LOWER BOUNDS FOR FROBENIUS TRACES

ENRICO BOMBIERI AND NICHOLAS M. KATZ

1. INTRODUCTION

This paper grew out of the following question. Given an ordinary elliptic curve $E/\mathbb{F}_q$ over a finite field $\mathbb{F}_q$, consider the sequence of integers $A(n)$, $n \geq 1$ defined by

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - A(n).$$

Is it true that as n grows we have $|A(n)| \rightarrow \infty$? Without the hypothesis “ordinary”, the answer can be no, because for a supersingular elliptic curve, one can have $A(n) = 0$ on entire arithmetic progressions of n . On the other hand, all the $A(n)$ in the supersingular case are divisible, as algebraic integers, by $q^{n/2}$, so the nonzero $A(n)$ must have $|A(n)| \geq q^{n/2}$. If $E/\mathbb{F}_q$ is ordinary, then all the $A(n)$ are nonzero, because they are all prime to p , the characteristic of $\mathbb{F}_q$, so this vanishing problem at least disappears.

Now the $A(n)$ are the traces of the iterates of a certain Frobenius endomorphism F , and this leads to the more general question of when we can assert that in the sequence $|Trace(F^n)|, n \geq 1$, the nonzero terms tend to ∞ .

In the first section, we establish a quite general result of this kind, using the theorem [ESS, Thm. 1.1] of Evertse-Schlichewei-Schmidt on the generalized unit equation. In the second section, we give a quantitative version of this same sort of result, based on the subspace theorem of these same authors, cf. especially [BG, Cor. 7.2.5], [E, Thm. page 228] and [ES, Thm. 3.1]. In the appendix, we give a sharper result for ordinary elliptic curves and for the classical Kloosterman sums, using the Baker-Wüstholz theorem [BW].

2. UNBOUNDEDNESS OF TRACES, VIA EVERTSE-SCHLICHEWEI-SCHMIDT

We first apply the theorem [ESS, Thm. 1.1] of Evertse-Schlichewei-Schmidt on the generalized unit equation to study the growth of traces. Let us begin by recalling the relevant special case of that theorem.

Theorem 2.1. ([ESS, Thm. 1.1]) *Fix an algebraically closed field K of characteristic zero. Fix an integer $n \geq 1$, n numbers $a_1, \dots, a_n$ in $K^\times$, none of which is a root of unity, and n numbers $\lambda_1, \dots, \lambda_n$ in $K^\times$. Then we have the following results.*

- (1) *The number of integers $k \in \mathbb{Z}$ for which there exists an n -tuple $(\zeta_1, \dots, \zeta_n)$ of roots of unity such that*

$$\sum_{i=1}^n \lambda_i \zeta_i (a_i)^k = 1$$

is at most $2^n \exp(2(6n)^{3n})$.

- (2) *Fix a nonzero number $M \in K^\times$. The number of integers $k \in \mathbb{Z}$ for which there exists an n -tuple $(\zeta_1, \dots, \zeta_n)$ of roots of unity such that*

$$\sum_{i=1}^n \zeta_i (a_i)^k = M$$

is at most $2^n \exp(2(6n)^{3n})$.

- (3) *In particular, the number of integers $k \in \mathbb{Z}$ such that*

$$\sum_{i=1}^n (a_i)^k = M$$

is at most $2^n \exp(2(6n)^{3n})$.

Proof. It suffices to prove the first assertion. Indeed, assertion (2) is the special case of (1) when, for all i , we take $\lambda_i = 1/M$. And the k which work in (3) are the subset of those which work in (2) having all $\zeta_i = 1$.

We now prove the first assertion. Consider the multiplicative subgroup $\Gamma_0 \subset (K^\times)^n$ generated by the single element $(a_1, \dots, a_n)$. Consider also the larger the multiplicative subgroup $\Gamma \subset (K^\times)^n$ generated by Γ_0 and by all n -tuples $(\zeta_1, \dots, \zeta_n)$ of roots of unity. Concretely, the elements of Γ are the n -tuples of the form $(\zeta_1 (a_1)^k, \dots, \zeta_n (a_n)^k)$, for some integer k and some roots of unity $\zeta_1, \dots, \zeta_n$. Because no a_i is a root of unity, this representation of an element of Γ is unique, i.e., both the integer k and the roots of unity $\zeta_1, \dots, \zeta_n$ are uniquely determined.

Γ_0 is a free abelian group of rank one, and Γ/Γ_0 is a torsion group, so Γ has $\mathbb{Q}$ -rank one. For each nonempty subset $S = \{s_1, \dots, s_d\} \subset \{1, 2, \dots, n\}$, we denote by $\Gamma_0(S) \subset (K^\times)^{\#S}$ and $\Gamma(S) \subset (K^\times)^{\#S}$ the corresponding subgroups formed using the $\#S$ numbers $(a_{s_1}, \dots, a_{s_d})$. Again, each group $\Gamma(S)$ has $\mathbb{Q}$ -rank one, and its elements have unique representations of the form $(\zeta_{s_1} (a_{s_1})^k, \dots, \zeta_{s_d} (a_{s_d})^k)$.

According to the theorem [ESS, Thm. 1.1], for any n nonzero numbers $(\lambda_i, \dots, \lambda_n) \in (K^\times)^n$, the equation

$$\sum_{i=1}^n \lambda_i x_i = 1$$

has at most $\exp(2(6n)^{3n})$ *nondegenerate* solutions in Γ , i.e., solutions with $(x_1, \dots, x_n) \in \Gamma$ an element with the additional property that for every nonempty proper subset $T \subset \{1, 2, \dots, n\}$, we have the nonvanishing

$$\sum_{t \in T} \lambda_t x_t \neq 0.$$

Concretely, this means that there are at most $\exp(2(6n)^{3n})$ $n+1$ -tuples $(k, \zeta_1, \dots, \zeta_n)$ such that $(x_1, \dots, x_n) := (\zeta_1(a_1)^k, \dots, \zeta_n(a_1)^k)$ is a nondegenerate solution. On the other hand, if we have a degenerate solution $(x_1, \dots, x_n) := (\zeta_1(a_1)^k, \dots, \zeta_n(a_1)^k)$, then by removing a maximal set T of “bad” variables we get a necessarily nondegenerate solution $(x_s)_{s \in S} = (\zeta_s(a_s)^k)_{s \in S}$ of the corresponding equation in a smaller (but necessarily nonempty) set, say S , of variables. But again by the theorem, applied now to $\Gamma(S)$ and to the S -equation $\sum_{s \in S} \lambda_s x_s = 1$, this equation has at most $\exp(2(6\#S)^{3\#S}) \leq \exp(2(6n)^{3n})$ nondegenerate solutions. In other words, the $\#S + 1$ -tuple $(k, (\zeta_s)_{s \in S})$ is on a list of at most $\exp(2(6n)^{3n})$ items. Now consider the first entry, k , of each of these $S + 1$ -tuples. As there are at most $2^n - 1$ possible S , there are at most $(2^n - 1)\exp(2(6n)^{3n})$ first entries k , i.e., at most that many integers k for which there exists an n -tuple $(\zeta_1, \dots, \zeta_n)$ of roots of unity such that $(x_1, \dots, x_n) := (\zeta_1(a_1)^k, \dots, \zeta_n(a_1)^k)$ is a solution, possibly degenerate, of $\sum_{i=1}^n \lambda_i x_i = 1$. $\square$

Corollary 2.2. *Let K be an algebraically closed field of characteristic zero, $n \geq 1$ an integer, and $F \in GL(n, K)$ an $n \times n$ invertible matrix whose reversed characteristic polynomial $\det(1 - FT)$ has integer coefficients. Suppose that no eigenvalue of F is a root of unity. Define a sequence of integers $A(n)$ by*

$$A(n) := \text{Trace}(F^n), n \geq 1.$$

Then the nonzero $A(n)$ have $|A(n)| \rightarrow \infty$. More precisely, for any integer $M \geq 1$, there exists an integer $k_M \geq 1$ such that if $k > k_M$, then either $|A(k)| > M$ or $A(k) = 0$.

Proof. We apply part (3) of the theorem to $(a_1, \dots, a_n)$, the n eigenvalues of F , taken in some fixed order. For each of the $2M$ nonzero integers M_0 with $|M_0| \leq M$, there are at most $2^n \exp(2(6n)^{3n})$

integers k with $\text{Trace}(F^k) = M_0$. But for any integer $k \geq 0$, $A(k)$ is an integer, by the integrality assumption on the coefficients of the characteristic polynomial. So there are at most $2M \exp(2(6n)^{3n})$ integers $k \geq 0$ for which $0 < |\text{Trace}(F^k)| \leq M$. Taking k_M to be the largest of these at most $2M \exp(2(6n)^{3n})$ integers, we get the assertion. $\square$

Here is another corollary, where we now apply part (2) of the theorem. As before, K is an algebraically closed field of characteristic zero, $n \geq 1$ an integer, and $F \in GL(n, K)$ an $n \times n$ invertible matrix whose reversed characteristic polynomial $P(T) := \det(1 - FT)$ has integer coefficients. Given an integer $k \geq 1$, we say that an element $G \in GL(n, K)$ is an “integral form” of F^k if the following two conditions hold.

- (1) The reversed characteristic polynomial $\det(1 - GT)$ has integer coefficients.
- (2) For some integer $d \geq 1$, we have $\det(1 - G^dT) = \det(1 - F^{dk}T)$.

Corollary 2.3. *Let K be an algebraically closed field of characteristic zero, $n \geq 1$ an integer, and $F \in GL(n, K)$ an $n \times n$ invertible matrix whose reversed characteristic polynomial $\det(1 - FT)$ has integer coefficients. Suppose that no eigenvalue of F is a root of unity. Then for any integer $M \geq 1$, there exists an integer $k_M \geq 1$ such that for $k > k_M$, and for any integral form G of F^k , either $\text{Trace}(G) = 0$ or $|\text{Trace}(G)| > M$.*

Proof. Apply part (2) of the theorem to $(a_1, \dots, a_n)$, the n eigenvalues of F , taken in some fixed order. $\square$

We now give some applications to varieties over finite fields, and to isotrivial families of such varieties. We begin with the case of curves over finite fields.

Theorem 2.4. *Let $X/\mathbb{F}_q$ be a proper, smooth, geometrically connected curve over a finite field $\mathbb{F}_q$ of characteristic $p > 0$. Define a sequence of integers $A(n)$, $n \geq 1$ by*

$$\#X(\mathbb{F}_{q^n}) = q^n + 1 - A(n).$$

Then the nonzero $A(n)$ have $|A(n)| \rightarrow \infty$.

Proof. This is the first corollary above, applied with K taken to be $\overline{\mathbb{Q}_\ell}$ for some $\ell \neq p$ and with F taken to be the action of the geometric Frobenius $\text{Frob}_{\mathbb{F}_q}$ on $H_{\text{et}}^1(X \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}, \overline{\mathbb{Q}_\ell})$. By the Lefschetz trace formula [Gr-Rat], we have $A(n) = \text{Trace}(F^n)$. By Weil [W, page 71], the eigenvalues of F all have archimedean absolute value $q^{1/2}$, so are not roots of unity. $\square$

Corollary 2.5. *Let $X/\mathbb{F}_q$ be a proper, smooth, geometrically connected curve over a finite field $\mathbb{F}_q$ of characteristic $p > 0$. Suppose that one of the following conditions holds.*

- (1) *The genus $g = 1$, and $X/\mathbb{F}_q$ is ordinary.*
- (2) *The genus g of X is prime to p , and the q 'th power map on $H^1(X, \mathcal{O}_X)$ is the identity, i.e., the Hasse-Witt matrix relative to $\mathbb{F}_q$ is the identity $g \times g$ matrix over $\mathbb{F}_q$, i.e., there are p^g points of order dividing p in the group $\text{Jac}(X)(\mathbb{F}_q)$ of rational points on the Jacobian.*
- (3) *For some integer $N \geq 1$ which is prime to p and modulo which $2g$ is nonzero, there are N^{2g} points of order dividing N in $\text{Jac}(X)(\mathbb{F}_q)$.*

Then for all $n \geq 1$, we have $A(n) \neq 0$, and (hence) $|A(n)| \rightarrow \infty$.

Proof. In case (1), each $A(n), n \geq 1$ is prime to p , so nonzero. In case (2), the congruence formula [SGA 7 II, XXII 3.1] shows that for $n \geq 1$, we have $A(n) \equiv g \pmod{p}$, so again $A(n) \neq 0$. In case (3), we have $A(n) \equiv 2g \pmod{N}$ for all $n \geq 1$, so again $A(n) \neq 0$. $\square$

We get similar results for complete intersections over finite fields.

Theorem 2.6. *Let $X/\mathbb{F}_q$ be a proper, smooth, geometrically connected complete intersection of dimension $d \geq 1$ over a finite field $\mathbb{F}_q$ of characteristic $p > 0$. Define a sequence of integers $A(n), n \geq 1$ by*

$$\#X(\mathbb{F}_{q^n}) = \sum_{i=0}^d q^{ni} + (-1)^d A(n).$$

Then the nonzero $A(n)$ have $|A(n)| \rightarrow \infty$.

Proof. This is the first corollary above, applied with K taken to be $\overline{\mathbb{Q}_\ell}$ for some $\ell \neq p$ and with F taken to be the action of the geometric Frobenius $\text{Frob}_{\mathbb{F}_q}$ on $\text{Prim}_{\text{et}}^d(X \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}, \overline{\mathbb{Q}_\ell})$. By the Lefschetz trace formula [Gr-Rat] and the known cohomological structure of complete intersections [SGA 7 II, XI, 1.6], we have $A(n) = \text{Trace}(F^n)$. By Deligne [De-Weil I], the eigenvalues of F all have archimedean absolute value $q^{d/2}$, so are not roots of unity. $\square$

Corollary 2.7. *Let $X/\mathbb{F}_q$ be a proper, smooth, geometrically connected complete intersection of dimension $d \geq 1$ over a finite field $\mathbb{F}_q$ of characteristic $p > 0$. Suppose that $g := \dim H^d(X, \mathcal{O}_X)$ is prime to p , and that the q 'th power map on $H^d(X, \mathcal{O}_X)$ is the identity. Then for all $n \geq 1$, we have $A(n) \neq 0$, and (hence) $|A(n)| \rightarrow \infty$.*

Proof. Again by the congruence formula [SGA 7 II, XXII 3.1], for $n \geq 1$, we have $A(n) \equiv g \pmod{p}$, so again $A(n) \neq 0$. $\square$

Here is a variant of the last result, when the geometric genus is one.

Corollary 2.8. *Let $X/\mathbb{F}_q$ be a proper, smooth, geometrically connected complete intersection of dimension $d \geq 1$ over a finite field $\mathbb{F}_q$ of characteristic $p > 0$. Suppose that $\dim H^d(X, \mathcal{O}_X) = 1$, and that the q 'th power map on $H^d(X, \mathcal{O}_X)$ is nonzero, say is multiplication by $a(1) \in \mathbb{F}_q^\times$. Then for all $n \geq 1$, $A(n)$ is prime to p , so $\neq 0$, and (hence) $|A(n)| \rightarrow \infty$.*

Proof. Again by the congruence formula [SGA 7 II, XXII 3.1], for $n \geq 1$, we have $A(n) \equiv a^n \pmod{p}$, hence for all n we have $A(n) \neq 0$. $\square$

We now turn to isotrivial families, and apply Corollary 2.3 above.

Theorem 2.9. *Let F_q be a finite field of characteristic $p > 0$, $S/\mathbb{F}_q$ a smooth, geometrically connected F_q -scheme of finite type with $S(\mathbb{F}_q)$ nonempty, and $\pi : X \rightarrow S$ a proper smooth morphism of relative dimension $d \geq 1$, all of whose geometric fibres are curves or, if $d \geq 2$, complete intersections. Suppose the morphism π is isotrivial, in the sense pulled back to a finite étale S -scheme T/S , it becomes constant. For each closed point $\mathcal{P}$ of S , consider the fibre $X_{\mathbb{F}_{\mathcal{P}}} := X \otimes_{\mathcal{O}_S} \mathbb{F}_{\mathcal{P}}/\mathbb{F}_{\mathcal{P}}$, and define the integer $A_{\mathcal{P}}$ by*

$$\#X_{\mathbb{F}_{\mathcal{P}}}(\mathbb{F}_{\mathcal{P}}) = \sum_{i=0}^d N(\mathcal{P})^i + (-1)^d A_{\mathcal{P}}.$$

Then the nonzero $A_{\mathcal{P}}$ have $|A_{\mathcal{P}}| \rightarrow \infty$ as $\deg(\mathcal{P}) \rightarrow \infty$. More precisely, for any integer $M \geq 1$, there exists an integer $k_M \geq 1$ such that for any $k > k_M$, and for any closed point $\mathcal{P}$ with $\deg(\mathcal{P}) = k$, either $A_{\mathcal{P}} = 0$ or $|A_{\mathcal{P}}| > M$.

Proof. We choose a point $s_0 \in S(\mathbb{F}_q)$, and denote by $X_0/\mathbb{F}_q$ the fibre of X/S over s_0 . We choose a prime $\ell \neq p$, and take for F the action of geometric $\text{Frob}_{\mathbb{F}_q}$ on $\text{Prim}_{\text{et}}^d(X_0 \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}, \overline{\mathbb{Q}_\ell})$. By the isotriviality of X/S , for any closed point $\mathcal{P}$ of S , the fibre $X_{\mathbb{F}_{\mathcal{P}}}$ becomes isomorphic to $X_0 \otimes \mathbb{F}_{\mathcal{P}}$ after extension of scalars to some finite extension of $\mathbb{F}_{\mathcal{P}}$. Therefore the geometric Frobenius $\text{Frob}_{\mathcal{P}}$ acting on $\text{Prim}_{\text{et}}^d(X_{\mathbb{F}_{\mathcal{P}}} \otimes_{\mathbb{F}_{\mathcal{P}}} \overline{\mathbb{F}_{\mathcal{P}}}, \overline{\mathbb{Q}_\ell})$ ($:= H^1$, if $d = 1$) is an integral form of $F^{\deg(\mathcal{P})}$. So the assertion results from Corollary 2.3 above. $\square$

Corollary 2.10. *If X/S as above is an isotrivial family of elliptic curves which are ordinary, i.e., if the constant j -invariant is ordinary, then all $A_{\mathcal{P}}$ are nonzero (because prime to p), and (hence) $|A_{\mathcal{P}}| \rightarrow \infty$ as $\deg(\mathcal{P}) \rightarrow \infty$.*

3. LOWER BOUNDS FOR TRACES, VIA THE EVERTSE-SCHLICHEWEI-SCHMIDT SUBSPACE THEOREM

We first reformulate [ESS, Thm. 1.1] in a "homogeneous" version.

Theorem 3.1. ([ESS, Thm. 1.1]) *Fix an algebraically closed field K of characteristic zero. Fix an integer $n \geq 1$, and n numbers $a_1, \dots, a_n$ in $K^\times$, such that for $i \neq j$, a_i/a_j is not a root of unity. Let $H \subset K^n$ be a hyperplane, say of equation $\sum_i \lambda_i X_i = 0$ for some n -tuple $(\lambda_1, \dots, \lambda_n) \in K^n$ with at least one nonzero λ_i . There are at most $F(n) := 2^{n-1} \exp(2(6(n-1))^{3(n-1)})$ integers d for which the vector*

$$v_d := (a_1^d, \dots, a_n^d)$$

lies in H .

Proof. As $F(n)$ is an increasing function of $n \geq 1$, we reduce immediately to the case where all the λ_i are nonzero. [Indeed, we may renumber so that the first $r \geq 1$ of the λ_i are nonzero, and the rest vanish. We then have a situation in r variables, with $(a_1, \dots, a_r)$ and $(\lambda_1, \dots, \lambda_r)$, where all the λ_i are nonzero.] If $n = 1$, there are no such d , simply because both $a_1 \neq 0$ and $\lambda_1 \neq 0$. For $n \geq 2$, we rewrite the equation

$$\sum_{i=1}^n \lambda_i a_i^d = 0$$

as

$$\sum_{i=1}^{n-1} (-\lambda_i/\lambda_n) (a_i/a_n)^d = 1.$$

No component of the $n-1$ -tuple $(a_1/a_n, \dots, a_{n-1}/a_n)$ is a root of unity, and all the λ_i/λ_n are nonzero, so the assertion is the $n-1$ case of Theorem 2.1, part 1. $\square$

Fix an integer $Q > 1$. In practice, Q will be a prime power p^w , but right now that is not important. An algebraic number $\alpha \in \overline{\mathbb{Q}}$ is called a Q -Weil number if, for every embedding $\iota : \overline{\mathbb{Q}} \subset \mathbb{C}$, we have $|\iota(\alpha)|_{\mathbb{C}} = Q^{1/2}$, for $|\cdot|_{\mathbb{C}}$ the usual complex absolute value $|x + iy|_{\mathbb{C}} := (x^2 + y^2)^{1/2}$. A Q -Weil number is called integral if in addition it is an algebraic integer. If $\alpha_1, \dots, \alpha_n$ are Q -Weil numbers, then the field $K := \mathbb{Q}(\alpha_1, \dots, \alpha_n)$ is either a totally real field or a CM field, since all possible "complex conjugations" in $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ agree on K , sending each α_i to Q/α_i .

For the reader's convenience, we recall some normalizations in the theory of heights. Let K be a number field, i.e., a finite extension of $\mathbb{Q}$. On $\mathbb{Q}$, for p either a prime or ∞ , we have the p -adic absolute value

$|\cdot|_p$, normalized by $|p|_p = 1/p$ if p is a prime, and by $|2|_\infty = 2$ if $p = \infty$. For each (finite or infinite) place v of K , the completion K_v is a finite extension of some $\mathbb{Q}_p$ (including $p = \infty$, with $\mathbb{Q}_\infty := \mathbb{R}$); we say that $v|p$. There is a unique absolute value $|\cdot|_v$ on K_v which on the subfield $\mathbb{Q}_p$ agrees with $|\cdot|_p$. We then *renormalize* these choices of absolute values on K by defining

$$||\cdot||_v := |\cdot|_v^{d(v)},$$

for $d(v)$ the rational number defined by

$$d(v) = \deg(K_v/\mathbb{Q}_p)/\deg(K/\mathbb{Q}).$$

[The reader should be warned that this $|\cdot|_v$ versus $||\cdot||_v$ notation is that of [E] and [ES], whereas in [BG] what we call $||\cdot||_v$ is called $|\cdot|_v$, and $||x||_v$ there is yet a third thing, the absolute value à la Weil, defined by the effect of multiplicative translation by x on (any chosen) Haar measure μ_v on the additive group K_v .] One important thing is that with these choices, we have the product formula; indeed for $x \in K^\times$ and any p , we have

$$\prod_{v|p} ||x||_v = |Norm_{K/\mathbb{Q}}(x)|_p^{1/\deg(K/\mathbb{Q})}.$$

Moreover, if L/K is any finite extension, then with these normalizations on places w of L as well, we have, for each place v of K , and each $x \in K^\times$,

$$\prod_{w|v} ||x||_w = ||x||_v.$$

Given an integer $n \geq 1$ and a nonzero n -tuple $x = (X_1, \dots, x_n) \in K^n$, we define, for each place v of K

$$||x||_v := \sup_i ||x_i||_v.$$

This is 1 for all but finitely many v , and we define

$$H(x) := \prod_v ||x||_v.$$

With these normalizations, we can define the height $H(x)$ of any n -tuple of algebraic numbers, by picking a number field $K/\mathbb{Q}$ containing them all and using the above definition; the resulting product is independent of this choice.

We now formulate the main technical result of this section.

Theorem 3.2. *Let $Q > 1$ and $n \geq 1$ be integers. Let $(\alpha_1, \dots, \alpha_n)$ be an n -tuple of integral Q -Weil numbers. Suppose that for $i \neq j$, the ratio*

α_i/α_j is not a root of unity. Let

$$L(X) := \sum_{i=1}^n \lambda_i X_i$$

be a nonzero linear form in n variables, with coefficients $\lambda_i \in \overline{\mathbb{Q}}$. Choose a number field K containing all the α_i , all the λ_i , and (for convenience) $\sqrt{-1}$. Fix an archimedean place v_0 of K . Fix a real number $\epsilon > 0$. Then for all but finitely many integers $d \geq 1$, we have the archimedean lower bound

$$\|L(\alpha_1^d, \dots, \alpha_n^d)\|_{v_0} \geq (\|\alpha_1^d\|_{v_0})^{1-\epsilon}.$$

Equivalently, given a complex embedding $\iota : K \subset \mathbb{C}$, we have, for all but finitely many integers $d \geq 1$, the lower bound

$$|\iota(L(\alpha_1^d, \dots, \alpha_n^d))|_{\mathbb{C}} \geq (Q^{d/2})^{1-\epsilon}.$$

Proof. We will use the absolute subspace theorem as stated in [BG, Cor. 7.2.5], but see [?][E] for explicit bounds. Let us briefly recall its statement. Thus K is a number field, S is a finite set of places of K including all the archimedean ones, and for each place $s \in S$ we are given n linearly independent linear forms in n variables, $L_{i,s}$, for $i = 1, \dots, n$, all with coefficients in K . We are also given a real number $\epsilon > 0$. Then there are finitely many hyperplanes $H_t \subset K^n$ such that any nonzero n -tuple $x \in \mathcal{O}_{S,K}^n$ of S -integers ($:=$ integers outside of S) of K satisfying the inequality

$$\prod_{s \in S} \prod_{i=1}^n \|L_{i,s}(x)\|_s < H(x)^{-\epsilon}$$

lies in one of these finitely many hyperplanes H_t .

To apply this, consider the vectors $v_d := (\alpha_1^d, \dots, \alpha_n^d)$. We claim that for $d \geq 1$, we have

$$H(v_d) \leq Q^{d/2}$$

. Indeed, since the α_i are algebraic integers, we have $\|v_d\|_v \leq 1$ for all nonarchimedean v . At each archimedean v , we have

$$\|v_d\|_v = \|\alpha_1^d\|_v = (Q^{d/2})^{2/\deg(K/\mathbb{Q})},$$

the first equality because all the α_i are Q -Weil numbers, and the second because all the archimedean places of K are complex (because we chose K to contain $\sqrt{-1}$). There are $\deg(K/\mathbb{Q})/2$ archimedean v , so we get

$$H(v_d) := \prod_{\text{all } v} \|v_d\|_v \leq \prod_{v|\infty} \|v_d\|_v = Q^{d/2}.$$

Combining the last two inequalities, and taking the chosen archimedean place v_0 , we get

$$H(v_d) \leq (\|v_d\|_{v_0})^N,$$

for the fixed constant

$$N := \deg(K/\mathbb{Q})/2.$$

So for any real $\epsilon > 0$, we have

$$(\|v_d\|_{v_0})^{-\epsilon} \leq H(v_d)^{-\epsilon/N}.$$

Now take for S the following set of places: all archimedean places, and all places over primes p which divide Q . We now specify which linear forms to take at these places. At places $s \in S$ other than the chosen archimedean place v_0 , take the n forms $L_{i,s}(X) := X_i$, for $i = 1, \dots, n$. At the chosen archimedean place v_0 , we must be a bit more careful. We have our given nonzero linear form L , and after renumbering the variables we may assume that the first variable X_1 occurs in L . Then at v_0 we take for the n linearly independent forms $L_{1,v_0} := L$ and $L_{i,v_0} := X_i$ for $i = 2, \dots, n$.

Observe that for $d \geq 1$ we have the identity

$$\prod_{s \in S} \prod_{i=1}^n \|L_{i,s}(v_d)\|_s = \|L(v_d)\|_{v_0} / \|\alpha_1^d\|_{v_0}.$$

Indeed, the ratio of the two sides is

$$\prod_{s \in S} \prod_i \|\alpha_i^d\|_s = \prod_i \left(\prod_{s \in S} \|\alpha_i^d\|_s \right).$$

As each α_i is a unit outside of S , this last expression is identically 1, by the product formula.

Now suppose that $d \geq 1$ is such that

$$L(v_d) < (\|\alpha_1^d\|_{v_0})^{1-\epsilon}.$$

Then

$$\prod_{s \in S} \prod_{i=1}^n \|L_{i,s}(v_d)\|_s = \|L(v_d)\|_{v_0} / \|\alpha_1^d\|_{v_0} < (\|\alpha_1^d\|_{v_0})^{-\epsilon} \leq H(v_d)^{-\epsilon/N}.$$

So by the subspace theorem, applied with this S and with ϵ/N , there exist finitely many hyperplanes $H_t \subset K^n$ such any vector v_d with

$$L(v_d) < (\|\alpha_1^d\|_{v_0})^{1-\epsilon}$$

lies in one of the finitely many hyperplanes H_t . By Theorem 3.1, any given hyperplane contains only finite many vectors v_d with $d \geq 1$. $\square$

We now apply this result to the traces of iterates.

Theorem 3.3. *Let $Q > 1$ and $n \geq 1$ be integers. Let $(\alpha_1, \dots, \alpha_n)$ be an n -tuple of integral Q -Weil numbers. Choose a number field K containing all the α_i . Fix a complex embedding $\iota : K \subset \mathbb{C}$, and a real number $\epsilon > 0$. Denote by D the order of the finite subgroup of $K^\times$ generated by all those roots of unity which can be written as α_i/α_j for some choice of i, j . For each integer $d \geq 1$, denote by $S(k)$ the sum*

$$S(k) := \sum_{i=1}^n \alpha_i^k.$$

For a fixed integer $0 \leq d < D$, consider the sums $S(d+kD)$ for variable integers $k \geq 1$. Then we have the following results.

- (1) *For a fixed integer $0 \leq d < D$, consider the sums $S(d+kD)$ for variable integers $k \geq 1$. Either $S(d+kD) = 0$ for all $k \geq 1$, or for all but finitely many integers $k \geq 1$, we have the archimedean lower bound*

$$|\iota S(d+kD)|_{\mathbb{C}} \geq (Q^{(d+kD)/2})^{1-\epsilon}.$$

- (2) *Suppose that any of the three following conditions holds.*
 - (a) $D = 1$.
 - (b) *For some α_{i_0} , no ratio α_{i_0}/α_j is a nontrivial root of unity.*
 - (c) *For some absolute value $\|\cdot\|_v$ on K , and for some real number r , there is a unique index i_0 such that $\|\alpha_{i_0}\|_v = r$.**Then $S(k)$ is nonzero for all but finitely many k , and hence for all k sufficiently large we have*

$$|\iota S(k)|_{\mathbb{C}} \geq (Q^{k/2})^{1-\epsilon}.$$

Proof. We first treat the case where, for all $i \neq j$, the ratio α_i/α_j is not a root of unity. Then we have $D = 1$, and we have only to apply the previous theorem, with the linear form there taken to be $L(X) := \sum_{i=1}^n X_i$. Consider next the most general case in which $D = 1$, i.e., the case in which for $i \neq j$, either α_i/α_j is not a root of unity, or $\alpha_i = \alpha_j$. In this case, we renumber so that $\alpha_1, \dots, \alpha_r$ are the distinct α 's which occur, with α_i occurring with multiplicity n_i . In this case, we apply the previous theorem to $(\alpha_1, \dots, \alpha_r)$ and to the linear form $L(X) := \sum_{i=1}^r n_i X_i$. So we have established asserted implication (2a) of the theorem.

Now let us consider the general case. Partition the α 's into equivalence classes according to the equivalence relation $a \equiv b$ if and only if b/a is a root of unity. Renumbering, we may assume that $\alpha_1, \dots, \alpha_r$ are representatives of these equivalence classes, and that the class of α_i consists of $\zeta_{i,j} \alpha_i$, for $j = 1, \dots, n_i$, where each $\zeta_{i,j}$ is some D 'th root of

unity. Then for a fixed integer $0 \leq d < D$, and any integer $k \geq 1$, we have the identity

$$S(d + kD) = \sum_{i=1}^r \left(\sum_{j=1}^{n_i} \zeta_{i,j}^d \right) \alpha_i^{d+kD}.$$

It may happen that for a given integer $0 \leq d < D$, all the coefficients $B(i, d) := \sum_{j=1}^{n_i} \zeta_{i,j}^d$ for $i = 1, \dots, r$ vanish. In this case, there is nothing to be done, all the sums $S(d + kD)$ vanish. If, on the other hand, for a given integer $0 \leq d < D$, at least one of these coefficients $B(i, d)$ is nonzero, then we have only to apply the previous theorem to $(\alpha_1, \dots, \alpha_r)$ and the nonzero linear form

$$L(X) := \sum_{i=1}^r B(i, d) X_i,$$

and then restrict attention to the arithmetic progression $\{d + kD\}_{k \geq 1}$ in question.

This concludes the proof of assertion (1). We have already proven (2a). If (2b) holds, then the α 's in the equivalence class of α_{i_0} are just repeats of α_{i_0} , say n_{i_0} times. Renumbering, we may assume that the index i_0 is one of the chosen indices, i.e., that $1 \leq i_0 \leq r$. Then for any given integer $0 \leq d < D$, the linear form

$$L(X) := \sum_{i=1}^r \left(\sum_{j=1}^{n_i} \zeta_{i,j}^d \right) X_i,$$

is nonzero, because the coefficient $B(i_0, d)$ of X_{i_0} is the integer n_{i_0} . Finally, if (2c) holds, then the equivalence class of α_{i_0} is a singleton, so we have a special case of (2b). $\square$

4. APPLICATION TO VARIETIES AND EXPONENTIAL SUMS OVER FINITE FIELDS

We begin with the qualitative version of the unboundedness results established in section 2.

Theorem 4.1. *Let $X/\mathbb{F}_q$ be a proper smooth variety over $\mathbb{F}_q$. Fix an integer $i \geq 1$, and a prime $\ell \neq p$. Consider the sequence of integers $A_i(n)$, $n \geq 1$, (independent of the auxiliary choice of ℓ , cf. [De-Weil II, 3.3.9]) defined as*

$$A_i(n) := \text{Trace}(\text{Frob}_q^n | H_{\text{et}}^i(X \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}, \mathbb{Q}_\ell)).$$

Fix a real number $\epsilon > 0$. Then for all sufficiently large n , either $A_i(n) = 0$ or

$$|A_i(n)| \geq (q^{id/2})^{1-\epsilon}.$$

Moreover, the set of $n \geq 1$ for which $A_i(n) = 0$ is the union of a finite set and of at most finitely many arithmetic progressions to some common modulus.

Proof. This is an immediate consequence of Deligne's theorem [De-Weil II, 3.3.9], by applying Theorem 3.3 to the eigenvalues of $Frob_q$ on H^i , which are integral q^i -Weil numbers. $\square$

We now turn to the situation with pure exponential sums. In nearly all examples, the situation is the following. We are given an *affine* smooth, geometrically connected variety $U/\mathbb{F}_q$ of some dimension $d \geq 1$, a prime number $\ell \neq p$, and a lisse $\overline{\mathbb{Q}}_\ell$ -sheaf $\mathcal{F}$ on U which is integral (all local Frobenii have algebraic integer eigenvalues) and pure of some integer weight $w_0 \geq 0$. We have somehow proven that for all i , the "forget supports" map

$$H_c^i(U \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q, \mathcal{F}) \rightarrow H^i(U \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q, \mathcal{F})$$

is an isomorphism. It then follows, cf. [De-Weil II, 3.3.6] and [Se], that $H^i = 0$ for $i \neq d$, and that, putting

$$w := d + w_0,$$

the Frobenius eigenvalues on H_c^d are integral q^w -Weil numbers. The sequence of algebraic integers

$$A(n) := \text{Trace}(Frob_q^n | H_c^d(U \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q, \mathcal{F}))$$

is the sequence of exponential sums, over bigger and bigger finite extensions of $\mathbb{F}_q$, that we are interested in.

So in any such situation, Theorem 3.3 assures us that for any chosen embedding ι of $\mathbb{Q}$ (the eigenvalues of $Frob_q$) into $\mathbb{C}$, and any chosen real number $\epsilon > 0$, we have that for all n sufficiently large, either $A(n) = 0$ or $|\iota A(n)|_{\mathbb{C}} \geq (q^{nw/2})^{1-\epsilon}$.

It is consequently of some interest to know in what situations of this type we know in addition that $A(n) \neq 0$ for n large. Here are three such situations, where in fact $A(n) \neq 0$ for all $n \geq 1$.

- (1) The d variable Kloosterman sums $Kl_d(\psi, a, \mathbb{F}_q)$, for $d \geq 2$, ψ a nontrivial additive character of $\mathbb{F}_q$, and $a \in \mathbb{F}_q^\times$, defined by

$$Kl_d(\psi, a, \mathbb{F}_q) := \sum_{x_1 x_2 \dots x_d = a, \text{ all } x_i \in \mathbb{F}_q} \psi\left(\sum_i x_i\right).$$

Here only the H_c^{d-1} is nonzero, and the d Frobenius eigenvalues are integral q^{d-1} -Weil numbers. This sum lies in $\mathbb{Z}[\zeta_p]$ and never vanishes, because mod the unique prime $\mathcal{P}$ lying over p , we have $Kl_d(a, \mathbb{F}_q) \equiv (q-1)^{d-1} \equiv (-1)^{d-1}$ (simply because ψ is trivial mod $\mathcal{P}$). Here the sequence of $A(n)$ is

$$A(n) = (-1)^{d-1} Kl_d(\psi \circ \text{Trace}_{\mathbb{F}_{q^n}/\mathbb{F}_q}, a, \mathbb{F}_{q^n}).$$

So in addition to Deligne's bound [De-ST, 7.1.3, 7.4], that for any complex embedding of $\mathbb{Z}[\zeta_p]$

$$|Kl_d(\psi \circ \text{Trace}_{\mathbb{F}_{q^n}/\mathbb{F}_q}, a, \mathbb{F}_{q^n})| \leq dq^{n(d-1)/2},$$

for any given real $\epsilon > 0$ we have the lower bound

$$|Kl_d(\psi \circ \text{Trace}_{\mathbb{F}_{q^n}/\mathbb{F}_q}, a, \mathbb{F}_{q^n})| \geq (q^{n(d-1)/2})^{1-\epsilon}$$

for all n sufficiently large.

- (2) Here we start with the projective line $\mathbb{P}^1/\mathbb{F}_q$ and remove a nonempty set S of $\mathbb{F}_q$ -rational points, with $\#S - 1$ invertible mod p . We take $U := \mathbb{P} \setminus S$. On U , we take a regular function $f \in H^0(U, \mathcal{O}_U)$ whose pole orders e_s at the points $s \in S$ are all prime to p . For ψ a nontrivial additive character of $\mathbb{F}_q$, we have the sum

$$S(\psi, f, \mathbb{F}_q) := \sum_{u \in U(\mathbb{F}_q)} \psi(f(u)).$$

Here only the H_c^1 is nonzero, and the $\#S - 2 + \sum_{s \in S} e_s$ Frobenius eigenvalues are integral q -Weil numbers. This sum lies in $\mathbb{Z}[\zeta_p]$ and never vanishes, because mod the unique prime $\mathcal{P}$ lying over p , it is congruent to $q + 1 - \#S \equiv 1 - \#S$, again because ψ is trivial mod $\mathcal{P}$ and we assumed $\#S - 1$ to be invertible mod p . The sequence $A(n)$ in this case is

$$A(n) = -S(\psi \circ \text{Trace}_{\mathbb{F}_{q^n}/\mathbb{F}_q}, f, \mathbb{F}_{q^n}).$$

So in addition to the Weil bound [W2], that for any complex embedding of $\mathbb{Z}[\zeta_p]$

$$|S(\psi \circ \text{Trace}_{\mathbb{F}_{q^n}/\mathbb{F}_q}, f, \mathbb{F}_{q^n})| \leq (\#S - 2 + \sum_{s \in S} e_s) q^{n/2},$$

for any given real $\epsilon > 0$ we have the lower bound

$$|S(\psi \circ \text{Trace}_{\mathbb{F}_{q^n}/\mathbb{F}_q}, f, \mathbb{F}_{q^n})| \geq (q^{n/2})^{1-\epsilon}$$

for all n sufficiently large.

- (3) Here we have a slight variant on example (2) above. Take for U the affine line $\mathbb{A}^1/\mathbb{F}_q$, $f \in \mathbb{F}_q[X]$ a polynomial of degree $d \geq 1$. Under the hypothesis that

$$p \equiv 1 \pmod{d},$$

Sperber [Sp, 3.11] tells us that the $d-1$ Frobenius eigenvalues on H_c^1 have all distinct $\mathcal{P}$ -adic valuations at any prime lying over p ; their $\mathcal{P}$ -adic ordinals, normalized so that q has $\text{ord}_{\mathcal{P}}(q) = 1$, are $1/d, 2/d, \dots, (d-1)/d$. Here the $A(n)$ are

$$A(n) = -S(\psi \circ \text{Trace}_{\mathbb{F}_{q^n}/\mathbb{F}_q}, f, \mathbb{F}_{q^n}),$$

they never vanish, and we have the same conclusion as in (2) above.

5. APPENDIX: APPLICATIONS OF BAKER-WÜSTHOLZ,

In some cases there are only two Frobenius eigenvalues, they are complex conjugates of each other, and their ratio is *not* a root of unity. These cases include an ordinary elliptic curve over $\mathbb{F}_q$, and also the classical Kloosterman sums, denoted $Kl_2(\psi, a, \mathbb{F}_q)$ in the previous section. In both of these cases, the two Frobenius eigenvalues are integral q -Weil numbers, say α and $\bar{\alpha}$, with $\alpha\bar{\alpha} = q$. After we fix a complex embedding, we can write the two eigenvalues as $q^{1/2}e^{\pm i\theta}$ for a unique $\theta \in [0, \pi]$. Then the $A(n)$ are given by

$$A(n) := \alpha^n + \bar{\alpha}^n = 2q^{n/2} \cos(n\theta).$$

Here is the key technical result, an immediate application of the Baker-Wüstholz, theorem [BW].

Theorem 5.1. *Let $\theta \in [0, \pi]$. Suppose that $e^{2i\theta}$ is not a root of unity, but is an algebraic number, algebraic of degree d over $\mathbb{Q}$. Define the real constant*

$$C(N, d) := 18(N+1)!N^{N+1}(32d)^{N+2} \log(2Nd).$$

Define

$$h'(e^{2i\theta}) := \text{Max}(\log(H(1, e^{2i\theta})), \theta/d, 1/d),$$

$$h'(-1) := \pi/d.$$

Then for any integer $n \geq 1$ and any integer k , we have the inequality

$$\log(|2n\theta - k\pi|) > -C(2, d)h'(e^{2i\theta})h'(-1) \log(2n).$$

Proof. Fix $n \geq 1$. Since $\theta \in [0, \pi]$, we have $2n\theta \in [0, 2n\pi]$. So the closest approach of $n\theta$ to an integer multiple of π occurs for some $k \in [0, 2n]$. [Indeed, for any integer k outside this interval, we trivially have $|2n\theta - k\pi| \geq \pi$, and $\log(\pi) > 0$.] Because $e^{2i\theta}$ is not a root of unity, $\log(e^{2i\theta}) = 2i\theta$ and $\log(-1) = i\pi$ are linearly independent over $\mathbb{Q}$. Now apply the Baker-Wüstholz theorem, to the $N = 2$ algebraic numbers $e^{2i\theta}$ and -1 , and to each of the linear forms $nX_1 - kX_2$ for $k = 0, 1, \dots, 2n$ in their logarithms. $\square$

Corollary 5.2. *Let $\theta \in [0, \pi]$ be as in the theorem. Given a real number $q > 1$, define the real constant*

$$c = c(\theta, q) := C(2, d)h'(e^{2i\theta})h'(-1)/\log(q).$$

Then for all integers $n \geq 1$, we have the estimates

$$\begin{aligned} |\cos(n\theta)| &\geq (1/\pi)q^{-c\log(2n)}, \\ |q^{n/2} \cos(n\theta)| &\geq (1/\pi)q^{n/2 - c\log(2n)}. \end{aligned}$$

Proof. Fix $n \geq 1$. By the theorem, for any integer k , we have the inequality

$$|2n\theta - k\pi| \geq q^{-c\log(2n)}.$$

So we have the inequality

$$|n\theta - k\pi/2| \geq q^{-c\log(2n)}/2.$$

For k an odd integer, $\cos(k\pi/2) = 0$ and $\sin(k\pi/2) = \pm 1$, so we have the trigonometric identity $\cos(n\theta) = \pm \sin(n\theta - k\pi/2)$. For the odd integer k_0 which minimizes $|n\theta - k\pi/2|$, we have

$$0 < |n\theta - k_0\pi/2| < \pi/2.$$

But for real x with $|x| \leq \pi/2$, we have the inequality

$$|\sin(x)| \geq (2/\pi)|x|.$$

Thus we find

$$|\cos(n\theta)| = |\sin(n\theta - k_0\pi/2)| \geq (2/\pi)|n\theta - k_0\pi/2| \geq q^{-c\log(2n)}/\pi.$$

$\square$

Let us make this explicit in the two cases of ordinary elliptic curves and of classical Kloosterman sums.

Corollary 5.3. *(1) Given an ordinary elliptic curve over $\mathbb{F}_q$, the sequence of its $A(n)$ has, for all $n \geq 1$, the archimedean lower bound*

$$|A(n)| \geq (1/\pi)q^{n/2 - 2^{39}\log(2n)}.$$

(2) Given a classical Kloosterman sum $Kl_2(\psi, a, \mathbb{F}_q)$ over $\mathbb{F}_q$, denote by p the characteristic of $\mathbb{F}_q$. If $p = 2$ or $p = 3$, the sequence of its $A(n)$ has, for all $n \geq 1$, the same archimedean lower bound as for ordinary elliptic curves,

$$|A(n)| \geq (1/\pi)q^{n/2-2^{39}\log(2n)}.$$

If $p \geq 5$, the sequence of its $A(n)$ has, for all $n \geq 1$, the archimedean lower bound

$$|A(n)| \geq (1/\pi)q^{n/2-c_p \log(2n)},$$

with c_p the constant

$$c_p := 18.3!.2^3.(32(p-1))^4.\log(4(p-1)).(5\pi/4).$$

Proof. We will compute, in the two cases, an explicit upper bound for the constant c of the previous corollary. Denote by α and $\bar{\alpha}$ the two Frobenius eigenvalues. After possibly interchanging them, we have $\alpha/\bar{\alpha} = e^{2i\theta}$. Thus

$$H(1, e^{2i\theta}) = H(\alpha, \bar{\alpha}) \leq q^{1/2},$$

simply because α and $\bar{\alpha}$ are integral q -Weil numbers.

In the case of an ordinary elliptic curve, α and $\bar{\alpha}$ lie in a quadratic imaginary field, and their ratio is irrational, so we have $d = 2$ in this case. Then

$$\begin{aligned} h'(e^{2i\theta}) &:= \text{Max}(\log(H(1, e^{2i\theta})), \theta/d, 1/d) \\ &= \text{Max}(\log(q)/2, \pi/2, 1/2) \leq 5 \log(q)/2, \end{aligned}$$

the factor 5 to take care of the worst case $q = 2$. So the constant c of the previous corollary is bounded by

$$c \leq C(2, 2)(5/2)(\pi/2) = 18.3!.2^3.(64)^4.\log(8).(5\pi/4) \leq 2^{39}.$$

In the case of a classical Kloosterman sum, the sum itself lies in $\mathbb{Q}(\zeta_p)^+$, the real subfield of $\mathbb{Q}(\zeta_p)$, and α and $\bar{\alpha}$ lie in a CM quadratic extension. Again their ratio is irrational (otherwise it would be a rational number of absolute value one, so ± 1), so in this case we have $2 \leq d \leq \text{Max}(p-1, 2)$. So again we have

$$h'(e^{2i\theta}) \leq 5 \log(q)/2.$$

For $p = 2$ and $p = 3$, we have $d = 2$, so again the bound

$$c \leq 2^{39}.$$

For $p \geq 5$, the bounds becomes worse, namely

$$c \leq C(2, p-1)(5\pi/4) = 18.3!.2^3.(32(p-1))^4.\log(4(p-1)).(5\pi/4).$$

□

REFERENCES

- [BG] Bombieri, E., Gubler, W., Heights in Diophantine geometry. New Mathematical Monographs, 4. Cambridge University Press, Cambridge, 2006.
- [BW] Baker, A., Wüstholz, G., Logarithmic forms and group varieties. J. Reine Angew. Math. 442 (1993), 19-62.
- [De-ST] Deligne, P., Applications de la formule des traces aux sommes trigonométriques, pp. 168-232 in SGA 4 1/2, cited below.
- [De-Weil I] Deligne, P., La conjecture de Weil. Publ. Math. IHES 43 (1974), 273-307.
- [De-Weil II] Deligne, P., La conjecture de Weil II. Publ. Math. IHES 52 (1981), 313-428.
- [E] Evertse, J.-H., An improvement of the quantitative subspace theorem. Compositio Math. 101 (1996), no. 3, 225-311.
- [ES] Evertse, J.-H., Schlickewei, H. P., A quantitative version of the absolute subspace theorem. J. Reine Angew. Math. 548 (2002), 2-127.
- [ESS] Evertse, J.-H., Schlickewei, P., Schmidt, W.M., Linear equations in variables which lie in a multiplicative group. Ann. Math. 155 (2002), 807-836.
- [Gr-Rat] Grothendieck, A., Formule de Lefschetz et rationalité des fonctions L . Séminaire Bourbaki, Vol. 9, Exp. No. 279, 41-55, Soc. Math. France, 1995.
- [Se] Serre, J.-P., Majorations de sommes exponentielles. (French) Journées Arithmétiques de Caen (Univ. Caen, Caen, 1976), pp. 111-126. Asterisque No. 41-42, Soc. Math. France, Paris, 1977.
- [SGA 4 1/2] Cohomologie Etale. Séminaire de Géométrie Algébrique du Bois Marie SGA 4 1/2. par P. Deligne, avec la collaboration de J. F. Boutot, A. Grothendieck, L. Illusie, et J. L. Verdier. Lecture Notes in Mathematics, Vol. 569, Springer-Verlag, 1977.
- [SGA 7 II] Groupes de Monodromie en Géométrie Algébrique. Séminaire de Géométrie Algébrique du Bois Marie SGA 7 II. par P. Deligne et N. Katz. Lecture Notes in Mathematics, Vol. 340, Springer-Verlag, 1973.
- [Sp] Sperber, S., On the p -adic theory of exponential sums. Amer. J. Math. 108 (1986), no. 2, 255-296.
- [W] Weil, A., Variétés abéliennes et courbes algébriques. (French) Actualités Sci. Ind., no. 1064, Publ. Inst. Math. Univ. Strasbourg 8 (1946). Hermann & Cie., Paris, 1948. 165 pp.
- [W2] Weil, A., On some exponential sums. Proc. Nat. Acad. Sci. U. S. A. 34, (1948). 204-207.

I.A.S., PRINCETON UNIVERSITY

E-mail address: eb@ias.edu, nmk@math.princeton.edu