# 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 $p \equiv 1 \bmod 3$ be a prime and $\omega$ a primitive cube root of unity in the finite field $\mathbb{F}_{p}=\{0,1, \ldots, p-1\}$. Also let $K=\mathbb{Q}(\zeta)$ be the $p$-th cyclotomic field, where $\zeta=e^{2 \pi i / p}$. Then, as $p \rightarrow \infty$,

$$
\begin{equation*}
\frac{1}{p} \log \left|N_{\mathbb{Q}}^{K}\left(\zeta+\zeta^{\omega}+\zeta^{\omega^{2}}\right)\right| \rightarrow L^{\prime}(-1, \chi)=.3231 \ldots \tag{1}
\end{equation*}
$$

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

Theorem 1. For $p \equiv 1 \bmod 3$

$$
\frac{1}{p} \log \left|N_{\mathbb{Q}}^{K}\left(\zeta+\zeta^{\omega}+\zeta^{\omega^{2}}\right)\right|=L^{\prime}(-1, \chi)+\mathrm{O}\left(p^{-1 / 2} \log p\right)
$$

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

[^0]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 $\left(n_{1}, \ldots, n_{p-1}\right) \in S^{p-1}$ of the equation

$$
\sum_{\ell \in \mathbb{F}_{p}^{*}} \ell n_{\ell}=t
$$

where $\mathbb{F}_{p}^{*}=\mathbb{F}_{p} \backslash\{0\}$. Clearly $N_{t}=N_{a t}$ 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 $S \mapsto a S+b$ 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

$$
N_{1}=\frac{1}{p}|S|^{p-1}-\frac{1}{p} \Delta \text { and } N_{0}=\frac{1}{p}|S|^{p-1}+\left(1-\frac{1}{p}\right) \Delta
$$

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

$$
\begin{equation*}
\Delta=\prod_{\ell \in \mathbb{P}_{p}^{*}} \sum_{n \in S} \zeta^{n \ell} . \tag{2}
\end{equation*}
$$

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

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

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 $\ell S$ 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 $\Delta$. 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 $\Delta$ 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 $p \equiv 1 \bmod |S|$ as $p \rightarrow \infty$. When $|S|=3$ so that $S=\left\{1, \omega, \omega^{2}\right\}$, he proved in [8] that

$$
\begin{equation*}
\frac{1}{p} \log |\Delta| \rightarrow \int_{0}^{1} \int_{0}^{1} \log |e(u)+e(v)+e(-u-v)| d u d v \tag{3}
\end{equation*}
$$

as $p \rightarrow \infty$ with $p \equiv 1 \bmod 3$. 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),

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

as giving an approximation to the integral in (3) by using the fact that $(\ell / p, \omega \ell / p)$ becomes uniformly distributed $(\bmod 1)$ as $\ell$ 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 $L^{\prime}(-1, \chi)$ for any set $S$ with $|S|=3$, provided that the "width" $\mathrm{w}(S)$ is large. Here, for any $S, \mathrm{w}(S)$ is defined to be the length of the smallest interval in $\{0,1,2, \ldots, p-1\}$ that contains an image $a S+b$ of $S$ under an affine transformation.

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

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

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 $S$.

To see that Theorem 1 follows from Theorem 2, it is enough to observe that $\mathrm{w}\left(\left\{1, \omega, \omega^{2}\right\}\right) \gg p^{1 / 2}$. 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 $c p^{1 / 2}$, 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 $(2 p-2) / 3$. Hence $3 a, 3 a \omega, 3 a \omega^{2}$ must be contained in an interval around 0 of length $3 c p^{1 / 2}$. Let $n$ and $m$ be the integers of smallest absolute value representing $3 a$ and $3 a \omega$, respectively. Then

$$
0<n^{2}+n m+m^{2} \equiv 0 \bmod p .
$$

This implies that $\frac{3}{2}\left(n^{2}+m^{2}\right) \geq p$, which is impossible for $c>0$ sufficiently small. Thus $\mathrm{w}\left(\left\{1, \omega, \omega^{2}\right\}\right) \gg p^{1 / 2}$. We remark that any set $S$ with $|S|=3$ satisfies $\mathrm{w}(S) \ll p^{1 / 2}$, 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

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

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

$$
\begin{equation*}
\mathrm{m}(f)=\log \mathrm{M}(f) \tag{4}
\end{equation*}
$$

Associated to $S=\left\{n_{1}, n_{2}, \ldots, n_{|S|}\right\}$ with $n_{1}<n_{2}<\cdots<n_{|S|}$, is the polynomial

$$
f_{S}(x)=x^{n_{1}}+x^{n_{2}}+\cdots+x^{n_{|S|}} .
$$

The following result shows that for fixed $S$ the basic asymptotic problem has a simple solution in terms of $\mathrm{m}\left(f_{S}\right)$.

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

$$
\frac{1}{p} \log |\Delta|=\mathrm{m}\left(f_{S}\right)+O\left(p^{-1} \log p\right)
$$

where the implied constant depends only on $S$.
Proof. Writing $f_{S}(x)=\prod_{\alpha}(x-\alpha)$, we see from (2) that

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

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

$$
\begin{equation*}
|S| \Delta=\prod_{\alpha}\left(1-\alpha^{p}\right) . \tag{5}
\end{equation*}
$$

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

$$
\begin{equation*}
\frac{1}{p} \log |\Delta|=\frac{1}{p} \sum_{\alpha} \log \left|1-\alpha^{p}\right|-\frac{1}{p} \log |S| \tag{6}
\end{equation*}
$$

If $|\alpha|>1$ then $\frac{1}{p} \log \left|1-\alpha^{p}\right|=\log |\alpha|+O\left(|\alpha|^{-p}\right)$ while if $|\alpha|<1$ then $\frac{1}{p} \log \left|1-\alpha^{p}\right|=O\left(|\alpha|^{p}\right)$. 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

$$
\log \left|1-\alpha^{p}\right|<_{\alpha} \log p
$$

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

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

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 $\left|1-\alpha^{p}\right|$ for $\alpha$ 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 $\mathrm{w}(S)$.

## 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 $\left|1-\alpha^{p}\right|$ 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 $\alpha$ a root of $f(x)=x^{n}+x^{m}+1=0$ with $|\alpha| \leq 1$ we have

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

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 $\ell \in \mathbb{Z}$

$$
\begin{equation*}
\left|\zeta^{\ell}-\alpha\right|>c_{1}(p n)^{-1} \tag{7}
\end{equation*}
$$

Fix $\ell$ and $\alpha$ and let $L$ denote the line segment from $\alpha$ to $\zeta^{\ell}$. By the complex mean value theorem given in [2] there are $z_{1}, z_{2} \in L$ so that

$$
\operatorname{Re} \frac{f\left(\zeta^{\ell}\right)-f(\alpha)}{\zeta^{\ell}-\alpha}=\operatorname{Re} f^{\prime}\left(z_{1}\right) \text { and } \operatorname{Im} \frac{f\left(\zeta^{\ell}\right)-f(\alpha)}{\zeta^{\ell}-\alpha}=\operatorname{Im} f^{\prime}\left(z_{2}\right)
$$

Thus

$$
\left|\frac{f\left(\zeta^{\ell}\right)-f(\alpha)}{\zeta^{\ell}-\alpha}\right| \leq 2 \max _{z \in L}\left|f^{\prime}(z)\right| \leq 4 n,
$$

which yields

$$
4 n\left|\zeta^{\ell}-\alpha\right| \geq\left|f\left(\zeta^{\ell}\right)\right|=\left|\zeta^{n \ell}+\zeta^{m \ell}+1\right|
$$

Since $p>3$ this sum three of $p$-th roots of unity cannot vanish and in fact must satisfy $\left|\zeta^{n \ell}+\zeta^{m \ell}+1\right| \geq c_{2} p^{-1}$ for some $c_{2}>0$ (see [9]), giving (7).

Write $\alpha=r e^{i \theta}$. By (7) there are constants $c_{3}, c_{4}>0$ so that at least one of the following holds:

$$
r<1-\frac{c_{3}}{p n} \quad \text { or } \quad\left|\theta-\frac{2 \pi \ell}{p}\right|>\frac{c_{4}}{p n} \quad \text { for all } \ell \in \mathbb{Z}
$$

In the first case

$$
\left|1-\alpha^{p}\right|>1-\left(1-\frac{c_{3}}{p n}\right)^{p}=\frac{c_{3}}{n}+O\left(n^{-2}\right)
$$

while in the second $|p \theta-2 \pi \ell|>c_{4} n^{-1}$ and hence

$$
\left|1-\alpha^{p}\right| \geq \sin \left(c_{4} n^{-1}\right)=\frac{c_{4}}{n}+O\left(n^{-3}\right)
$$

since $\sin \left(c_{4} n^{-1}\right)$ is the minimal distance from 1 to the ray at angle $c_{4} n^{-1}$. 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 $n=\mathrm{w}(S)$. 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

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

with an absolute implied constant.

Proof. By (5) we are reduced to considering

$$
\begin{equation*}
\Delta=\frac{1}{3} \prod_{\alpha}\left(1-\alpha^{p}\right) \tag{8}
\end{equation*}
$$

where $\alpha$ runs over all the zeros of $f$. Now

$$
\begin{aligned}
\sum_{\alpha} \log \left|1-\alpha^{p}\right|-p \mathrm{~m}(f) & =\sum_{\substack{|\alpha| \leq 1}} \log \left|1-\alpha^{p}\right|+\sum_{|\alpha|>1} \log \left|1-\alpha^{-p}\right| \\
& \ll n \log n
\end{aligned}
$$

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

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

Thus by (8) we have

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

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 $s=\lceil\sqrt{p}\rceil=[\sqrt{p}]+1$ and observe that at least one difference $k \ell-j \ell$ for $0 \leq j<k \leq s$ 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 $a S_{p}+b \subset\{0,1, \ldots, 2 s\}$. It follows that $n \ll p^{1 / 2}$.

## 6. Limits of Mahler measures

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

$$
\begin{equation*}
\mathrm{m}(f)=\int_{0}^{1} \int_{0}^{1} \log |f(e(u), e(v))| d u d v \tag{9}
\end{equation*}
$$

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

$$
\begin{equation*}
\int_{0}^{1} \log |e(u)-z| d u=\log ^{+}|z| \tag{10}
\end{equation*}
$$

where $\log ^{+} z=\log \max (1,|z|)$.
The following result expresses $\mathrm{m}(x+y+1)$ 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 $(m, n)=1$

$$
\mathrm{m}\left(x^{n}+x^{m}+1\right)=\mathrm{m}(x+y+1)+\alpha(m+n) n^{-2}+O\left(m n^{-3}\right)
$$

where

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

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

$$
\begin{equation*}
\log \left(1+x^{m}+x^{n}\right)=\log \left(1+x^{m}\right)+\sum_{\ell \geq 1} \frac{(-1)^{\ell-1}}{\ell}\left(\frac{x^{n}}{1+x^{m}}\right)^{\ell} \tag{12}
\end{equation*}
$$

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

$$
\begin{equation*}
\log \left(1+x^{m}+x^{n}\right)=\log \left(x^{n}\right)+\sum_{\ell \geq 1} \frac{(-1)^{\ell-1}}{\ell}\left(\frac{1+x^{m}}{x^{n}}\right)^{\ell} \tag{13}
\end{equation*}
$$

By (10) applied in (9)

$$
\begin{align*}
\mathrm{m}(x+y+1) & =\int_{0}^{1} \log ^{+}|1+e(u)| d u  \tag{14}\\
& =\int_{0}^{1} \log ^{+}|1+e(m u)| d u=\int \log |1+e(m u)| d u
\end{align*}
$$

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

$$
\begin{equation*}
I_{1}(\ell)=\int e(n \ell u)(1+e(m u))^{-\ell} d u \tag{15}
\end{equation*}
$$

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

$$
\begin{equation*}
I_{2}(\ell)=\int e(-n \ell u)(1+e(m u))^{\ell} d u \tag{16}
\end{equation*}
$$

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) $\mathrm{m}\left(x^{n}+x^{m}+1\right)=\mathrm{m}(x+y+1)+\operatorname{Re} \sum_{\ell \geq 1} \frac{(-1)^{\ell-1}}{\ell}\left(I_{1}(\ell)+I_{2}(\ell)\right)$.

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

$$
\begin{array}{r}
I_{1}(\ell)=\frac{1}{m} \sum_{k=0}^{m-1}\left(\int_{k}^{k+1 / 3}+\int_{k+2 / 3}^{k+1}\right) e\left(\frac{n \ell u}{m}\right)(1+e(u))^{-\ell} d u \\
=\frac{2}{m} \operatorname{Re} \sum_{k=0}^{m-1} e\left(\frac{k n \ell}{m}\right) \int_{0}^{1 / 3} e\left(\frac{n \ell u}{m}\right)(1+e(u))^{-\ell} d u \\
=2 \operatorname{Re} \int_{0}^{1 / 3} e(n q u)(1+e(u))^{-q m} d u \tag{18}
\end{array}
$$

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

$$
\begin{equation*}
I_{2}(\ell)=2 \operatorname{Re} \int_{1 / 3}^{1 / 2} e(-n q u)(1+e(u))^{q m} d u \tag{19}
\end{equation*}
$$

when $\ell=q m$ and $I_{2}(\ell)=0$ otherwise. Integrating by parts three times in (18) and (19) we get after some calculation that

$$
\begin{equation*}
I_{1}(q m)+I_{2}(q m)=\frac{\sqrt{3}}{\pi} \frac{m}{n^{2} q}(-1)^{q m} \cos \left(\frac{2 \pi}{3}(m+n) q\right)+O\left(\frac{m^{2}}{n^{3} q}\right) \tag{20}
\end{equation*}
$$

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

$$
\begin{array}{r}
\int_{0}^{1 / 3}|1+e(u)|^{-q m-3} d u=\int_{0}^{1 / 3}(2+2 \cos u)^{(-q m-3) / 2} d u \\
\leq \int_{0}^{1 / 3}(4-9 u)^{(-q m-3) / 2} d u \ll(q m)^{-1}
\end{array}
$$

and similarly

$$
\int_{1 / 3}^{1 / 2}|1+e(u)|^{q m-3} d u \ll(q m)^{-1}
$$

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 $n=\mathrm{w}(S) \ll p^{1 / 2}$, which was proved in Theorem 5.

THEOREM 7. Suppose that $|S|=3$ and that $n=\mathrm{w}(S)$. Then

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

with an absolute implied constant.
Proof. In the notation of $\S 5$, 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]):

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

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

[1] 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


[^0]:    Research supported in part by NSF Grant DMS-0355564.
    AMS Classification: 05A15 (12A15) .

