

# A NOTE ON LOWER BOUNDS FOR FROBENIUS TRACES

ENRICO BOMBIERI AND NICHOLAS M. KATZ

## I. INTRODUCTION

This paper grew out of the following question. Given an ordinary elliptic curve  $E/\mathbb{F}_q$  over a finite field  $\mathbb{F}_q$  of characteristic  $p$ , 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 instead  $E/\mathbb{F}_q$  is ordinary, then all the  $A(n)$  are nonzero because they are all prime to  $p$ , so this vanishing problem at least disappears.

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  $|\text{Trace}(F^n)|$ ,  $n \geq 1$ , the nonzero terms tend to  $\infty$ .

The purpose of this note is to explain how classical results on recurrent sequences answer these questions. Because of the “culture gap” between the communities of those who know these classical results and those who are interested in traces of Frobenius, we have written this note so to make it accessible to members of both communities, at the risk that readers may find parts of this note overly detailed.

We will use three different methods to approach the problem. The Skolem–Mahler–Lech theorem on recurrent sequences is easy to prove and provides a “soft” answer, soft in the sense that it gives no estimate of the rate at which the nonzero terms tend to  $\infty$ . The other two methods lie much deeper. A theorem due independently to Evertse and to van der Poorten and Schlickewei, itself based on an improved version of Schmidt’s subspace theorem, gives such a rate, albeit ineffective in certain parameters. For elliptic curves (and some other two-dimensional sums, including classical Kloosterman sums), the Baker–Wüstholz theorem gives an even better rate, this time effective in all parameters.

The problem of obtaining effective lower bounds in the most general case remains unsolved and probably lies very deep.

It is a pleasure to thank Umberto Zannier for his helpful comments on an earlier version of this paper.

## II. UNBOUNDEDNESS, VIA SKOLEM'S METHOD

We begin by recalling the relevant version of the Skolem–Mahler–Lech theorem. For the convenience of the reader, we also recall its proof.

**THEOREM 2.1.** *Let  $K$  be an algebraically closed field of characteristic zero. Fix an integer  $n \geq 1$ ,  $n$  numbers  $a_1, \dots, a_n$  in  $K^\times$ , the “eigenvalues”, and  $n$  polynomials  $\lambda_1(x), \dots, \lambda_n(x)$  in  $K[x]$ , the “coefficients”, not all of which are zero. For each integer  $k \geq 1$ , define*

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

*Then we have the following results.*

- (i) *Suppose that no ratio  $\alpha_i/\alpha_j$ ,  $i \neq j$ , is a root of unity. Then there are only finitely many integers  $k \geq 1$  for which  $A(k) = 0$ .*
- (ii) *The integers  $k \geq 1$  for which  $A(k) = 0$  are the union of a (possibly empty) finite set together with a finite number, possibly zero, of arithmetic progressions to some common modulus  $D$ ; we can take  $D$  to be the order of the group of roots of unity generated by all those roots of unity which are of the form  $\alpha_i/\alpha_j$  for some  $i, j$ .*
- (iii) *Suppose that for some index  $i_0$ ,  $\lambda_{i_0}(x) \neq 0$  and, for any  $j \neq i_0$ , the ratio  $\alpha_j/\alpha_{i_0}$  is not a root of unity. Then there are only finitely many integers  $k \geq 1$  for which  $A(k) = 0$ .*
- (iv) *Suppose that no  $\alpha_i$  is a root of unity. Then for any  $\mu \neq 0$  in  $K$ , there are at most finitely many integers  $k \geq 1$  with  $A(k) = \mu$ .*

**PROOF:** (i) Let  $\Lambda$  be the set of coefficients of the polynomials  $\lambda_i(x)$ . It is standard that for almost all primes  $p$  we can embed the finitely generated ring

$$\mathbb{Z}[\alpha_1, 1/\alpha_1, \dots, \alpha_n, 1/\alpha_n, \Lambda, \mu]$$

into the ring of integers  $\mathcal{O}_{\mathcal{P}}$  in a finite extension  $E_{\mathcal{P}}$  of  $\mathbb{Q}_p$ , cf. [C1] for an elementary proof or [Ka], 5.9.3. (In Cassels it is shown that if  $K$  is any finitely generated field of zero characteristic and  $C$  is a finite subset of  $K^\times$  then there is a set of primes  $p$  of positive density such that, for each  $p$  in this set, there is an embedding of  $K$  in the  $p$ -adic field  $\mathbb{Q}_p$  in which all elements of  $C$  are units.)

We choose such an embedding, denote by  $\pi \in \mathcal{O}_{\mathcal{P}}$  a uniformizing parameter, by  $|\cdot|_p$  the extension of the usual  $p$ -adic absolute value to  $E_{\mathcal{P}}$ , by  $\text{ord}_{\mathcal{P}}$  the associated additive valuation, and by  $L$  the cardinality of the finite group  $\mathcal{O}_{\mathcal{P}}^\times/(1 + p\pi\mathcal{O}_{\mathcal{P}})$ .

For each  $i$ , we have

$$(\alpha_i)^L \in 1 + p\pi\mathcal{O}_{\mathcal{P}}.$$

Hence in each arithmetic progression  $\{a + kL\}_{k \in \mathbb{Z}}$  modulo  $L$ , we have

$$A(a + kL) = \sum_{i=1}^n \alpha_i^a \lambda_i(a + kL) (\alpha_i^L)^k,$$

which we can view as the case where the eigenvalues are the  $\alpha_i^L$  and the coefficients are  $\alpha_i^a \lambda_i(a + xL)$ . Notice that the new eigenvalues  $\alpha_i^L$  continue to satisfy the condition that their ratios are not roots of unity.

Looking at each of these progressions separately, it suffices to prove (i) under the additional hypothesis that the  $n$  numbers  $\alpha_i$  each lie in  $1 + p\pi\mathcal{O}_p$ . The key observation is that the functions

$$\log(1 + z) = \sum_{m=1}^{\infty} (-1)^{m-1} \frac{z^m}{m}$$

and

$$\exp(z) = \sum_{m=1}^{\infty} \frac{z^m}{m!}$$

are a pair of inverse group isomorphisms between the multiplicative group  $1 + p\pi\mathcal{O}_p$  and the additive group  $p\pi\mathcal{O}_p$ . (Indeed, for any element  $m \in \mathcal{O}_p$  with  $m^{p-1} \in p\mathcal{O}_p$ ,  $\log$  and  $\exp$  are inverse group isomorphisms between the multiplicative group  $1 + m\mathcal{O}_p$  and the additive group  $m\mathcal{O}_p$ , see [DGS], p.52.) Thus distinct elements  $\alpha_i \in 1 + p\pi\mathcal{O}_p$  have distinct logarithms

$$\beta_i := \log(\alpha_i) = \sum_{m=1}^{\infty} (-1)^{m-1} \frac{(\alpha_i - 1)^m}{m} \in p\pi\mathcal{O}_p.$$

The power functions  $n \mapsto \alpha_i^n = \exp(\beta_i)^n = \exp(\beta_i n)$  are interpolated by the functions  $z \mapsto \exp(\beta_i z)$ , whose power series are easily seen to lie in  $\mathcal{O}_p[[\pi z]]$ .

We next show that these  $n$  analytic functions  $\exp(\beta_i z)$  have power series that are linearly independent over  $E_p[z]$ . For completeness, we repeat here the standard proof. Suppose that  $P_i(z)$  are nonzero polynomials in  $E_p[z]$ , of degree  $\delta_i$ . We will show that the  $n$  power series  $f_i(z) := P_i(z)e^{\beta_i z}$  are linearly independent over  $E_p$ . It suffices to show that their Wronskian

$$\Delta := \det \left( \left( \frac{d}{dz} \right)^{j-1} f_i(z) \right)_{i,j=1,\dots,n}$$

is nonzero. The  $(i, j)$ th entry of the matrix is easily calculated to be

$$(p_{i0} \beta_i^{j-1} z^{\delta_i} + \text{lower degree terms}) e^{\beta_i z},$$

where  $p_{i0} \neq 0$  is the leading coefficient of  $P_i(z)$ . Therefore, the determinant is

$$\Delta = \left\{ \left( \prod_{i=1}^n p_{i0} \right) z^{\sum \delta_i} + \text{lower degree terms} \right\} \text{Vand}(\beta_1, \dots, \beta_n) e^{(\sum \beta_i) z}$$

with Vand the Vandermonde determinant. The  $\beta_i, i = 1, \dots, n$ , are distinct, hence the Vandermonde determinant is not 0.

We now return to the proof of part (i) of the theorem. Since not all coefficients  $\lambda_i(x)$  vanish, the function

$$F(z) := \sum_{i=1}^n \lambda_i(z) \exp(\beta_i z)$$

is nonzero in  $\mathcal{O}_{\mathcal{P}}[[\pi z]]$ . It follows that  $F(z)$  has at most finitely many zeroes in  $\mathcal{O}_{\mathcal{P}}$  and *a fortiori* has at most finitely many integer zeroes, which will prove what we want. This is an easy consequence of the Weierstrass Preparation Theorem applied to the power series ring  $\mathcal{O}_{\mathcal{P}}[[\pi z]]$  (see Lang [La], Th. 9.2), or of the theory of Newton polygons (see, for example, Dwork [Dw], Th. 1.1 or Dwork, Gerotto, Sullivan [DGS], II.2.1). In its most elementary form, this finiteness of the number of zeroes follows from Strassmann's Theorem:

*If  $f(z) = \sum a_m z^m$  is convergent for  $|z|_{\mathcal{P}} \leq 1$  and not identically 0, and  $M$  is the largest index  $m$  for which  $|a_m|_{\mathcal{P}}$  reaches its maximum, then the equation  $f(z) = 0$  has at most  $M$  zeroes  $\zeta$  with  $\text{ord}_{\mathcal{P}}(\zeta) \geq 0$ .*

The following simple proof by induction on  $M$  can be found in Cassels [C2], Th. 4.1. Since  $\sum a_m z^m$  is convergent for  $|z|_{\mathcal{P}} \leq 1$ , we have  $|a_m|_{\mathcal{P}} \rightarrow 0$ , hence  $M$  exists. If  $M = 0$ , there is nothing to prove. Now if  $f(\zeta) = 0$  we have

$$\begin{aligned} f(z) &= f(z) - f(\zeta) = \sum a_m (z^m - \zeta^m) \\ &= (z - \zeta) \sum_{m=1}^{\infty} \sum_{j=0}^{m-1} a_m z^j \zeta^{m-1-j} = (z - \zeta) \sum_{m=0}^{\infty} b_j z^j \\ &= (z - \zeta)g(z), \end{aligned}$$

say, with

$$b_j = \sum_{m=j+1}^{\infty} a_m \zeta^{m-1-j}.$$

From this, it is clear (we are dealing with an ultrametric valuation) that  $|b_j|_{\mathcal{P}} \rightarrow 0$  as  $j \rightarrow \infty$ . Moreover, it is immediate that  $|b_j|_{\mathcal{P}} \leq |a_M|_{\mathcal{P}}$  for all  $j$ ,  $|b_{M-1}|_{\mathcal{P}} = |a_M|_{\mathcal{P}}$ , and  $|b_j|_{\mathcal{P}} < |a_M|_{\mathcal{P}}$  if  $j > M$ ; the result follows by induction applied to  $g(z) = \sum b_j z^j$ , which we may because  $|b_j|_{\mathcal{P}} \rightarrow 0$ , so the sum is convergent in  $|z|_{\mathcal{P}} \leq 1$ .

A refinement of Strassmann's Theorem is the  $p$ -adic Rouché's theorem (see [DGS], IV.4.2 and its more general formulation for quotients of analytic functions, rather than just power series in  $E_{\mathcal{P}}[[z]]$ ):

*Let  $f(z) = \sum a_m z^m \in E_{\mathcal{P}}[[z]]$  be a power series convergent in  $|z|_{\mathcal{P}} \leq 1$  and let  $\|f\| := \max_m |a_m|_{\mathcal{P}}$ . If  $h(z) \in E_{\mathcal{P}}[[z]]$  is another power series convergent in  $|z|_{\mathcal{P}} \leq 1$  and with  $\|h\| < \|f\|$ , then  $f$  and  $f + h$  have the same finite number of zeroes in the disk  $|z|_{\mathcal{P}} \leq 1$ .*

Once we have (i), we get (ii) and (iii) by partitioning the eigenvalues  $\alpha_i$  into equivalence classes according to the equivalence relation where  $a \equiv b$  if and only if  $b/a$  is a root of unity. By renumbering, we may assume that  $\alpha_1, \dots, \alpha_r$  are representatives of these equivalence classes, and that the class of  $\alpha_i$  consists of  $\zeta_{i,j}\alpha_i$ , for  $j = 1, \dots, n_i$ , with suitable roots of unity  $\zeta_{i,j}$  of order dividing some positive integer  $D$ . Then for a fixed integer  $0 \leq a < D$ , and any integer  $k \geq 1$ , the sequence  $k \mapsto A(a + kD)$  is of the same form, with  $r$  eigenvalues  $\alpha_i^{\frac{D}{k}}$ ,  $i = 1, \dots, r$ , except that now it may be the case that all the coefficients vanish. We do not care about the exact formulas for these coefficients, except to note that for each equivalence class which is a singleton, say  $\alpha_{i_0}$ , the new coefficient of  $\alpha_{i_0}$  is  $\alpha_{i_0}^a \lambda_{i_0}(a + xD)$ . If all coefficients vanish, then we have vanishing on the entire progression. If not, then by (i) we only have finitely many vanishing terms in the progression. This gives (ii) and (iii).

Suppose now that no  $\alpha_i$  is a root of unity. We get (iv) by applying (iii) to the situation with  $n+1$  eigenvalues  $(\alpha_1, \dots, \alpha_n, 1)$  and coefficients  $(\lambda_1(x), \dots, \lambda_n(x), -\mu)$ , for here the equivalence class of the eigenvalue 1 is a singleton, whose coefficient  $-\mu$  is nonzero.  $\square$

**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*

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

*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:** Apply Theorem 2.1 to the eigenvalues  $\alpha_i$  of  $F$ , taking all  $\lambda_i = 1$ . For any integer  $k \geq 0$ ,  $A(k)$  is an integer, by the integrality assumption on the coefficients of the characteristic polynomial. There are at most finitely many integers  $k \geq 0$  for which  $0 < |\text{Trace}(F^k)| \leq M$ , hence taking  $k_M$  to be the largest of these, we get the assertion.  $\square$

Here is another corollary. As before,  $K$  is an algebraically closed field of characteristic zero,  $n \geq 1$  an integer, and  $F \in GL(n, K)$  is 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.

- (i) The reversed characteristic polynomial  $\det(1 - GT)$  has integer coefficients.
- (ii) 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: Denote by  $\alpha_i$  the eigenvalues of  $F$ . An integral form  $G$  of  $F^k$  has eigenvalues  $\zeta_i \alpha_i^k$ , for some choice of roots of unity  $\zeta_i$ . We claim that given  $F$ , there is an integer  $D \geq 1$  such for any  $k \geq 1$  and any integral form  $G$  of  $F^k$ , the possible  $\zeta_i$  are all  $D$ th roots of unity. Granting this claim, we get the result by applying Theorem 2.1 to the  $\alpha_i$  and to each of the  $D^n$   $n$ -tuples  $(\lambda_1, \dots, \lambda_n)$  with  $\lambda_i$  a  $D$ th root of unity.

To prove the claim, we argue as follows. Since  $\det(1 - FT)$  has integer coefficients, the  $\alpha_i$  are algebraic numbers, so lie in some finite Galois extension  $K_0/\mathbb{Q}$ . If we pick a prime  $p$  which splits completely in  $K_0$ , we can view all the  $\alpha_i$  as lying in the  $p$ -adic field  $\mathbb{Q}_p$ . The fact that  $\det(1 - GT)$  has integer coefficients shows that each product  $\zeta_i \alpha_i^k$  is algebraic of degree at most  $n$  over  $\mathbb{Q}$ , and hence of degree at most  $n$  over  $\mathbb{Q}_p$ . On the other hand,  $\alpha_i^k \in \mathbb{Q}_p$ , so  $\zeta_i$  lies in an extension of  $\mathbb{Q}_p$  of degree at most  $n$ . Since  $\mathbb{Q}_p$  has only finitely many extensions of given degree, the  $\zeta_i$  lie in a single finite extension, say  $E_{\mathcal{P}}$ , of  $\mathbb{Q}_p$ , and any such finite extension contains only finitely many roots of unity.  $\square$

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  $A(n)$  satisfy  $|A(n)| \rightarrow \infty$ .*

PROOF: This follows from Corollary 2.3 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  $H_{\text{ét}}^1(X \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}, \overline{\mathbb{Q}_\ell})$ . By the Lefschetz trace formula [Gr], we have  $A(n) = \text{Trace}(F^n)$ . By Weil's Riemann hypothesis for curves over finite fields [W1], p.70, 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 three conditions holds.*

- (i) *The genus  $g = 1$ , and  $X/\mathbb{F}_q$  is ordinary.*
- (ii) *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.*

(iii) 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 (i), each  $A(n), n \geq 1$ , is prime to  $p$ , so is nonzero. In case (ii), the congruence formula [DK] 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 (iii), 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 again follows from Corollary 2.5 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  $\text{Prim}_{\acute{e}t}^d(X \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}, \overline{\mathbb{Q}_\ell})$  (the ‘‘primitive’’ part  $\text{Prim}_{\acute{e}t}^d$  of the cohomology  $H_{\acute{e}t}^d$  of a smooth complete intersection  $X$  is simply  $H_{\acute{e}t}^d$  if  $d$  is odd and, if  $d$  is even, it is  $H_{\acute{e}t}^d$  of  $X$  modulo the image of  $H_{\acute{e}t}^d$  of the ambient projective space, see [DK], XI, 1.6(iv)). By the Lefschetz trace formula [Gr] and the known cohomological structure of complete intersections [DK] XI, 1.6, we have  $A(n) = \text{Trace}(F^n)$ . By Deligne’s Riemann hypothesis for varieties over finite fields [De2], the eigenvalues of  $F$  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 [DK] 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  $a \in \mathbb{F}_q^\times$ . Then, for all  $n \geq 1$ ,  $A(n)$  is prime to  $p$ , so it is nonzero and (hence)  $|A(n)| \rightarrow \infty$ .*

PROOF: Again by the congruence formula [DK] 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 2.8 above.

THEOREM 2.9. *Let  $\mathbb{F}_q$  be a finite field of characteristic  $p > 0$ ,  $S/\mathbb{F}_q$  a smooth, geometrically connected  $\mathbb{F}_q$ -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  $\pi$  is isotrivial, in the sense that when pulled back to a suitable 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*

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

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  $\text{Prim}_{\text{ét}}^d(X_0 \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}, \overline{\mathbb{Q}}_{\ell})$ . 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  $\text{Prim}_{\text{ét}}^d(X_{\mathbb{F}_{\mathcal{P}}} \otimes_{\mathbb{F}_{\mathcal{P}}} \overline{\mathbb{F}_{\mathcal{P}}}, \overline{\mathbb{Q}}_{\ell})$  is an integral form of  $F^{\deg(\mathcal{P})}$ . So the assertion results from Corollary 2.8 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  $\deg(\mathcal{P}) \rightarrow \infty$ .*

### III. LOWER BOUNDS, VIA THE SUBSPACE THEOREM

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.

Lower bounds come from the following special case of a theorem of Evertse [Ev], Cor. 2, also due independently to van der Poorten and Schlickewei [PS], Theorem 3.

**THEOREM 3.1.** *Let  $Q > 1$  and  $n \geq 1$  be integers. Let  $\alpha_1, \dots, \alpha_n$  be integral  $Q$ -Weil numbers. For each integer  $k \geq 1$ , define*

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

*Given a real number  $\varepsilon > 0$ , there exists a real constant  $C_1 > 0$  such that for any integer  $k \geq 1$ , either  $A(k) = 0$  or, for any archimedean absolute value on  $\overline{\mathbb{Q}}$ , we have*

$$|A(k)| \geq C_1 Q^{k(1-\varepsilon)}.$$

**PROOF:** This is the following special case of [Ev], Cor. 2. Take for  $K$  a number field containing all the  $\alpha_i$ . Take for  $S$  the set of all places of  $K$  which are either archimedean or which lie over primes dividing  $Q$ . Take for  $T \subset S$  a single archimedean place. Since the absolute norm of every  $\alpha_i$  is a power of  $Q$ , the algebraic integers  $\alpha_i$  are all  $S$ -units.

Then, for each integer  $k \geq 1$  with  $A(k) = 0$ , simply apply [Ev], Cor. 2, to the  $S$ -units  $x_i := \alpha_i^k$ .  $\square$

We can trivially make the constant  $C_1$  disappear if we insist that  $k$  be sufficiently large.

**COROLLARY 3.2.** *Under the hypotheses of the theorem, given a real number  $\varepsilon > 0$ , there exists an integer  $k_0$  such that for all integers  $k \geq k_0$ , either  $A(k) = 0$  or, for any archimedean absolute value on  $\overline{\mathbb{Q}}$ , we have*

$$|A(k)| \geq Q^{k(1-2\varepsilon)}.$$

**THEOREM 3.3.** *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  $\ell$ , cf. [De3], 3.3.9) defined as*

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

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

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

**PROOF:** This is an immediate consequence of Deligne's theorem [De3] 3.3.9, by applying Theorem 3.3 to the eigenvalues of  $\text{Frob}_q$  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 Frobeniuses 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. [De3], 3.3.6, and [Se], that  $H_c^i = 0$  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

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

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  $\iota$  of the number field  $\mathbb{Q}(\{\text{eigenvalues of Frob}_q\})$  into  $\mathbb{C}$ , and any chosen real number  $\varepsilon > 0$ , we have that for all  $n$  sufficiently large either  $A(n) = 0$  or  $|\iota A(n)|_{\mathbb{C}} \geq (q^{nw/2})^{1-\varepsilon}$ .

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  $n \geq 1$ .

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

$$(-1)^{d-1} Kl_d(\psi, a, \mathbb{F}_q) := \sum_{x_1 x_2 \dots x_d = a, \text{ all } x_i \in \mathbb{F}_q} \psi(x_1 + \dots + x_n).$$

Only  $H_c^{d-1}$  is nonzero, and the  $d$  Frobenius eigenvalues are integral  $q^{d-1}$ -Weil numbers [De1], 7.1.3, 7.4. This sum lies in  $\mathbb{Z}[\zeta_p]$  and never vanishes, because modulo the unique prime ideal  $\mathfrak{p}$  of  $\mathbb{Z}[\zeta_p]$  lying over  $p$  we have

$$(-1)^{d-1} Kl_d(a, \mathbb{F}_q) \equiv (q-1)^{d-1} \equiv (-1)^{d-1} \pmod{\mathfrak{p}}$$

(simply because  $\psi$  is trivial  $\pmod{\mathfrak{p}}$ ). Here the sequence of  $A(n)$  is

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

Therefore, for any given real  $\varepsilon > 0$  we have the lower bound

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

for all  $n$  sufficiently large.

- (ii) 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  $\pmod{p}$ . We take  $U := \mathbb{P}^1 \setminus S$ . 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  $\psi$  a nontrivial additive character of  $\mathbb{F}_q$ , we have the sum

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

Only the first cohomology group with compact support  $H_c^1$  is nonzero, and the  $\#S - 2 + \sum_{s \in S} e_s$  Frobenius eigenvalues are integral  $q$ -Weil

numbers [W2]. This sum lies in  $\mathbb{Z}[\zeta_p]$  and never vanishes, because modulo the unique prime ideal  $\mathfrak{p}$  of  $\mathbb{Z}[\zeta_p]$  lying over  $p$ , it is congruent to  $-(q + 1 - \#S) \equiv \#S - 1$ , which by assumption is nonzero mod  $p$ . The sequence  $A(n)$  in this case is

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

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

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

for all sufficiently large  $n$ .

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

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

Sperber [Sp] 3.11, shows 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 orders, 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 (ii) above.

#### IV. EFFECTIVE LOWER BOUNDS, VIA BAKER'S METHOD

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  $\alpha$  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 deep Baker–Wüstholz theorem [BW]. For the definition of height, we refer to [BG], section 1.5.

**THEOREM 4.1.** *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*

$$\begin{aligned} C(N, d) &:= 18(N + 1)!N^{N+1}(32d)^{N+2} \log(2Nd), \\ h'(e^{2i\theta}) &:= \max(\log(H((1 : e^{2i\theta}))), \theta/d, 1/d), \\ h'(-1) &:= \pi/d, \end{aligned}$$

where  $H((x_0 : \cdots : x_r))$  is the Weil height of an (algebraic) point  $(x_0 : \cdots : x_r)$  in projective space  $\mathbb{P}^r$ .

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  $\pi$  occurs for some  $k \in [0, 2n]$ . (Indeed, for any integer  $k$  outside of 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, with the  $N = 2$  algebraic numbers  $e^{2i\theta}$  and  $-1$ , and to the linear combination of logarithms  $n \log(e^{2i\theta}) - k \log(-1)$ .  $\square$

COROLLARY 4.2. Let  $\theta \in [0, \pi]$  be as in the theorem. Given a real number  $q > 1$ , define

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

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

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

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

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

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

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

Also, for real  $x$  with  $|x| \leq \pi/2$ , we have the well-known inequality

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

Thus we find

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

completing the proof.  $\square$

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

COROLLARY 4.3. The following holds.

- (i) 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

$$|A(n)| \geq (2/\pi)q^{n/2 - 2^{37} \log(2n)}.$$

- (ii) 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,

$$|A(n)| \geq (2/\pi)q^{n/2-2^{37} \log(2n)}.$$

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

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

with  $c_p$  the constant  $c_p = 2^{33}p^4 \log p$ .

PROOF: We will compute, in the two cases, an explicit upper bound for the constant  $c$  of the previous corollary.

Denote by  $\alpha$  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  $\alpha$  and  $\bar{\alpha}$  are integral  $q$ -Weil numbers.

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

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

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

$$c \leq C(2, 2)(5/2)(\pi/2) = 18 \cdot 3! \cdot 2^3 \cdot (64)^4 \cdot \log(8) \cdot (5\pi/4) \leq 2^{37}.$$

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  $\alpha$  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  $\pm 1$ ), hence in this case we have  $2 \leq d \leq \max(p-1, 2)$ . So again we have

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

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

$$c \leq 2^{37}.$$

For  $p \geq 5$  the bound becomes dependent on  $p$ , namely

$$\begin{aligned} c &\leq C(2, p-1)(5\pi/4) \\ &= 18 \cdot 3! \cdot 2^3 \cdot (32(p-1))^4 \cdot \log(4(p-1)) \cdot (5\pi/4) < 2^{33}p^4 \log p. \end{aligned}$$

This completes the proof.  $\square$

## V. CONCLUDING REMARKS

As mentioned in the introduction, the main open problem here is obtaining effective lower bounds. On the other hand, much is known about the number of zeroes in a linear recurrence sequence. A theorem of Evertse, Schlickewei, and Schmidt [ESS] states the following.

*Let  $K$  be a field of characteristic 0, let  $\Gamma$  be a subgroup of  $(K^\times)^n$  of finite  $\mathbb{Q}$ -rank  $r$ , and let  $a_1, \dots, a_n \in K^\times$ . Let  $\mathcal{X}$  be the set of those solutions  $(x_1, \dots, x_n) \in \Gamma$  of the equation*

$$a_1x_1 + \dots + a_nx_n = 1$$

*for which no proper subsum of  $a_1x_1 + \dots + a_nx_n$  vanishes. Then  $\mathcal{X}$  is a finite set of cardinality*

$$\#\mathcal{X} \leq e^{(6n)^{3n}(r+1)}.$$

This can be applied easily to obtain further information on the set of zeroes of the sequences  $A(n)$  examined here, since in this case we have  $r = 1$ . The Skolem–Mahler–Lech theorem shows that the zero set of the sequence  $A(n)$  is the union of a finite set  $S_0$  of isolated solutions and of finitely many arithmetic progressions. Theorem 1.2 of [ESS] immediately shows that

$$\#S_0 + \#(\text{arithmetic progressions}) \leq e^{(12g)^{6g}}.$$

Although this is not directly relevant to the applications we have treated in this paper, a similar result also holds for any linear recurrence of order  $n$  (where the coefficients  $\lambda_i$  are allowed to be polynomials), with a bound  $\exp \exp \exp(3n \log n)$  for the corresponding number of isolated solutions and of arithmetic progressions, see Schmidt [Sc].

The proof of these results is difficult and rather intricate, but it is a remarkable fact that these bounds depends only on  $n$  and the rank of  $\Gamma$ .

A more delicate problem has also been treated, namely the study of the intersection of two distinct recurrences and the “total multiplicity” of a recurrence, namely  $A(m) = B(n)$  and  $A(m) = A(n)$  for  $m \neq n$ . Under certain natural conditions one can prove that the number of admissible pairs  $(m, n)$  for which these equations hold is finite, see Evertse [Ev], Th. 3, for the equation  $A(m) = A(n)$  with recurrences of order at least 2 (this avoids the example  $A(n) = n2^n$ ), and Laurent [Lau] for qualitative results for the equation  $A(m) = B(n)$ . Quantitative results, but not as strong as those mentioned above for the cardinality of the zero-set of a recurrence, can be found in Schlickewei and Schmidt [SS].

The extension of these results to larger classes of polynomial–exponential equations in several variables remains a central and very challenging open problem. As an example, the famous Ramanujan equation  $m^2 + 7 = 2^k$  has only the solutions  $(m, k) = (1, 3), (3, 4), (5, 5), (11, 7), (181, 15)$  in positive integers, which is not difficult to prove using Skolem’s method. The modified equation  $m^2 + 7^n =$

$2^k + (r - 1)3^r$  associated to the group of rank 3

$$\{(1^m, 2^k, 3^r, 7^n)\}_{m,k,r,n \in \mathbb{Z}}$$

has, besides the five solutions with  $n = 1$  and  $r = 1$  inherited from the Ramanujan equation, seven new solutions  $(m, k, r, n) = (2, 1, 2, 1), (7, 1, 3, 1), (14, 1, 4, 2), (3, 2, 3, 2), (13, 9, 1, 3), (113, 11, 7, 4), (407, 13, 9, 1)$ . Are there any other solutions in positive integers to this equation?

#### REFERENCES

- [BG] BOMBIERI, E. and GUBLER, W. *Heights in Diophantine Geometry*, new mathematical monographs 4, reprinted with corrections, Cambridge University Press, Cambridge 2007. xvi+652pp.
- [BW] BAKER, A. and WÜSTHOLZ, G. Logarithmic forms and group varieties, *J. reine angew. Math.* 442 (1993), 19-62.
- [C1] CASSELS, J.W.S. An embedding theorem for fields, *Bull. Australian Math. Soc.* 14 (1976), 193–198. – Addendum: “An embedding theorem for fields”, *ibidem*, 479–480.
- [C2] CASSELS, J.W.S. *Local Fields*, London Math. Soc. Student Texts, 3. Cambridge University Press, Cambridge 1986. xiv+360pp.
- [De1] DELIGNE, P. Applications de la formule des traces aux sommes trigonométriques, in *SGA 4 1/2, 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 569, Springer-Verlag, Berlin–New York 1977, 168-232.
- [De2] DELIGNE, P. La conjecture de Weil, *Publ. Math. IHES* 43 (1974), 273–307.
- [De3] DELIGNE, P. La conjecture de Weil II, *Publ. Math. IHES* 52 (1981), 313–428.
- [DGS] DWORK, B., GEROTTO, G., SULLIVAN F. *An Introduction to G-functions*, Annals of Mathematics Studies, 133. Princeton University Press, Princeton NJ 1994. xxi+323pp.
- [DK] *Groupes de Monodromie en Géométrie Algébrique. Séminaire de Géométrie Algébrique du Bois Marie SGA 7 II, Dirigé par P. Deligne et N. Katz*. Lecture Notes in Mathematics 340, Springer-Verlag, Berlin–New York 1973.
- [Dw] DWORK, B. On the zeta function of a hypersurface, *Inst. Hautes Etudes Sci. Publ. Math. No. 12* 1962, 5-68.
- [Ev] EVERTSE, J.-H. On sums of S-units and linear recurrences, *Compositio Math.* 53 (1984), 225–244.
- [ESS] EVERTSE, J.-H., SCHLICKWEI H.P., SCHMIDT, W.M. Linear equations in variables which lie in a multiplicative group, *Annals of Math. (2)* 155 (2002), 807–836.
- [Gr] GROTHENDIECK, A. Formule de Lefschetz et rationalité des fonctions L. *Séminaire Bourbaki, Vol. 9, Exp. No. 279*, 41-55, Soc. Math. France 1995.
- [Ka] KATZ, N. *Rigid Local Systems*, Annals of Mathematics Studies, 139. Princeton University Press, Princeton NJ 1996. viii+223pp.
- [La] LANG, S. *Algebra*, revised third edition. Graduate Texts in Mathematics, 211. Springer-Verlag, New York 2002. xvi+914pp.
- [Lau] LAURENT, M. Équations exponentielles polynômes et suites récurrentes linéaires, *Astérisque* 147–148, 121–139. Soc. Math. de France 1987.
- [Le] LECH, C. A note on recurring series, *Ark. Mat.* 2 (1953), 417-421.
- [M] MAHLER, K. Eine arithmetische Eigenschaft der Taylor-koeffizienten rationaler Funktionen, *Akad. Wetensch. Amsterdam, Proc.* 38 (1935), 50-60.
- [PS] VAN DER POORTEN, A.J. and SCHLICKWEI, H.P. Additive relations in fields, *J. Austral. Math. Soc. (Series A)* 51 (1991), 154-170.

- [SS] SCHLICKWEI, H.P. and SCHMIDT, W.M. The intersection of recurrence sequences, *Acta Arith.* 72 (1995), 1–44.
- [Sc] SCHMIDT, W.M. The zero multiplicity of linear recurrence sequences, *Acta Math.* 182 (1999), 243282.
- [Se] SERRE, J.-P. Majorations de sommes exponentielles, in *Journées Arithmétiques de Caen (Univ. Caen, Caen, 1976)*, 111–126. Astérisque No. 41–42, Soc. Math. France, Paris 1977.
- [Sk] SKOLEM, TH. Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen, *C. r. 8 congr. scand. at Stockholm 1934*, 163-188.
- [Sp] SPERBER, S. On the  $p$ -adic theory of exponential sums, *Amer. J. Math.* 108 (1986), 255-296.
- [W1] WEIL, A. *Sur les Courbes Algébriques et les Variétés qui s'en Déduisent*. Actualités Sci. Ind., no. 1041, Publ. Inst. Math. Univ. Strasbourg (1945). Hermann & Cie., Paris 1948. 86pp.
- [W2] WEIL, A. On some exponential sums, *Proc. Nat. Acad. Sci. U.S.A.* 34 (1948), 204-207.

E. Bombieri  
School of Mathematics  
Institute for Advanced Study  
Princeton, New Jersey 08540, USA

e-mail: eb@ias.edu

N.M. Katz  
Department of Mathematics  
Princeton University  
Princeton, New Jersey 08544, USA

e-mail: nmk@math.princeton.edu