(P-1)-TH ROOTS OF UNITY MOD P^n, GENERALIZED HEILBRONN SUMS, LIND-LEHMER CONSTANTS, AND FERMAT QUOTIENTS

TODD COCHRANE, DILUM DE SILVA, AND CHRISTOPHER PINNER

Abstract. For \( n \geq 3 \) we obtain an improved estimate for the generalized Heilbronn sum \( \sum_{x=1}^{p-1} e_{p^n}(yx^{p^n-1}) \), and use it to show that any interval \( I \) of points in \( \mathbb{Z}_{p^n} \) of length \( |I| \gg p^{1.825} \) for \( n = 2 \), \( |I| \gg p^{2.959} \) for \( n = 3 \), \( |I| \geq p^{n-3.269(34/151)+o(1)} \) for \( n \geq 4 \), contains a \((p-1)\)-th root of unity. As a consequence, we derive an improved estimate for the Lind-Lehmer constant for the abelian group \( \mathbb{Z}_{p^n}^\ast \), and improved estimates for Fermat quotients.

1. Introduction

Let \( p \) be a prime, \( n \in \mathbb{N} \), \( \mathbb{Z}_{p^n}^\ast \) be the group of units mod \( p^n \) and \( G_n \subset \mathbb{Z}_{p^n}^\ast \) be the subgroup of \((p-1)\)-th roots of unity,

\[
G_n := \{ x \in \mathbb{Z}_{p^n}^\ast : x^{p-1} = 1 \} = \{ x^{p^{n-1}} : 1 \leq x \leq p-1 \}.
\]

For \( y \in \mathbb{Z} \) let \( S_n(y) \) denote the generalized Heilbronn sum

\[
S_n(y) := \sum_{x \in G_n} e_{p^n}(yx) = \sum_{x=1}^{p-1} e_{p^n}(yx^{p^n-1}),
\]

where \( e_{p^n}(\cdot) = e^{2\pi i \cdot / p^n} \), and let

\[
H_n = \max_{p^n \nmid y} |S_n(y)|.
\]

Our interest here is in estimating \( H_n \) and studying the distribution of points in \( G_n \).

In particular, we wish to determine how large \( M \) must be so that any interval of length \( M \) is guaranteed to contain an element of \( G_n \). Equivalently, we wish to determine an upper bound on the maximal gap between consecutive \((p-1)\)-th roots of unity. It is well known that an estimate for \( H_n \) leads to a corresponding estimate on the size of the gap. We make this explicit in Corollary 3.1 where we prove that any interval of length \( |I| \geq 3p^{n-1}H_n \) contains an element of \( G_n \).

The current best estimate for \( H_2 \) is due to Shkredov [17, Theorem 15],

\[
H_2 \ll p^{2} \log^{2} p,
\]

improving on earlier bounds of Heath-Brown [7], Heath-Brown and Konyagin [8], and Shkredov [16], and we make no further improvement here. For \( n \geq 3 \), Malykhin...
[14, Corollary 1] obtained $H_n \ll_n p^{1-\frac{3.906}{n}}$ for $n \geq 3$. Bourgain and Chang [1, Corollary 4.4] also obtained a nontrivial bound of the type $H_n \ll p^{1-\delta_n}$, for some undetermined constant $\delta_n > 0$, as a special case of their very general exponential sum estimate over subgroups of $\mathbb{Z}_n^*$, with $m$ composite. Here, we use the bound for $H_2$ in (1.2) and a recent energy estimate of Shkredov, Solodkova, and Vyugin [18] to refine the estimate of Malykhin, obtaining in Theorem 8.1 and Corollary 8.1

\begin{align}
H_3 &\ll p^{1-\frac{2}{9}} + o(1) = p^{0.9568} + o(1), \\
H_n &\ll p^{1-3.269\left(\frac{\pi}{15}\right)^n} + o(1), \quad \text{for } n \geq 4.
\end{align}

The same estimate for $H_3$ was also obtained recently by Shteinikov [21, Theorem 13], in a similar manner.

We deduce at once from Corollary 3.1 the following result for $n \geq 3$.

**Theorem 1.1.** Any interval $\mathcal{I} \subset \mathbb{Z}_{p^n}$ of length as given below contains an element of $G_n$.

\[ |\mathcal{I}| \geq \begin{cases} 
p^{2-\frac{29}{30}} + o(1), & \text{if } n = 2; \\
p^{3-\frac{29}{30}} + o(1), & \text{if } n = 3; \\
p^n - 3.269\left(\frac{29}{15}\right)^n + o(1), & \text{if } n \geq 4.
\end{cases} \]

To be precise, for $n = 2$ the $o(1)$ is an undetermined function of $p$ that goes to 0 as $p \to \infty$, while for $n \geq 3$, $o(1) = c_n \log \log p/\log p$ for some effectively computable constant $c_n$. The estimate given for the case $n = 2$ does not follow from Theorem 3.1, but requires instead a method of Konyagin and Shparlinski [10] given in Section 4; the proof for $n = 2$ following in Section 5. As a consequence of the theorem we obtain an improved estimate for the Lind-Lehmer constant for the abelian group $\mathbb{Z}_p^n$ (Section 2), and improved estimates for Fermat quotients (Section 6).

### 2. The Lind-Lehmer Constant for Finite Abelian Groups

Our interest in the distribution of elements of $G_n$ was originally motivated by the problem of determining the Lind-Lehmer constant for the group $\mathbb{Z}_p^n$.

For a polynomial $F(x) = a_0 \prod_{i=1}^{m} (x - \alpha_i) \in \mathbb{C}[x]$ one defines the traditional Mahler measure $M(F) = |a_0| \prod_{i=1}^{m} \max\{1, |\alpha_i|\}$ and the logarithmic Mahler measure $m(F) = \log M(F)$. Famously Lehmer [11] asked whether there exists a constant $c > 0$ such that for any polynomial $F$ in $\mathbb{Z}[x]$ either $m(F) = 0$ or $m(F) > c$.

By Jensen’s formula one can write

\[ m(F) = \int_0^1 \log |F(e^{2\pi ix})| \, dx \]

allowing one to generalize the concept of Mahler measure to $F \in \mathbb{C}[x_1, \ldots, x_n]$

\[ m(F) := \int_0^1 \cdots \int_0^1 \log |F(e^{2\pi ix_1}, \ldots, e^{2\pi ix_n})| \, dx_1 \cdots dx_n. \]

Since, see for example Boyd [4],

\[ m(F(x_1, x_2, \ldots, x_n)) = \lim_{k \to +\infty} m(F(x, x^k, x^{k^2}, \ldots, x^{k^{n-1}})), \]

the infimum of positive measures over polynomials in $\mathbb{Z}[x_1, \ldots, x_n]$ reduces to the classical one variable Lehmer problem.
Lind [13], viewing (2.1) as an integral over the group \( \mathbb{R}/\mathbb{Z} \times \cdots \times \mathbb{R}/\mathbb{Z} \) and \( F(e^{2\pi i x_1}, \ldots, e^{2\pi i x_n}) \) as a linear sum of characters on that group, generalized the concept of Mahler measure to an arbitrary compact abelian group \( G \) with normalized Haar measure \( \mu \) and dual group of characters \( \hat{G} \), defining, for an \( f \) in \( \mathbb{Z}[\hat{G}] \),

\[
m_G(f) = \int_G \log |f| d\mu.
\]

Analogous to the Lehmer problem one can ask what is the smallest positive measure for that group and define a Lind-Lehmer constant

\[
\lambda(G) := \inf \{ m_G(f) : f \in \mathbb{Z}[\hat{G}], \ m_G(f) > 0 \}.
\]

For example, for a finite abelian group \( G = \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n} \), and \( F \in \mathbb{C}[x_1, \ldots, x_n] \) one can define, as a natural counterpart to (2.1), the measure

\[
m_G(F) = \frac{1}{|G|} \sum_{j_1=1}^{m_1} \cdots \sum_{j_n=1}^{m_n} \log |F(e^{2\pi i j_1/m_1}, \ldots, e^{2\pi i j_n/m_n})|;
\]

and \( \lambda(G) \) will be the minimum positive measure \( m_G(F) \) over the \( F \in \mathbb{Z}[x_1, \ldots, x_n] \).

In [22] the latter two authors showed that

\[
\lambda(\mathbb{Z}_2^n) = \frac{1}{2^n} \log (2^n - 1),
\]

and for an odd prime \( p \) that

\[
\lambda(\mathbb{Z}_p^n) = \frac{1}{p^n} \log M_n,
\]

where,

\[
M_n := \min \{ 2 \leq a \leq p^n - 1 : a \in G_n \}.
\]

Thus an upper bound on the Lehmer constant \( \lambda(\mathbb{Z}_p^n) \) will follow at once from any limitation on the size of an interval not containing an element of \( G_n \). In the next section we relate this to bounds on the Heilbronn sums, in particular we show that

\[
M_n \leq 3p^{n-1}H_n.
\]

3. Using estimates for \( H_n \) to estimate gap sizes

In this section we use the standard method to obtain a basic theorem relating the distribution of elements of \( G_n \) to the estimation of the Heilbronn sum. In fact the result we obtain can be stated for any subgroup \( G \) of \( \mathbb{Z}_{p^n}^* \). Set

\[
\Phi_G = \max_{p^n \mid \mathbb{Z}} \left| \sum_{x \in G} e_{p^n}(yx) \right|.
\]

**Theorem 3.1.** For any prime power \( p^n \) and subgroup \( G \) of \( \mathbb{Z}_{p^n}^* \), any interval \( \mathcal{I} \subset \mathbb{Z}_{p^n} \) of length \( |\mathcal{I}| \geq 2(\Phi_G/|G|)p^n \) contains an element of \( G \).

Applying the theorem to \( G_n \) and using the fact that \( |G_n| = p - 1 \geq \frac{3}{5}p \), for odd \( p \), we obtain the following corollary. (The statement is trivial for \( p = 2 \).)

**Corollary 3.1.** For any prime power \( p^n \), any interval \( \mathcal{I} \subset \mathbb{Z}_{p^n} \) of length \( |\mathcal{I}| \geq 3p^{n-1}H_n \) contains an element of \( G_n \).
Proof of Theorem 3.1. Let $\alpha : \mathbb{Z}_{p^n} \to \mathbb{R}$ be a real valued function supported on an interval $\mathcal{I}$ as given in (1.1). If we can show that $\sum_{x \in \mathcal{G}} \alpha(x) > 0$ then it follows that $G \cap \mathcal{I}$ is nonempty. To this end, we let $\alpha(x) = \sum_{y=1}^{p^n} a(y)e_{p^n}(yx)$, be the Fourier expansion of $\alpha$, where for any $y$, $a(y) = p^{-n}\sum_{x=1}^{p^n} e_{p^n}(-yx)\alpha(x)$. Also, for any integer $y$, put

$$S(y) := \sum_{x \in \mathcal{G}} e_{p^n}(yx).$$

Then

$$\sum_{x \in \mathcal{G}} \alpha(x) = \sum_{x \in \mathcal{G}} \sum_{y=1}^{p^n} a(y)e_{p^n}(yx)$$

$$= p^{-n}|G|\sum_{x=1}^{p^n} \alpha(x) + \sum_{y=1}^{p^n-1} a(y)S(y) := M_{\alpha} + E_{\alpha},$$

say. We call $M_{\alpha}$ the main term of (3.1), and $E_{\alpha}$ the error term.

The simplest way to bound the error term $E_{\alpha}$ is just to say

$$|E_{\alpha}| \leq \sum_{y=1}^{p^n-1} |a(y)||S(y)| \leq \Phi_G \sum_{y=1}^{p^n-1} |a(y)|.$$  

We apply this estimate to the weighted function $\alpha = 1_{\mathcal{J}} * 1_{\mathcal{K}}$, where

$$\mathcal{J} = \{1, 2, \ldots, [M/2]\}, \quad \mathcal{K} = \{a, \ldots, a + [M/2]\}.$$  

Here, $1_{\mathcal{J}}$ and $1_{\mathcal{K}}$ are the characteristic functions of the intervals $\mathcal{J}, \mathcal{K}$, say with Fourier coefficients $a_{\mathcal{J}}(y), a_{\mathcal{K}}(y)$ respectively, and $*$ denotes convolution. We note that $\alpha$ is supported on $\mathcal{I},$

$$M_{\alpha} = p^{-n}|G|\sum_{x=1}^{p^n} \alpha(x) = p^{-n}|G||\mathcal{J}||\mathcal{K}|,$$

and that

$$a(y) = p^n a_{\mathcal{J}}(y)a_{\mathcal{K}}(y).$$

Thus, by the Cauchy-Schwarz inequality and Parseval’s identity,

$$\sum_{y=1}^{p^n} |a(y)| = p^n \sum_{y=1}^{p^n} |a_{\mathcal{J}}(y)||a_{\mathcal{K}}(y)| \leq p^n \left( \sum_{y=1}^{p^n} |a_{\mathcal{J}}(y)|^2 \right)^{1/2} \left( \sum_{y=1}^{p^n} |a_{\mathcal{K}}(y)|^2 \right)^{1/2}$$

$$= p^n p^{-n} \left( \sum_{x=1}^{p^n} |1_{\mathcal{J}}(x)|^2 \right)^{1/2} \left( \sum_{x=1}^{p^n} |1_{\mathcal{K}}(x)|^2 \right)^{1/2} = |\mathcal{J}|^{1/2}|\mathcal{K}|^{1/2},$$

and so the main term $M_{\alpha}$ in (3.1) exceeds the error term $E_{\alpha}$ provided that

$$p^{-n}|G||\mathcal{J}||\mathcal{K}| > \Phi_G |\mathcal{J}|^{1/2}|\mathcal{K}|^{1/2},$$

that is,

$$|\mathcal{J}||\mathcal{K}| > \Phi_G |\mathcal{J}|^{1/2}|\mathcal{K}|^{1/2}.$$  

Since $|\mathcal{J}||\mathcal{K}| = [M/2] \left(1 + \left[ M/2 \right]\right) > M^2/4$, we see that it suffices to have $M \geq 2(\Phi_G/|G|)^{1/2}$, establishing the theorem. \qed
4. Improving the Error estimate

We can improve the estimate of the error term in certain cases using a method of Konyagin and Shparlinski [10, Chapter 7]. The same method was also used for related problems in [3] and [2]. Let \( q = p^n \) and \( G \) be any subgroup of \( \mathbb{Z}_q^* \). Partition \( \mathbb{Z}_q^* \) into the different cosets of \( G \),

\[ \mathbb{Z}_q^* = Gy_1 \cup Gy_2 \cup \cdots \cup Gy_L, \]

where \( L = (p^n - p^{n-1})/|G| \). Fix a parameter \( h < p \), to be determined later, and let

\[ N_i := \# \{ y \in Gy_i : 0 < |y| \leq h \}, \]

and

\[ \phi_i := |S(y_i)|. \]

It is plain that \( \phi_i \) just depends on the coset \( Gy_i \) and not on the representative \( y_i \). Let

\[ \alpha = 1_{J_1} * 1_{J_2} * \cdots * 1_{J_k} \]

where the \( J_i \) are intervals of length \( m = \lfloor \frac{M}{2} \rfloor \), chosen so that \( \alpha \) is supported on \( I \). Then the Fourier coefficients of \( \alpha \) satisfy

\[ a(0) = q^{-1}m^k, \]

and for any \( y \neq 0 \), with \( |y| \leq q/2 \), we have

\[ |a(y)| = \frac{1}{q} \frac{\left| \sin^k(\pi ym/q) \right|}{\sin^k(\pi y/q)} \leq \min \left\{ \frac{m^k}{q}, \frac{q^{k-1}}{2^k|y|^k} \right\}. \]

Thus, to estimate the error term in (3.1), we write

\[ |E_\alpha| = \sum_{y=1}^{q-1} a(y)S(y) = \left| \sum_{0 < |y| \leq q/2} a(y)S(y) \right| \leq \sum_{0 < |y| \leq h} |a(y)||S(y)| + \sum_{h < |y| \leq q/2} |a(y)||S(y)| = \Sigma_1 + \Sigma_2, \]

say. Noting that for \( 0 < |y| \leq h < p \) we must have \( y \in \mathbb{Z}_q^* \), we obtain

\[ \Sigma_1 \leq \frac{m^k}{q} \sum_{0 < |y| < h} |S(y)| = \frac{m^k}{q} \sum_{i=1}^L \sum_{0 < |y| < h, y \in Gy_i} \phi_i = \frac{m^k}{q} \sum_{i=1}^L N_i \phi_i, \]

while for \( \Sigma_2 \) we have by the definition of \( \Phi_G \) and (4.1),

\[ \Sigma_2 \leq \max_{y \neq 0} |S(y)| \sum_{h \leq |y| \leq q/2} \frac{q^{k-1}}{2^k|y|^k} \leq \Phi_G \frac{q^{k-1}}{2^k-1} \left( \frac{1}{h^k} + \frac{1}{(k-1)h^{k-1}} \right) \leq \Phi_G q^{k-1}(k + h - 1) \frac{1}{2^k-1} \frac{1}{h^{k-1}(k - 1)}. \]

We succeed with this method provided that \( \Sigma_1 \leq \frac{1}{2}M_\alpha \) and \( \Sigma_2 < \frac{1}{2}M_\alpha \), with \( M_\alpha \) the main term in (3.1),

\[ M_\alpha = q^{-1}|G| \sum_x \alpha(x) = q^{-1}|G|m^k. \]
Thus, it suffices to have
\[
\frac{\Phi_G q^{k-1}(k + h - 1)}{2^{k-1}h^k(k-1)} < \frac{mk|G|}{2q}, \quad \text{and} \quad \frac{m}{q} \sum_{i=1}^{L} N_i \phi_i \leq \frac{|G|m^k}{2},
\]
or equivalently
\[
m > \left( \frac{4\Phi_G(k + h - 1)}{|G|(k-1)} \right) \frac{q}{h}, \quad \text{and} \quad \sum_{i=1}^{L} N_i \phi_i \leq \frac{|G|}{2}.
\]
Taking \( k = \lfloor \log p \rfloor \) and observing that
\[
\left( \frac{4\Phi_G(k + h - 1)}{|G|(k-1)} \right)^\frac{q}{h} \leq \left( \frac{4(k + h - 1)}{k-1} \right)^\frac{q}{h} \leq 4 \left( 1 + \frac{p}{|\log p|} \right)^\frac{q}{h} < 6,
\]
(the maximum value of the latter expression, 5.2915..., occurring at \( p = 7 \)), we see that the first condition holds provided that \( m \geq \frac{3q}{4} \). Thus we arrive at the following generalization and refinement of [10, Lemma 7.1], which was stated for the case of subgroups of \( \mathbb{Z}_p^* \).

**Proposition 4.1.** Suppose \( q = p^n \) is a prime power, \( G \) is a subgroup of \( \mathbb{Z}_p^* \) and that \( h < p \) is such that \( \sum_{i=1}^{L} N_i \phi_i < \frac{|G|}{2} \). Then any interval of length \( M \geq \frac{3q}{4}|\log p| \), contains a point in \( G \).

In comparison, the result of [10, Lemma 7.1] for \( n = 1 \), requires \( M \gg_{\epsilon} p^{1+\epsilon}/h \) for the same conclusion.

We can estimate the sum \( \sum_{i=1}^{L} N_i \phi_i \) using the Hölder inequality,

\[
(4.3) \quad \sum_{i=1}^{L} N_i \phi_i \leq \left( \sum_{i=1}^{L} N_i \right)^{\frac{1}{2}} \left( \sum_{i=1}^{L} N_i^2 \right)^{\frac{1}{2}} \left( \sum_{i=1}^{L} \phi_i^4 \right)^{\frac{1}{4}}.
\]

Now
\[
\sum_{i=1}^{L} N_i = \sum_{i=1}^{L} \sum_{y \in G y_i, |y| \leq h} 1 = \sum_{y \in \mathbb{Z}_p^*} 1 \leq 2h,
\]
\[
\sum_{i=1}^{L} N_i^2 = \sum_{i=1}^{L} \# \{(y, z) : y, z \in G y_i, |y| \leq h, |z| \leq h\} = N(h),
\]
where
\[
N(h) := \# \{(y, z) : y/z \in G, |y| \leq h, |z| \leq h\},
\]
and
\[
\sum_{i=1}^{L} \phi_i^4 = \sum_{i=1}^{L} \left| \sum_{x \in G} e_q(y_i x) \right|^4 = \frac{1}{|G|} \sum_{y \in \mathbb{Z}_p^*} \left| \sum_{x \in G} e_q(y x) \right|^4
\]
\[
\leq \frac{1}{|G|} \sum_{y \in \mathbb{Z}_p^*} \left| \sum_{x \in G} e_q(y x) \right|^4 = \frac{q}{|G|} T_2(G),
\]
where \( T_2(G) \) is the additive energy of \( G \),
\[
T_2(G) := \# \{(x_1, x_2, y_1, y_2) : x_1, y_i \in G, x_1 + x_2 = y_1 + y_2\}.
\]
Thus, by (4.3), we have

\[(4.4)\quad \sum_{i=1}^{L} N_i \phi_i \leq \sqrt{2h^{\frac{1}{2}}} N(h)^{\frac{1}{2}} \left( \frac{q}{|G|} \right)^{\frac{1}{4}} T_2(G)^{\frac{1}{4}}.\]

In order to proceed further, one needs good estimates for \(N(h)\) and for \(T_2(G)\). It was established by Bourgain, Konyagin and Shparlinski [3, Theorem 1], that for any nonnegative integer \(q\), subgroup \(G\) of \(\mathbb{Z}_q^*\) and positive integer \(\nu\),

\[N(h) \leq hq^{\frac{1}{4\nu}} + o(1) + h^{2}q^{-\frac{1}{2\nu}+o(1)},\]

where the \(o(1)\) indicates a function that tends to zero as \(q \to \infty\). The optimal choice for our application is \(\nu = 6\), where we have

\[(4.5)\quad N(h) \leq hq^{\frac{1}{6}} + o(1) + h^{2}q^{-\frac{1}{6}+o(1)}.\]

In the next section we apply this estimate to the subgroup \(G_2\) of \((p - 1)\)-th roots of unity in \(\mathbb{Z}_p^*\).

5. Proof of the \(n = 2\) Case of Theorem 1.1

Inserting the bound for \(N(h)\) in (4.5), and the current record breaking bound for \(T_2(G_2)\) due to Shkredov, Solodkova, and Vyugin, [18, Theorem 24]

\[(5.1)\quad T_2(G_2) \ll p^{\frac{11}{12}} \log^{\frac{11}{12}} p \ll p^{2.46153... + o(1)},\]

we obtain from (4.4),

\[(5.2)\quad \sum_{i=1}^{L} N_i \phi_i \ll h^{\frac{1}{2}} \left( h^{\frac{1}{2}} p^{\frac{3793}{1000}+o(1)} + h^{\frac{1}{2}} p^{-\frac{3793}{1000}+o(1)} \right) p^{\frac{1}{4}} (p^{\frac{11}{12}} \log^{\frac{11}{12}} p)^{\frac{1}{4}} \leq h^{\frac{3}{2}} p^{\frac{3793}{1000}+o(1)} + hp^{\frac{257}{1000}+o(1)}.\]

Thus, Proposition 4.1 applies provided that \(h \ll p^{\frac{3793}{1000}+o(1)}\), and so we see that any interval of length \(|I| \geq p^{\frac{3793}{1000}+o(1)} = p^{1.82448...+o(1)}\) contains a \(p\)-th power, proving the \(n = 2\) case of Theorem 1.1.

Remark 5.1. It is conjectured [3] that for \(\epsilon > 0\), and \(h < p^{n-1}\),

\[(5.3)\quad N(h) \ll \epsilon hq^\epsilon.\]

See also the analogous conjecture in [10, Question 7.8] for the case of prime moduli. Such a bound follows from GRH as we demonstrate in the following proposition.

If we use the conjectured upper bound on \(N(h)\) in the argument above we would obtain the improvement \(|I| \geq p^{\frac{3793}{1000}+\epsilon} = p^{1.81481...+\epsilon}\).

Proposition 5.1. On the assumption of GRH we have that for \(h < q\),

\[N(h) \ll \epsilon h^2 p^{-\epsilon} + hq^\epsilon.\]
Proof. We have
\[
N(h) = \frac{1}{p^{n-1}} \sum_{|y| \leq h} \sum_{|z| \leq h} \sum_{\chi(y/z) \neq \chi_0} \chi(y/z) \\
\ll \frac{h^2}{p^{n-1}} + \frac{1}{p^{n-1}} \sum_{\chi \neq \chi_0} \left| \sum_{y=1}^{h} \chi(y) \right|^2 \\
\ll \epsilon \frac{h^2}{p^{n-1}} + \frac{1}{p^{n-1}} h^{n-1} \left( h^{1/2} q^2 \right)^2,
\]
the latter inequality being a consequence of GRH, as noted by Montgomery and Vaughan [15]. □

Remark 5.2. The estimate for \( n = 2 \) has strong parallels with the following result of Shteinikov [21, Theorem 10] for subgroups of \( \mathbb{Z}_p^* \). We restate his result in the notation of this paper.

**Theorem 5.1.** Let \( G \) be a subgroup of \( \mathbb{Z}_p^* \) of order \( |G| \geq \sqrt{p} \). Then any interval \( I \) of length \( |I| \geq p^{\frac{1}{5977} + o(1)} \) contains an element of \( G \).

The square root threshold needed for applying the theorem, in the context of subgroups of \( \mathbb{Z}_p^* \), is satisfied by \( G_2 \) when \( n = 2 \), where \( |G_2| = (p - 1) \) is roughly \( \sqrt{p} \), but fails for \( G_n \) with \( n > 2 \). This is why we were able to obtain the improvement for \( n = 2 \) but not for \( n > 2 \). The proof in [21] follows a similar line of argument as our proof above for \( n = 2 \). Indeed, its main appeal is to the result of Konyagin and Shparlinski [10, Lemma 7.1] (analogous to our Proposition 4.1) and to the estimate of Bourgain, Konyagin and Shparlinski in (4.5) (with \( q = p \)).

6. Fermat Quotients

For prime power \( p^n \) with \( n \geq 2 \) and integer \( u \) with \( p \nmid u \), we define the Fermat quotient \( q_{p^{n-1}}(u) \) to be the unique integer with \( 0 \leq q_{p^{n-1}}(u) \leq p^{n-1} - 1 \) and
\[
q_{p^{n-1}}(u) \equiv \frac{u^{p-1} - 1}{p} \pmod{p^{n-1}}.
\]
It is plain that \( q_{p^{n-1}} \) is constant on any coset of \( G_n \) and that it takes on distinct values on distinct cosets of \( G_n \). Thus the Fermat quotients take on all values from 0 to \( p^{n-1} - 1 \) as \( u \) runs through a complete residue system mod \( p^n \). Following Shparlinski [19], we define \( \Lambda_{p^{n-1}} \) to be the minimal value \( L \) such that on any interval of length \( L \), \( q_{p^{n-1}}(u) \) takes on a full spectrum of values from 0 to \( p^{n-1} - 1 \),
\[
\Lambda_{p^{n-1}} := \min \{ L : \forall K \in \mathbb{Z}, \text{ we have } \# \{ q_{p^{n-1}}(K + 1), \ldots, q_{p^{n-1}}(K + L) \} = p^{n-1} \}.
\]
A value \( L \) is permissible if for any coset of \( G_n \) and any interval \( I \) of length \( L \), \( I \) contains an element of the coset. It is plain from the proof of Theorem 1.1 that the theorem holds identically with \( G_n \) replaced with any coset of \( G_n \). Thus we obtain,

**Theorem 6.1.** We have
\[
\Lambda_{p^{n-1}} \leq \begin{cases}
  p^{2 - \frac{12}{34n} + o(1)}, & \text{if } n = 2; \\
  p^{3 - \frac{10}{32} + o(1)}, & \text{if } n = 3; \\
  p^{n - 3.269 \left( \frac{34}{n} \right)} + o(1), & \text{if } n \geq 4.
\end{cases}
\]
Theorem 6.2. i) We have \( u / \ell \) have been obtained that hold for almost all primes, \( \ell \) taking \(|I| \leq n \) above. For the convenience of the reader, we include a proof here. The estimate weaker than the bound in part i). The estimate in i) is the result of [18] mentioned ii) for \( n \) above. For the convenience of the reader, we include a proof here. The estimate in i) is the result of [18] mentioned

From Bourgain, Ford, Konyagin and Shparlinski [2] to \( \ell_p \leq (\log p)^{3276+o(1)} \) as \( p \to \infty \), by Shkredov [16] to \( \ell_p \leq (\log p)^{463+o(1)} \), and by Shkredov, Solodkova and Vyugin [18, Theorem 28] to \( \ell_p \leq (\log p)^{3276+o(1)} = (\log p)^{1.82448\ldots+o(1)} \). Sharper estimates have been obtained that hold for almost all primes, \( \ell_p \leq (\log p)^{3/2+\epsilon} \) in [2] and \( \ell_p \leq (\log p)^{2+\epsilon} \) in [20]. Granville [6, Conj. 10] conjectured that \( \ell_p = o(\log^{1/p} p) \). Lenstra [12] suggested that the truth may in fact be \( \ell_p \leq 3 \) for all \( p \).

Here, we generalize the problem to any prime power \( p^n \) with \( n \geq 2 \), defining \( \ell_{p^{n-1}} \) to be the minimal positive integer \( u \) such that \( p^n \) is not a divisor of \( p^{n-1} - 1 \), that is \( u \notin G_n \).

**Theorem 6.2.** i) We have \( \ell_p \leq (\log p)^{2-\frac{3276}{\log p}+o(1)} \), as \( p \to \infty \).

ii) For \( n \geq 2 \), given an upper bound \( H_n \leq p^{1-\epsilon_n} \) on the Heilbronn sum, we have

\[
\ell_{p^{n-1}} \leq n(\log p)^{1+\frac{1}{\log p}+o(1)},
\]

as \( p^n \to \infty \).

We note that the upper bound in ii) for \( n = 2 \) using \( H_2 \ll p^{1/2+o(1)} \), is slightly weaker than the bound in part i). The estimate in i) is the result of [18] mentioned above. For the convenience of the reader, we include a proof here. The estimate in ii) for \( n = 3 \), using \( H_3 \leq p^{1-\frac{3793}{\log p}+o(1)} \), was obtained by Shkredov [21, Theorem 16]. For \( n \geq 4 \), using the estimate for \( H_n \) in (1.4), we obtain from ii),

\[
(6.1) \quad \ell_{p^{n-1}} \leq n(\log p)^{1+\frac{1}{\log p} - \frac{3276}{\log p} (\frac{34}{151})^n + o(1)}.
\]

**Proof.** i) The proof follows identically as in [2] (and its subsequent improvements), and so we sketch only the outline here. One starts with the upper bound of [3, Lemma 12], which in the notation of Section 4 can be stated for any interval \( I \) of points in \( \mathbb{Z}_{p^n} \),

\[
|G_n \cap I| \ll_{\epsilon} \frac{(p-1)}{q} |I| + \frac{|I|}{q} \sum_{i=1}^{L} N_i \phi_i,
\]

with \( h = \min\{q^1+\epsilon/|I|, q/2\} \). Using the upper bound in (5.2), we have for \( n = 2 \),

\[
|G_2 \cap I| \ll_{\epsilon} \frac{|I|}{p^2} \left( p + h^2 p^{\frac{3793}{463}+o(1)} + hp^{\frac{375}{463}+o(1)} \right).
\]

Taking \( |I| = |p^2 - \frac{375}{463}+3\epsilon | \), we have \( h \ll p^{\frac{375}{463}-\epsilon} \), and

\[
|G_2 \cap I| \ll_{\epsilon} \frac{|I|}{p^2}.
\]

Next, let \( I = [1,M] \), with \( M = |p^2 - \frac{375}{463}+3\epsilon | \). Since \( u^{p-1} \equiv 1 \) (mod \( p^2 \)) for all \( u \leq \ell_p \), the same is true for all integers in \( I \) comprised of prime factors \( \leq \ell_p \). By [9, Theorem 2.1], the number of such integers is at least \( M^{1-\log \log M / \log \ell_p} \), and thus

\[
M^{1-\log \log M / \log \ell_p} \ll M/p,
\]
from which the theorem follows.

ii) For $n \geq 3$, we follow the method of Section 3, taking (with $M$ even) $I = [1, M]$, $J = [-\frac{M}{2} + 1, \frac{M}{2}]$, $\alpha = 1_I \ast 1_J$. Noting that $\alpha(x) \geq M/2$ on $I$, we obtain the upper bound

$$|G_n \cap I| \leq \frac{2}{M} \sum_{x \in G_n} \alpha(x) \leq \frac{2}{M} \left( p^{-n} |G_n|M^2 + H_n M \right) < \frac{|I|}{p^{n-1}} + 2H_n.$$

Say $H_n \leq p^{1-\epsilon_n}$. Then with $M = \lceil p^{n-\epsilon_n} \rceil$ we have $|G_n \cap I| \leq 4 \frac{M}{p^{n-1}}$ and so as above,

$$M^{1-\log \log M/\log \ell_{n-1}} \leq 4M/p^n,$$

from which we derive

$$\ell_{p^{n-1}} \leq n(\log p)^{1+\frac{1}{16} + o(1)},$$

as $p^n \to \infty$.

\[ \square \]

7. Asymptotic Formula for $T_k(G_n)$

For $k \in \mathbb{N}$, let $G_n^{2k}$ denote the cartesian product of $G_n$ with itself $2k$-times and

$$T_k(G_n) = \# \{(x, y) \in G_n^{2k} : x_1 + \cdots + x_k = y_1 + \cdots + y_k \}$$

$$= \# \left\{ (x, y) \in \mathbb{Z}^{2k} : 1 \leq x_i, y_i \leq p-1, \sum_{i=1}^k x_i^{p^{n-1}} = \sum_{i=1}^k y_i^{p^{n-1}} \pmod{p^n} \right\}.$$

In particular, $T_1(G_n) = |G_n|$ and $T_2(G_n)$ denotes the additive energy of the group $G_n$. As noted by Malykhin [14] we have the elementary estimate,

\begin{equation}
(7.1) \quad T_k(G_n) \leq T_k(G_{n-1})
\end{equation}

for any $k, n$ with $n \geq 2$. The estimate follows from the observation that if $1 \leq x_i, y_i < p$ are integers such that

$$x_1^{p^{n-1}} + \cdots + x_k^{p^{n-1}} = y_1^{p^{n-1}} + \cdots + y_k^{p^{n-1}} \pmod{p^n},$$

then, since $x_i^{p^{n-1}} \equiv x_i^{p^{n-2}} \pmod{p^{n-1}}$, we also have

$$x_1^{p^{n-2}} + \cdots + x_k^{p^{n-2}} \equiv y_1^{p^{n-2}} + \cdots + y_k^{p^{n-2}} \pmod{p^{n-1}}.$$

As noted in (5.1), Shkredov, Solodkova, and Vyugin established that $T_2(G_2) \ll p^{\frac{\sqrt{5}}{2} \log \frac{\sqrt{5}}{2}}$. In the next section we obtain $T_3(G_2) \ll p^{\frac{\sqrt{14}}{2} \log \frac{\sqrt{14}}{2}}$, and prove asymptotic results for $T_k(G_n)$. The key lemma needed for proving these is as follows.

**Lemma 7.1.** For any positive integers $n, k, l$ with $k \geq l$ we have

$$T_k(G_n) = (p-1)^{2k}p^{-n} + O(H_n^{2k-2l}T_l(G_n)),$$

where the constant in the big-$O$ is less than 1.
Proof. We have for \( k \geq l \),

\[
T_k(G_n) = p^{-n} \sum_{\lambda=0}^{p^n-1} \sum_{x \in G_n} \sum_{y \in G_n} e_{p^n}(\lambda(x_1 + \cdots + x_k - y_1 - \cdots - y_k))
\]

\[
= p^{-n}|G_n|^2k + p^{-n} \sum_{\lambda=1}^{p^n-1} |S_n(\lambda)|^{2k}
\]

\[
= p^{-n}|G_n|^2k + O\left(p^{-n}H_n^{2k-2l} \sum_{\lambda=1}^{p^n-1} |S_n(\lambda)|^{2l}\right)
\]

\[
= (p-1)^2k p^{-n} + O\left(H_n^{2k-2l}T_l(G_n)\right).
\]

\( \square \)

For \( n = 2 \), using \( H_2 \ll p^{\frac{5}{6}} \log^2 p \), \( T_2(G_2) \ll p^{\frac{32}{13}} \log^{\frac{13}{6}} p \), (though in fact much weaker bounds will do) we obtain from the lemma,

\[
T_k(G_2) = p^{2k-2} + O(p^{2k-3}) + O(p^{\frac{5}{3}k-\frac{34}{3}+o(1)}),
\]

for \( k \geq 2 \), and thus the asymptotic formula \( T_k(G_2) \sim p^{2k-2} \) holds for \( k \geq 4 \). The asymptotic result for \( n \geq 3 \) is given in the next section.

In order to state our next lemma we define

\[
H'_n := \max_{p \nmid y} |S_n(y)|.
\]

Plainly, for \( n \geq 2 \),

\[
H_n = \max\{H'_n, H_{n-1}\}.
\]

The key lemma needed for estimating the higher order Heilbronn sums is the well known H"older-type inequality relating \( H'_n \) to the \( T_k(G_n) \) (see for example [10]). A proof is provided in the appendix for the convenience of the reader.

**Lemma 7.2.** For any positive integers \( n, k, l \) we have

\[
H'_n \leq \left(p^n T_k(G_n)T_l(G_n)\right)^\frac{1}{2k}\left(p-1\right)^{1-\frac{n}{2k}-\frac{1}{l}}.
\]

**8. Estimation of \( H_n \) and \( T_k(G_n) \)**

From Lemma 7.1, Lemma 7.2 and (7.1), we obtain an iterative process for estimating successive \( H_n, T_k(G_n) \), starting from estimates for \( H_2 \) and \( T_2(G_2) \). We suppose that

\[
(8.1) \quad H_2 \ll p^{\gamma}, \quad T_2(G_2) \ll p^{\lambda}
\]

and define

\[
(8.2) \quad \beta := \max\{4, 2\gamma + \lambda\}.
\]

From Lemma 7.1 we thus have \( T_k(G_2) \sim p^{2k-2} \) for \( k \geq 4 \) and

\[
(8.3) \quad T_3(G_2) = p^{4} + O(H_2^2T_2(G_2)) \ll p^\beta.
\]

The exponents \( \gamma = \frac{5}{6} + o(1), \lambda = \frac{32}{13} + o(1) \) mentioned above give \( \beta = \frac{161}{39} + o(1) = 4.1282 \ldots \).
Theorem 8.1. Let \( \{\ell_n\} \) and \( \{k_n\} \) be the sequences of positive integers defined by
\[
\ell_2 := 4, \quad \ell_3 := \left\lceil \frac{3\beta}{9-2\beta} \right\rceil, \quad \ell_{n+1} := \left\lceil \frac{8-\beta}{5-\beta} \ell_n \right\rceil \quad \text{for } n \geq 3,
\]
and
\[
k_2 := 3, \quad k_3 := \left\lceil \frac{3\beta}{9-2\beta} \right\rceil, \quad k_{n+1} := \left\lceil \frac{8-\beta}{5-\beta} \ell_n \right\rceil \quad \text{for } n \geq 3.
\]
For \( n \geq 2 \) we have \( T_k(G_n) \ll p^{2k-n} \) for \( k \geq \ell_n \) with \( T_k(G_n) \sim p^{2k-n} \) for \( k > k_n \).

For \( n \geq 3 \) we have
\[
H_n \ll p^{1-\epsilon_n}, \quad \epsilon_n := \begin{cases} \frac{(9-2\beta)}{18}, & \text{for } n = 3, \\ \frac{(5-\beta)}{(6\ell_{n-1})}, & \text{for } n \geq 4. \end{cases}
\]

Proof. From Lemma 7.2, (7.1) and (8.3)
\[
H'_3 \leq (p^3T_3(G_3^2))^\frac{1}{3} + p^\frac{3}{4}T_3(G_3^2) \leq p^\frac{3}{4}T_3(G_2^2) \ll p^{\frac{3}{4} + \epsilon} = p^{1-\epsilon_3}.
\]

Since \( \frac{1}{2} + \frac{3}{4} \geq 1 + \frac{1}{6} > \gamma \), we also have
\[
H_3 = \max\{H'_3, H_2\} \ll p^{1-\epsilon_3}.
\]

Hence from Lemma 7.1, for \( k \geq 3 \)
\[
T_k(G_3) = (p-1)^{2k-p-3} + O\left(H_3^{2k-6}T_3(G_2)\right),
\]
\[
= p^{2k-3} + O\left(p^{2k-4} + O\left(p^\left(\frac{1}{2} + \epsilon\right)\right)\right).
\]

For \( k > \frac{3\beta}{9-2\beta} \) the exponent \( 2k-3 \) dominates, and we get \( T_k(G_3) \sim p^{2k-3} \), with
\[
T_k(G_3) \ll p^{2k-3}, \quad k \geq \ell_3, \quad \text{and} \quad T_k(G_3) \ll p^{(\frac{1}{2} + \epsilon)(2k-6)+\beta}, \quad 3 \leq k < \ell_3,
\]

establishing the \( n = 3 \) case of Theorem 8.1.

For \( n > 3 \) we proceed by induction. Let’s say that for a given \( n \) we have already established that
\[
H_n \ll p^{1-\epsilon_n},
\]
\[
T_k(G_n) \ll p^{2k-n}, \quad \text{for } k \geq \ell_n.
\]

Hence, by Lemma 7.2, (7.1), (8.3) and (8.5),
\[
H_{n+1}' \leq (p^{n+1}T_3(G_{n+1})T_{\ell_n}(G_{n+1}))^\frac{1}{n}p^\frac{n+1}{n} - \frac{1}{n}
\]
\[
\leq (p^{n+1}T_3(G_2)T_{\ell_n}(G_n))^\frac{1}{n}p^\frac{n+1}{n} - \frac{1}{n}
\]
\[
\ll p^{\frac{n+1}{n}p} \leq p^{(2\ell_n-n)}p^{\frac{1}{n}}p^\left(\frac{1-\epsilon}{\ell_n}\right) = p^{1-\frac{1}{n}(\frac{8-\beta}{5-\beta})} = p^{1-\epsilon_{n+1}},
\]

and thus, since \( \epsilon_{n+1} < \epsilon_n \),
\[
H_{n+1} = \max\{H'_{n+1}, H_n\} \ll p^{1-\epsilon_{n+1}}.
\]

Therefore, by Lemma 7.1 and (7.1), for \( k \geq \ell_n \) we have
\[
T_k(G_{n+1}) = (p-1)^{2k-p-(n+1)} + O\left(H_{n+1}^{2k-2\ell_n}T_{\ell_n}(G_n)\right)
\]
\[
= p^{2k-(n+1)} \left(1 + O(p^{-1}) + O(p^{1-\epsilon_{n+1}(2k-2\ell_n)})\right).
\]

Consequently, for \( k > \ell_n + \frac{1}{2\ell_{n+1}} \)
\[
T_k(G_{n+1}) \ll p^{2k-(n+1)} \quad \text{for } k \geq \ell_{n+1},
\]
and
\[ T_k(G_{n+1}) \ll p^{2k-n-\frac{(5-\beta)}{2}}(2k-2l_n) \] for \( l_n \leq k < l_{n+1} \),
and we recover the claim of the theorem for \((n+1)\).

In the following corollary we make the growth with \(n\) explicit.

**Corollary 8.1.** For \( n \geq 4 \) we have
\[ H_n \ll n p^{1-\frac{(5-\beta)n^3}{6(5-\beta)}}. \]

**Proof.** This follows at once from the bound
\[
\ell_n = \left[ \left(\frac{8-\beta}{5-\beta}\right) \ell_{n-1} \right] \leq \left(\frac{8-\beta}{5-\beta}\right) \ell_{n-1} + 1, \\
\leq \left(\frac{8-\beta}{5-\beta}\right)^{n-3} \ell_3 + \left(\frac{8-\beta}{5-\beta}\right)^{n-4} \ell_3 + \cdots + 1 = \ell_3 \left(\frac{8-\beta}{5-\beta}\right)^{n-3} + \left(\frac{8-\beta}{5-\beta}\right)^{n-3} - 1 \\
< \left(\ell_3 + \frac{5-\beta}{\beta}\right) \left(\frac{8-\beta}{5-\beta}\right)^{n-3}.
\]

Thus when \( \beta = 161/39 + o(1) \), the optimal value currently available, we have \( k_2 = 3, k_3 = 16, k_4 = 75, k_5 = 337, \ldots \), and \( H_3 \ll p^{0.95868} \), \( H_4 \ll p^{0.99145} \), \( H_5 \ll p^{0.99808} \), with \( k_n \leq l_n \leq 0.1974 \left(\frac{151}{34}\right)^n \), and \( H_n \ll p^{1-3.269} \left(\frac{n}{14}\right)^n \).

**ACKNOWLEDGEMENT**

The authors wish to thank Igor Shparlinski for his valuable discussions on this paper, in particular for leading us to the improvement in Theorem 1.1 for \( n = 2 \), and to the improvements in the estimates of the Fermat quotients. We also wish to thank the referee for his valuable comments and directing our attention to the recent work of Shteinikov [21], which has strong parallels with this work.

**9. APPENDIX: PROOF OF LEMMA 7.2**

We shall use the following version of Hölder’s inequality.

**Lemma 9.1.** For any nonnegative real numbers \( a_i, b_i, 1 \leq i \leq n \), and any positive real number \( \ell \), we have
\[
\sum_{i=1}^{n} a_i b_i \leq \left( \sum_{i=1}^{n} a_i^{\ell} \right)^{1-\frac{1}{\ell}} \left( \sum_{i=1}^{n} b_i^{\ell} \right)^{\frac{1}{\ell}}.
\]

First we note that for any integer \( \lambda \), and positive integer \( k \), we have
\[
(p-1) \left( \sum_{x \in G_n} e_{p^n}(\lambda x) \right)^k = \sum_{y \in G_n} \left( \sum_{x \in G_n} e_{p^n}(\lambda yx) \right)^k = \sum_{x_1 \in G_n} \cdots \sum_{x_k \in G_n} \sum_{y \in G_n} e_{p^n}(\lambda y(x_1 + \cdots + x_k)) = \sum_{b=0}^{p^n-1} n(b) \sum_{y \in G_n} e_{p^n}(\lambda yb),
\]
where
\[ n(b) = \#\{(x_1, \ldots, x_k) : x_i \in G_n, 1 \leq i \leq k, x_1 + \cdots + x_k = b\}. \]

By Lemma 9.1 and the elementary identities,
\[ p^n - 1 \sum_{b=0}^{p^n-1} n(b) = T_k(G_n), \]
we obtain for any positive integer \( l \) and integer \( \lambda \) with \( p \nmid \lambda \),
\[
(p - 1) \left| \sum_{x \in G_n} e_{p^n}(\lambda x) \right|^k \leq \left( \sum_{b=0}^{p^n-1} n(b) \right)^{1+\frac{k}{2}} \left( \sum_{b=0}^{p^n-1} n(b)^2 \right)^{\frac{k}{2}} \left( \sum_{y \in G_n} \left| \sum_{b=0}^{p^n-1} e_{p^n}(\lambda y b) \right|^{2l} \right)^{\frac{1}{2l}}
= (p - 1)^{(k-1)(1-\frac{1}{2l})} T_k(G_n)^{\frac{1}{2l}} (T_{l}(G_n)p^n)^{\frac{1}{2l}}.
\]

Dividing by \((p - 1)\) and taking the \( k \)-th root yields the lemma.

References

[1] J. Bourgain and M.-C. Chang, Exponential sum estimates over subgroups and almost sub-
groups of \( \mathbb{Z}^*Q \), where \( Q \) is composite with few prime factors, Geom. Funct. Anal. 16 (2006),
no. 2, 327-366.
lates of subgroups in residue rings, and fixed points of the discrete logarithm, Int. Math. Res.
[6] A. Granville, Some conjectures related to Fermat’s last theorem, Number theory (Banff,
Proceedings of a conference in honor of Heini Halberstam, (Birkhauser, Boston, 1996),
451-463.
[8] D. R. Heath-Brown and S. V. Konyagin, New bounds for Gauss sums derived from \( k \)
[10] S. V. Konyagin and I. E. Shparlinski, Character sums with exponential functions and their ap-
1999.
1411-1416.
748-752; translated from Mat Zametki 80, no. 5 (2006), 793-796.
[15] H. L. Montgomery and R. C. Vaughan, Exponential sums with multiplicative coefficients,
[17] I. D. Shkredov, On exponential sums over multiplicative subgroups of medium size, Finite Fields
Appl. 30 (2014), 72-87.
[18] I. D. Shkredov, E. V. Solodkova and I. V. Vyugin, Intersections of multiplicative subgroups


DEPARTMENT OF MATHEMATICS, KANSAS STATE UNIVERSITY, MANHATTAN, KS 66506

E-mail address: cochrane@math.ksu.edu

DEPARTMENT OF MATHEMATICS, BOWLING GREEN STATE UNIVERSITY, FIRELANDS, HURON, OH 44839.

E-mail address: dilumd@bgsu.edu

DEPARTMENT OF MATHEMATICS, KANSAS STATE UNIVERSITY, MANHATTAN, KS 66506

E-mail address: pinner@math.ksu.edu