Distribution of alternative power sums and Euler polynomials modulo a prime

Yan Li\textsuperscript{a}, Min-Soo Kim\textsuperscript{b}, Su Hu\textsuperscript{b,}\textdagger

\textsuperscript{a} Department of Applied Mathematics, China Agriculture University, Beijing 100083, China
\textsuperscript{b} Department of Mathematical Sciences, Korea Advanced Institute of Science and Technology (KAIST), 373-1 Guseong-dong, Yuseong-gu, Daejeon 305-701, South Korea

Received 27 April 2011; received in revised form 19 September 2011; accepted 21 September 2011

Communicated by H.W. Broer

Abstract

For a fixed integer $s \geq 2$, we estimate exponential sums with alternative power sums

$$A_s(n) = \sum_{i=0}^{n} (-1)^i i^s$$

individually and on average, where $A_s(n)$ is computed modulo $p$. Our estimates imply that, for any $\epsilon > 0$, the sets

$$\{A_s(n) : n < p^{1/2+\epsilon}\} \quad \text{and} \quad \{(−1)^n E_s(n) : n < p^{1/2+\epsilon}\}$$

are uniformly distributed modulo a sufficient large $p$, where $E_s(x)$ are Euler polynomials. Comparing with the results in Garaev et al. (2006) [M. Z. Garaev, F. Luca and I. E. Shparlinski, Distribution of harmonic sums and Bernoulli polynomials modulo a prime, Math. Z., 253 (2006), 855–865], we see that the uniform distribution properties for the alternative power sums and Euler polynomials modulo a prime are better than those for the harmonic sums and Bernoulli polynomials.

\textcopyright 2011 Royal Netherlands Academy of Arts and Sciences. Published by Elsevier B.V. All rights reserved.

Keywords: Uniform distribution; Alternative power sums; Euler polynomials

\textdagger Corresponding author.
E-mail addresses: liyan_00@mails.tsinghua.edu.cn (Y. Li), minsookim@kaist.ac.kr (M.-S. Kim), hus04@mails.tsinghua.edu.cn, husu@kaist.ac.kr (S. Hu).

0019-3577/S - see front matter \textcopyright 2011 Royal Netherlands Academy of Arts and Sciences. Published by Elsevier B.V. All rights reserved.
doi:10.1016/j.indag.2011.09.010
1. Introduction

Throughout this paper, \( p \) is an odd prime.

Recently, some uniformly distributed properties have been found for special functions modulo a sufficient large \( p \), such as \( n! \) [4], \( n!m! \) [5] and Fermat quotients [8].

By estimating exponential sums with harmonic sums

\[
H_s(n) = \sum_{i=1}^{n} \frac{1}{i^s}
\]

individually and on average, Garaev et al. [6] showed that for any \( \epsilon > 0 \), the set \( \{H_s(n) : n < p^{1/2+\epsilon}\} \) is uniformly distributed modulo a sufficient large \( p \).

The Bernoulli polynomials \( B_k(t) \) are defined by the generating function

\[
\left( \frac{x}{e^x - 1} \right) e^{xt} = \sum_{k=0}^{\infty} B_k(t) \frac{x^k}{k!}.
\]

In particular, \( B_k = B_k(0) \), are Bernoulli numbers.

From the congruence

\[
B_{p-s}(n) \equiv B_{p-s} - sH_s(n) (\text{mod } p),
\]

their results also imply the uniformly distributed property modulo a sufficient large \( p \) for the values \( B_{p-r}(n) \) of Bernoulli polynomials where \( r \) is fixed.

Let \( \chi(n) \) be a quadratic character modulo a prime \( p \). For a fixed integer \( s \), by estimating certain exponential sums with truncated \( L \)-functions

\[
L_{s,p}(n) = \sum_{i=1}^{n} \frac{\chi(i)}{i^s} \quad (n = 1, 2, \ldots).
\]

Shparlinski [9] also proved certain uniform distribution of reductions of \( L_{s,p}(n) \) modulo \( p \).

The Euler polynomials are defined by the generating function

\[
\left( \frac{2}{e^x + 1} \right) e^{xt} = \sum_{k=0}^{\infty} E_k(t) \frac{x^k}{k!}.
\]

The alternative power sums \( A_s(n) \) are closely related to the Euler polynomials, as follows,

\[
A_s(n) = \sum_{i=0}^{n} (-1)^i \frac{1}{i^s} = \frac{(-1)^n E_s(n + 1) + E_s(0)}{2}, \tag{1.1}
\]

where \( 0^s = 1 \) for \( s = 0 \), and \( 0^s = 0 \) otherwise. (See Equation (23.1.4) in [1], and also see Theorem 2.1 in Zhi-Wei Sun’s lecture [10].)

In this paper, we obtain nontrivial results about the distribution of \( A_s(n) \) modulo \( p \). For a fixed integer \( s \geq 2 \), we estimate certain exponential sums with \( A_s(n) \), that is, the sums

\[
T_s(a; M, N) = \sum_{n=M+1}^{M+N} e(a A_s(n)),
\]

where

\[
e(z) = \exp(2\pi iz/p),
\]
and $A_s(n)$ is computed modulo $p$ for $0 \leq M < M + N < p$. In fact, we prove

**Theorem 1.1.** Let $M$ and $N$ be integers with $0 \leq M < M + N < p$. Then for every fixed integer $s \geq 2$, uniformly for any $(a, p) = 1$, the following bound holds:

$$|T_s(a; M, N)| \ll \sqrt{p} \log p.$$ 

Let

$$\widehat{T}_s(a; M, N) = \sum_{n=M+1}^{M+N} e(a H_s(n)).$$

In [6], Garaev et al. proved

$$|\widehat{T}_s(a; M, N)| \ll N^{3/4} p^{1/8} (\log p)^{1/4},$$

uniformly for any $(a, p) = 1$. (See Theorem 1 of [6].)

The bound $\sqrt{p} \log p$ is better than the bound $N^{3/4} p^{1/8} (\log p)^{1/4}$. Since $\widehat{T}_s(a; M, N)$ has trivial bound $N$, if the estimation of [6] is nontrivial, then the following inequality must hold:

$$N^{3/4} p^{1/8} (\log p)^{1/4} \leq N,$$

which is equivalent to

$$\sqrt{p} \log p \leq N.$$

If the above inequality holds, then one has

$$\sqrt{p} \log p \leq N^{3/4} p^{1/8} (\log p)^{1/4}.$$ 

The reason our bound is stronger is that the sum $T_s(a; M, N)$ is easier to handle than the sum $\widehat{T}_s(a; M, N)$. In our case, the alternative power sums $A_s(n)$ are essentially polynomials of $n$ by (1.1), so the Weil bound can be used. For the harmonic sums $H_s(n)$, they are not even rational functions of $n$, so their exponential sums are difficult to treat.

From the above inequalities, for any $\epsilon > 0$, the sets

$$\{A_s(n) : n < p^{1/2+\epsilon}\} \quad \text{and} \quad \{H_s(n) : n < p^{1/2+\epsilon}\}$$

are uniformly distributed modulo a sufficient large prime $p$. Compared with $H_s(n)$, the bounds of exponential sums with $A_s(n)$ are smaller, so the discrepancies of $A_s(n)$ are also smaller. (See Theorem 3 of [6] and Theorem 3.1.) This implies that the uniform distribution property for the alternative power sums modulo a prime is better than that for the harmonic sums.

Furthermore, from (1.1), uniformly for any $(a, p) = 1$, we have the bound

$$\sum_{n=M+1}^{N+M} e(a(-1)^n E_s(n)) \ll \sqrt{p} \log p$$

(for details, see Section 2).

Finally, by estimating the sums $T_s(a; M, N)$ on average, we study the number of solutions to the congruence

$$A_s(n_1) + \cdots + A_s(n_r) \equiv \lambda (\mod p), \quad M + 1 \leq n_1, \ldots, n_r \leq M + N.$$ 

Notice that, the implied constants in symbols “$O$” and “$\ll$” in this paper may depend on the integer parameter $s$. 
2. Proof of Theorem 1.1

From (1.1), we have
\[
\left| \sum_{n=M+1}^{M+N} e(a A_s(n)) \right| = \left| \sum_{n=M+1}^{M+N} e\left( \frac{-1}{2} E_s(n+1) \right) \cdot e\left( \frac{E_s(0)}{2} \right) \right|
\]
\[
= \left| \sum_{n=M+1}^{M+N} e\left( \frac{-1}{2} E_s(n+1) \right) \right|
\]
\[
= \left| \sum_{n=1+M+2}^{M+N+1} e\left( \frac{(-1)^{n+1} E_s(n+1)}{2} \right) \right|.
\]

(2.1)

Substituting \( n \) for \( n+1 \), \( a \) for \( -a/2 \) and \( M \) for \( M + 1 \) in (2.1), it suffices to estimate the following sum
\[
\left| \sum_{n=M+1}^{M+N} e(a (-1)^n E_s(n)) \right|.
\]

(2.2)

Splitting (2.2) into odd and even ones, it is bounded by
\[
\left| \sum_{(M+1)/2 \leq n \leq (M+N)/2} e(a E_s(2n)) \right| + \left| \sum_{M/2 \leq n \leq (M+N-1)/2} e(-a E_s(2n+1)) \right|.
\]

Since \( E_s(2x) \) and \( E_s(2x + 1) \) are also polynomials of degree \( s \) in \( x \), so are \( a E_s(2x) + cx \) and \( -a E_s(2x + 1) + cx \) modulo \( p \), for any \( 1 \leq a \leq p - 1 \) and \( 1 \leq c \leq p \).

From Weil's bound and the standard reduction of incomplete sums to complete ones (see [2]), we have
\[
\left| \sum_{(M+1)/2 \leq n \leq (M+N)/2} e(a E_s(2n)) \right| = O(\sqrt{p} \log p),
\]
\[
\left| \sum_{M/2 \leq n \leq (M+N-1)/2} e(-a E_s(2n+1)) \right| = O(\sqrt{p} \log p).
\]

(2.3)

Therefore,
\[
\left| \sum_{n=M+1}^{M+N} e(a (-1)^n E_s(n)) \right| = O(\sqrt{p} \log p),
\]
which concludes the proof. \( \square \)

3. Discrepancy

The discrepancy \( D \) of a sequence of \( M \) points \( (\gamma_j)_{j=1}^M \) of the unit interval \([0, 1]\) is defined as
\[
D = \sup_{\mathcal{I}} \left| \frac{A(\mathcal{I})}{M} - \mathcal{I} \right|,
\]
where the supremum is taken over all interval $I = [\alpha, \beta] \subset [0, 1], |I| = \beta - \alpha$ is the length of $I$ and $A(I)$ is the number of points of this set which belongs to $I$ (see [3,7]).

For an integer $a$ with $\gcd(a, p) = 1$, we denote by $D(M, N)$ the discrepancy of the sequence of fractional parts

$$\left\{ \frac{(-1)^n E_s(n)}{p} \right\}, \quad M + 1 \leq n \leq M + N.$$

Using the Erdős–Turán bound (see [3,7]), which gives a discrepancy bound in terms of exponential sums, we derive

**Theorem 3.1.** Let $M$ and $N$ be integers with $0 \leq M < M + N < p$. Then, for every fixed integer $s \geq 2$, the following bound holds:

$$D(M, N) \ll N^{-1} \sqrt{p} (\log p)^2.$$

4. Exponential sums on average and an application

In this section, we estimate the sums $T_s(a; M, N)$ on average. Let

$$J_{s,l}(M, N) = \frac{1}{p} \sum_{a=0}^{p-1} |T_s(a; M, N)|^{2l}.$$

**Theorem 4.1.** Let $M$ and $N$ be integers with $0 \leq M < M + N < p$. Then, for any fixed integers $s \geq 2$ and $l \geq 1$, the following bound holds:

$$J_{s,l}(M, N) \ll N^{2l-1}.$$

**Proof.** Changing the order of summation, we get

$$J_{s,l}(M, N) = \sum_{M+1 \leq n_1, \ldots, n_{2l} \leq M + N} \frac{1}{p} \sum_{a=0}^{p-1} e(a(A_s(n_1) + \cdots + A_s(n_l) - A_s(n_{l+1}) - \cdots - A_s(n_{2l})))$$

$$= \tilde{J}_{s,l}(M, N),$$

where $\tilde{J}_{s,l}(M, N)$ is the number of solutions to the congruence

$$A_s(n_1) + \cdots + A_s(n_l) - A_s(n_{l+1}) - \cdots - A_s(n_{2l}) \equiv 0 \pmod{p} \quad (4.1)$$

with $M + 1 \leq n_1, \ldots, n_{2l} \leq M + N$.

For fixed values of $n_1, \ldots, n_{2l-1}$, by Eq. (1.1), there are at most $2s$ values of $n_{2l}$ such that (4.1) holds, as the Euler polynomial $E_s(x)$ has degree $s$. Thus

$$\tilde{J}_{s,l}(M, N) \leq 2s N^{2l-1}.$$ 

Therefore,

$$J_{s,l}(M, N) \ll N^{2l-1}. \quad \square$$
Let $I_{s,r}(\lambda, M, N)$ be the number of solutions to the congruence
\[ A_s(n_1) + \cdots + A_s(n_r) \equiv \lambda \pmod{p}, \quad M + 1 \leq n_1, \ldots, n_r \leq M + N. \]

As in [6], combining Theorems 1.1 and 4.1, we get the following upper bound of $I_{s,r}(\lambda, M, N)$.

**Theorem 4.2.** Let $M$ and $N$ be integers with $0 \leq M < M + N < p$. Then, for any integers $s \geq 2$ and $r/2 \geq l \geq 1$, the following bound holds:
\[
\max_{\lambda=0,\ldots,p-1} \left| I_{s,r}(\lambda, M, N) - \frac{N^r}{p} \right| \ll p^{r/2-l}(\log p)^{r-2l}N^{2l-1}.
\]

**Proof.** From the orthogonal property, we have
\[
I_{s,r}(\lambda, M, N) = \sum_{M+1 \leq n_1, \ldots, n_r \leq M+N+1} \frac{1}{p} \sum_{a=0}^{p-1} e\left(a(A_s(n_1) + \cdots + A_s(n_r) - \lambda)\right).
\]

Changing the order of summation and separating the term corresponding to $a = 0$, we have
\[
I_{s,r}(\lambda, M, N) = \frac{N^r}{p} + \frac{1}{p} \sum_{a=1}^{p-1} e\left(-a\lambda\right) \sum_{M+1 \leq n_1, \ldots, n_r \leq M+N} e\left(a(A_s(n_1) + \cdots + A_s(n_r))\right)
\]
\[
= \frac{N^r}{p} + O\left(\frac{1}{p} \sum_{a=1}^{p-1} \left| \sum_{M+1 \leq n_1, \ldots, n_r \leq M+N} e\left(aA_s(n)\right)\right|^{r} \right).
\]

Using Theorem 1.1, we get
\[
\left| I_{s,r}(\lambda, M, N) - \frac{N^r}{p} \right| \ll \left( p^{r/2-l}(\log p)^{r-2l} \right) \frac{1}{p} \sum_{a=1}^{p-1} \left| \sum_{M+1 \leq n \leq M+N} e\left(aA_s(n)\right)\right|^{2l}.
\]

Applying Theorem 4.1, we get the desired result.

The same technique can also be used to get better upper bound for $J_{s,l}(M, N)$, i.e., the number of solutions of (4.1), in the case that $N$ is large.

**Theorem 4.3.** Let $M$ and $N$ be integers with $0 \leq M < M + N < p$. Then, for any integers $s \geq 2$ and $l \geq r \geq 1$, the following bound holds:
\[
\left| J_{s,l}(M, N) - \frac{N^{2l}}{p} \right| \ll p^{r}(\log p)^{2r}N^{2(l-r)-1}.
\]

**Acknowledgments**

The first author was supported by National Natural Science Foundation of China (Grant No. 11001145 and Grant No. 11071277). The second and third authors were supported by the
The authors are very grateful to the anonymous referee for his helpful comments and suggestions, in particular for the simplification of the proof of Theorem 1.1.

References