies in the strat* H_i. *Then after any field embedding of* $\bar{\mathbb{Q}}_\ell$ *into* $\mathbb{C}$, *we have the estimate*

$$\Big|\sum_{v \in V(k)} \chi(g(v))\psi\Big(f(v)+\sum_i h_i x_i(v)\Big)\Big| \leqq C \times (\sqrt{\#k})^{d+n-\eta_i}.$$

Proof. We take for $\mathscr{V}$ the stratification $\{V\}$ consisting of V alone. Denote by M the order of the character χ. Over $\mathbb{Z}[1/M]$, consider the M-th power endomorphism

$$[M]\colon \mathbb{G}_m[1/M] \to \mathbb{G}_m[1/M].$$

It is a finite etale morphism, so the sheaf $[M]_*\bar{\mathbb{Q}}_\ell$ on $\mathbb{G}_m[1/M\ell]$ is lisse of rank M, and pure of weight zero. Form the pullback sheaf

$$\mathscr{L}(M,g) := g^*([M]_*\bar{\mathbb{Q}}_\ell)$$

on $V[1/M\ell]$. It is lisse, i.e. adapted to $\mathscr{V}[1/M]$, and punctually pure of weight zero. The finite field k has order $\# k \equiv 1 \bmod M$, because $k^\times$ has a character χ of order M. So after pullback to $V \otimes k$, we have a direct sum decomposition

$$\mathscr{L}(M,g) \otimes k \cong \bigoplus_{\substack{\text{characters } \rho \text{ of } k^\times \\ \text{of order} | M}} \mathscr{L}_{\rho(g \otimes k)}$$

of $\mathscr{L}(M,g) \otimes k$ as a direct sum of Kummer sheaves.

We take for K on $V[1/M\ell]$ the semiperverse object $\mathscr{L}(M,g)[d]$, which is mixed of weight $\leqq d$ and adapted to $\mathscr{V}$. We take the shifted Kummer sheaf $\mathscr{L}_{\chi(g\otimes k)}[d]$ as the direct factor L of $K \otimes k$. Because $\mathscr{L}_{\chi(g\otimes k)}$ is lisse of rank one on $V \otimes k$, the function $\|L\|$ on $V \otimes k$ is identically one. So the assertion is indeed a special case of the previous theorem. QED

Proof of Theorem 1.1. Theorem 1.1 concerns only fields k with sufficiently large prime cardinality (what happens when p is small is absorbed by increasing the value of C). Given $V \subset \mathbb{A}^n_{\mathbb{Z}}$ as in Theorem 1.1, with $\dim(V_{\mathbb{C}}) \leqq d$, we have $\dim(V \otimes_{\mathbb{Z}} \mathbb{F}_p) \leqq d$ for all p sufficiently large, say for all $p > M$. So we may apply Corollary 3.2 to $V[1/M!] \subset \mathbb{A}^n_{\mathbb{Z}}$, to get a stratification of $H[1/N]$ by strats H_i. We define the closed subschemes X_j as follows. We first define X_j° as the closure in $H[1/N]$ of the (finite) union of the strats H_i, with dimension $\eta_i \leqq n - j$. We then define X_j to be the schematic closure of X_j° in H. Note that the X_j form a decreasing sequence of closed subschemes of relative dimension $\leqq n - j$. If $p > N$ and if h in $\mathbb{A}^n(\mathbb{F}_p)$ does not belong to X_j, it means that it belongs to some H_i of dimension $\eta_i \geqq n - j + 1$ (because the H_i form of a partition). Corollary 3.2 at once gives the claimed upper bound for the trigonometric sum. QED

4. Second application to estimates for exponential sums: the role of A-numbers

We continue to work in the general setting of the previous section. Thus we are given

$$(V \text{ locally closed in } \mathbb{A}^n_{\mathbb{Z}}, d, f, \mathscr{V}, \ell, M \geqq 1, K \text{ on } V[1/\ell M]).$$

As in the previous section, we denote by H the n-dimensional affine space over $\mathbb{Z}$ with coordinates $h_1, \dots, h_n$. The proof of Theorem 3.1, produced an integer $N \geqq 1$, a constant C and a stratification $\mathscr{H}$ of $H[1/N]$, which will also be used in this section.

We now impose additional conditions on this data.

4.0.1. There is an integer $D \geqq 1$ such that $V[1/D]$ is a closed subscheme of $\mathbb{A}^n_{\mathbb{Z}[1/D]}$ and $V[1/D]/\mathbb{Z}[1/D]$ is smooth and surjective of relative dimension d, with geometrically connected fibres.

4.0.2. The object K on $V[1/\ell M]$ is adapted to $\mathscr{V}$, is fibrewise semiperverse, and is fibrewise mixed of weight $\leqq d$.

4.0.3. K on $V[1/\ell MD]$ is fibrewise perverse, geometrically irreducible, and pure of weight d: for every finite field k of characteristic not dividing ℓMD, $K \otimes k$ on $V \otimes k$ is perverse, geometrically irreducible (i.e. remains irreducible on $V \otimes \bar{k}$), and pure of weight d.

For each pair (k,ψ) consisting of a finite field k of characteristic not dividing $DM\ell$, and a $\bar{\mathbb{Q}}_\ell^\times$-valued non-trivial additive character ψ of k, we have on $V\otimes k$ the geometrically irreducible perverse sheaf $(K\otimes k)\otimes\mathscr{L}_{\psi(f)}$. Its extension by zero to $\mathbb{A}^n\otimes k$, $i_!\big((K\otimes k)\otimes\mathscr{L}_{\psi(f)}\big)$, is perverse, geometrically irreducible and pure of weight d. So its Fourier Transform $\mathrm{FT}_\psi\big(i_!\big((K\otimes k)\otimes\mathscr{L}_{\psi(f)}\big)\big)$ on $H\otimes k$ is perverse, geometrically irreducible, and pure of weight $n+d$. So on a dense open set U of $H\otimes k$, $\mathrm{FT}_\psi\big(i_!\big((K\otimes k)\otimes\mathscr{L}_{\psi(f)}\big)\big)$ is of the form $\mathscr{F}[n]$, for $\mathscr{F}$ a lisse sheaf on U which is geometrically irreducible and pure of weight d.

In what follows, the question of whether or not the sheaf $\mathscr{F}$ is identically zero or not will be essential. With that in mind, we define the A-number of the data (V,f,K,k,ψ) to be the rank of $\mathscr{F}$, and denote it $A(V,f,K,k,\psi)$. In the special case when the function f is identically zero, we write simply $A(V,K,k,\psi)$. If in addition K is $\bar{\mathbb{Q}}_\ell[d]$, we write simply $A(V,k,\psi)$.

Lemma 4.1 (Uniformity Lemma for A-numbers). *Hypotheses and notations as in* 4.0.1–3 *above, as (k,ψ) varies over all pairs with* $\mathrm{char}(k)$ *prime to $DMN\ell$, the A-number $A(V,f,K,k,\psi)$ has a constant value. Moreover, this constant value depends on the object K only through its χ-function $\chi(K)$ on $V[1/DNM\ell]$.*

Proof. For any such (k,ψ), $\mathrm{FT}_\psi\big(i_!\big((K\otimes k)\otimes\mathscr{L}_{\psi(f)}\big)\big)$ is χ-adapted to the stratification $\mathscr{H}\otimes k$. On the unique strat $H_{\max}\otimes k$ which has maximal dimension n,

$$\mathrm{FT}_\psi\big(i_!\big((K\otimes k)\otimes\mathscr{L}_{\psi(f)}\big)\big)$$

is $\mathscr{F}[n]$ for a lisse sheaf, whose rank is the A-number $A(V,f,K,k,\psi)$. The object K is, by hypothesis, χ-adapted to $\mathscr{V}[1/\ell]$. Therefore $\mathrm{FT}_\psi\big(i_!\big((K\otimes k)\otimes\mathscr{L}_{\psi(f)}\big)\big)$ is χ-adapted to $\mathscr{H}\otimes k$, and its χ-function is related to that of K by

$$\chi\big(\mathrm{FT}_\psi\big(i_!\big((K\otimes k)\otimes\mathscr{L}_{\psi(f)}\big)\big)\big)=(V,f)_!\big(\chi(K)\big).$$

On the strat $H_{\max}\otimes k$ the function $\chi\big(\mathrm{FT}_\psi\big(i_!\big((K\otimes k)\otimes\mathscr{L}_{\psi(f)}\big)\big)\big)$ is constant, with value $(-1)^nA(V,f,K,k,\psi)$. But the value of $\chi\big(\mathrm{FT}_\psi\big(i_!\big((K\otimes k)\otimes\mathscr{L}_{\psi(f)}\big)\big)\big)$ at any point of *any* strat of $\mathscr{H}[1/DMN\ell]$ is the constant value of the $\mathscr{H}$-adapted function $(V,f)_!\big(\chi(K)\big)$ on that strat. QED

Lemma 4.2. *Hypotheses and notations as in* 4.0.1–3 *above, for a given pair (k,ψ), the A-number $A(V,f,K,k,\psi)$ is the common value of the Euler characteristic*

$$\chi_c(V\otimes\bar{k},K\otimes\mathscr{L}_{\psi(f+\sum_i h_ix_i)})$$

for h in a dense open set of $H\otimes k$.

Proof. At every h in $H\otimes k$, $(-1)^n\chi_c(V\otimes\bar{k},K\otimes\mathscr{L}_{\psi(f+\sum_i h_ix_i)})$ is the local Euler characteristic of $\mathrm{FT}_\psi\big(i_!\big((K\otimes k)\otimes\mathscr{L}_{\psi(f)}\big)\big)$. So for h in any dense open set U of $H\otimes k$ on which $\mathrm{FT}_\psi\big(i_!\big((K\otimes k)\otimes\mathscr{L}_{\psi(f)}\big)\big)$ is $\mathscr{F}[n]$ for a lisse sheaf $\mathscr{F}$, $\chi_c(V\otimes\bar{k},K\otimes\mathscr{L}_{\psi(f+\sum_i h_ix_i)})$ is the rank of $\mathscr{F}$. QED

Lemma 4.3. *Hypotheses and notations as in* 4.0.1–3 *above, for a given pair* (k,ψ), *the following conditions are equivalent*:

1) $A(V,f,K,k,\psi)=0$.

2) *There exists a dense open set* U_1 *in* $H\otimes k$ *such that, for any finite extension E of k and any E-valued point h in* $U_1(E)$, *denoting by* ψ_E *the additive character* $\psi\circ\mathrm{Trace}_{E/k}$ *of E, the exponential sum*

$$\sum_{v\in V(E)}\mathrm{Trace}(\mathrm{Frob}_{E,v}|L)\psi_E\Bigl(f(v)+\sum_i h_i x_i(v)\Bigr)$$

vanishes.

3) *There exists a dense open set* U_1 *in* $H\otimes k$ *on which the trace function of* $\mathrm{FT}_\psi\bigl(i_!\bigl((K\otimes k)\otimes\mathscr{L}_{\psi(f)}\bigr)\bigr)$ *vanishes identically.*

Proof. Assertions 2) and 3) are trivially equivalent, since the sum in 2) is the value at h in $U_1(E)$ of the trace function. To show 1) ⇒ 3), we argue as follows. If

$$A(V,f,K,k,\psi)=0,$$

then there is a dense open set in U in $H\otimes k$ on which $\mathrm{FT}_\psi\bigl(i_!\bigl((K\otimes k)\otimes\mathscr{L}_{\psi(f)}\bigr)\bigr)$ vanishes. If this is the case, then its trace function vanishes on U as well. Conversely, suppose the trace function of $\mathrm{FT}_\psi\bigl(i_!\bigl((K\otimes k)\otimes\mathscr{L}_{\psi(f)}\bigr)\bigr)$ vanishes identically on some dense open set U_1 of $H\otimes k$. We know there is a dense open set U in $H\otimes k$ on which

$$\mathrm{FT}_\psi\bigl(i_!\bigl((K\otimes k)\otimes\mathscr{L}_{\psi(f)}\bigr)\bigr)$$

is $\mathscr{F}[n]$ for $\mathscr{F}$ a single lisse sheaf. So on some dense open set $U\cap U_1$, the trace function of $\mathscr{F}$ vanishes identically. By Chebotarev, $\mathscr{F}$ as representation of $\pi_1(U\cap U_1,\text{ base point})$ has identically vanishing trace function. But its trace at the identity is the rank of $\mathscr{F}$, which is in turn the A-number $A(v,f,K,k,\psi)$. QED

We will prove

Theorem 4.4. *Hypotheses and notations as in* 4.0.1–3 *above, suppose in addition that* $A(V,f,K,k,\psi)\neq 0$ *whenever the characteristic of the finite field k does not divide* $DMN\ell$. *Then for any finite field k of characteristic p not dividing* ℓMN, *any* $\bar{\mathbb{Q}}_\ell^\times$*-valued nontrivial additive character* ψ *of k, and any point h in* $H(k)$, *we have the following estimate. Suppose that h lies in the strat* H_i. *Then after any field embedding of* $\bar{\mathbb{Q}}_\ell$ *into* $\mathbb{C}$, *we have the estimate*

$$\Bigl|\sum_{v\in V(k)}\mathrm{Trace}(\mathrm{Frob}_{k,v}|K)\psi\Bigl(f(v)+\sum_i h_i x_i(v)\Bigr)\Bigr|$$
$$\leqq C\times\Bigl(\sup_{v\in V\otimes k}\|K\|(v)\Bigr)\times(\sqrt{\#k})^{\sup(d,d+n-1-\eta_i)}.$$

Proof. The key point is that the object $\mathrm{FT}_\psi\bigl(i_!(K\otimes k)\bigr)$ on $H\otimes k$ is on the one hand, perverse, geometrically irreducible, pure of weight $n+d$, and on the other hand it is adapted to the stratification $\mathscr{H}\otimes k$. Denote by $\mathscr{H}^a$ its a'th cohomology sheaf $\mathscr{H}^a\big(\mathrm{FT}_\psi\big(i_!\big((K\otimes k)\otimes\mathscr{L}_{\psi(f)}\big)\big)\big)$. Just as is the proof of the general estimate, we have

$$\mathscr{H}^a|H_i\otimes k \neq 0 \Rightarrow a \leqq -\eta_i.$$

What we must show here is the extra vanishing

$$\mathscr{H}^{-\eta_i}|H_i\otimes k = 0 \quad \text{whenever } \eta_i < n.$$

Because $\mathscr{H}^{-\eta_i}|H_i\otimes k$ is lisse, and $H_i\otimes k$ is equidimensional of dimension η_i, this vanishing in turn results from the following statement:

$$\text{for } a<n, \quad \dim\operatorname{Supp}\mathscr{H}^{-a} \leqq a-1.$$

This support condition is satisfied by the cohomology sheaves of *any* geometrically irreducible perverse object L on any geometrically connected smooth Y/k of dimension n (here $\mathbb{A}^n\otimes k$) such that L is generically non-zero. The point is that such an L has the following simple structure, cf. [BBD], 4.3.1. There is a dense affine open set U in Y, with inclusion map $j\colon U\to Y$, such that $L|U$ is $\mathscr{F}[n]$, for a lisse, geometrically irreducible lisse sheaf $\mathscr{F}$ on U, and L is the middle extension $j_{!*}(\mathscr{F}[n])$. For *any* lisse sheaf $\mathscr{F}$ on a dense affine open U in Y, its middle extension $j_{!*}(\mathscr{F}[n])$ satisfies the support condition

$$\text{for } a<n, \quad \dim\operatorname{Supp}\mathscr{H}^{-a}\big(j_{!*}(\mathscr{F}[n])\big) \leqq a-1,$$

cf. [BBD], 2.1.11. QED

Corollary 4.5. *Hypotheses and notations as in* 4.0.1–3 *above, suppose in addition that* $A(V,f,k,\psi)\neq 0$ *whenever the characteristic of the field k does not divide* $DMN\ell$. *Then for any finite field k of characteristic p not dividing* ℓNM, *any* $\bar{\mathbb{Q}}_\ell^\times$*-valued non-trivial additive character* ψ *of k, and any point h in* $H(k)$, *we have the following estimate. Suppose that h lies in the strat* H_i. *Then after any field embedding of* $\bar{\mathbb{Q}}_\ell$ *into* $\mathbb{C}$, *we have the estimate*

$$\Big|\sum_{v\in V(k)}\psi\Big(f(v)+\sum_i h_i x_i(v)\Big)\Big| \leqq C\times\big(\sqrt{\#k}\big)^{\sup(d,\,d+n-1-\eta_i)}.$$

Proof. Take K to be $\bar{\mathbb{Q}}_\ell[d]$ on V in Theorem 4.4. QED

Corollary 4.6. *Hypotheses and notations as in* 4.0.1–3 *above, suppose in addition that* $A(V,k,\psi)\neq 0$ *whenever the characteristic of the field k does not divide* $DMN\ell$. *Then for any finite field k of characteristic p not dividing* ℓNM, *any* $\bar{\mathbb{Q}}_\ell^\times$*-valued non-trivial additive character* ψ *of k, and any point h in* $H(k)$, *we have following estimate. Suppose that h lies in the strat* H_i. *Then after any field embedding of* $\bar{\mathbb{Q}}_\ell$ *into* $\mathbb{C}$, *we have the estimate*

$$\Big|\sum_{v\in V(k)}\psi\Big(\sum_i h_i x_i(v)\Big)\Big| \leqq C\times\big(\sqrt{\#k}\big)^{\sup(d,\,d+n-1-\eta_i)}.$$

Proof. Take $f\equiv 0$ in Corollary 4.5. QED

Remarks. 1) The strats $H_i \otimes k$ form a partition of $\mathbb{A}^n \otimes k$ into a finite disjoint union of smooth locally closed equidimensional subschemes, so there is precisely one strat whose dimension η_i is n. On this strat, there is no improvement in the estimate we get here over the general estimate obtained in Theorem 3.1. But on every other strat, we have an improvement by a factor $\sqrt{\#k}$ over the general estimate.

2) What happens in the theorem if, for a given (k,ψ) such that $\mathrm{char}(k)$ does not divide $DMN\ell$, we have $A(V,f,K,k,\psi) = 0$, i.e. when $\mathrm{FT}_\psi\big(i_!\big((K\otimes k)\otimes \mathscr{L}_{\psi(f)}\big)\big)$ has dimension of support $r < n$? In this case, there is a geometrically irreducible closed subscheme Z in $H\otimes k$ of dimension r, and a dense affine open set U in Z which is smooth over k and such that $\mathrm{FT}_\psi\big(i_!\big((K\otimes k)\otimes \mathscr{L}_{\psi(f)}\big)\big)|U$ is of the form $\mathscr{F}[r]$ for a geometrically irreducible $\bar{\mathbb{Q}}_\ell$-sheaf $\mathscr{F}$ on U which is pure of weight $d+n-r$. Moreover, denoting by $j\colon U\to Z$ and $i\colon Z\to H\otimes k$ the inclusions, $\mathrm{FT}_\psi\big(i_!\big((K\otimes k)\otimes \mathscr{L}_{\psi(f)}\big)\big)$ is $i_*j_{!*}(\mathscr{F}[r])$. Therefore we have

$$\mathscr{H}^{-a} = 0 \quad \text{for } a > r,$$

$$\dim \mathrm{Supp}\,\mathscr{H}^{-r} = r,$$

$$\dim \mathrm{Supp}\,\mathscr{H}^{k-r} \leqq r-1-k \quad \text{for } k \geqq 1.$$

But nonetheless, $\mathrm{FT}_\psi\big(i_!\big((K\otimes k)\otimes \mathscr{L}_{\psi(f)}\big)\big)$ is adapted to the stratification $\mathscr{H}\otimes k$, i.e. each $\mathscr{H}^a|H_i\otimes k$ is lisse. So for h in a strat $H_i\otimes k$ of dimension $\eta_i > r$, we have

$$\sum_{v\in V(k)} \mathrm{Trace}(\mathrm{Frob}_{k,v}|K)\psi\Big(f(v)+\sum_i h_i x_i(v)\Big) = 0 \quad \text{if } \eta_i > r.$$

For h in a strat $H_i\otimes k$ of dimension $\eta_i \leqq r$, we have the estimate

$$\Big|\sum_{v\in V(k)} \mathrm{Trace}(\mathrm{Frob}_{k,v}|K)\psi\Big(f(v)+\sum_i h_i x_i(v)\Big)\Big|$$
$$\leqq C\times\Big(\sup_{v\in V\otimes k}\|K\|(v)\Big)\times(\sqrt{\#k})^{\sup(d+n-r,\,d+n-1-\eta_i)}.$$

Thus on strats of dimension r, we have the general estimate of Theorem 3.1, and on strats of dimension $< r$ we have an improvement by a factor $\sqrt{\#k}$ over the general estimate.

For example, suppose V is a linear subspace of $\mathbb{A}^n$ of dimension $d > 0$ and codimension $r := n-d$. Suppose K is $\bar{\mathbb{Q}}_\ell[d]$ on V, and $f\equiv 0$. Denote by $V^\perp$ the r-dimensional annihilator of V in H. Then $\mathrm{FT}_\psi\big(i_!\big((K\otimes k)\otimes \mathscr{L}_{\psi(f)}\big)\big)$ is the constant sheaf $\bar{\mathbb{Q}}_\ell[r](r-n)$ on $V^\perp$, extended by 0.

Proof of Theorem 1.2. Because $V_{\mathbb{C}}$ is smooth and irreducible of dimension d, there exists an integer $D_1 \geqq 2$ such that $V[1/D_1]$, is smooth over $\mathbb{Z}[1/DD_1]$, with geometrically connected fibres of dimension d. We first prove part 1) of Theorem 1.2 for $V[1/D_1]\subset \mathbb{A}^n_{\mathbb{Z}[1/DD_1]}$, deducing it from Corollary 4.6 in exactly the same way we deduced Theorem 1.1 from Corollary 3.2, with the same definition of the closed sets $X_j\subset \mathbb{A}^n_{\mathbb{Z}[1/DD_1]}$.

To prove 2), we argue as follows.

For each $j = 1, \dots, n$, pick generators $F_{\alpha,j}(X)$ for the ideals I_j defining X_j in $\mathbb{A}^n_{\mathbb{Z}[1/DD_1]}$. Write each $F_{\alpha,j}(X)$ as the sum of its homogeneous part

$$F_{\alpha,j}(X) = \sum_k F_{\alpha,j,k}(X),$$

with $F_{\alpha,j,k}(X)$ a homogeneous form of degree k.

Let K be an upper bound for the integers k, such that some $F_{\alpha,j,k}$ is non-zero. Denote by D_2 the non-zero integer defined by

$$D_2 := \prod_{0 \leqq a < b \leqq K} \big((D_1)^a - (D_1)^b\big).$$

Denote by

$$X_j^{\mathrm{proj}} \subset X_j \subset \mathbb{A}^n_{\mathbb{Z}[1/DD_1]}$$

the closed subscheme of X_j defined by the vanishing of all the homogeneous components $F_{\alpha,j,k}$ of all the chosen generators $F_{\alpha,j}$ of the ideal I_j. Then extend the X_j^{proj} to homogeneous closed subschemes of $\mathbb{A}_{\mathbb{Z}[1/D]}$ by taking schematic closure. It suffices to show that for $p \nmid DD_1D_2$, ψ any non trivial additive character of $\mathbb{F}_p$, and any $h \notin X_j^{\mathrm{proj}}(\mathbb{F}_p)$, we have

$$(*)_j \qquad \Big| \sum_{x \in V(\mathbb{F}_p)} \psi(h_1x_1 + \cdots + h_nx_n) \Big| \leqq Cp^{\sup(\frac{d}{2}, \frac{d+j-2}{2})}.$$

(Then we increase C to absorb what happens at the finitely many primes $p \nmid D$ which divide D_1D_2.)

To see this, we argue as follows. We know that $(*)_j$ holds for $h \notin X_j(\mathbb{F}_p)$, for *any* non-trivial ψ. So for any fixed $\alpha \in \mathbb{F}_p^\times$, $(*)_j$ holds if $\alpha h \in X_j(\mathbb{F}_p)$ for any non-trivial ψ. (The point is that $h \mapsto \alpha h$ has the same effect in the sum as $\psi(x) \mapsto \psi(\alpha x)$.) Take α to be successively $(D_1)^a$ for $a = 0, \dots, K$. Then $(*)_j$ holds for $h \in \mathbb{A}^n(\mathbb{F}_p)$ (and all non-trivial ψ) if there exists some integer a in $[0, K]$ such that $(D_1)^a h \notin X_j(\mathbb{F}_p)$. In other words, $(*)_j$ holds for $h \in \mathbb{A}^n(\mathbb{F}_p)$ unless h is an $\mathbb{F}_p$-valued zero of *all* the polynomials

$$F_{\alpha,j}\big((D_1)^a X\big),$$

all α, all $a = 0, \dots, K$. Write these in terms of homogeneous components

$$F_{\alpha,j}\big((D_1)^a X\big) = \sum_k (D_1)^{ak} F_{\alpha,j,k}(X).$$

Over $\mathbb{Z}[1/DD_1D_2]$, the linear span of these is precisely the same as the linear span of the homogeneous components $F_{\alpha,j,k}$, all α, all k, thanks to the Vandermonde determinant. And these homogeneous components define X_j^{proj}. Thus $(*)_j$ holds for $h \notin X_j^{\mathrm{proj}}$, as required. QED

5. Lower bounds for A-numbers of level sets of homogeneous forms, via B-numbers

In the previous section, we worked over $\mathbb{Z}$ and our emphasis was on uniformity results for exponential sums over $\mathbb{F}_p$ as p varied. We needed to see if the A-number $A(V, f, K, k, \psi)$ was non-zero for all (k, ψ) with $\mathrm{char}(k)$ sufficiently large. For a given (k, ψ), this A-number, the generic rank of $\mathrm{FT}_\psi\big(i_!\big((K \otimes k) \otimes \mathscr{L}_{\psi(f)}\big)\big)$ is an invariant of the data $(V \otimes k \subset \mathbb{A}^n \otimes k, f \otimes k, K \otimes k, \psi)$.

In this section, we work over a finite field k, and pick a prime ℓ invertible in k. We fix an integer $n \geqq 1$, and a non-zero homogeneous form over k in n variables,

$$F(x_1, \dots, x_n) \quad \text{in } k[x_1, \dots, x_n].$$

We make the following two hypotheses:

1) The degree of F, $\deg(F)$, is invertible in k.

2) For any integer $r \geqq 2$ which divides $\deg(F)$, F is not an r'th power in the ring $\bar{k}[x_1, \dots, x_n]$.

It results from these two hypotheses that for any β in $\bar{k}^\times$, the hypersurface

$$V_\beta; \quad F = \beta \quad \text{in } \mathbb{A}^n \otimes \bar{k}$$

of equation $F = \beta$ over $\bar{k}$ is smooth of dimension $n - 1$ and geometrically irreducible, cf. [Ka-PES], proof of 6.5.

Denote by i_β: $V_\beta \to \mathbb{A}^n \otimes \bar{k}$ the inclusion. We are interested in the A-number of V_β. We take K the perverse sheaf $\bar{\mathbb{Q}}_\ell[n-1]$ on V_β, f the function 0, ψ any nontrivial $\bar{\mathbb{Q}}_\ell^\times$-valued additive character of k, and look at $\mathrm{FT}_\psi\big(i_{\beta!}(\bar{\mathbb{Q}}_\ell[n-1])\big)$ on the dual affine space $H \otimes k$. We know that on some dense open set U in $H \otimes k$, $\mathrm{FT}_\psi\big(i_{\beta!}(\bar{\mathbb{Q}}_\ell[n-1])\big)$ is of the form $\mathscr{F}_\beta[n]$ for $\mathscr{F}_\beta$ a lisse, geometrically irreducible $\bar{\mathbb{Q}}_\ell$-sheaf on U which is pure of weight $n-1$, and we define

$$A(V_\beta) := \text{the rank of } \mathscr{F}_\beta.$$

Lemma 5.1. *Hypotheses and notations as above, for any β in $\bar{k}^\times$, we have $A(V_\beta) = A(V_1)$.*

Proof. Pick a $\deg(F)$'th root of β, say $\alpha^{\deg(F)} = \beta$, with α in $\bar{k}^\times$. Because F is homogeneous, the homothety $x \mapsto \alpha x$ defines an isomorphism from V_1 to V_β. So the object $\mathrm{FT}_\psi\big(i_{\beta!}(\bar{\mathbb{Q}}_\ell[n-1])\big)$ on $H \otimes \bar{k}$ is the pullback by the homothety $h \mapsto \alpha h$ of $\mathrm{FT}_\psi\big(i_{\beta!}(\bar{\mathbb{Q}}_\ell[n-1])\big)$. Pick a dense open set U_1 in $H \otimes \bar{k}$ on which $\mathrm{FT}_\psi\big(i_{\beta!}(\bar{\mathbb{Q}}_\ell[n-1])\big)$ is $\mathscr{F}_1[n]$ for a lisse $\mathscr{F}_1$. Then on U_β: $[h \mapsto \alpha h]^{-1}(U_1), \mathrm{FT}_\psi\big(i_{\beta!}(\bar{\mathbb{Q}}_\ell[n-1])\big)$ is $\mathscr{F}_\beta[n]$, with $\mathscr{F}_\beta$ the lisse sheaf $[h \mapsto \alpha h]^*(\mathscr{F})$. QED

Given *any* hypersurface in $\mathbb{A}^n \otimes k$, with inclusion i_X, $\bar{\mathbb{Q}}_\ell[n-1]$ on X is perverse [Ka-PESII], Lemma 2.1, and mixed of weight $\leqq n-1$. Its extension by zero to $\mathbb{A}^n \otimes k$, $i_{X!}\big(\bar{\mathbb{Q}}_\ell[n-1]\big)$, is perverse on $\mathbb{A}^n \otimes k$. So $\mathrm{FT}_\psi\big(i_{X!}(\bar{\mathbb{Q}}_\ell[n-1])\big)$ is perverse on the dual affine space $H \otimes k$. Hence there is some dense open set U_X in $H \otimes k$ on which $\mathrm{FT}_\psi\big(i_{X!}(\bar{\mathbb{Q}}_\ell[n-1])\big)$ is of the form $\mathscr{F}_X[n-1]$, for some lisse $\bar{\mathbb{Q}}_\ell$-sheaf $\mathscr{F}_X$ on U_X which is mixed of weight $\leqq n-1$. We define

$$B(X) := \text{the rank of } \mathscr{F}_X.$$

If X is smooth over k, and geometrically irreducible, then its B-number $B(X)$ is equal to its A-number $A(X)$. In [Ka-PES] and [PESII], we defined the A-number of X to be the rank of the pure of weight $n-1$ quotient of $\mathscr{F}_X$. With this definition of $A(X)$ for a possibly singular hypersurface X we have an a priori inequality

$$B(X) \geqq A(X).$$

In what follows, we will apply these considerations to $X := V_0$, the hypersurface of equation $F = 0$.

Theorem 5.2. *Hypotheses and notations as above, for any β in $k^\times$ we have the inequality*

$$A(V_\beta) \geqq B(V_0).$$

Proof. Replacing F by $\beta^{-1}F$, we reduce to proving

$$A(V_1) \geqq B(V_0).$$

Given β in $\bar{k}$, we say that a point h in $H(\bar{k})$ computes the A-number of V_β if there is an open neighborhood of h in $H \otimes \bar{k}$ over which $\mathrm{FT}_\psi\big(i_{\beta!}(\bar{\mathbb{Q}}_\ell[n-1])\big)$ is of the form (a lisse sheaf) $[n]$. In particular, if h computes the A-number of V_β, then the stalks of the cohomolgy sheaves of $\mathrm{FT}_\psi\big(i_{\beta!}(\bar{\mathbb{Q}}_\ell[n-1])\big)$ at h vanish for $a \neq -n$:

$$\mathscr{H}^a\big(\mathrm{FT}_\psi\big(i_{X!}(\bar{\mathbb{Q}}_\ell[n-1])\big)\big)_h = 0 \quad \text{for } a \neq -n.$$

In more down to earth terms, we have

$$H_c^b\big(V_\beta \otimes_{k(\beta)} \bar{k}, \mathscr{L}_{\psi(\sum_i h_i x_i)}\big) = 0 \quad \text{for } b \neq n-1.$$

It is proven in [Ka-PESII], 8.2 that given any finite set S of β's in $\bar{k}$, we can pick an $h \neq 0$ in $H(\bar{k})$ which computes the A-number of V_β for all β in S, and which also computes the A-number of V_β for all but finitely many values of β in $\bar{k}$. We take for S the set $\{0,1\}$, and fix a choice of h in $H(\bar{k})$ which computes the A-numbers of V_0, V_1 and V_β for all but finitely many β in $\bar{k}$, say for all β outside the finite set T.

Now view the homogeneous form F as a map from $\mathbb{A}^n \otimes k$ to $\mathbb{A}^1 \otimes k$, and endow the source with the lisse sheaf $\mathscr{L}_{\psi(\sum_i h_i x_i)}$. Consider the Leray spectral sequence

$$E_2^{a,b}\colon H_c^a\big(\mathbb{A}^1 \otimes \bar{k}, R^b F_! \mathscr{L}_{\psi(\sum_i h_i x_i)}\big) \Rightarrow H_c^{a+b}\big(\mathbb{A}^n \otimes \bar{k}, \mathscr{L}_{\psi(\sum_i h_i x_i)}\big).$$

It is proven in [Ka-PESII], 8.3 and 8.4 that

1) the sheaves $R^bF_!\mathscr{L}_{\psi(\sum\limits_i h_ix_i)}$ vanish for $b \neq n-1$,

2) the sheaf $\mathscr{R} := R^{n-1}F_!\mathscr{L}_{\psi(\sum\limits_i h_ix_i)}$ has $H_c^*(\mathbb{A}^1 \otimes \bar{k}, \mathscr{R}) = 0$,

3) for $j\colon U \to \mathbb{A}^1$ the inclusion of any dense open set in $\mathbb{A}^1$ on which $\mathscr{R} := R^{n-1}F_!\mathscr{L}_{\psi(\sum\limits_i h_ix_i)}$ is lisse, we have $\mathscr{R} \cong j_*j^*\mathscr{R}$.

We claim that $\mathscr{R} := R^{n-1}F_!\mathscr{L}_{\psi(\sum\limits_i h_ix_i)}$ is lisse at the point $\beta = 1$. To see this, we argue as follows. According to 3) above, $\mathscr{R} \cong j_*j^*\mathscr{R}$, so the points β at which $\mathscr{R}$ is lisse are precisely the points at which the stalk $\mathscr{R}_\beta$ has maximum dimension. There are finitely many points in $\mathbb{A}^1(\bar{k})$ at which the stalk has less than the maximum dimension. So to show that $\dim \mathscr{R}_1$ is the maximum, it suffices to show that for all but finitely many β's in $\bar{k}^*$, $\dim \mathscr{R}_\beta = \dim \mathscr{R}_1$.

For this, we use the homogeneity of F. Let us denote by d the degree of F. For t in $\bar{k}^\times$, the homothety $x \mapsto tx$ of $\mathbb{A}^n$ induces an isomorphism

$$V_1 \cong V_{t^d}.$$

And this same isomorphism carries $\mathscr{L}_{\psi(t\sum\limits_i h_ix_i)}$ on V_1 to $\mathscr{L}_{\psi(\sum\limits_i h_ix_i)}$ on V_{t^d}. So we have an isomorphism

$$\begin{aligned}\mathscr{R}_{t^d} &:= H_c^{n-1}\big(V_{t^d} \otimes_{k(\beta^d)} \bar{k}, \mathscr{L}_{\psi(\sum\limits_i h_ix_i)}\big)\\ &\cong H_c^{n-1}\big(V_1 \otimes_k \bar{k}, \mathscr{L}_{\psi(t\sum\limits_i h_ix_i)}\big).\end{aligned}$$

We claim that the point th in $H(\bar{k})$ computes the A-number of V_1 for all but finitely many t in $\bar{k}$. (If this is true, then

$$\dim \mathscr{R}_{t^d} = A(V_1)$$

for all but finitely many t in $\bar{k}$, and consequently $\mathscr{R}$ is lisse at $t = 1$.) Pick an open neighborhood U of h in $H \otimes \bar{k}$ on which $\mathrm{FT}_\psi\big(i_{1!}(\bar{\mathbb{Q}}_\ell[n-1])\big)$ is of the form (a lisse sheaf) $[n]$. Consider the map

$$\rho\colon \mathbb{A}^1 \otimes \bar{k} \to H \otimes \bar{k}, \quad t \mapsto th.$$

Then $\rho^{-1}(U)$ is an open set in $\mathbb{A}^1 \otimes \bar{k}$, and it is nonempty because it contains the point $t = 1$. Therefore $\rho^{-1}(U)$ is a dense open set of $\mathbb{A}^1 \otimes \bar{k}$, so the complement of a finite set. For any t in $\rho^{-1}(U)(\bar{k})$, th computes the A-number of V_1.

Now that we know that $\mathscr{R}$ is lisse at $t = 1$, we have

$$A(V_1) = \text{generic rank of } \mathscr{R}.$$

On the other hand, h computes the A-number of V_0, so we have

$$B(V_0) = \dim H_c^{n-1}(V_0 \otimes_k \bar{k}, \mathscr{L}_{\psi(\sum_i h_i x_i)}).$$

But

$$H_c^{n-1}(V_0 \otimes_k \bar{k}, \mathscr{L}_{\psi(t\sum_i h_i x_i)}) = \mathscr{R}_0 = (j_* j^* \mathscr{R})_0 := \mathscr{R}^{I(0)}.$$

Thus $A(V_1)$ is the generic rank of $\mathscr{R}$, and $B(V_0)$ is the dimension of the inertial invariants at $t = 0$ in $\mathscr{R}$. So we have asserted inequality $A(V_1) \geqq B(V_0)$. QED

Remark. In [Ka-PESII], 7.1, (1), we related the A-number of V_1 to the A-number of V_0. In the application of Theorem 5.2 in the next section (Theorem 6.2) we cannot make do with [Ka-PESII], 7.1, (1) because V_0 has A-number zero in that application.

6. Calculation of a B-number

In this section, we take for F the homogeneous form of degree four in four variables a, b, c, d

$$(6.1) \qquad \Delta_3(a,b,c,d) := b^2c^2 + 18abcd - 27a^2d^2 - 4b^3d - 4c^3a,$$

the discriminant of the binary cubic form $aX^3 + bX^2Y + cXY^2 + dY^3$.

Over any field k in which 2 is invertible, Δ_3 is not a square in the polynomial ring $k[a,b,c,d]$. Indeed, if we put $b = d = 0$, the resulting form $\Delta_3(a,0,c,0) = -4c^3a$ is not a square. So for any β in $k^\times$, the equation $\Delta_3 = \beta$ defines a smooth, geometrically irreducible hypersurface

$$V_\beta\colon \Delta_3 = \beta \quad \text{in } \mathbb{A}^4 \otimes k.$$

Theorem 6.1. *Over any finite field k of odd characteristic, $B(V_0) = 1$, and for any β in $k^\times$ we have $A(V_\beta) \geqq 2$.*

Proof. We will show that on a dense open set U_0 of $H \otimes k$, the lisse sheaf $\mathscr{F}_0$ whose rank is the B-number $B(V_0)$ is $\bar{\mathbb{Q}}_\ell(-1)$. Once we have this result, then in the notation of the proof of Theorem 5.2, we have $\mathscr{R}^{I(0)} = \bar{\mathbb{Q}}_\ell(-1)$, which is pure of weight 2. But $\mathscr{R}$ is, on any dense open set where it is lisse, pure of weight 3. By [De-WII], 1.8.4, we may infer that the local monodromy of $\mathscr{R}$ at 0 contains a unipotent Jordan block of dimension two. Therefore $\mathscr{R}$ has generic rank $\geqq 2$, which means precisely that $A(V_1) \geqq 2$. Replacing Δ_3 by $\beta^{-1}\Delta_3$ and repeating the argument, we get $A(V_\beta) \geqq 2$ for any β in $k^\times$.

Consider now any dense open set U_0 in $H \otimes k$ over which $\mathrm{FT}(i_{0!}(\bar{\mathbb{Q}}_\ell[3]))$ is of the form $\mathscr{F}_0[4]$ for a lisse sheaf $\mathscr{F}_0$ on U_0. In order to show that $\mathscr{F}_0$ is $\bar{\mathbb{Q}}_\ell(-1)$ on U_0, it suffices to show that for some dense open set $U \subset U_0$, we have $\mathscr{F}_0|U \cong \bar{\mathbb{Q}}_\ell(-1)$ (just because $\pi_1(U)$ maps onto $\pi_1(U_0)$). To show that $\mathscr{F}_0|U \cong \bar{\mathbb{Q}}_\ell(-1)$, it suffices, by Chebotarev, to show that for all finite extensions E/k, and for all E-valued points h in $U(E)$, we have $\mathrm{Trace}(\mathrm{Frob}_{E,h}|\mathscr{F}_0) = \#E$. At any point h in $U(E)$, we have

$$H_c^a(V_0 \otimes_k \bar{k}, \mathscr{L}_{\psi(t\sum_i h_i x_i)}) = 0 \quad \text{for } a \neq 3,$$

$$H_c^3(V_0 \otimes_k \bar{k}, \mathscr{L}_{\psi(t\sum_i h_i x_i)}) = (\mathscr{F}_0)_h.$$

Thus we find

$$\begin{aligned}\mathrm{Trace}(\mathrm{Frob}_{E,h}|\mathscr{F}_0) &= \mathrm{Trace}\big(\mathrm{Frob}_E|H_c^3(V_0 \otimes_k \bar{k}, \mathscr{L}_{\psi(\sum_i h_i x_i)})\big) \\ &= -\sum_a (-1)^a \mathrm{Trace}\big(\mathrm{Frob}_E|H_c^a(V_0 \otimes_k \bar{k}, \mathscr{L}_{\psi(t\sum_i h_i x_i)})\big) \\ &= \sum_{x \in V_0(E)} \psi_E\Big(\sum_i h_i x_i\Big),\end{aligned}$$

for ψ_E the nontrivial additive character $\psi \circ \mathrm{Trace}_{E/k}$ of E.

So what we must show is that there exists a dense open set U in $H \otimes k$ such that for any finite extension E/k, and any h in $U(E)$, we have

$$\sum_{x \in V_0(E)} \psi_E\Big(\sum_i h_i x_i\Big) = -\#E.$$

Because V_0 is defined by the vanishing of a homogeneous form, $V_0(E)$ is stable by $E^\times$-homotheties of the ambient $\mathbb{A}^4(E)$. So the sum is independent of the nontrivial character: we have

$$\begin{aligned}&\sum_{x \in V_0(E)} \psi_E\Big(\sum_i h_i x_i\Big) \\ &\quad = 1 + \sum_{x \neq 0 \in V_0(E)} \psi_E\Big(\sum_i h_i x_i\Big) \\ &\quad = 1 + (1/\#E^\times) \sum_{t \in E} \sum_{x \neq 0 \in V_0(E)} \psi_E\Big(t \sum_i h_i x_i\Big) \\ &\quad = 1 + (1/\#E^\times) \sum_{x \neq 0 \in V_0(E)} \Big(-1 + \sum_{t \in E} \psi_E\Big(t \sum_i h_i x_i\Big)\Big) \\ &\quad = 1 - (1/\#E^\times)\Big(\sum_{x \neq 0 \in V_0(E)} 1\Big) + (\#E)(1/\#E^\times) \sum_{\substack{x \neq 0 \in V_0(E) \\ \sum_i h_i x_i = 0}} 1 \\ &\quad = 1 - (1/\#E^\times)\big(\#V_0(E) - 1\big) + (\#E/\#E^\times)\Big(\#\Big(V_0(E) \cap \Big(\sum_i h_i x_i = 0\Big)\Big) - 1\Big).\end{aligned}$$

Let us rewrite this in terms of the projective variety V_0^{proj} in $\mathbb{P}^3$ defined by the vanishing of Δ_3, and its hyperplane section $\sum_i h_i x_i = 0$.

$$\sum_{x \in V_0(E)} \psi_E\Big(\sum_i h_i x_i\Big) = 1 - \#V_0^{\mathrm{proj}}(E) + (\#E)\#\Big(V_0^{\mathrm{proj}} \cap \Big(\sum_i h_i x_i = 0\Big)\Big)(E).$$

So what we must show is that

$$\#E + 1 + (\#E)\#\Big(V_0^{\mathrm{proj}} \cap \Big(\sum_i h_i x_i = 0\Big)\Big)(E) = \#V_0^{\mathrm{proj}}(E),$$

for h in some dense open set.

Now a point of $V_0^{\mathrm{proj}}(E)$ is a nonzero binary cubic form (up to homothety) with at least a double root. Such a double root must be E-rational, so the form in question can be written

$$(\alpha X + \beta Y)^2(\gamma X + \delta Y),$$

for an ordered pair of nonzero linear forms $(\alpha X + \beta Y)$ and $(\gamma X + \delta Y)$ over E. This ordered pair of forms is unique up to the action of $E^\times \times E^\times$ defined by having (s,t) in $E^\times \times E^\times$ act as

$$\alpha X + \beta Y, \quad \gamma X + \delta Y \mapsto t(\alpha X + \beta Y), \quad st^{-2}(\gamma X + \delta Y).$$

So we may view this ordered pair as an E-valued point in $\mathbb{P}^1 \times \mathbb{P}^1$. Thus we have

$$\#V_0^{\mathrm{proj}}(E) = (\#E + 1)^2.$$

What happens if we look at the intersection $V_0^{\mathrm{proj}} \cap \Big(\sum_i h_i x_i = 0\Big)$ in terms of this identification of V_0^{proj} with $\mathbb{P}^1 \times \mathbb{P}^1$? If we multiply out

$$(\alpha X + \beta Y)^2(\gamma X + \delta Y) = \alpha^2\gamma X^3 + (2\alpha\beta\gamma + \alpha^2\delta)X^2Y + (2\alpha\beta\delta + \beta^2\gamma)XY^2 + \beta^2\delta Y^3,$$

then a point of $V_0^{\mathrm{proj}} \cap \Big(\sum_i h_i x_i = 0\Big)$ is a point $\big((\alpha,\beta)(\gamma,\delta)\big)$ in $\mathbb{P}^1 \times \mathbb{P}^1$ which also satisfies

$$h_1(\alpha^2\gamma) + h_2(2\alpha\beta\gamma + \alpha^2\delta) + h_3(2\alpha\beta\delta + \beta^2\gamma) + h_4(\beta^2\delta) = 0.$$

For fixed h, this is the vanishing of a bihomogeneous form of bidegree $(2,1)$ in $\mathbb{P}^1 \times \mathbb{P}^1$, namely

$$\gamma(h_1\alpha^2 + 2h_2\alpha\beta + h_3\beta^2) + \delta(h_2\alpha^2 + 2h_3\alpha\beta + h_4\beta^2) = 0.$$

Unless the two quadrics

$$h_1\alpha^2 + 2h_2\alpha\beta + h_3\beta^2 \quad \text{and} \quad h_2\alpha^2 + 2h_3\alpha\beta + h_4\beta^2$$

have a common zero in $\mathbb{P}^1$, we can solve uniquely for (γ,δ), in which case projecting onto (α,β) is a bijection

$$\Big(V_0^{\mathrm{proj}} \cap \Big(\sum_i h_i x_i = 0\Big)\Big)(E) \cong \mathbb{P}^1(E).$$

So for h such that the two binary quadrics

$$h_1\alpha^2 + 2h_2\alpha\beta + h_3\beta^2 \quad \text{and} \quad h_2\alpha^2 + 2h_3\alpha\beta + h_4\beta^2$$

have no common zero in $\mathbb{P}^1$, we find

$$\begin{aligned}\#E + 1 + (\#E)\#\Bigl(V_0^{\mathrm{proj}} \cap \Bigl(\sum_i h_i x_i = 0\Bigr)\Bigr)(E) &= \#E + 1 + (\#E)(\#E + 1)\\ &= (\#E + 1)^2 = \#V_0^{\mathrm{proj}}(E)\end{aligned}$$

as required. It remains to see that for general h, the two binary quadrics

$$h_1\alpha^2 + 2h_2\alpha\beta + h_3\beta^2 \quad \text{and} \quad h_2\alpha^2 + 2h_3\alpha\beta + h_4\beta^2$$

have no common zero in $\mathbb{P}^1$. This condition defines an open set in $H \otimes k$. The particular point $h := (1, 0, 0, 1)$ shows it is a non-empty and hence dense open set. QED

Remarks. This computation is already in [Be-Fo], 3.a.1–2, pp. 235–236, where we find a precise description of the closed set where the two quadrics have a common zero: it is defined by $\Delta_3(h_1, 3h_2, 3h_3, h_4) = 0$.

7. Nonvanishing of *B*-numbers by congruence considerations

In this section, we work over a finite field k and pick a prime ℓ invertible in k. We fix an integer $n \geqq 1$ and a non-zero homogeneous form over k in n variables,

$$F(x_1, \dots, x_n) \in k[x_1, \dots, x_n],$$

about which we assume, for the moment, nothing.

We denote by $X \subset \mathbb{A}^n \otimes k$ the affine hypersurface of equation $F = 0$, and by X^{proj} the projective hypersurface in $\mathbb{P}^{n-1} \otimes k$ defined by $F = 0$. We are interested in criteria which will guarantee that $B(X)$ is non-zero.

Recall that for any finite extension E of k, any non-trivial $\bar{\mathbb{Q}}_\ell^\times$-valued character ψ of E, and any point h in $H(E)$

$$\sum_{x \in X(E)} \psi\Bigl(\sum_i h_i x_i\Bigr) = 1 + (\#E)\#\bigl(X^{\mathrm{proj}} \cap (h \cdot x = 0)\bigr) - \#X^{\mathrm{proj}}(E).$$

On the other hand, we know that there is a dense open set U in $H \otimes k$, and a lisse sheaf $\mathscr{F}_X$ on U, such that for h in $U(E)$, we have

$$\mathrm{Trace}(\mathrm{Frob}_{E,h}|\mathscr{F}_X) = (-1)^{n-1} \sum_{x \in X(E)} \psi\Bigl(\sum_i h_i x_i\Bigr).$$

The rank of $\mathscr{F}_X$ is the B-number $B(X)$. If $B(X) = 0$, then $\mathscr{F}_X$ is the zero sheaf, and its trace function vanishes. Thus we find

Lemma 7.1. *If $B(X) = 0$, then there exists a dense open set U in $H \otimes k$, such that for any finite extension E/k, and any point h in $U(E)$, we have*

$$\#X^{\text{proj}}(E) = 1 + (\#E)\#\big(X^{\text{proj}} \cap (h \cdot x = 0)\big)(E).$$

Corollary 7.2. *If $B(X) = 0$, then for every finite extension E/k of sufficiently high degree, we have the congruence*

$$\#X^{\text{proj}}(E) \equiv 1 \bmod \#E.$$

Proof. The set $U(E)$ is nonempty for $\#E$ sufficiently large.

Corollary 7.3. *If $B(X) = 0$, then for every finite extension E/k, we have the congruence*

$$\#X^{\text{proj}}(E) \equiv 1 \bmod (\operatorname{char} k).$$

Proof. Let us denote by p the characteristic of k. Given a finite extension E/k, and an integer $r \geqq 1$, denote by E_{p^r}/E the extension of E of degree p^r. Then for any separated E-scheme V/E of finite type, we have

$$\#V(E_{p^r}) \equiv \#V(E) \bmod p.$$

Indeed, when $\operatorname{Gal}(E_{p^r}/E) \cong \mathbb{Z}/p^r\mathbb{Z}$ acts on $V(E_1)$, each orbit has size 1 or size p^a for some $a \geqq 1$. The orbits of size 1 are exactly the points of $V(E)$. But for $r \gg 0$, the previous corollary gives

$$\#X^{\text{proj}}(E_{p^r}) \equiv 1 \bmod \#E_{p^r}. \quad \text{QED}$$

Thus we find the following criterion:

Theorem 7.4. *Notations as above, if for some finite extension E/k we have*

$$\#X^{\text{proj}}(E) \not\equiv 1 \bmod (\operatorname{char} k)$$

then $B(X) \neq 0$.

We can be slightly more precise. The trace function of the sheaf $\mathscr{F}_X$ takes values in $\mathbb{Z}$. For any finite extension E/k, and any point h in $U(E)$, the characteristic polynomial

$$\det(1 - T\,\mathrm{Frob}_{E,h}|\mathscr{F}_X)$$

has coefficients in $\mathbb{Z}$. Thus it makes sense to speak of the reduction $\bmod\, p$ of $\det(1 - T\,\mathrm{Frob}_{E,h}|\mathscr{F}_X)$ as an element of $1 + T\mathbb{F}_p[T]$.

Fix h in $U(E)$. Denote by E_r/E the extension of degree r. For each $r \geqq 1$, we have the identity

$$(-1)^n \operatorname{Trace}\big((\mathrm{Frob}_{E,h})^r|\mathscr{F}_X\big) = \#X^{\text{proj}}(E_r) - 1 - (\#E_r)\#\big(X^{\text{proj}} \cap (h \cdot x = 0)\big)(E_r).$$

So we get an identity of power series in $1 + T\mathbb{Z}[[T]]$:

$$\begin{aligned}&\det(1 - T\,\mathrm{Frob}_{E,h}|\mathscr{F}_X)^{(-1)^{n-1}}\\ &\quad = (1 - T)\,\mathrm{Zeta}\big((X^{\mathrm{proj}} \otimes_k E/E, T)\big)/\mathrm{Zeta}\big(X^{\mathrm{proj}} \cap (h \cdot x = 0)/E, (\#E)T\big).\end{aligned}$$

Since $\mathrm{Zeta}\big(X^{\mathrm{proj}} \cap (h \cdot x = 0)/E, T\big)$ lies in $1 + T\mathbb{Z}[[T]]$, we may reduce $\bmod\, p$ and get a congruence

$$\det(1 - T\,\mathrm{Frob}_{E,h}|\mathscr{F}_X)^{(-1)^{n-1}} \equiv (1 - T)\,\mathrm{Zeta}(X^{\mathrm{proj}} \otimes_k E/E, T) \bmod^{\times} 1 + T\mathbb{Z}[[T]].$$

On the other hand, there is a $\bmod\, p$ congruence formula for the zeta function of any projective variety, say V over a finite field E of characteristic p, in terms of the action of the $\#E$'th power map Frob_E on the coherent cohomology groups $H^i(V, \mathcal{O}_V)$. One has

$$\mathrm{Zeta}(V/E, T) \equiv \prod_{i=0}^{\dim V} \det\big(1 - T\,\mathrm{Frob}_E|H^i(V, \mathcal{O}_V)\big)^{(-1)^{i+1}}$$

in $1 + T\mathbb{F}_p[[T]]$, cf. [SGA 7], XXII, 3.1.1.

If V is a projective hypersurface in $\mathbb{P}^{n-1}$, of degree $d \geqq 1$, the cohomology groups $H^i(V, \mathcal{O}_V)$ vanish unless i is 0 or $n - 2$. Suppose now $n \geqq 3$. Then for $i = 0$,

$$H^0(V, \mathcal{O}_V) = E$$

and Frob_E acts as the identity. So the congruence above becomes

$$\det(1 - T\,\mathrm{Frob}_{E,h}|\mathscr{F}_X) \equiv \det\big(1 - T\,\mathrm{Frob}_E|H^{n-2}(X^{\mathrm{proj}}, \mathcal{O}_{X^{\mathrm{proj}}})\big)$$

in $\mathbb{F}_p[T]$. Now consider the degrees of the polynomials in this congruence. As a $\mathbb{Z}$-polynomial $\det(1 - T\,\mathrm{Frob}_{E,h}|\mathscr{F}_X)$ has degree equal to the rank of $\mathscr{F}_X$, i.e. equal to the B-number $B(X)$. The degree of its reduction $\bmod\, p$ can only be lower, so we get

Theorem 7.5. *Suppose $n \geqq 3$. We have the inequality*

$$B(X) \geqq \textit{degree of the } \mathbb{F}_p[T] \textit{ polynomial } \det\big(1 - T\,\mathrm{Frob}_E|H^{n-2}(X^{\mathrm{proj}}, \mathcal{O}_{X^{\mathrm{proj}}})\big).$$

This inequality is useless if either $H^{n-2}(X^{\mathrm{proj}}, \mathcal{O}_{X^{\mathrm{proj}}}) = 0$ or if Frob_E is nilpotent on $H^{n-2}(X^{\mathrm{proj}}, \mathcal{O}_{X^{\mathrm{proj}}})$. Let us discuss these questions. In homogeneous coordinates $x_1, \ldots, x_n$, X^{proj} is defined by the equation $F = 0$, with F homogeneous of degree denoted d. On the ambient $\mathbb{P} := \mathbb{P}^{n-1}$, with $i := X^{\mathrm{proj}} \to \mathbb{P}$ the inclusion, we have the short exact sequence

$$0 \longrightarrow \mathcal{O}_{\mathbb{P}}(-d) \xrightarrow{\times F} \mathcal{O}_{\mathbb{P}} \longrightarrow i_*\mathcal{O}_{X^{\mathrm{proj}}} \longrightarrow 0.$$

Since $H^i(\mathbb{P}^{n-1}, \mathcal{O})$ vanishes for all $i > 0$, we get (remember $n \geqq 3$)

$$H^{n-2}(X^{\mathrm{proj}}, \mathcal{O}_{X^{\mathrm{proj}}}) \cong H^{n-1}\big(\mathbb{P}, \mathcal{O}_{\mathbb{P}}(-d)\big).$$

Now $H^{n-1}\big(\mathbb{P}, \mathcal{O}_{\mathbb{P}}(-d)\big)$ has a simple description. It is the k-span of those Laurent monomials $x^w := \prod_i (x_i)^{w(i)}$ which satisfy the two conditions

$$\sum_i w(i) = -d, \quad \text{for all } i, w(i) < 0.$$

We view this space as the quotient space of the k-span of all Laurent polynomials of degree $-d$ by the subspace spanned by those Laurent monomials x^w of degree $-d$ which, for some i, have $w(i) \geqq 0$, cf. [Ha], p. 226, 2nd par. This description shows that

$$H^{n-2}(X^{\mathrm{proj}}, \mathcal{O}_{X^{\mathrm{proj}}}) \neq 0 \Leftrightarrow d \geqq n.$$

Using the above isomorphism, how do we describe the action of Frob_E on

$$H^{n-2}(X^{\mathrm{proj}}, \mathcal{O}_{X^{\mathrm{proj}}})?$$

Write $\# E$ as p^ν. The p'th power map ("absolute Frobenius") induces a p-linear endomorphism $\mathrm{Frob}_{\mathrm{abs}}$ of the k-space $H^{n-2}(X^{\mathrm{proj}}, \mathcal{O}_{X^{\mathrm{proj}}})$, the Hasse-Witt map, and its ν'th iterate is the k-linear endomorphism Frob_E. The action of $\mathrm{Frob}_{\mathrm{abs}}$ becomes the p-linear action on $H^{n-1}(\mathbb{P}, \mathcal{O}_{\mathbb{P}}(-d))$ induced by the p-linear action

$$G \mapsto F^{p-1} G^p$$

on the space of all Laurent forms G of degree $-d$.

A projective hypersurface X^{proj} of dimension $n-2 \geqq 1$ and degree d is called ordinary if $d \geqq n$ and if $\mathrm{Frob}_{\mathrm{abs}}$ (or equivalently Frob_E) is an automorphism of $H^{n-2}(X^{\mathrm{proj}}, \mathcal{O}_{X^{\mathrm{proj}}})$, and it is called non-special if $d \geqq n$ and if $\mathrm{Frob}_{\mathrm{abs}}$ (or equivalently Frob_E) is not nilpotent on $H^{n-2}(X^{\mathrm{proj}}, \mathcal{O}_{X^{\mathrm{proj}}})$. Thus X^{proj} is non-special if and only if for some (or equivalently for every) finite extension E/k, the polynomial

$$\det\bigl(1 - T\,\mathrm{Frob}_E | H^{n-2}(X^{\mathrm{proj}}, \mathcal{O}_{X^{\mathrm{proj}}})\bigr)$$

is not identically 1. In general (cf. [SGA 7], XXII, 1.0), there is a direct sum decomposition

$$H^{n-2}(X^{\mathrm{proj}}, \mathcal{O}_{X^{\mathrm{proj}}}) = H^{n-2}(X^{\mathrm{proj}}, \mathcal{O}_{X^{\mathrm{proj}}})_{\mathrm{ss}} \oplus H^{n-2}(X^{\mathrm{proj}}, \mathcal{O}_{X^{\mathrm{proj}}})_{\mathrm{nilp}}$$

into $\mathrm{Frob}_{\mathrm{abs}}$-stable summands, such that $\mathrm{Frob}_{\mathrm{abs}}$ is invertible on the first summand, and nilpotent on the second.

The dimension of the first summand is called the "stable rank" of X^{proj}. Thus the stable rank is equal to the degree of the polynomial $\det\bigl(1 - T\,\mathrm{Frob}_E | H^{n-2}(X^{\mathrm{proj}}, \mathcal{O}_{X^{\mathrm{proj}}})\bigr)$.

Thus a restatement of the previous inequality is

Theorem 7.6. *We have the inequality*

$$B(X) \geqq \textit{stable rank of } X^{\mathrm{proj}}.$$

In particular, $B(X)$ is non-zero if X^{proj} is non-special.

Unfortunately, given a homogeneous form F of degree $d \geqq n$, there is no fast algorithm to compute the stable rank of X^{proj}, or even to tell if the stable rank is non-zero. One has only

Lemma 7.7. *Suppose $d \geqq n \geqq 3$.*

1) *If for some finite extension E/k, we have*

$$\#X^{\mathrm{proj}}(E) \not\equiv 1 \bmod p,$$

then X^{proj} is non-special.

2) *If $d \geqq n$ and $\dim H^{n-2}(X^{\mathrm{proj}}, \mathcal{O}_{X^{\mathrm{proj}}}) < p$ then X^{proj} is non-special if and only if there exists a finite extension E/k for which*

$$\#X^{\mathrm{proj}}(E) \not\equiv 1 \pmod{p}.$$

3) *Suppose $d = n$. Then the following equations are equivalent*:

3a) *X^{proj} is non-special.*

3b) $\#X^{\mathrm{proj}}(k) \not\equiv 1 \pmod{p}$.

3c) *The coefficient of $(x_1x_2\dots x_n)^{p-1}$ in $F(x_1,\dots,x_n)^{p-1}$ is non-zero.*

Proof. 1) Indeed the congruence formula gives

$$\#X^{\mathrm{proj}}(E) - 1 \equiv (-1)^{n-2}\operatorname{Trace}\bigl(\mathrm{Frob}_E | H^{n-2}(X^{\mathrm{proj}}, \mathcal{O}_{X^{\mathrm{proj}}})\bigr).$$

If the trace is non-zero, Frob_E cannot be nilpotent.

2) Suppose $\mathrm{Frob}_{\mathrm{abs}}$ is not nilpotent on $H^{n-2}(X^{\mathrm{proj}}, \mathcal{O}_{X^{\mathrm{proj}}})$. Then the linear operator Frob_k is not nilpotent so in $\bar{k}$ its eigenvalues $\lambda_1,\dots,\lambda_{\dim}$ are not all zero. Since every non-zero element of $\bar{k}^\times$ is a root of unity, for some finite extension E/k the eigenvalues of $\mathrm{Frob}_E := (\mathrm{Frob}_k)^{\deg(E/k)}$ are all 0 or 1, and the number of eigenvalues 1 is the stable rank, say s. Thus we get a congruence

$$\#X^{\mathrm{proj}}(E) - 1 \equiv (-1)^{n-2} \times s \bmod p.$$

Since $s \leqq \dim H^{n-2}(X^{\mathrm{proj}}, \mathcal{O}_{X^{\mathrm{proj}}}) < p$, and $s \neq 0$ by hypothesis, we get

$$\#X^{\mathrm{proj}}(E) \not\equiv 1 \bmod p.$$

3) If $d = n$, then $H^{n-2}(X^{\mathrm{proj}}, \mathcal{O}_{X^{\mathrm{proj}}})$ is one dimensional, with basis $(x_1x_2\dots x_n)^{-1}$. The coefficient, say HW, of $(x_1x_2\dots x_n)^{p-1}$ in F^{p-1} is the matrix of the p-linear map $\mathrm{Frob}_{\mathrm{abs}}$ in this basis, the Hasse invariant, cf. [Ka-ASDE], 2.3.7.17. The matrix of the linear map Frob_k is $\mathrm{Norm}_{k/\mathbb{F}_p}(\mathrm{HW})$. By the congruence formula, we have

$$\#X^{\mathrm{proj}}(E) - 1 \equiv (-1)^{n-2}\,\mathrm{Norm}_{k/\mathbb{F}_p}(\mathrm{HW}). \quad \text{QED}$$

Examples. We will give some examples of forms F of degree n in n variables whose Hasse invariant

$$\mathrm{HW} := \text{the coefficient of } (x_1x_2\dots x_n)^{p-1} \quad \text{in } F^{p-1}$$

is non-zero.

1) $F = x_1x_2\dots x_n$. Here HW$= 1$.

2) Take any finite separable k-algebra $\mathbb{E}/k$ of degree n and any k-basis $e_1,\dots,e_n$. Take F the norm form

$$F(x_1,\dots,x_n) = \mathrm{Norm}_{\mathbb{E}/k}\Big(\sum_i e_ix_i\Big).$$

Indeed over a finite extension E/k, $\mathbb{E}\otimes_k E$ becomes $E\times E\times\cdots\times E$ and so after a linear change of variable over E, F becomes $x_1x_2\dots x_n$.

3) For F the Fermat form $\sum_i (x_i)^n$, HW is nonzero if and only if $p\equiv 1 \bmod n$, in which case, writing $p-1 = an$, HW is $(an)!/(a!)^n$.

8. Nonvanishing of A-numbers by congruence considerations

We now return to the setting of section 4. Thus V is a closed subscheme of $\mathbb{A}^n_{\mathbb{Z}}$, and there exists an integer $D \geqq 1$ such that $V[1/D]/\mathbb{Z}[1/D]$ is smooth and surjective of relative dimension d, with geometrically connected fibres. We take for K the object $\bar{\mathbb{Q}}_\ell[d]$ on $V[1/\ell]$. It is adapted to $\mathscr{V}$ ($\mathscr{V} :=$ the stratification of V consisting of V alone), it is fibrewise semiperverse, and is fibrewise mixed of weight $\leqq d$. On $V[1/\ell D]$, $\bar{\mathbb{Q}}_\ell[d]$ is fibrewise perverse, geometrically irreducible, and pure of weight d. We also take an *arbitrary* function f on V.

With this data, Theorem 3.1 produces an integer $N\geqq 1$, a stratification $\mathscr{H}$ of $H[1/N]$ and a map

$$(V,f)_!\colon \{\text{functions } f\colon V\to\mathbb{Z}, \text{constant on } \mathscr{V}\}$$
$$\to \{\text{functions } f\colon H[1/N]\to\mathbb{Z},\ \text{constant on } \mathscr{H}\}.$$

For each pair (k,ψ) consisting of a finite field k of characteristic not dividing $D\ell$, and a $\bar{\mathbb{Q}}_\ell^\times$-valued nontrivial additive character ψ of k, we have the A-number $A(V,f,k.\psi)$. We have seen (Lemma 4.1) that this A-number is constant as k varies over finite fields of characteristic prime to $DN\ell$.

Theorem 8.1. *Suppose that for an infinite set P of primes p, there exists a finite field E of characteristic p such that $\#V(E)$ is prime to p. Then the A-number $A(V,f,k,\psi)$ is nonzero for all finite field k of characteristic prime to $DN\ell$.*

Proof. Denote by $H_{\max}$ the unique strat of $\mathscr{H}$ which is of relative dimension n over

$\mathbb{Z}[1/N]$. We know that $H_{\max}[1/N]$ is smooth over $\mathbb{Z}[1/N]$ with geometrically irreducible factors. So by Lang-Weil, for all sufficiently large primes p, $H_{\max}(\mathbb{F}_p)$ is non-empty.

We know by Lemma 4.1, that as (k,ψ) varies with char(k) prime to $DN\ell$, the A-number $A(V,f,k,\psi)$ is constant. Take a prime in our infinite set P which is prime to $DN\ell$ and sufficiently large that $H_{\max}(\mathbb{F}_p)$ is non-empty. Pick a point h in $H_{\max}(\mathbb{F}_p)$ and a non-trivial additive character ψ on $\mathbb{F}_p$. On $H_{\max}\otimes\mathbb{F}_p$, $\mathrm{FT}_\psi\big(i_!(\mathscr{L}_{\psi(f)}[d])\big)$ is $\mathscr{F}[n]$ for a lisse sheaf, whose rank is the A-number $A(V,f,\mathbb{F}_p,\psi)$. We must show that $\mathscr{F}$ is non-zero. For this it suffices to show that, for $E/\mathbb{F}_p$ the finite field for which $\#V(E)$ is prime to p, we have $\mathrm{Trace}(\mathrm{Frob}_{E,h}|\mathscr{F}) \neq 0$. But $\mathscr{F}[n]$ is equal to $\mathrm{FT}_\psi\big(i_!(\mathscr{L}_{\psi(f)}[d])\big)$ on all of $H_{\max}$, so at h we have

$$\mathrm{Trace}(\mathrm{Frob}_{E,h}|\mathscr{F}) = (-1)^d \sum_{v\in V(E)} \psi_E\Big(f(v)+\sum_i h_i x_i(v)\Big).$$

The sum on the right hand side is $(-1)^d$ times a sum of p'th roots of unity in $\bar{\mathbb{Q}}_\ell$. So it lies in $\mathbb{Z}[\zeta_p]$ after any embedding of $\bar{\mathbb{Q}}_\ell$ into $\mathbb{C}$. Fix one such embedding. Modulo the unique maximal ideal $\mathfrak{p}$ in $\mathbb{Z}[\zeta_p]$ lying over p, namely $\mathfrak{p}=(\zeta_p-1)$, each p'th root of unity is 1 $\bmod \mathfrak{p}$. Thus we obtain a congruence

$$\sum_{v\in V(E)} \psi_E\Big(f(v)+\sum_i h_i x_i(v)\Big) \equiv \#V(E) \bmod \mathfrak{p}.$$

But E was chosen so that $\#V(E)$ is prime to p, so nonzero $\bmod \mathfrak{p}$. Therefore $\sum_{v\in V(E)} \psi_E\Big(f(v)+\sum_i h_i x_i(v)\Big)$ must itself be non-zero, since it is non-zero $\bmod \mathfrak{p}$. Thus $\mathrm{Trace}(\mathrm{Frob}_{E,h}|\mathscr{F})$ is non-zero, whence $\mathscr{F}$ is non-zero. QED

Examples. We give now examples of V's in $\mathbb{A}^n/\mathbb{Z}$ to which this theorem applies. The most striking is perhaps the $n-1$ torus, of equation

$$x_1x_2\dots x_n = 1.$$

Or a translated $n-1$-torus

$$Ax_1x_2\dots x_n = B,$$

with A and B non-zero integers which are relatively prime, or more generally

$$Ax_1^{a_1}\dots x_n^{a_n} = B,$$

with any integers $a_i \geqq 1$, such that $\gcd(a_1,\dots,a_n)=1$. For then some a_i is odd; for any p such that $p-1$ is relatively prime to this a_i (e.g. $p\equiv 2 \bmod a_i$), $X\mapsto X^{a_i}$ is a bijection on $\mathbb{F}_p^\times$ so we can solve for x_i, and $\#V(\mathbb{F}_p)$ is $(p-1)^{n-1}$.

Or we could take a number field $K/\mathbb{Q}$ of degree n, an order $\mathcal{O}$ in K, a $\mathbb{Z}$-basis $e_1,\dots,e_n$ of $\mathcal{O}$ and the norm equation

$$\mathrm{Norm}_{\mathcal{O}/\mathbb{Z}}\Big(\sum_i e_i x_i\Big) = 1,$$

or more generally a translated norm equation

$$A \times \mathrm{Norm}_{\mathcal{O}/\mathbb{Z}}\Big(\sum_i e_i x_i\Big) = B,$$

for A and B non-zero integers which are relatively prime.

Here is a less obvious example. Fix $n \geqq 3$ odd and $d \geqq 1$ odd. In $\mathbb{A}^n_{\mathbb{Z}}$, consider the closed subscheme defined by the two equations

$$\begin{cases} \prod_{1 \leqq i \leqq n} x_i = 1, \\ \sum_{1 \leqq i \leqq n} a_i x_i^d = 0 \end{cases}$$

with g.c.d.$(a_1, \ldots, a_n) = 1$. We claim that all geometric fibres of $V/\mathbb{Z}$ have dimension $\leqq n-2$. Indeed in the $n-1$-torus $(\mathbb{G}_{m,\mathbb{Z}})^{n-1}$ over $\mathbb{Z}$ with coordinates $x_1, \ldots, x_{n-1}$, which is smooth over $\mathbb{Z}$, everywhere of relative dimension $n-1$, V is defined by one equation

$$\sum_{1 \leqq i \leqq n-1} a_i x_i^d + a_n/(x_1 x_2 \ldots x_{n-1})^d = 0$$

or equivalently by one equation

$$\Big(\prod_{1 \leqq i \leqq n-1} x_i\Big)^d \times \Big(\sum_{1 \leqq i \leqq n-1} a_i x_i^d\Big) = -a_n.$$

Because g.c.d.$(a_1, \ldots, a_n) = 1$, this equation is non-zero modulo every prime p. So V is flat over $\mathbb{Z}$, and everywhere of relative dimension $\leqq n-2$.

We next claim that if we put $D := n \times d \times \prod_{1 \leqq i \leqq n} a_i$, then $V[1/D]$ is smooth over $\mathbb{Z}[1/D]$, with geometrically connected fibres. We first show that these fibres are all geometrically irreducible. Over any algebraically closed field k in which D is invertible, $V \otimes k$ is the closed subscheme of the $n-1$-torus $(\mathbb{G}_{m,k})^{n-1}$ defined by one equation

$$F = -a_n,$$

for

$$F := \Big(\prod_{1 \leqq i \leqq n-1} x_i\Big)^d \times \Big(\sum_{1 \leqq i \leqq n-1} a_i x_i^d\Big).$$

We must show that $F + a_n$ is irreducible in the ring of Laurent polynomials

$$k[x_1, \ldots, x_{n-1}]/[1/x_1 x_2 \ldots x_{n-1}].$$

For this, it suffices to show that $F + a_n$ is irreducible in the polynomial ring $k[x_1, \ldots, x_{n-1}]$. But F is *homogeneous* of degree nd, and a_n is non-zero. So $F + a_n$ is irreducible unless F is an r'th power in $k[x_1,\ldots,x_{n-1}]$ for some $r \geqq 2$. We claim F is not such a power. This is obvious from the given factorization of F. For $n > 3$ the form $\sum_{1 \leqq i \leqq n-1} a_i x_i^d$ is itself irreducible and F is divisible just once by it. If $n = 3$, then F is $(xy)^d(ax^d + by^d)$ with ab non-zero. Since abd is non-zero in $k = \bar{k}$, $ax^d + by^d$ is the product of d distinct linear forms involving both variables, and each of these linear forms is an irreducible which occurs in F to the first power.

To see that $V \otimes k$ is smooth over any algebraically closed field k in which $D := d \times \prod_{1 \leqq i \leqq n} a_i$ is invertible, go back to viewing V as defined in $\mathbb{A}_k^n$ by the two equations

$$\begin{cases} \prod_{1 \leqq i \leqq n} x_i = 1, \\ \sum_{1 \leqq i \leqq n} a_i x_i^d = 0. \end{cases}$$

A singular point in $V \otimes k$ with values in k is a point x in $\mathbb{A}^n(k)$ where the gradients of the two functions

$$f\colon \prod_{1 \leqq i \leqq n} x_i \quad \text{and} \quad g\colon \sum_{1 \leqq i \leqq n} a_i x_i^d$$

are proportional, and where $f = 1$ and $g = 0$. The gradient of f is the vector $(\ldots, f/x_i, \ldots)$, that of g is the vector $(\ldots, a_i x_i^d/x_i, \ldots)$. The two are proportional at points where for all $1 \leqq i < j \leqq n$ the determinant of the 2×2 matrix

$$\begin{pmatrix} f/x_i & f/x_j \\ a_i x_i^d/x_i & a_j x_j^d/x_j \end{pmatrix}$$

vanishes. At any point of $V \otimes k$, all the x_i are invertible, and $f = 1$, so $\mathrm{Sing}(V \otimes k)$ is the intersection of $V \otimes k$ with the locus

$$a_i x_i^d = a_j x_j^d, \quad \text{for all } 1 \leqq i < j \leqq n.$$

But as $\sum_{1 \leqq i \leqq n} a_i x_i^d = 0$ on V, and n is invertible in k, we infer that at any singular point of $V \otimes k$, we have $a_i x_i^d = 0$ for all i. As all a_i are non-zero in k, we find $x_i = 0$ in k. But the point $(0,\ldots,0)$ does not lie on V.

We next exhibit an infinite set of primes P such that for p in P, $\#V(\mathbb{F}_p)$ is prime to p. We take

$$P := \{p; p \nmid D, p \equiv 2 \bmod nd\}.$$

(Remember that both n and d are odd, so P is indeed infinite.) For p in P, $p - 1$ is relatively prime to d and it is relatively prime to n. Therefore on $\mathbb{F}_p$, the map $X \mapsto X^p$ is bijective, and on $\mathbb{F}_p^\times$ the map $X \mapsto X^n$ is bijective.

To see that $\#V(\mathbb{F}_p)$ is prime to p for p in P, we argue as follows. Regard n and the coefficients $a_1, \dots, a_n$ as fixed, and denote by V_d the subscheme of $\mathbb{A}^n_{\mathbb{Z}}$ we have been calling V. In this notation, V_1 is then the closed subscheme of $\mathbb{A}^n_{\mathbb{Z}}$ defined by the two equations

$$\begin{cases} \prod\limits_{1 \leqq i \leqq n} x_i = 1, \\ \sum\limits_{1 \leqq i \leqq n} a_i x_i = 0. \end{cases}$$

The endomorphism

$$[d]\colon (x_1, \dots, x_n) \mapsto \big((x_1)^d, \dots, (x_n)^d\big)$$

of $\mathbb{A}^n_{\mathbb{Z}}$ maps V_d to V_1. We claim that for p in P, this map induces a bijection from $V_d(\mathbb{F}_p)$ to $V_1(\mathbb{F}_p)$. Indeed, this map induces a bijection of $\mathbb{A}^n(\mathbb{F}_p)$ with itself, so it certainly induces an injective map from $V_d(\mathbb{F}_p)$ to $V_1(\mathbb{F}_p)$. To see that this map from $V_d(\mathbb{F}_p)$ to $V_1(\mathbb{F}_p)$ is surjective, we argue as follows. Given a point $(y_1, \dots, y_n)$ in $V_1(\mathbb{F}_p)$, consider the unique point $(x_1, \dots, x_n)$ in $\mathbb{A}^n(\mathbb{F}_p)$ with $x_i^d = y_i$ for every i. Because $(y_1, \dots, y_n)$ is in $V_1(\mathbb{F}_p)$, the point $(x_1, \dots, x_n)$ satisfies

$$\begin{cases} \Big(\prod\limits_{1 \leqq i \leqq n} x_i\Big)^d = 1, \\ \sum\limits_{1 \leqq i \leqq n} a_i x_i^d = 0. \end{cases}$$

But $\mu_d(\mathbb{F}_p) = \{1\}$, so from the first equation we infer that

$$\prod_{1 \leqq i \leqq n} x_i = 1,$$

and hence the point $(x_1, \dots, x_n)$ lies in $V_d(\mathbb{F}_p)$.

So now, we are reduced to showing that for p in P, $\# V_1(\mathbb{F}_p)$ is prime to p. To see this, we consider, for each β in $\mathbb{F}_p$, the closed subscheme $V_{1,\beta}$ of $\mathbb{A}^n_{\mathbb{F}_p}$ defined by the two equations

$$\begin{cases} \prod\limits_{1 \leqq i \leqq n} x_i = \beta, \\ \sum\limits_{1 \leqq i \leqq n} a_i x_i = 0. \end{cases}$$

So V_1 is $V_{1,1}$ in this notation. We view all the $V_{1,\beta}$'s as subschemes of the hyperplane $H \subset \mathbb{A}^n_{\mathbb{F}_p}$ of equation $\sum\limits_{1 \leqq i \leqq n} a_i x_i = 0$. In this hyperplane, they are exactly the fibres over the $\mathbb{F}_p$ valued points in $\mathbb{A}^1$ of the map $H \to \mathbb{A}^1$ defined by the function $\prod\limits_{1 \leqq i \leqq n} x_i$. So the $V_{1,\beta}(\mathbb{F}_p)$ form a partition of $H(\mathbb{F}_p)$ and thus we have

$$\sum_{\beta \in \mathbb{F}_p} \# V_{1,\beta}(\mathbb{F}_p) = \# H(\mathbb{F}_p) = p^{n-1}.$$

We next claim that for any non-zero β, we have

$$\#V_{1,\beta}(\mathbb{F}_p) = \#V_{1,1}(\mathbb{F}_p).$$

To see this, use the fact that $X \mapsto X^n$ is bijective on $\mathbb{F}_p^\times$ to write our non-zero β as α^n for some α in $\mathbb{F}_p^\times$. Then the homothety α on the ambient space H induces an isomorphism $V_{1,1} \cong V_{1,\beta}$. So we can rewrite the above sum formula as

$$\#V_{1,0}(\mathbb{F}_p) + (p-1)\,\#V_{1,1}(\mathbb{F}_p) = p^{n-1}.$$

Thus we find a congruence

$$\#V_{1,0}(\mathbb{F}_p) \equiv \#V_{1,1}(\mathbb{F}_p) \bmod p.$$

Recalling that $V_{1,1}$ is V_1, we see that we are reduced to proving that $\#V_{1,0}(\mathbb{F}_p)$ is prime to p. We will show this is true for any prime $p \geqq n$ modulo of which all the a_i are non-zero.

Now $V_{1,0}$ is defined over $\mathbb{F}_p$ by the two equations

$$\begin{cases} \prod\limits_{1\leqq i\leqq n} x_i = 0, \\ \sum\limits_{1\leqq i\leqq n} a_i x_i = 0. \end{cases}$$

Making the change of variables $y_i := a_i x_i$, $V_{1,0}$ becomes the zero locus of the two equations

$$\begin{cases} \prod\limits_{1\leqq i\leqq n} x_i = 0, \\ \sum\limits_{1\leqq i\leqq n} x_i = 0. \end{cases}$$

In the hyperplane H of equation $\sum\limits_{1\leqq i\leqq n} x_i = 0$, with coordinates $x_1, \dots, x_{n-1}$, $V_{1,0}$ becomes the hypersurface in $\mathbb{A}^{n-1}$ over $\mathbb{F}_p$ of equation

$$F := \Bigl(\sum_{1\leqq i\leqq n-1} x_i\Bigr)\Bigl(\prod_{1\leqq i\leqq n-1} x_i\Bigr) = 0.$$

We first give a cohomological proof that $\#V_{1,0}(\mathbb{F}_p)$ is prime to p. Let us denote by $X \subset \mathbb{P}^{n-2}$ the projective hypersurface over $\mathbb{F}_p$ of the same equation $F = 0$. We have

$$\#V_{1,0}(\mathbb{F}_p) = 1 + (p-1)\,\#X(\mathbb{F}_p) \equiv 1 - \#X(\mathbb{F}_p) \bmod p.$$

By the congruence formula [SGA 7], XXII, 3.1.1 for the hypersurface X, we have

$$\#X(\mathbb{F}_p) \equiv 1 + (-1)^{n-3}\,\mathrm{Trace}\bigl(\mathrm{Frob}_{\mathbb{F}_p} | H^{n-3}(X, \mathcal{O}_X)\bigr).$$

So we have

$$\#V_{1,0}(\mathbb{F}_p) \equiv (-1)^n\,\mathrm{Trace}\bigl(\mathrm{Frob}_{\mathbb{F}_p} | H^{n-3}(X, \mathcal{O}_X)\bigr) \bmod p.$$

As we have seen in section 7, in the discussion of the Hasse-Witt invariant, for X a hypersurface of degree n, $H^{n-3}(X, \mathcal{O}_X)$ is the span of the monomials x^{-w} in $n-1$ variables x_i, $1 \leqq i \leqq n-1$, with all $w_i \geqq 1$ and $\sum_i w_i = n$. There are precisely $n-1$ such monomials, namely

$$e(j) := 1/x_j \Big(\prod_{1 \leqq i \leqq n-1} x_i \Big), \quad \text{for } 1 \leqq j \leqq n-1.$$

In this basis, the Hasse-Witt matrix, i.e. the matrix of $\mathrm{Frob}_{\mathbb{F}_p}$ on $H^{n-3}(X, \mathcal{O}_X)$ is given as follows:

$$\mathrm{Frob}_{\mathbb{F}_p}\big(e(a)\big) = \sum_{i,j} \mathrm{HW}_{i,j} e(b),$$

$$\begin{aligned}
\mathrm{HW}_{a,b} &:= \text{the coefficient of } e(b) \text{ in } F^{p-1} e(a)^p \\
&= \text{the coef. of } 1/x_b \Big(\prod_{1 \leqq i \leqq n-1} x_i \Big) \\
&\quad \text{in } \Big[\Big(\sum_{1 \leqq i \leqq n-1} x_i \Big) \Big(\prod_{1 \leqq i \leqq n-1} x_i \Big) \Big]^{p-1} \Big/ x_a^p \Big(\prod_{1 \leqq i \leqq n-1} x_i \Big)^p \\
&= \text{the coef. of } 1/x_b \text{ in } \Big(\sum_{1 \leqq i \leqq n-1} x_i \Big)^{p-1} / x_a^p \\
&= \text{the coef. of } x_a^p / x_b \text{ in } \Big(\sum_{1 \leqq i \leqq n-1} x_i \Big)^{p-1} \\
&= \delta_{a,b}.
\end{aligned}$$

Thus $\mathrm{Frob}_{\mathbb{F}_p}$ on $H^{n-3}(X, \mathcal{O}_X)$ is the identity on this $n-1$ dimensional space. So

$$\mathrm{Trace}\big(\mathrm{Frob}_{\mathbb{F}_p} | H^{n-3}(X, \mathcal{O}_X)\big) = n-1.$$

Thus we get

$$\# V_{1,0}(\mathbb{F}_p) \equiv (-1)^n (n-1) \bmod p.$$

Since $p \geqq n$, $\# V_{1,0}(\mathbb{F}_p)$ is prime to p as required.

There is an elementary way to prove this same congruence. As above, $V_{1,0}$ is the affine hypersurface $F = 0$ in $\mathbb{A}^{n-1}$, and F is the product of n linear forms, any $n-1$ of which are linearly independent. Thus $V_{1,0}(\mathbb{F}_p)$ is the union of n hyperplanes $H_i(\mathbb{F}_p)$, $i = 1, \ldots, n$, any $n-1$ of which are in general position. So by inclusion-exclusion

$$\begin{aligned}
\# V_{1,0}(\mathbb{F}_p) = \# \Big(\bigcup_i H_i(\mathbb{F}_p) \Big) &= \sum_i \# H_i(\mathbb{F}_p) - \sum_{i<j} \# \big(H_i(\mathbb{F}_p) \cap H_j(\mathbb{F}_p) \big) + \cdots \\
&= n p^{n-2} - \binom{n}{2} p^{n-3} + \binom{n}{3} p^{n-4} + \cdots + (-1)^n \binom{n}{n-1} 1 + (-1)^{n+1} \binom{n}{n} 1 \\
&\equiv (-1)^n (n-1) \bmod p. \quad \text{QED}
\end{aligned}$$

9. Proof of Corollary 1.3

This proof follows the proof of [Fo1], so we will only sketch the proof, referring to [Fo1] or to [Be-Fo] for details. For Δ a fundamental positive discriminant, we denote by $\mathscr{H}(\Delta)$ the quantity

$$\mathscr{H}(\Delta) = \frac{3^{r_3(\Delta)} - 1}{2}$$

where $r_3(\Delta)$ is the 3-rank of the ideal class group of the ring of integers of $\mathbb{Q}(\sqrt{\Delta})$. Note the inequality $\mathscr{H}(\Delta) \geqq 0$ and the equivalence

$$\mathscr{H}(\Delta) = 0 \Leftrightarrow 3 \nmid h(\Delta).$$

We owe to Davenport and Heilbronn [Da-He1], 2, a complete interpretation of $\mathscr{H}(\Delta)$ in terms of classes of binary cubic forms, under the action of $\mathrm{Gl}(2, \mathbb{Z})$. From their work, we will first recall the

Lemma 9.1. *Let $\Delta_3(a,b,c,d)$ be defined by* (6.1). *Then for any positive fundamental Δ, we have*

$$\mathscr{H}(\Delta) = \frac{1}{2}\,\#\{(a,b,c,d) \in \tilde{\mathscr{V}}; aX^3 + bX^2Y + cXY^2 + dY^3 \textit{ irreducible } \Delta_3(a,b,c,d) = \Delta\},$$

where $\tilde{\mathscr{V}}$ is the subset of $\mathbb{R}^4$ defined as the set of quadruples (a,b,c,d) satisfying

$$a \geqq 1 \textit{ and } \begin{cases} \textit{either} & -A < B \leqq A < C, \\ \textit{or} & 0 \leqq B \leqq A = C, \end{cases}$$

with A, B and C defined by

$$A = b^2 - 3ac, \quad B = bc - 9ad, \quad C = c^2 - 3bd.$$

This is Proposition 3.1 of [Fo1]. We extend the definition of $\mathscr{H}$ by setting $\mathscr{H}(n) = 0$ if $n \geqq 1$ is not a fundamental discriminant. Now we enlarge the set $\tilde{\mathscr{V}}$ to the set $\mathscr{V}$, where

$$\mathscr{V} = \{(a,b,c,d); a \geqq 1, |B| \leqq A \leqq C\}.$$

Let $g(n)$ be the function

$$g(n) = \#\{(a,b,c,d) \in \mathscr{V}; \Delta_3(a,b,c,d) = n\}, \quad \text{for } n \geqq 1$$

(note the inequality $\mathscr{H}(n) \leqq \frac{1}{2}g(n)$). We introduce an auxiliary integer $P \geqq 3$, which later will be taken arbitrarily large and will be used to ensure that $p + 4$ is squarefree. We define the function $g_P(n)$ by

- $g_P(n) = 0$ if n is not congruent to 1, 5, 8, 9, 12 or 13 modulo 16, or if n is divisible by the square of an odd prime number less than P,

- $g_P(n) = g(n)$ otherwise.

Note that the above congruence classes modulo 16 correspond to the congruence classes to which a fundamental discriminant belongs and that the following inequality holds for every n and every $P \geqq 3$:

$$\mathscr{H}(n) \leqq \frac{1}{2} g_P(n). \tag{9.1}$$

As usual the Möbius function is denoted by μ.

Proposition 9.2. *For every positive ε and for every $P \geqq 3$, we have the estimate*

$$\sum_{q \leqq X^{\frac{2}{5}-\varepsilon}} \mu^2(q) \left| \sum_{\substack{n \leqq X \\ q \mid n}} g_P(n+4) - \frac{\nu_P(q)}{q} \sum_{n \leqq X} g(n) \right| = O_{\varepsilon,P}(X \log^{-2} X)$$

with

$$\nu_P(q) = \prod_{p \mid q} \frac{\rho(p,4)}{p^3} \prod_{\substack{p \leqq P \\ p \nmid q/(2,q)}} \left(1 - \xi(p) \frac{(2,q,p)^4}{\rho\big((2,q,p),4\big)}\right),$$

with ξ and ρ the multiplicative functions defined by

- $\xi(p) = \dfrac{2}{p^2} - \dfrac{1}{p^4}$ *for* $p \geqq 2$
- $\rho(2,4) = 10$ *and* $\rho(p,4) = p^3 - p$ *for* $p \geqq 3$.

This is the statement of Proposition 4.1 of [Fo1] but with the exponent $\frac{1}{3} - \varepsilon$ replaced by $\frac{2}{5} - \varepsilon$. This improvement of the exponent is the key point of the proof. Note that any exponent $> \frac{1}{3}$ would be sufficient to prove Corollary 1.3.

9.a. First reduction of the proof of Proposition 9.2. The first reductions follow exactly what was done in [Fo1], 4.a and b. Recall only that we treat on average the contribution of the cusp of $\mathscr{V}$, and we divide the remaining volume into a certain number of hypercubes $\mathscr{B}_i$, with $i \in \mathscr{I}$. Each side of these four dimensional hypercubes has length

$$Q = X^{\frac{1}{4}-5\eta},$$

with η a small positive constant, which will be chosen to be

$$\eta = \frac{\varepsilon}{100}.$$

The contribution of points of $\mathscr{V}$ which are not in $\bigcup_{i \in \mathscr{I}} \mathscr{B}_i$ is also negligible, by taking advantage of the summation over q. In other words, to prove Proposition 9.2, it is sufficient to prove a result of equidistribution not in $\mathscr{V}$ but in each $\mathscr{B}_i$, of the form

$$(9.2)\qquad \sum_{\substack{M\in\mathscr{B}_i,\,\Delta_3(M)\equiv 0\ (\mathrm{mod}\,r^2)\\ \Delta_3(M)-4\equiv 0\ (\mathrm{mod}\,q)}} 1 = \prod_{p|q}\frac{\rho(p,4)}{p^4}\prod_{p|r}\xi(p)\sum_{M\in\mathscr{B}_i}1 + O_{\varepsilon,r}(q^{-1}Q^4\log^{-3}X)$$

for all squarefree $q \leqq X^{\frac{2}{5}-\varepsilon}$, all positive ε, and all squarefree r coprime with q. This is exactly [Fo1], (4.6) (however in that formula, "$\Delta_3(M)+4$" should have been "$\Delta_3(M)-4$").

We suppose now that $\mathscr{B}_i = \mathscr{B} = [b_1; b_1+Q]\times\cdots\times[b_4; b_4+Q]$ and we suppose also that

$$(9.3)\qquad Q \leqq qr^2.$$

The case $qr^2 < Q$ is easier and will be treated at §9.e.

We develop in Fourier series the characteristic function of each interval $[b_i; b_i+Q]$ in terms of additive characters modulo qr^2, which means that the sum

$$\frac{1}{qr^2}\sum_{h\,\mathrm{mod}\,qr^2}\ \sum_{b\leqq x\leqq b+Q}\exp\left(2\pi i\frac{h(n-x)}{qr^2}\right)$$

is 1 or 0 according to whether $n(\mathrm{mod}\,qr^2)$ belongs to $\{x(\mathrm{mod}\,qr^2); b\leqq x\leqq b+Q\}$ or not.

The left hand side of (9.2) becomes

$$(9.4)\qquad \frac{1}{q^4r^8}\sum_{\boldsymbol{h}\,\mathrm{mod}\,qr^2}\ \sum_{\boldsymbol{x}\in\mathscr{B}}\exp\left(-2\pi i\,\frac{h_1x_1+h_2x_2+h_3x_3+h_4x_4}{qr^2}\right)S(\boldsymbol{h};q,r^2),$$

with $\boldsymbol{h}=(h_1,h_2,h_3,h_4)$, $\boldsymbol{x}=(x_1,x_2,x_3,x_4)$ and

$$S(\boldsymbol{h};q,r^2) = \sum_{(a,b,c,d)}\exp\left(2\pi i\,\frac{ah_1+bh_2+ch_3+dh_4}{qr^2}\right)$$

where the sum is taken over the (a,b,c,d) modulo qr^2 such that

$$\Delta_3(a,b,c,d)-4\equiv 0\ (\mathrm{mod}\,q)\quad\text{and}\quad \Delta_3(a,b,c,d)\equiv 0\ (\mathrm{mod}\,r^2).$$

This trigonometric sum satisfies a cross multiplicativity property

$$(9.5)\qquad S(\boldsymbol{h};q_1q_2,r^2) = S(\overline{q_1r^2}\,\boldsymbol{h};q_2,1)S(\overline{q_2r^2}\,\boldsymbol{h};q_1,1)S(\overline{q_1q_2}\,\boldsymbol{h};1,r^2),$$

for $(q_1,q_2)=(q_1,r)=(q_2,r)=1$. The notation $\bar{n}$ means that we take the multiplicative inverse of n modulo q_2, q_1 and r^2 respectively.

Here appears the crucial rôle of the sum

$$S(\boldsymbol{h},\psi,p) = \sum_{\substack{(a,b,c,d)\in\mathbb{F}_p^4\\ \Delta_3(a,b,c,d)-4\equiv 0\ (\mathrm{mod}\,p)}}\psi(ah_1+bh_2+ch_3+dh_4)$$

(with ψ a non trivial additive character of $\mathbb{F}_p$) to which we may apply Theorem 1.2. The fact the A-number is non-zero is proved in Theorem 6.1. The smoothness and geometric irreducibility were noted in section 6.

Lemma 9.3. *There exists an absolute C and closed subschemes X_j $(j = 1, 2, 3)$, $X_1 \supset X_2 \supset X_3 = \{0\}$, in $\mathbb{A}^4_{\mathbb{Z}}$ of dimension $\leqq 3 - j$, such that, for every p, for every nontrivial additive character ψ on $\mathbb{F}_p$, we have*

$$|S(\boldsymbol{h}, \psi, p)| \leqq Cp^{\frac{3}{2}} \tag{9.6}$$

for $\boldsymbol{h} \notin X_1(\mathbb{F}_p)$,

$$|S(\boldsymbol{h}, \psi, p)| \leqq Cp^2 \tag{9.7}$$

for $\boldsymbol{h} \notin X_2(\mathbb{F}_p)$,

$$|S(\boldsymbol{h}, \psi, p)| \leqq Cp^{\frac{5}{2}}, \tag{9.8}$$

for $\boldsymbol{h} \notin X_3(\mathbb{F}_p)$.

The equality $X_3 = \{0\}$ is a consequence of homogeneity and also a consequence of [Fo1], Lemme 2.4.i. This lemma improves [Fo1], Lemme 2.4, by decreasing by 1 the dimensions of the exceptional sets X_j. The contribution to (9.4) of the term $\boldsymbol{h} = \boldsymbol{0}$ is exactly the main term appearing in (9.2). So to prove (9.2) for $q \geqq Qr^{-2}$, it remains to prove that

$$\frac{1}{q^4 r^8} \sum_{\boldsymbol{h} \neq \boldsymbol{0} \bmod qr^2} \sum_{\boldsymbol{x} \in \mathscr{B}} \exp\left(-2\pi i \frac{h_1 x_1 + h_2 x_2 + h_3 x_3 + h_4 x_4}{qr^2}\right) S(\boldsymbol{h}; q, r^2) = O_{\varepsilon,r}(q^{-1} Q^4 \log^{-3} X), \tag{9.9}$$

under the condition q squarefree $\leqq X^{\frac{2}{5}-\varepsilon}$.

We will now follow the proof of [Fo1], Prop. 2.5. We recall the classical upper bound for geometric progressions

$$\sum_{b \leqq x \leqq b+Q} \exp\left(2\pi i \frac{hx}{q}\right) = O\left(\Xi\left(\frac{h}{q}\right)\right),$$

valid for any b, with $\Xi(\alpha) = \min(Q, \|\alpha\|^{-1})$, where $\|\alpha\|$ denotes the distance of α to the nearest integer. We see that the left hand side of (9.9) is $\ll K(Q; q.r^2)$, with

$$K(Q; q, r^2) := \frac{1}{q^4 r^8} \sum_{\boldsymbol{h} \neq \boldsymbol{0} \bmod qr^2} \prod_{1 \leqq i \leqq 4} \Xi\left(\frac{h_i}{q}\right) |S(\boldsymbol{h}; q, r^2)|. \tag{9.10}$$

The proof of (9.9) is reduced to the proof of

$$K(Q; q, r^2) = O_{\varepsilon,r}(q^{-1} Q^4 \log^{-3} X), \tag{9.11}$$

for any squarefree q, any integer r coprime with q, satisfying $Qr^{-2} \leqq q \leqq X^{\frac{2}{5}-\varepsilon}$.

We use the multiplicativity (9.5), Lemma 9.3 (noticing that the closed subsets X_j are independent of the non trivial character ψ) and the trivial bound $|S(\boldsymbol{h}; 1, r^2)| \leqq r^8$ to write the inequality

$$|S(\boldsymbol{h}; q, r^2)| \leqq C^s r^8 q^{\frac{3}{2}} \prod_{\substack{p|q \\ \boldsymbol{h} \bmod p \in X_1(\mathbb{F}_p)}} p^{\frac{1}{2}} \prod_{\substack{p|q \\ \boldsymbol{h} \bmod p \in X_2(\mathbb{F}_p)}} p^{\frac{1}{2}} \prod_{\substack{p|q \\ \boldsymbol{h} \bmod p \in X_3(\mathbb{F}_p)}} p^{\frac{1}{2}}.$$

In the above formula, s is the number of prime factors of q, so we have $C^s = O(q^\eta)$. Inserting this bound into (9.10), inverting summation and using the inclusion

$$X_3 \subset X_2 \subset X_1,$$

we finally get the inequality

$$K(Q; q, r^2) \leqq q^{-\frac{5}{2}} C^s \sum_{\delta_3|\delta_2|\delta_1|q} \delta_1^{\frac{1}{2}} \delta_2^{\frac{1}{2}} \delta_3^{\frac{1}{2}} \sum_{\boldsymbol{h}} \Xi\left(\frac{h_1}{qr^2}\right) \Xi\left(\frac{h_2}{qr^2}\right) \Xi\left(\frac{h_3}{qr^2}\right) \Xi\left(\frac{h_4}{qr^2}\right), \tag{9.12}$$

where the last sum is made over the $\boldsymbol{h}$ modulo qr^2, satisfying $\boldsymbol{h} \not\equiv \mathbf{0}$ modulo qr^2, and

for all $1 \leqq i \leqq 3$, *for all* $p|\delta_i$, *we have* $\boldsymbol{h} \bmod p \in X_i(\mathbb{F}_p)$.

(Note that (9.12) is a corrected version of [Fo1], (2.1) which is incorrect (though it is correct when q is prime, and its right hand side contains enough of the essential terms that [Fo1], Prop. 2.5 remains correct). We thank Cécile Dartyge for pointing out a similar error in an earlier version of this paper.)

One of the difficulties is that q is not necessarily prime. Nevertheless we first treat the prime case in order to give lemmas which will be useful in sections 9.c, 10 and 11 and illustrate the situation.

9.b. The particular case when *q* is prime. The first lemma recalls some general facts about varieties. This is Lemma 2.1 of [Fo2].

Lemma 9.4. *Let $\mathscr{V}$ a closed subscheme of $\mathbb{A}^n_{\mathbb{Z}}$ of relative dimension $\leqq d$. Let π_{n-1} be the projection of $\mathbb{A}^n_{\mathbb{Z}}$ on $\mathbb{A}^{n-1}_{\mathbb{Z}}$ defined by $\pi_{n-1}(z_1, \dots, z_n) = (z_1, \dots, z_{n-1})$. Then*

i) *$\pi_{n-1}(\mathscr{V})$ is contained in a closed subscheme of $\mathbb{A}^{n-1}_{\mathbb{Z}}$ of relative dimension $\leqq d$, called $\bar{\pi}_{n-1}(\mathscr{V})$,*

ii) *the set of points M in $\mathbb{A}^{n-1}_{\mathbb{Z}}$ such that the fiber $\pi^{-1}_{n-1}(M)$ is contained in $\mathscr{V}$ (or in other words such that the fiber has an infinite number of points of intersection with $\mathscr{V}$) is contained in a closed subscheme $\Phi_{n-1}(\mathscr{V})$ of $\mathbb{A}^{n-1}_{\mathbb{Z}}$ of relative dimension $\leqq d-1$.*

Now we deal with a more general question, already treated in [Fo2], 2.6.

Lemma 9.5. *Let N be an integer $\geqq 1$, x be a positive real number and let $\mathscr{V}$ be a closed subscheme of $\mathbb{A}^s_{\mathbb{Z}}$ of relative dimension $\leqq d$. Let $\nabla(\mathscr{V}, x, N, d, s)$ be the sum*

$$\nabla(\mathscr{V},x,N,d,s) := \sum_{\boldsymbol{h}\in\mathscr{V}(\mathbb{F}_p)} \left(\min\left(x, \left\|\frac{h_1}{Np}\right\|^{-1}\right)\right) \times\cdots\times \left(\min\left(x, \left\|\frac{h_s}{Np}\right\|^{-1}\right)\right).$$

Then we have the inequality

$$\nabla(\mathscr{V},x,N,d,s) \ll (Np)^d x^{s-d} (\log Np)^d$$

for every $x \leqq Np$.

Proof. The proof proceeds by induction on s. There exists an integer, say K, such that, for every p, every line of $\mathbb{A}^s(\mathbb{F}_p)$ which is parallel to one of the coordinate axis is either contained in $\mathscr{V}(\mathbb{F}_p)$ or has at most K points with $\mathscr{V}$. Summing first over h_s and using the notations of Lemma 9.4, we get

$$\begin{aligned}(9.13)\qquad &\nabla(\mathscr{V},x,N,d,s)\\ &\ll Kx \sum_{\boldsymbol{h}\in\pi_{s-1}(\mathscr{V})(\mathbb{F}_p)} \left(\min\left(x, \left\|\frac{h_1}{Np}\right\|^{-1}\right)\right) \times\cdots\times \left(\min\left(x, \left\|\frac{h_{s-1}}{Np}\right\|^{-1}\right)\right)\\ &\quad + O\left(Np\log(Np) \sum_{\boldsymbol{h}\in\Phi_{s-1}(\mathscr{V})(\mathbb{F}_p)} \left(\min\left(x, \left\|\frac{h_1}{Np}\right\|^{-1}\right)\right)\right.\\ &\quad\left.\times\cdots\times \left(\min\left(x, \left\|\frac{h_{s-1}}{Np}\right\|^{-1}\right)\right)\right).\end{aligned}$$

In the right hand side of (9.13), the dimensions of both the ambient space and of the variety have decreased. So (9.13) gives

$$\begin{aligned}(9.14)\qquad \nabla(\mathscr{V},x,N,d,s) &\ll Kx\nabla\big(\mathscr{V}',x,N,\min(d,s-1),s-1\big)\\ &\quad + pN\log(pN)\nabla(\mathscr{V}'',x,N,d-1,s-1),\end{aligned}$$

where $\mathscr{V}'$ and $\mathscr{V}''$ are the varieties in $\mathbb{A}^{s-1}$ given by $\bar{\pi}_{s-1}(\mathscr{V})$ and $\Phi_{s-1}(\mathscr{V})$ respectively.

For $s=1$, Lemma 9.5 is trivial, since we have $\nabla(\mathscr{V},x,N,1,1) = O\big(Np\log(Np)\big)$ and $\nabla(\mathscr{V},x,N,0,1) = O(x)$. Also for $d=s$, we have

$$\nabla(\mathscr{V},x,N,s,s) \leqq \big(\nabla(\mathbb{A}^1,x,N,d,s)\big)^s \ll \big(Np\log(Np)\big)^s,$$

so Lemma 9.5 is true also in that case. To pass from the value $s-1$ to the value s of the dimension of the ambient space, we use (9.14) and the hypothesis of induction, giving

$$\begin{aligned}\nabla(\mathscr{V}, x, N, d, s) &\ll Kx(Np)^{\min(d,s-1)} x^{s-1-\min(d,s-1)} \big(\log(Np)\big)^{\min(d,s-1)} \\ &\quad + Np \cdot \log(Np) \cdot (Np)^{d-1} x^{s-d} \big(\log(Np)\big)^{d-1} \\ &\ll (Np)^{d} x^{s-d} \big(\log(Np)\big)^{d}. \quad \text{QED}\end{aligned}$$

It is now easy to deduce the proof of (9.11) in the particular case q prime and $r = 1$. Indeed, in this case, the values of the different sums over $\boldsymbol{h}$, on the right hand side of (9.12) are respectively

$$\begin{aligned}&\ll q^4 \log^4 q && \text{when} \quad \delta_1 = \delta_2 = \delta_3 = 1, \\ &\ll q^2 Q^2 \log^2 q && \text{when} \quad \delta_1 = q, \delta_2 = \delta_3 = 1, \\ &\ll q Q^3 \log q && \text{when} \quad \delta_1 = \delta_2 = q, \delta_3 = 1, \\ &= 0 && \text{when} \quad \delta_1 = \delta_2 = \delta_3 = q.\end{aligned}$$

Summing these upper bounds, by (9.12) we get, when q is prime

$$K(Q; q, 1) \ll_\varepsilon q^\eta (q^{\frac{3}{2}} + Q^2 + q^{-\frac{1}{2}} Q^3).$$

which implies (9.11) in that particular case. The proof of (9.11) in the general case is much more delicate in its combinatorial aspects. However, the main ideas are the same.

9.c. A recursive bound. In this section, we give a general bound, which, when applied, will lead to the treatment of $K(Q; q, r^2)$, by reducing step by step the dimension of the ambient space. This reduction will be made by the functions Φ_{n-1} and π_{n-1} of Lemma 9.4. In some sense, it generalizes the proof of Lemma 9.5, but for a modulus not necessarily prime.

Let s and n be integers with $n \geqq 1$. Let $\delta_1, \ldots, \delta_s$ be integers such that $\delta_1 \ldots \delta_s | q$. Let $V_1, \ldots, V_s$ be closed subschemes of $\mathbb{A}^n_{\mathbb{Z}}$, satisfying

$$\dim V_i \leqq a_i,$$

where the a_i are given integers satisfying $-1 \leqq a_i \leqq n$ with the convention that the empty set has dimension -1. We consider the sum Σ_n defined by

$$\begin{aligned}\Sigma_n := \sum_{h_1 \bmod qr^2} \min\nolimits_1 \sum \cdots \sum_{h_{n-1} \bmod qr^2} \min\nolimits_{n-1} \\ \times \mathfrak{S}\big(h_1, \ldots, h_{n-1}, (V_1, \delta_1, a_1), \ldots, (V_s, \delta_s, a_s)\big),\end{aligned}$$

where

$$\min\nolimits_i = \Xi\left(\frac{h_i}{qr^2}\right) = \min\left(Q, \left\|\frac{h_i}{qr^2}\right\|^{-1}\right),$$

and

$$\mathfrak{S}\big(h_1, \dots, h_{n-1}, (V_1, \delta_1, a_1), \dots, (V_s, \delta_s, a_s)\big) = \sum_{h_n} \min{}_n$$

where the sum is over $h_n \bmod qr^2$ satisfying the extra condition

$$\forall 1 \leqq i \leqq s, \quad \forall p | \delta_i, (h_1, \dots, h_n) \in V_i(\mathbb{F}_p).$$

(Note that if $a_i = -1$ and $\delta_i > 1$ then $\mathfrak{S} = 0$.) Actually, we want to give an expression of Σ_n in terms of sums in spaces of lower dimension.

By Lemma 9.4 we know that the closed subscheme $\Phi_{n-1}(V_i)$ of $\mathbb{A}_{\mathbb{Z}}^{n-1}$ has dimension $\leqq a_i - 1$, and that the closed subscheme $\bar{\pi}_{n-1}(V_i)$ of $\mathbb{A}_{\mathbb{Z}}^{n-1}$ has dimension $\leqq \min(n-1, a_i)$. We must take into account all the possibilities. So we factor δ_i into $\delta_i = \gamma_i \gamma_i'$. We see that if for all i

- $(h_1, \dots, h_{n-1}) \in \Phi_{n-1}(V_i)(\mathbb{F}_p)$ for all $p | \gamma_i$,
- $(h_1, \dots, h_{n-1}) \in \bar{\pi}_{n-1}(V_i)(\mathbb{F}_p) - \Phi_{n-1}(V_i)(\mathbb{F}_p)$ for all $p | \gamma_i'$,

then, by the Chinese Remainder Theorem, h_n in the definition of $\mathfrak{S}$, can be written in the form

$$h_n = v + \lambda \prod_i \gamma_i', \tag{9.15}$$

where v takes $O(q^{\frac{\eta}{2}})$ values between 0 and $\prod_i \gamma_i' - 1$ and λ is any integer between 0 and $(qr^2 / \prod_i \gamma_i') - 1$. Summing the function $\min_n$ over the h_n of the form (9.15), we get

$$\begin{aligned}
\sum_{h_n} \min{}_n &\ll \sum_v \sum_{\lambda = 0 \text{ or } (qr^2/\prod \gamma_i') - 1} Q + \sum_v \sum_{0 < \lambda < (qr^2/\prod \gamma_i') - 1} \left\| \frac{v + \lambda \prod_i \gamma_i'}{qr^2} \right\|^{-1} \\
&\ll q^{\frac{\eta}{2}} \left(Q + \sum_{1 \leqq \lambda \leqq qr^2/2\prod \gamma_i'} \frac{qr^2}{\lambda \prod \gamma_i'} \right) \\
&\ll q^{\eta} \left(Q + \frac{qr^2}{\prod \gamma_i'} \right).
\end{aligned}$$

In conclusion, the sum Σ_n is bounded by

$$\begin{aligned}
\Sigma_n \ll q^{\eta} &\sum_{\gamma_1 \gamma_1' = \delta_1} \cdots \sum_{\gamma_s \gamma_s' = \delta_s} \left(Q + \frac{qr^2}{\prod_i \gamma_i'} \right) \\
&\times \sum_{h_1 \bmod qr^2} \min{}_1 \cdots \sum_{h_{n-2} \bmod qr^2} \\
&\times \min{}_{n-2} \mathfrak{S}\big(h_1, \dots, h_{n-2}, (\mathfrak{W}_1), (\mathfrak{W}_1'), \dots, (\mathfrak{W}_s), (\mathfrak{W}_s')\big),
\end{aligned} \tag{9.16}$$

where $(\mathfrak{W}_i)$ and $(\mathfrak{W}_i')$ are the triples

$$(\mathfrak{W}_i) = (W_i,\gamma_i,a_i-1), \quad (\mathfrak{W}_i') = \big(W_i',\gamma_i',\min(a_i,n-1)\big) \quad (1 \leqq i \leqq s),$$

with W_i and W_i' closed subschemes of $\mathbb{A}_{\mathbb{Z}}^{n-1}$. Note that in (9.16), the number of varieties has doubled, but the ambient space dimension has decreased by one.

9.d. Proof of (9.11). Let $M(\delta_1,\delta_2,\delta_3)$ be the sum over $\boldsymbol{h}$ on the right hand side of (9.12). So this inequality can be written as

$$K(Q;q,r^2) \leqq q^{-\frac{5}{2}}C^s \sum_{\delta_3|\delta_2|\delta_1|q} \delta_1^{\frac{1}{2}}\delta_2^{\frac{1}{2}}\delta_3^{\frac{1}{2}} M(\delta_1,\delta_2,\delta_3). \tag{9.17}$$

Since we have the inclusions $X_3 \subset X_2 \subset X_1$, since q is squarefree (so the numbers δ_3, δ_2/δ_3 and δ_1/δ_2 are coprime) we can write M in the form

$$\begin{aligned} M(\delta_1,\delta_2,\delta_3) = &\sum_{h_1 \bmod qr^2} \min\nolimits_1 \sum_{h_2 \bmod qr^2} \min\nolimits_2 \sum_{h_3 \bmod qr^2} \min\nolimits_3 \\ &\times \mathfrak{S}\big(h_1,h_2,h_3,(X_1,\delta_1/\delta_2,2),(X_2,\delta_2/\delta_3,1),(X_3,\delta_3,0)\big), \end{aligned}$$

where we use the notations of §9.c. We factor δ_1/δ_2 and δ_2/δ_3 into $\gamma_1\gamma_1'$ and $\gamma_2\gamma_2'$ (it is useless to factorize δ_3) and use the recursive formula (9.16) to write

$$\begin{aligned} &M(\delta_1,\delta_2,\delta_3) \\ &\ll q^\eta \sum_{\gamma_1\gamma_1'=\delta_1/\delta_2} \sum_{\gamma_2\gamma_2'=\delta_2/\delta_3} \left(Q+\frac{qr^2}{\gamma_1'\gamma_2'\delta_3}\right) \sum_{h_1 \bmod qr^2} \min\nolimits_1 \sum_{h_2 \bmod qr^2} \min\nolimits_2 \\ &\quad \times \mathfrak{S}\big(h_1,h_2,(X_{1,1},\gamma_1,1),(X_{1,2},\gamma_1',2),(X_{2,1},\gamma_2,0),(X_{2,2},\gamma_2',1),(X_3,\delta_3,0)\big). \end{aligned} \tag{9.18}$$

In this expression, we put together the varieties of the same dimension to write for

$$S_2 := \sum_{h_1} \min\nolimits_1 \sum_{h_2} \min\nolimits_2 \mathfrak{S}(\ldots)$$

the upper bound

$$S_2 \leqq \sum_{h_1} \min\nolimits_1 \sum_{h_2} \min\nolimits_2 \mathfrak{S}\big(h_1,h_2,(Y_0,\gamma_2\delta_3,0),(Y_1,\gamma_1\gamma_2',1),(Y_2,\gamma_1',2)\big). \tag{9.19}$$

We follow the same technique: we factor $\gamma_1\gamma_2'$ and γ_1' into $\beta_1\beta_1'$ and $\beta_2\beta_2'$ and put together varieties of the same dimension to transform (9.19) into

$$\begin{aligned} S_2 \ll q^\eta &\sum_{\beta_1\beta_1'=\gamma_1\gamma_2'} \sum_{\beta_2\beta_2'=\gamma_1'} \left(Q+\frac{qr^2}{\beta_1'\beta_2'\gamma_2\delta_3}\right) \sum_{h_1} \min\nolimits_1 \\ &\times \mathfrak{S}\big(h_1,(Z_0,\beta_1\gamma_2\delta_3,0),(Z_1,\beta_1'\beta_2,1),(Z_2,\beta_2',2)\big). \end{aligned} \tag{9.20}$$

Since Z_2 is of dimension at most 2 in the ambient space of dimension 2, we can drop this variety in $\mathfrak{S}$. We write for

$$S_1 := \sum_{h_1} \min{}_1 \mathfrak{S}(\ldots)$$

the inequality

$$S_1 \leqq \sum_{h_1} \min{}_1 \mathfrak{S}\big(h_1, (Z_0, \beta_1\gamma_2\delta_3, 0), (Z_1, \beta_1'\beta_2, 1)\big). \tag{9.21}$$

We again apply the recursive formula in (9.21) giving

$$S_1 \ll q^\eta \sum_{\alpha_1\alpha_1' = \beta_1'\beta_2} \left(Q + \frac{qr^2}{\alpha_1'\beta_1\gamma_2\delta_3}\right) \mathfrak{S}\big((U_0, \alpha_1\beta_1\gamma_2\delta_3, 0)\big). \tag{9.22}$$

It is easy to obtain the inequality

$$\mathfrak{S}\big((U_0, \alpha_1\beta_1\gamma_2\delta_3, 0)\big) \ll q^\eta \left(Q + \frac{qr^2}{\alpha_1\beta_1\gamma_2\delta_3}\right). \tag{9.23}$$

Inserting (9.23) in (9.22), and summing over α_1 and α_1' we get

$$S_1 \ll q^{3\eta}\left(Q^2 + \frac{qr^2Q}{\beta_1\gamma_2\delta_3} + \frac{q^2r^4}{\beta_1^2\beta_1'\beta_2\gamma_2^2\delta_3^2}\right). \tag{9.24}$$

We insert (9.24) into (9.20) and sum over β_1, β_1', β_2 and β_2' to get

$$S_2 \ll q^{5\eta}\left(Q^3 + \frac{qr^2Q^2}{\gamma_2\delta_3} + \frac{q^2r^4Q}{\gamma_1\gamma_2^2\gamma_2'\delta_3^2} + \frac{q^3r^6}{\gamma_1^2\gamma_1'\gamma_2^3\gamma_2'^2\delta_3^3}\right). \tag{9.25}$$

Inserting (9.25) into (9.18), and summing over γ_1, γ_1', γ_2 and γ_2', we finally obtain

$$M(\delta_1, \delta_2, \delta_3) \ll q^{7\eta}\left(Q^4 + \frac{qr^2Q^3}{\delta_3} + \frac{q^2r^4Q^2}{\delta_2\delta_3} + \frac{q^3r^6Q}{\delta_1\delta_2\delta_3} + \frac{q^4r^8}{\delta_1^2\delta_2\delta_3}\right). \tag{9.26}$$

We use (9.26) in (9.17) to produce an upper bound for $K(Q; q, r^2)$, but we will only use it when δ_3 is not too large, $\delta_3 \leqq \Delta_3$ say. The value of Δ_3 will be fixed later. The remaining $\delta_3 > \Delta_3$ will be treated trivially. We have

$$\begin{aligned} K(Q; q, r^2) \ll q^{-\frac{5}{2}+7\eta} C^s \sum_{\substack{\delta_3|\delta_2|\delta_1|q \\ \delta_3 \leqq \Delta_3}} \delta_1^{\frac{1}{2}}\delta_2^{\frac{1}{2}}\delta_3^{\frac{1}{2}} \left(Q^4 + \frac{qr^2Q^3}{\delta_3} + \frac{q^2r^4Q^2}{\delta_2\delta_3} + \frac{q^3r^6Q}{\delta_1\delta_2\delta_3} + \frac{q^4r^8}{\delta_1^2\delta_2\delta_3}\right) \\ + q^{-\frac{5}{2}} C^s \left(\frac{q}{\Delta_3}\right) \sum_{\substack{\delta_3|q \\ \delta_3 \geqq \Delta_3}} \delta_3^{\frac{3}{2}} \sum_{\substack{\boldsymbol{h} \neq \boldsymbol{0} \bmod qr^2 \\ \delta_3|(h_1, \ldots, h_4)}} \min{}_1 \ldots \min{}_4 \end{aligned}$$

which gives

$$(9.27)\quad K(Q;q,r^2) \ll q^{-\frac{5}{2}+8\eta}(qQ^4\Delta_3^{\frac{1}{2}} + q^2r^2Q^3 + q^{\frac{5}{2}}r^4Q^2 + q^3r^6Q + q^4r^8) + q^{-\frac{5}{2}}C^s\left(\frac{q}{\Delta_3}\right)\sum_{\substack{\delta_3|q\\ \delta_3\geqq\Delta_3}} \delta_3^{\frac{3}{2}}M^*(\delta_3),$$

say. To evaluate $M_3^*(\delta_3)$, we separate the $\boldsymbol{h}$ according to the number of the h_i which are 0 modulo qr^2. We get

$$M^*(\delta_3) \ll q^{\eta}\left(\left(\frac{qr^2}{\delta_3}\right)Q^3 + \left(\frac{qr^2}{\delta_3}\right)^2Q^2 + \left(\frac{qr^2}{\delta_3}\right)^3Q + \left(\frac{qr^2}{\delta_3}\right)^4\right)$$
$$\ll q^{\eta}\left(\left(\frac{qr^2}{\delta_3}\right)Q^3 + \left(\frac{qr^2}{\delta_3}\right)^4\right).$$

By inserting this bound into (9.27), we get

$$(9.28)\quad K(Q;q,r^2) \ll q^{-\frac{5}{2}+8\eta}(qQ^4\Delta_3^{\frac{1}{2}} + q^2r^2Q^3 + q^{\frac{5}{2}}r^4Q^2 + q^3r^6Q + q^4r^8) + q^{-\frac{5}{2}+2\eta}(q^{\frac{5}{2}}r^2Q^3\Delta_3^{-1} + q^5r^8\Delta_3^{-\frac{7}{2}}).$$

We choose now

$$\Delta_3 = q^{1-18\eta}$$

and (9.28) becomes

$$K(Q;q,r^2) \ll (q^{-1-\eta}Q^4 + q^{-\frac{1}{2}+8\eta}Q^3 + q^{8\eta}Q^2 + q^{\frac{1}{2}+8\eta}Q + q^{\frac{3}{2}+8\eta}) + q^{-1+65\eta}Q^3.$$

It is easy to see that (9.11) is proved for q squarefree, satisfying $Qr^{-2} \leqq q \leqq X^{\frac{2}{5}-\varepsilon}$, if ε is sufficiently small.

9.e. The case $q \leqq Qr^{-2}$. Coming back to (9.2), we see that the length of the sides of $\mathscr{B}_i$ is larger than the modulus qr^2. We decompose $\mathscr{B}_i$ into a certain number of hypercubes with sides of length qr^2 (we call them $\mathscr{B}_{i,j}$, their number is $\left[\frac{Q}{qr^2}\right]^4$) and into $O\big((Q/qr^2)^3\big)$ incomplete hypercubes $\mathscr{C}_{i,k}$ (incomplete means that all the sides have length $\leqq qr^2$ and at least one has length $< qr^2$). Since we have a complete set of residues we have the equality

$$(9.29)\quad \sum_{\substack{M\in\mathscr{B}_{i,j},\,\Delta_3(M)\equiv 0\ (\mathrm{mod}\, r^2)\\ \Delta_3(M)-4\equiv 0\ (\mathrm{mod}\, q)}} 1 = \prod_{p|q}\frac{\rho(p,4)}{p^4}\prod_{p|r}\xi(p)\sum_{M\in\mathscr{B}_{i,j}} 1.$$

For the incomplete hypercubes $\mathscr{C}_{i,k}$, we develop in Fourier series the characteristic function of each edge (which is of length $\leqq qr^2$). We get

$$(9.30)\quad \sum_{\substack{M\in\mathscr{C}_{i,k},\,\Delta_3(M)\equiv 0\ (\mathrm{mod}\, r^2)\\ \Delta_3(M)-4\equiv 0\ (\mathrm{mod}\, q)}} 1 = \prod_{p|q}\frac{\rho(p,4)}{p^4}\prod_{p|r}\xi(p)\sum_{M\in\mathscr{C}_{i,k}} 1 + O\big(K(qr^2;q,r^2)\big),$$

with

$$K(qr^2; q, r^2) := \frac{1}{q^4 r^8} \sum_{\boldsymbol{h} \neq \boldsymbol{0} \bmod qr^2} \prod_{1 \leqq i \leqq 4} \Xi'\left(\frac{h_i}{q}\right) |S(\boldsymbol{h}; q, r^2)|,$$

with $\Xi'(\alpha) = \min(qr^2, \|\alpha\|^{-1})$. We use Lemma 9.3(9.8), in the form

$$|S(\boldsymbol{h}; q, r^2)| \ll C^s q^{\frac{5}{2}} r^8 (\boldsymbol{h}, q)^{\frac{1}{2}}.$$

We get, for any positive η

$$\begin{aligned} K(qr^2; q, r^2) &\ll q^{-\frac{3}{2}+\eta} \sum_{\boldsymbol{h} \neq \boldsymbol{0} \bmod qr^2} \prod_{1 \leqq i \leqq 4} \Xi'\left(\frac{h_i}{q}\right) (\boldsymbol{h}, q)^{\frac{1}{2}}, \\ &\ll q^{-\frac{3}{2}+\eta} \sum_{\delta | q} \delta^{\frac{1}{2}} \sum_{\substack{\boldsymbol{h} \neq \boldsymbol{0} \bmod qr^2 \\ \delta | \boldsymbol{h}}} \prod_{1 \leqq i \leqq 4} \Xi'\left(\frac{h_i}{q}\right) \\ &\ll q^{-\frac{3}{2}+2\eta} \sum_{\delta | q} \delta^{\frac{1}{2}} (qr^2)^3 (qr^2 \delta^{-1}). \end{aligned}$$

This gives

$$K(qr^2; q, r^2) \ll q^{\frac{5}{2}+3\eta} r^8. \tag{9.31}$$

Summing formula (9.29) over the j and using formula (9.30) with K bounded by (9.31), we get

$$\sum_{\substack{M \in \mathscr{B}_i, \Delta_3(M) \equiv 0 \ (\mathrm{mod}\, r^2) \\ \Delta_3(M) - 4 \equiv 0 \ (\mathrm{mod}\, q)}} 1 = \prod_{p|q} \frac{\rho(p, 4)}{p^4} \prod_{p|r} \xi(p) \sum_{M \in \mathscr{B}_i} 1 + O\big((Q/q)^3 \cdot q^{\frac{5}{2}+3\eta}\big).$$

This error term is $O\big(q^{-1} Q^4 (\log x)^{-3}\big)$, for every $q \leqq Qr^{-2}$. This ends the proof of (9.2) in all cases and so also ends the proof of Proposition 9.2.

9.f. End of the proof of Corollary 1.3. Let $\mathscr{A}$ be the set $\mathscr{A} = \{a; 1 \leqq a \leqq x\}$, each a given the weight $w(a) := \mathscr{H}(a+4)$ (recall that this weight is zero when $a+4$ is not a fundamental discriminant). Let also P be an integer, which will be chosen larger and larger. Instead of sieving $\mathscr{A}$, we will rather sieve $\tilde{\mathscr{A}} := \{a; 1 \leqq a \leqq x\}$, each a taken with weight $\tilde{w}(a) := \frac{1}{2} g_P(a+4)$. The relation (9.1) implies

$$w(a) \leqq \tilde{w}(a). \tag{9.32}$$

Let us recall the classical notations of sieve theory

$$S(\mathscr{A}, \mathscr{P}, z) = \sum_{\substack{a \leqq x \\ p | a \Rightarrow p \geqq z}} w(a), \quad S(\tilde{\mathscr{A}}, \mathscr{P}, z) = \sum_{\substack{a \leqq x \\ p | a \Rightarrow p \geqq z}} \tilde{w}(a).$$

Here $\mathscr{P}$ is the set of all the prime numbers. Let $C(x)$ be defined by

$$\#\{\sqrt{x} \leqq p \leqq x, p \equiv 1 (\mathrm{mod}\, 4), \mu^2(p+4) = 1, 3 \nmid h(p+4)\} = C(x)\frac{x}{\log x}.$$

We intend to prove the inequality $C(x) \geqq c_0$ for x sufficiently large. Since the weight $w(a)$ takes values either 0 or greater than 1, we have the inequality

$$S(\mathscr{A}, \mathscr{P}, x^{\frac{1}{2}}) + C(x)\frac{x}{\log x} \geqq \#\{\sqrt{x} \leqq p \leqq x; p \equiv 1 (\mathrm{mod}\, 4), \mu^2(p+4) = 1\}. \tag{9.33}$$

By [Fo1], Lemme 5.1, we know that the right hand side of (9.31) is equal to

$$\left(\frac{1}{2} + o(1)\right)\Gamma\frac{x}{\log x}, \tag{9.34}$$

where Γ is the infinite product $\Gamma = \prod\limits_{p>2}\big(1 - 1/p(p-1)\big)$. Now (9.32) implies the inequality

$$S(\mathscr{A}, \mathscr{P}, x^{\frac{1}{2}}) \leqq S(\tilde{\mathscr{A}}, \mathscr{P}, x^{\frac{1}{2}}). \tag{9.35}$$

Proposition 9.2 says that we can write

$$\sum_{\substack{n \leqq x \\ q \mid n}} g_P(n+4) = \frac{\omega(q)}{q}\prod_{2 \leqq p \leqq P}\big(1 - \xi(p)\big)\Big(\sum_{n \leqq x} g(n)\Big) + r(x, q)$$

with

$$\omega(q) = \prod_{2 \mid q}\frac{8}{15}\prod_{\substack{2 < p \leqq P \\ p \mid q}}\big(1 - \xi(p)\big)\prod_{p \mid q}\frac{\rho(p, 4)}{p^3},$$

and where the error term satisfies

$$\sum_{q \leqq x^{\frac{2}{5}-\varepsilon}} \mu^2(q)|r(x, q)| = O(x \log^{-2} x).$$

We see that ω satisfies the conditions of the linear sieve, and that $\tilde{\mathscr{A}}$ has level of distribution $x^{\frac{2}{5}-\varepsilon}$. It is time to apply the classical formula of the upper bound sieve [Iw], Thm. 1. We get

$$\begin{aligned} S(\tilde{\mathscr{A}}, \mathscr{P}, x^{\frac{1}{2}}) \leqq \left(\frac{1}{2} + \eta\right) V(x^{\frac{1}{2}}) \prod_{2 \leqq p \leqq P}\big(1 - \xi(p)\big)\Big(\sum_{n \leqq x} g(n)\Big) \\ \cdot 2e^{\gamma}\frac{\log x^{\frac{1}{2}}}{\log x^{\frac{2}{5}-\varepsilon}} + O(x \log^{-2} x), \end{aligned} \tag{9.36}$$

for any positive η and $x > x_0(\eta)$. An easy computation shows that the Euler product $V(x^{\frac{1}{2}}) := \prod\limits_{p \leqq x^{\frac{1}{2}}}\left(1 - \dfrac{\omega(p)}{p}\right)$ satisfies

$$V(x^{\frac{1}{2}}) \sim c_P \cdot \Gamma \cdot \frac{\pi^2}{3} \frac{\mathrm{e}^{-\gamma}}{\log x}, \tag{9.37}$$

where c_P is some constant which tends to 1 as P tends to infinity (see [Fo1], (5.6)). To conclude, by [Da], Lemmas 4,5 we have

$$\sum_{n \leqq x} g(n) \sim \frac{\pi^2}{36} x. \tag{9.38}$$

Inserting (9.37) and (9.38) into (9.36), we get

$$S(\tilde{\mathscr{A}}, \mathscr{P}, x^{\frac{1}{2}}) \leqq \left(\frac{5}{12} + \eta\right) \cdot \Gamma \cdot \frac{x}{\log x}, \tag{9.39}$$

for every $\eta > 0$ and $x > x_0(\eta)$. Inserting now (9.39) into (9.35) and then (9.34) into (9.33) we see that $C(x)$ satisfies the inequality

$$C(x) + \left(\frac{5}{12} + \eta\right) \cdot \Gamma \geqq \left(\frac{1}{2} + o(1)\right) \cdot \Gamma,$$

for every η under the condition $x > x_0(\eta)$. Hence we obtain the lower bound

$$C(x) \geqq \frac{\Gamma}{13}$$

for x sufficiently large. QED

10. Proof of Corollary 1.4

The method is absolutely classical. By Weyl's criterion, it suffices to prove that, for every non trivial additive character ψ of $\mathbb{F}_p$ and for every fixed non-zero r-tuple $a = (a_1, \ldots, a_r)$, the exponential sum S defined by

$$S = \sum_{0 \leqq x_i \leqq w(p)} \psi\big(a_1 P_1(x) + \cdots + a_r P_r(x)\big) \tag{10.1}$$

satisfies

$$S = o\big(w(p)^n\big) \tag{10.2}$$

for $p \to \infty$. We first prove (10.2) for $1 \leqq w(p) < p$. On the additive group $\mathbb{F}_p$, we develop the characteristic function Ψ of the integers in $[0, w(p)]$ in a finite Fourier series: the function

$$\Psi(n) := \frac{1}{p} \sum_{0 \leqq m \leqq w(p)} \sum_{0 \leqq h < p} \psi\big(h(m - n)\big) \tag{10.3}$$

is equal to 1 for $0 \leqq n \leqq w(p)$, and 0 if $w(p) < n < p$. Inserting (10.3) into the definition (10.1), we obtain

$$S = \frac{1}{p^n} \sum_{h \in \mathbb{A}^n(\mathbb{F}_p)} \prod_{1 \leqq i \leqq n} \sum_{0 \leqq m \leqq w(p)} \psi(h_i m) \sum_{x \in \mathbb{A}^n(\mathbb{F}_p)} \psi\big(a \cdot P(x) - h \cdot x\big),$$

where $h \cdot x$ is the usual scalar product in dimension n. If ψ is of the form

$$\psi(t) = \exp\left(\frac{2\pi i b t}{p}\right)$$

with some b non divisible by p, we get

$$(10.4) \quad S \ll \frac{1}{p^n} \sum_{h \in \mathbb{A}^n(\mathbb{F}_p)} \prod_{1 \leqq i \leqq n} \min\big(w(p), \|bh_i/p\|^{-1}\big) \Big| \sum_{x \in \mathbb{A}^n(\mathbb{F}_p)} \psi\big(a \cdot P(x) - h \cdot x\big) \Big|.$$

For any $a \neq 0$ and for any h the function $a \cdot P(x) - h \cdot x$ is not $\equiv 0$ by assumption. So Weil's bound for exponential sums over polynomial in several variables implies

$$(10.5) \qquad \sum_{x \in \mathbb{A}^n(\mathbb{F}_p)} \psi\big(a \cdot P(x) - h \cdot x\big) = O(p^{n - \frac{1}{2}})$$

where the constant depends only on the P_i. We apply Theorem 1.1 with $f = a \cdot P$, $g = 1$, $V = \mathbb{A}^n_{\mathbb{Z}}$. So we introduce the varieties X_j of dimension $\leqq n - j$, and we define $X_0 = \mathbb{A}^n_{\mathbb{Z}}$. With these conventions and with the remark (10.5), we transforn (10.4) into

$$S \ll \frac{1}{p^n} \sum_{j=1}^{n} p^{\frac{n}{2} + \frac{j-1}{2}} \sum_{h \in X_{j-1}(\mathbb{F}_p)} \prod_{1 \leqq i \leqq n} \min\big(w(p), \|bh_i/p\|^{-1}\big).$$

By Lemma 9.5, we have

$$\sum_{h \in X_{j-1}(\mathbb{F}_p)} \prod_{1 \leqq i \leqq n} \min\big(w(p), \|bh_i/p\|^{-1}\big) \ll p^{n-(j-1)} w(p)^{j-1} (\log p)^{n-(j-1)}.$$

Hence we get

$$(10.6) \qquad S \ll p^{\frac{n}{2}} (\log p)^n \sum_{j=1}^{n} \left(\frac{w(p)}{\sqrt{p} \log p}\right)^{j-1} \ll p^{\frac{1}{2}} w(p)^{n-1} \log p,$$

which proves (10.2) in the case $w(p) < p$.

When $w(p) \geqq p$, we dissect the hypercube of summation over $(x_1, \ldots, x_n)$ into $\ll \big(w(p)/p\big)^n$ hypercubes $\mathscr{C}_i$ with all their sides with length $< p$. Let $S(\mathscr{C}_i)$ be the exponential sum

$$S(\mathscr{C}_i) = \sum_{x \in \mathscr{C}_i} \psi\big(a_1 P_1(x) + \cdots + a_r P_r(x)\big).$$

Proving for $S(\mathscr{C}_i)$ a formula similar to (10.4), and using (10.5), we get

$$S(\mathscr{C}_i) \ll p^{n-\frac{1}{2}}(\log p)^n.$$

Summing over all the $\mathscr{C}_i$, we get also (10.2) in that case. QED

11. Proof of Corollary 1.5

As in (10.3) we develop in Fourier series the characteristic function of the interval $[0, x[$. We get

$$\#V(\mathbb{F}_p, x) = \frac{1}{p^s} \sum_{(h_1, \dots h_s) \in \mathbb{F}_p^s} \prod_{1 \leqq i \leqq s} \sum_{0 \leqq m < x} \exp\left(-2\pi i \frac{h_i m}{p}\right) \cdot S(V; h, p)$$

where

$$S(V; h, p) = \sum_{x \in V(\mathbb{F}_p)} \exp\left(2\pi i \frac{h_1 x_1 + \cdots + h_s x_s}{p}\right).$$

The term corresponding to $h = 0$ is the main term $\#V(\mathbb{F}_p)\left(\frac{x}{p}\right)^s$. The error term comes from the contribution of the other terms. It is $O(S)$, with

$$S := \frac{1}{p^s} \sum_{h \neq 0 \in \mathbb{F}_p^s} \prod_{1 \leqq i \leqq s} \min\left(x, \left\|\frac{h_i}{p}\right\|^{-1}\right) |S(V; h, p)|.$$

Since $V_{\mathbb{C}}$ does not lie in a hyperplane, we have for any $h \neq 0$ the upper bound

$$|S(V; h, p)| \leqq C p^{d-\frac{1}{2}}, \tag{11.1}$$

see [Fo2], Prop 1.2 for instance. Let $X_2, X_3, \dots, X_d$ be the closed subschemes introduced in Theorem 1.2 (note that (11.1) implies that X_{d+1} can be taken to be equal to $\{0\}$ and need not be considered). So we have the inequality

$$S \ll \frac{1}{p^s}\left(p^{\frac{d}{2}} \sum_{h \in \mathbb{F}_p^s} \prod_{1 \leqq i \leqq s} \min\left(x, \left\|\frac{h_i}{p}\right\|^{-1}\right) + \sum_{j=2}^{d} p^{\frac{d+j-1}{2}} \sum_{h \in X_j} \prod_{1 \leqq i \leqq s} \min\left(x, \left\|\frac{h_i}{p}\right\|^{-1}\right)\right).$$

We know that the X_j are of dimension $\leqq s - j$, so Lemma 9.5 gives at once

$$S \ll \frac{1}{p^s}\left(p^{\frac{d}{2}} \cdot p^s (\log p)^s + \sum_{j=2}^{d} p^{\frac{d+j-1}{2}} \cdot x^j p^{s-j} (\log p)^{s-j}\right).$$

Summing over j we get

$$S \ll p^{\frac{d}{2}} (\log p)^s \left\{1 + \frac{1}{\sqrt{p}}\left(\left(\frac{x}{\sqrt{p}\log p}\right)^2 + \left(\frac{x}{\sqrt{p}\log p}\right)^d\right)\right\}.$$

This ends the proof of Corollary 1.5.

References

[BBD] *A. A. Beilinson*, *I. N. Bernstein* and *P. Deligne*, Faisceaux pervers, Conférence de Luminy, juillet 1981, Analyse et Topologie sur les espaces singuliers, I, Astérisque **100** (1982).

[Be-Fo] *K. Belabas* and *E. Fouvry*, Sur le 3-rang des corps quadratiques de discriminant premier ou presque premier, Duke Math. J. **98** (1999), 217–268.

[Da] *H. Davenport*, On the class number of binary cubic forms, I, J. London Math. Soc. **26** (1951), 183–192; erratum, ibid. **27** (1951), 512.

[Da-He1] *H. Davenport* and *H. Heilbronn*, On the density of discriminants of cubic fields, Bull. Lond. Math. Soc. **1** (1969), 345–348.

[Da-He2] *H. Davenport* and *H. Heilbronn*, On the density of discriminants of cubic fields. II, Proc. Roy. Soc. Lond. A **322** (1971), 405–420.

[De-WI] *P. Deligne*, La conjecture de Weil, Publ. Math. I. H. E. S. **43** (1974), 273–307.

[De-WII] *P. Deligne*, La conjecture de Weil II, Publ. Math. I. H. E. S. **52** (1980), 313–428.

[Fo1] *E. Fouvry*, Sur les propriétés de divisibilité des nombres de classes des corps quadratiques, Bull. Soc. Math. France **127** (1999), 95–113.

[Fo2] *E. Fouvry*, Consequences of a Theorem of N. Katz and G. Laumon Concerning Trigonometric Sums, Israel J. Math. **120** (2000), 81–96.

[Ha] *R. Hartshorne*, Algebraic Geometry, Springer Grad. Texts Math. **52** (1977).

[Iw] *H. Iwaniec*, Rosser's Sieve, Acta Arith. **36** (1980), 171–202.

[Ka-ASDE] *N. Katz*, Algebraic Solutions of Differential Equations (p-curvature and the Hodge Filtration), Inv. Math. **18** (1972), 1–118.

[Ka-SE] *N. Katz*, Sommes Exponentielles, Astérisque **79** (1980), SMF.

[Ka-PES] *N. Katz*, Perversity and Exponential Sums, Algebraic Number Theory—in honor of K. Iwasawa, Adv. Stud. Pure Math. **17** (1989), 209–259.

[Ka-PESII] *N. Katz*, Perversity and Exponential Sums II: Estimates for and Inequalities among A-Numbers, Barsotti Symposium in Algebraic Geometry, Academic Press (1994), 205–252.

[K-L] *N. Katz* and *G. Laumon*, Transformation de Fourier et majoration de sommes exponentielles, Publ. Math. I. H. E. S. **62** (1985), 361–418; corrigendum **69**, p. 233.

[SGA 4] Théorie des topos et cohomologie étale des schémas, Springer Lect. Notes Math. **269**, **270** and **305** (1972–1973).

[SGA 7] Groupes de monodromie en géométrie algébrique, Springer Lect. Notes Math. **288** and **340** (1972–1973).

Mathématiques, Bâtiment 425, Université de Paris-Sud, 91405 Orsay Cedex, France

Department of Mathematics, Princeton University, Princeton, New Jersey 08544, USA

Eingegangen 14. Februar 2000, in revidierter Fassung 29. November 2000