A combinatorial problem related to Mahler's measure

W. Duke

ABSTRACT. We give a generalization of a result of Myerson on the asymptotic behavior of norms of certain Gaussian periods. The proof exploits properties of the Mahler measure of a trinomial.

1. Introduction

This paper was motivated by the following remarkable asymptotic result of Myerson [8] about the norm of a Gaussian period. Let $p \equiv 1 \mod 3$ be a prime and ω a primitive cube root of unity in the finite field $\mathbb{F}_p = \{0, 1, \dots, p-1\}$. Also let $K = \mathbb{Q}(\zeta)$ be the *p*-th cyclotomic field, where $\zeta = e^{2\pi i/p}$. Then, as $p \to \infty$,

(1)
$$\frac{1}{p}\log|N_{\mathbb{Q}}^{K}(\zeta+\zeta^{\omega}+\zeta^{\omega^{2}})| \to L'(-1,\chi) = .3231\ldots$$

where $L(s, \chi)$ is the Dirichlet *L*-function with χ the nontrivial character mod 3. As a consequence of a more general result we will give the following refinement of (1).

THEOREM 1. For $p \equiv 1 \mod 3$

$$\frac{1}{n}\log|N_{\mathbb{O}}^{K}(\zeta+\zeta^{\omega}+\zeta^{\omega^{2}})| = L'(-1,\chi) + \mathcal{O}(p^{-1/2}\log p),$$

with an absolute implied constant.

The method of proof behind Theorem 1 differs from that of Myerson and develops further an interesting relationship between a certain combinatorial problem and Mahler's measure. In the next section we introduce this combinatorial problem, briefly describe Myerson's approach to (1), state the general result, Theorem 2 and show

Research supported in part by NSF Grant DMS-0355564. AMS Classification: 05A15 (12A15).

that it implies Theorem 1. The five sections that follow contain results of independent interest that lead up to the proof of Theorem 2.

2. The combinatorial problem

Let *S* be an arbitrary subset of cardinality |S| of \mathbb{F}_p , for *p* an odd prime. For a given $t \in \mathbb{F}_p$ denote by N_t the number of solutions $(n_1, \ldots, n_{p-1}) \in S^{p-1}$ of the equation

$$\sum_{\ell \in \mathbb{F}_p^*} \ell \, n_\ell = t,$$

where $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$. Clearly $N_t = N_{at}$ for $a \in \mathbb{F}_p^*$ so that N_t takes on only the two values N_0 and N_1 . Furthermore, N_0 and N_1 are invariant under affine maps $S \mapsto aS + b$ for $a \in \mathbb{F}_p^*$ and $b \in \mathbb{F}_p$. The combinatorial problem of interest here is to determine N_0 and N_1 as precisely as possible in terms of p and (the affine equivalence class of) S.

Since it is obvious that $N_0 + (p-1)N_1 = |S|^{p-1}$, this problem reduces to the determination of $\Delta = N_0 - N_1$, in terms of which

$$N_1 = \frac{1}{p} |S|^{p-1} - \frac{1}{p} \Delta$$
 and $N_0 = \frac{1}{p} |S|^{p-1} + (1 - \frac{1}{p}) \Delta$.

We have that $\Delta = \sum_{t \in \mathbb{F}_p} N_t \zeta^t$, which yields the basic formula

(2)
$$\Delta = \prod_{\ell \in \mathbb{F}_p^*} \sum_{n \in S} \zeta^{n\ell}.$$

The counting problem is thus equivalent to computing the norm of the cyclotomic integer $\sum_{n \in S} \zeta^n$.

As a consequence of the arithmetic-geometric inequality applied in (2) it follows that

$$|\Delta| \le |S|^{\frac{p}{2}-1}.$$

This shows that the values $\sum_{\ell} \ell n_{\ell}$ are very well distributed among the values of \mathbb{F}_p . It also follows easily from (2) that for $|S| \leq 2$ we have $\Delta = 1$ so we may restrict attention to *S* where $|S| \geq 3$.

In case *S* is a subgroup of \mathbb{F}_p^* such problems were discussed by Myerson [7, 8]. Here the values of ℓS run over the cosets of *S* exactly |S| times. He actually considered the problem of counting the number of representations of *t* as a sum of distinct elements of these cosets. It is easily seen from (2) that this counting problem reduces to the determination of a natural |S|-th root of Δ . This is a well known problem of cyclotomy in that it entails the explicit evaluation of the norm of a Gaussian period. Except for some subgroups of small index (see [7]) or of size $|S| \leq 2$, such evaluations are apparently unknown.

In lieu of an explicit evaluation of Δ when S is a subgroup of \mathbb{F}_p^* of fixed size, Myerson introduced the idea of determining the asymptotic behavior of $|\Delta|$ as a function of $p \equiv 1 \mod |S|$ as $p \to \infty$. When |S| = 3 so that $S = \{1, \omega, \omega^2\}$, he proved in [8] that

(3)
$$\frac{1}{p} \log |\Delta| \to \int_0^1 \int_0^1 \log |e(u) + e(v) + e(-u - v)| \, du \, dv,$$

as $p \to \infty$ with $p \equiv 1 \mod 3$. The statement (1) then follows from (2) and the evaluation of the integral in (3), which follows from [11]. The idea of the proof of (3) is to interpret the formula from (2),

$$\frac{1}{p}\log|\Delta| = \frac{1}{p}\sum_{\ell}\log|\sum_{n\in S}e(n\ell/p)|,$$

as giving an approximation to the integral in (3) by using the fact that $(\ell/p, \omega \ell/p)$ becomes uniformly distributed (mod 1) as ℓ runs over \mathbb{F}_p^* . The difficulty lies in the fact that the integrand has singularities, but it is tractable since they are isolated from the points $(\ell/p, \omega \ell/p)$. Using special arguments he was able to quantify this statement well enough to prove (3). Myerson also conjectured in [8] a result like (3) for subgroups of any fixed size. However, for |S| > 4 (the case |S| = 4 being simpler), the singular set is infinite and this seems to present a serious obstacle in the way of a proof. See [10] and chapter 10 of the book of Konyagin and Shparlinski [4] for some further developments of these ideas.

This paper will show that $\frac{1}{p} \log |\Delta|$ is actually well approximated by $L'(-1, \chi)$ for any set S with |S| = 3, provided that the "width" w(S) is large. Here, for any S, w(S) is defined to be the length of the smallest interval in $\{0, 1, 2, ..., p - 1\}$ that contains an image aS + bof S under an affine transformation.

THEOREM 2. Suppose that |S| = 3. Then

$$\frac{1}{p}\log|\Delta| = L'(-1,\chi) + O\left(\frac{\log w(S)}{w(S)}\right),$$

with an absolute implied constant.

The proof of Theorem 2 uses a uniform asymptotic estimate for $\frac{1}{p} \log |\Delta|$ given in terms of the Mahler measure of a certain trinomial. This is then related to a two dimensional Mahler measure like the integral in (3). Although this method differs significantly from that described above, it also encounters difficulties with larger sets *S*.

W. DUKE

To see that Theorem 1 follows from Theorem 2, it is enough to observe that $w(\{1, \omega, \omega^2\}) \gg p^{1/2}$. Suppose that for some $a \in \mathbb{F}_p^*$ and some c > 0 the three elements $a, a\omega, a\omega^2$ are all contained in some interval of length $cp^{1/2}$, where this is interpreted in the obvious way. Since $a + a\omega + a\omega^2 = 0$ this interval must contain either 0, (p-1)/3 or (2p-2)/3. Hence $3a, 3a\omega, 3a\omega^2$ must be contained in an interval around 0 of length $3cp^{1/2}$. Let n and m be the integers of smallest absolute value representing 3a and $3a\omega$, respectively. Then

$$0 < n^2 + nm + m^2 \equiv 0 \mod p.$$

This implies that $\frac{3}{2}(n^2 + m^2) \ge p$, which is impossible for c > 0 sufficiently small. Thus $w(\{1, \omega, \omega^2\}) \gg p^{1/2}$. We remark that any set S with |S| = 3 satisfies $w(S) \ll p^{1/2}$, as will be seen in the proof of Theorem 5 below.

3. The asymptotic problem for fixed *S*

Before turning to the proof of Theorem 2, consider first the asymptotic problem when *S* is a *fixed* subset of \mathbb{Z} , interpreted for each (sufficiently large) *p* as a subset of \mathbb{F}_p . Recall that the Mahler measure of a monic $f \in \mathbb{C}[x]$ is given by

$$\mathcal{M}(f) = \prod_{\alpha} \max(1, |\alpha|),$$

where α runs over the zeros of f, counted with multiplicity. As is standard we write

(4)
$$m(f) = \log M(f).$$

Associated to $S = \{n_1, n_2, ..., n_{|S|}\}$ with $n_1 < n_2 < ... < n_{|S|}$, is the polynomial

$$f_S(x) = x^{n_1} + x^{n_2} + \dots + x^{n_{|S|}}$$

The following result shows that for fixed *S* the basic asymptotic problem has a simple solution in terms of $m(f_S)$.

THEOREM 3. Suppose that S is fixed. Then for p sufficiently large

$$\frac{1}{p}\log|\Delta| = \mathrm{m}(f_S) + O(p^{-1}\log p),$$

where the implied constant depends only on S.

PROOF. Writing $f_S(x) = \prod_{\alpha} (x - \alpha)$, we see from (2) that

$$\Delta = \prod_{\alpha} \prod_{\ell \in \mathbb{F}_p^*} (\alpha - \zeta^{\ell}) = \prod_{\alpha} \frac{1 - \alpha^p}{1 - \alpha},$$

using that p - 1 is even. Since $\prod_{\alpha} (1 - \alpha) = f_S(1) = |S|$ we obtain

(5)
$$|S| \Delta = \prod_{\alpha} (1 - \alpha^p).$$

This quantity was studied by D.H. Lehmer in his influential paper of 1933 [6]. Thus we have for *p* sufficiently large

(6)
$$\frac{1}{p}\log|\Delta| = \frac{1}{p}\sum_{\alpha}\log|1-\alpha^p| - \frac{1}{p}\log|S|.$$

If $|\alpha| > 1$ then $\frac{1}{p} \log |1 - \alpha^p| = \log |\alpha| + O(|\alpha|^{-p})$ while if $|\alpha| < 1$ then $\frac{1}{p} \log |1 - \alpha^p| = O(|\alpha|^p)$. Only in case $|\alpha| = 1$ is there any difficulty, and this may be handled as in [3, Lemma 1.10] by an application of Baker's Theorem, giving that for p sufficiently large

$$\log|1 - \alpha^p| \ll_\alpha \log p.$$

Note that the restriction in [3, Lemma 1.11] that α not be a root of unity is unnecessary here since *p* is a prime. Thus

$$\frac{1}{p} \sum_{\alpha} \log |1 - \alpha^{p}| = m(f_{S}) + O(p^{-1} \log p).$$

By (6) we finish the proof.

This proof serves to underscore that the main challenge in understanding the behavior of $|\Delta|$ when S is not fixed, at least by this method, is to control small values of $|1 - \alpha^p|$ for α a zero of f_S in terms of p. Baker's theorem does not seem to yield enough information without making some very restrictive assumptions on w(S).

4. Zeros of a trinomial

The assumption that |S| = 3 allows us to control how close a root of f_S , which is a trinomial, can be to a *p*-th root of unity. This in turn can be used to estimate how small $|1 - \alpha^p|$ can be. The following theorem formulates this idea precisely.

THEOREM 4. Suppose that p > 3 and 0 < m < n. Then there is an absolute constant c > 0 so that for α a root of $f(x) = x^n + x^m + 1 = 0$ with $|\alpha| \le 1$ we have

$$|1 - \alpha^p| > \frac{c}{n}.$$

PROOF. As before let $\zeta = e^{2\pi i/p}$. We first show that there is an absolute constant $c_1 > 0$ so that for all $\ell \in \mathbb{Z}$

(7)
$$|\zeta^{\ell} - \alpha| > c_1(pn)^{-1}.$$

5

Fix ℓ and α and let *L* denote the line segment from α to ζ^{ℓ} . By the complex mean value theorem given in [**2**] there are $z_1, z_2 \in L$ so that

$$\operatorname{Re} \frac{f(\zeta^{\ell}) - f(\alpha)}{\zeta^{\ell} - \alpha} = \operatorname{Re} f'(z_1) \text{ and } \operatorname{Im} \frac{f(\zeta^{\ell}) - f(\alpha)}{\zeta^{\ell} - \alpha} = \operatorname{Im} f'(z_2).$$

Thus

$$\left|\frac{f(\zeta^{\ell}) - f(\alpha)}{\zeta^{\ell} - \alpha}\right| \le 2 \max_{z \in L} |f'(z)| \le 4n,$$

which yields

$$4n|\zeta^{\ell} - \alpha| \ge |f(\zeta^{\ell})| = |\zeta^{n\ell} + \zeta^{m\ell} + 1|.$$

Since p > 3 this sum three of *p*-th roots of unity cannot vanish and in fact must satisfy $|\zeta^{n\ell} + \zeta^{m\ell} + 1| \ge c_2 p^{-1}$ for some $c_2 > 0$ (see [9]), giving (7).

Write $\alpha = re^{i\theta}$. By (7) there are constants $c_3, c_4 > 0$ so that at least one of the following holds:

$$r < 1 - \frac{c_3}{pn}$$
 or $\left|\theta - \frac{2\pi\ell}{p}\right| > \frac{c_4}{pn}$ for all $\ell \in \mathbb{Z}$.

In the first case

$$|1 - \alpha^p| > 1 - \left(1 - \frac{c_3}{pn}\right)^p = \frac{c_3}{n} + O(n^{-2}),$$

while in the second $|p\theta - 2\pi\ell| > c_4 n^{-1}$ and hence

$$|1 - \alpha^p| \ge \sin(c_4 n^{-1}) = \frac{c_4}{n} + O(n^{-3}),$$

since $\sin(c_4n^{-1})$ is the minimal distance from 1 to the ray at angle c_4n^{-1} . This finishes the proof.

5. The Mahler measure of a trinomial

Suppose that for some p > 3 we have a set $S \subset \mathbb{F}_p$ with |S| = 3. This S can be transformed by an affine transformation to one of the form $\{0, m, n\}$, where 0 < m < n and n is minimal: that is n = w(S). Write $f(x) = x^n + x^m + 1$ for some such choice of m.

THEOREM 5. *Given* S with |S| = 3 and f as above, we have

$$\frac{1}{p}\log|\Delta| = \mathrm{m}(f) + O(p^{-1/2}\log n)$$

with an absolute implied constant.

6

PROOF. By (5) we are reduced to considering

(8)
$$\Delta = \frac{1}{3} \prod_{\alpha} (1 - \alpha^p),$$

where α runs over all the zeros of f. Now

$$\sum_{\alpha} \log |1 - \alpha^{p}| - p \operatorname{m}(f) = \sum_{|\alpha| \le 1} \log |1 - \alpha^{p}| + \sum_{|\alpha| > 1} \log |1 - \alpha^{-p}| \\ \ll n \log n$$

by Theorem 4 applied to f(x) and its reciprocal

$$x^{n}f(x^{-1}) = x^{n} + x^{n-m} + 1.$$

Thus by (8) we have

$$\frac{1}{p}\log|\Delta| = \mathrm{m}(f) + O\Big(\frac{n\log n}{p}\Big).$$

To finish the proof of Theorem 5 we will show that $n \ll p^{1/2}$. By performing a suitable affine transformation we may suppose that $S_p = \{0, 1, \ell\}$ where $1 < \ell < p$. Let $s = \lceil \sqrt{p} \rceil = \lfloor \sqrt{p} \rceil + 1$ and observe that at least one difference $k\ell - j\ell$ for $0 \le j < k \le s$ must lie in $\{1, 2, \ldots, s\}$ or $\{p - s, p - s + 1, \ldots, p - 1\}$. Taking a = k - j and some b we see that $aS_p + b \subset \{0, 1, \ldots, 2s\}$. It follows that $n \ll p^{1/2}$. \Box

6. Limits of Mahler measures

Recall that the Mahler measure of a non-zero polynomial $f \in \mathbb{C}[x, y]$ is defined by

(9)
$$m(f) = \int_0^1 \int_0^1 \log |f(e(u), e(v))| \, du \, dv$$

This reduces to (4) for monic $f \in \mathbb{C}[x]$ by Jensen's formula [3, p.7], which states that for any $z \in \mathbb{C}$,

(10)
$$\int_0^1 \log |e(u) - z| \, du = \log^+ |z|,$$

where $\log^{+} z = \log \max(1, |z|)$.

The following result expresses m(x + y + 1) as a uniform limit of Mahler measures of trinomials. The proof is modeled after that of Boyd, who gave the case m = 1 in [1, p.463].

THEOREM 6. For
$$0 < m < n$$
 with $(m, n) = 1$
 $m(x^n + x^m + 1) = m(x + y + 1) + \alpha(m + n)n^{-2} + O(mn^{-3}),$

where

(11)
$$\alpha(n) = \begin{cases} -\frac{\sqrt{3}\pi}{6}, & \text{if } n \equiv 0 \mod 3; \\ \frac{\sqrt{3}\pi}{18}, & \text{otherwise.} \end{cases}$$

PROOF. For $x = e(u) = e^{2\pi i u}$ with $\cos(2\pi m u) > -1/2$ we have

(12)
$$\log(1+x^m+x^n) = \log(1+x^m) + \sum_{\ell \ge 1} \frac{(-1)^{\ell-1}}{\ell} \Big(\frac{x^n}{1+x^m}\Big)^\ell,$$

while when $\cos(2\pi mu) < -1/2$ we have that

(13)
$$\log(1+x^m+x^n) = \log(x^n) + \sum_{\ell \ge 1} \frac{(-1)^{\ell-1}}{\ell} \Big(\frac{1+x^m}{x^n}\Big)^{\ell}.$$

By (10) applied in (9)

(14)
$$m(x+y+1) = \int_0^1 \log^+ |1+e(u)| \, du$$

= $\int_0^1 \log^+ |1+e(mu)| \, du = \int \log |1+e(mu)| \, du$,

where the range of the last integral consists of those subintervals of [0,1] that satisfy $\cos(2\pi m u) > -1/2$. Thus set

(15)
$$I_1(\ell) = \int e(n\ell \, u)(1 + e(mu))^{-\ell} du,$$

where the range of integration is over those subintervals of [0,1] that satisfy $\cos(2\pi m u) > -1/2$, and

(16)
$$I_2(\ell) = \int e(-n\ell \, u)(1+e(mu))^\ell du,$$

where the range of integration is over those subintervals of [0, 1] that satisfy $\cos(2\pi m u) < -1/2$. By (12-14) we have the identity

(17)
$$m(x^n + x^m + 1) = m(x + y + 1) + \operatorname{Re} \sum_{\ell \ge 1} \frac{(-1)^{\ell-1}}{\ell} (I_1(\ell) + I_2(\ell)).$$

After changing variables $u \mapsto mu$ we have from (15)

(18)

$$I_{1}(\ell) = \frac{1}{m} \sum_{k=0}^{m-1} \left(\int_{k}^{k+1/3} + \int_{k+2/3}^{k+1} \right) e(\frac{n\ell u}{m}) (1+e(u))^{-\ell} du$$

$$= \frac{2}{m} \operatorname{Re} \sum_{k=0}^{m-1} e(\frac{kn\ell}{m}) \int_{0}^{1/3} e(\frac{n\ell u}{m}) (1+e(u))^{-\ell} du$$

$$= 2 \operatorname{Re} \int_{0}^{1/3} e(nq u) (1+e(u))^{-qm} du$$

when $\ell = qm$ and $I_1(\ell) = 0$ otherwise. Here we use the assumption that (n, m) = 1. Similarly, from (16)

(19)
$$I_2(\ell) = 2 \operatorname{Re} \int_{1/3}^{1/2} e(-nq \, u) (1 + e(u))^{qm} du$$

when $\ell = qm$ and $I_2(\ell) = 0$ otherwise. Integrating by parts three times in (18) and (19) we get after some calculation that

(20)
$$I_1(qm) + I_2(qm) = \frac{\sqrt{3}}{\pi} \frac{m}{n^2 q} (-1)^{qm} \cos\left(\frac{2\pi}{3}(m+n)q\right) + O\left(\frac{m^2}{n^3 q}\right).$$

Here the real part of the sum of the boundary terms obtained after the first integration by parts vanishes and we use that $(nq \pm 1)^{-1} =$ $(nq)^{-1} + O((nq)^{-2})$ in the boundary terms after the second integration by parts. Also, we estimate the final integrals that arise by

$$\int_{0}^{1/3} |1+e(u)|^{-qm-3} du = \int_{0}^{1/3} (2+2\cos u)^{(-qm-3)/2} du$$
$$\leq \int_{0}^{1/3} (4-9u)^{(-qm-3)/2} du \ll (qm)^{-1},$$

and similarly

$$\int_{1/3}^{1/2} |1 + e(u)|^{qm-3} du \ll (qm)^{-1}.$$

Theorem 6 now follows easily from (17) and (20).

7. A uniform result

Theorem 2 is a consequence of the the following more precise result together with the fact that $n = w(S) \ll p^{1/2}$, which was proved in Theorem 5.

9

THEOREM 7. Suppose that |S| = 3 and that n = w(S). Then

$$\frac{1}{2}\log|\Delta| = L'(-1,\chi) + O(p^{-1/2}\log n + n^{-2}),$$

with an absolute implied constant.

PROOF. In the notation of §5, since $\{0, m, n\}$ is assumed minimal we must have that (m, n) = 1. Thus Theorem 7 follows from Theorems 5 and 6 together with Smyth's evaluation [11] (see also [1, p.462]):

$$m(x+y+1) = \frac{3\sqrt{3}}{4\pi}L(2,\chi) = L'(-1,\chi).$$

Some of the ingredients in the proof of Theorem 7 generalize to sets S with |S| > 3. For instance, an analogue of Theorem 4 holds for quadrinomials, since one has a lower bound for the non-zero sum of four p-th roots of unity. Also, nontrivial upper bounds for the width of a set can be given more generally and an analogue of Theorem 5 can be proved for sets S with |S| = 4. Also, Theorem 6 can be generalized in certain ways (see [1] and [5]). However, the next interesting case of Myerson's conjectured asymptotic when S is a subgroup occurs for |S| = 5, and here no sufficiently strong lower bound for non-zero sums of five p-th roots of unity is known (see [9]). In fact, this interesting problem seems to be the central difficulty in extending the methods given in this paper to prove this conjecture.

Acknowledgements. This paper is the result of a visit in September, 2006 to the Division of Information and Communication Sciences at Macquarie University as a Visiting Fellow in Computing. I thank them for their support and hospitality. I also thank Igor Shparlinski for inviting me, Gerry Myerson for introducing me to the problems treated in this paper and both for their helpful suggestions. Finally, I thank the referee for several useful comments.

References

- D.W. Boyd, Speculations concerning the range of Mahler's measure. Canad. Math. Bull. 24 (1981), 453–469.
- [2] J.-Cl. Evard and F. Jafari, A complex Rolle's theorem. Amer. Math. Monthly 99 (1992), 858–861.
- [3] G. Everest and T. Ward, *Heights of polynomials and entropy in algebraic dynamics*. Universitext. Springer-Verlag London, Ltd., London, 1999.
- [4] S.V. Konyagin and I. E. Shparlinski, *Character sums with exponential functions and their applications*. Cambridge University Press, Cambridge, 1999.
- [5] W. M. Lawton, A problem of Boyd concerning geometric means of polynomials. J. Number Theory 16 (1983), 356–362.

- [6] D.H. Lehmer, Factorization of certain cyclotomic functions. Ann. of Math. (2) 34 (1933), 461–479.
- [7] G. Myerson, A combinatorial problem in finite fields. I. Pacific J. Math. 82 (1979), 179–187.
- [8] G. Myerson, A combinatorial problem in finite fields. II. Quart. J. Math. Oxford Ser. (2) 31 (1980), 219–231.
- [9] G. Myerson, Unsolved Problems: How Small Can a Sum of Roots of Unity Be? Amer. Math. Monthly 93 (1986), 457–459.
- [10] G. Myerson, A sampler of recent developments in the distribution of sequences. Number theory with an emphasis on the Markoff spectrum (Provo, UT, 1991), 163–190, Lecture Notes in Pure and Appl. Math., 147, Dekker, New York, 1993.
- [11] C.J. Smyth, On measures of polynomials in several variables. Bull. Austral. Math. Soc. 23 (1981), 49–63.

UCLA MATHEMATICS DEPT., BOX 951555, LOS ANGELES, CA 90095, USA *E-mail address*: wdduke@ucla.edu