Bull. Aust. Math. Soc. **102** (2020), 31–38
doi:10.1017/S0004972719001187

LOWER BOUNDS FOR PERIODS OF DUCCI SEQUENCES

FLORIAN BREUER and IGOR E. SHPARLINSKI✉

(Received 13 September 2019; accepted 25 September 2019; first published online 22 November 2019)

Abstract

A Ducci sequence is a sequence of integer n-tuples obtained by iterating the map

$$D : (a_1, a_2, \dots, a_n) \mapsto (|a_1 - a_2|, |a_2 - a_3|, \dots, |a_n - a_1|).$$

Such a sequence is eventually periodic and we denote by $P(n)$ the maximal period of such sequences for given odd n. We prove a lower bound for $P(n)$ by counting certain partitions. We then estimate the size of these partitions via the multiplicative order of two modulo n.

2010 *Mathematics subject classification*: primary 11B83; secondary 11P83, 11T30.

Keywords and phrases: Ducci sequence, finite field, multiplicative order, partition.

1. Introduction

Let n be a positive integer. A Ducci sequence is a sequence of integer n-tuples obtained by iterating the map $D : \mathbb{Z}^n \to \mathbb{Z}^n$ defined by

$$D : (a_1, a_2, \dots, a_n) \mapsto (|a_1 - a_2|, |a_2 - a_3|, \dots, |a_n - a_1|).$$

There is a long literature on Ducci sequences (see, for example, [3–9, 15, 16, 23]).

Ducci sequences are eventually periodic. For each n, the largest period is denoted by $P(n)$; it is the period of the sequence starting with $(0, 0, \dots, 0, 1)$. The sequence $P(1), P(2), \dots$ is entry A038553 in the On-line Encyclopedia of Integer Sequences [18]. Since $P(2^k) = 1$ and $P(2^k m) = 2^k P(m)$, if m is not a power of two by [9, Theorem 4], we restrict our attention to odd n.

Denote by $t = \mathrm{ord}_{(\mathbb{Z}/n\mathbb{Z})^*}(2)$ the multiplicative order of two modulo n. If there exists an integer M for which $2^M \equiv -1 \bmod n$, then we say that *n is 'with -1'*. It is convenient to introduce the quantities

$$B_1(n) = 2^t - 1 \quad \text{and} \quad B_2(n) = n(2^{t/2} - 1). \tag{1.1}$$

The following upper bounds on $P(n)$ are known. The first is proved in [15], the second in [9] and the third in [3].

The second author was supported in part by the Australian Research Council Grant DP180100201.

THEOREM 1.1. *Let n be an odd integer and let t be the multiplicative order of two modulo n.*

(1) *$P(n)$ divides $B_1(n)$.*
(2) *If n is with -1, then $P(n)$ divides $B_2(n)$.*
(3) *Suppose that $n = p^k$ with $p \equiv 5 \bmod 8$ prime and 2 is a primitive root modulo p^k. If the equation $x^2 - py^2 = -4$ has no solutions in odd integers $x, y \in \mathbb{Z}$, then $P(n)$ divides $\frac{1}{3}B_2(n)$.*

As for lower bounds, the first of the following results is found in [9] and the rest are in [12].

THEOREM 1.2. *Let n be an odd integer.*

(1) *n divides $P(n)$.*
(2) *$P(n) = n$ if and only if $n = 2^r - 1$ for some positive integer r.*
(3) *If n is with -1, then $P(n) \geqslant n(n-2)$.*
(4) *If n is with -1, then $P(n) = n(n-2)$ if and only if $n = 2^r + 1$ for some positive integer r.*

The goal of the present paper is to prove new asymptotic lower bounds for $P(n)$ in terms of t and n. Our starting point is the fact from [4] that $P(n)$ is the lowest common multiple of the multiplicative orders of the elements $\zeta + 1$, where $\zeta \neq 1$ ranges over the nth roots of unity in the finite field $\mathbb{F}_{2^t}$.

Since our results require that $t > \sqrt{2n}$, in Section 5, we also give a short survey of known results about the size of t.

2. Multiplicative orders and partitions

Let $1 \leqslant a < n$ be an integer prime to n.

Consider the set of representatives, chosen in the interval $[1, n]$, of the coset $a\langle 2\rangle \subseteq (\mathbb{Z}/n\mathbb{Z})^*$ of the multiplicative group $\langle 2\rangle$ generated by 2 in the residue ring modulo n, that is,

$$\mathcal{S}_{a,n} := \{j \in \mathbb{Z}_{>0} : \ 1 \leqslant j \leqslant n, \gcd(j, n) = 1, \ \exists e_j \in \mathbb{Z}_{\geqslant 0}, j \equiv a2^{e_j} \bmod n\}.$$

Its cardinality is $\#\mathcal{S}_{a,n} = t$.

Next, we consider the set of partitions of numbers $\leqslant t - 1$ into distinct parts from $\mathcal{S}_{a,n}$: that is,

$$\mathcal{P}_{a,n} := \left\{(u_j)_{j\in\mathcal{S}_{a,n}} \in \{0,1\}^t : \sum_{j\in\mathcal{S}_{a,n}} u_j j \leqslant t - 1\right\}. \tag{2.1}$$

Our main result is the following theorem.

THEOREM 2.1. *Suppose that n is odd and a is relatively prime to n. Then $P(n) \geqslant \#\mathcal{P}_{a,n}$.*

https://doi.org/10.1017/S0004972719001187 Published online by Cambridge University Press

Proof. It follows from [4, Theorem 3.9] that $P(n)$ is the lowest common multiple of the multiplicative orders of $\zeta + 1$, where $\zeta \neq 1$ ranges over all nth roots of unity $\zeta \in \mathbb{F}_{2^t}$.

Let $\zeta \in \mathbb{F}_{2^t}$ be a primitive nth root of unity. The idea is to show that every partition in $\mathcal{P}_{a,n}$ leads to a distinct power of $\zeta + 1$. For this, we follow the strategy of [1].

Let $u = (u_j)_{j \in \mathcal{S}_{a,n}} \in \mathcal{P}_{a,n}$ and set

$$Q_u = \sum_{j \in \mathcal{S}_{a,n}} u_j 2^{e_j},$$

where $j \equiv a2^{e_j} \bmod n$. We also choose an integer b for which $ab \equiv 1 \bmod n$. Now

$$\begin{aligned}(\zeta + 1)^{Q_u} &= \prod_{j \in \mathcal{S}_{a,n}} (\zeta + 1)^{u_j 2^{e_j}} = \prod_{j \in \mathcal{S}_{a,n}} (\zeta^{2^{e_j}} + 1)^{u_j} \\ &= \prod_{j \in \mathcal{S}_{a,n}} (\zeta^{bj} + 1)^{u_j} = \prod_{j \in \mathcal{S}_{a,n}} (\vartheta^j + 1)^{u_j},\end{aligned}$$

where $\vartheta = \zeta^b \in \mathbb{F}_{2^t}$ is another primitive nth root of unity.

Let

$$v = (v_j)_{j \in \mathcal{S}_{a,n}} \in \mathcal{P}_{a,n}$$

be another partition distinct from u. We must show that v gives rise to a distinct power of $\zeta + 1$. Suppose that $(\zeta + 1)^{Q_u} = (\zeta + 1)^{Q_v}$, so

$$\prod_{j \in \mathcal{S}_{a,n}} (\vartheta^j + 1)^{u_j} = \prod_{j \in \mathcal{S}_{a,n}} (\vartheta^j + 1)^{v_j}.$$

Denote by $f(X) \in \mathbb{F}_2[X]$ the minimal polynomial of ϑ; it has degree t. Then $f(X)$ must divide $U(X) - V(X)$, where

$$U(X) = \prod_{j \in \mathcal{S}_{a,n}} (X^j + 1)^{u_j} \quad \text{and} \quad V(X) = \prod_{j \in \mathcal{S}_{a,n}} (X^j + 1)^{v_j}.$$

Since these polynomials have degree $\leqslant t - 1 < \deg f$, it follows that $U(X) = V(X)$. After removing common factors from both polynomials (corresponding to $u_j = v_j$), we obtain the identity

$$\prod_{h \in \mathcal{H}} (X^h + 1)^{u_h} = \prod_{k \in \mathcal{K}} (X^k + 1)^{v_k}, \tag{2.2}$$

where $\mathcal{H}$ and $\mathcal{K}$ are disjoint subsets of $\mathcal{S}_{a,n}$. But now we find that the term of smallest positive degree is x^e, where e is the smallest element of $\mathcal{H} \cup \mathcal{K}$, and this term only appears on one side of the identity (2.2). This contradiction concludes the proof. □

Remark 2.2. Some parts of the proof of Theorem 2.1 can be shortened by appealing to [20, Lemma 1]. However, for completeness and since [20] may not be easily accessible, we present a full self-contained proof.

https://doi.org/10.1017/S0004972719001187 Published online by Cambridge University Press

3. Counting partitions

Now we construct lower bounds for the cardinality of $\mathcal{P}_{a,n}$ for n of prescribed arithmetic structure. As we have mentioned, these bounds are only useful if t is not too small, specifically, $t > \sqrt{2n}$.

First, suppose that $t = \varphi(n)$, that is, 2 is a primitive root modulo n. In this case, $n = p^k$ must be a power of an odd prime p.

When $n = p$, we find that $\mathcal{P}_{a,n}$ contains the set of partitions of $n - 2$ into distinct parts, and the standard asymptotic (see, for example, [2, Theorem 6.4]) gives the following result.

Corollary 3.1. *Suppose that $n = p$ is an odd prime and 2 is a primitive root modulo p. Then, as $n \to \infty$,*

$$P(n) \geqslant \exp\left[\left(\frac{\pi}{\sqrt{3}} + o(1)\right)\sqrt{n}\right].$$

Corollary 3.1 is already contained in [19, Theorem 1]; in particular, the completely explicit lower bound (for 2 a primitive root modulo $n = p$),

$$P(n) \geqslant (80(n-2))^{-\sqrt{2}} \exp\left(\pi\sqrt{\frac{n-2}{3}}\right),$$

follows from [19, Corollary 4]. (See also [20] for some related results.)

Next, suppose that $n = p^k$ and 2 is a primitive root modulo n. For this, it suffices that 2 is a primitive root modulo p and p is not a Wieferich prime, that is, $2^{p-1} \not\equiv 1 \bmod p^2$.

We have $t = p^{k-1}(p-1)$ and $\mathcal{P}_{a,n}$ contains the set of partitions of $t - 1$ into distinct parts which are not divisible by p. An asymptotic formula for the number of such partitions appears in [13, Corollary 7.2], leading to the following result.

Corollary 3.2. *Fix an odd non-Wieferich prime p and suppose that 2 is a primitive root modulo p. For $n = p^k$, as $k \to \infty$,*

$$P(n) \geqslant \exp\left[\left(\frac{\pi}{\sqrt{3}}\sqrt{\frac{p-1}{p}} + o(1)\right)\sqrt{n}\right].$$

If $t < \varphi(n)$, then, inspired by [11], we estimate the cardinality of $\mathcal{P}_{a,n}$ as follows. Let $2 \leqslant N < t$ be an integer and set $\mathcal{S}_{a,n}(N) = \mathcal{S}_{a,n} \cap [1, N]$. Each subset $\mathcal{J} \subseteq \mathcal{S}_{a,n}(N)$ of cardinality $\#\mathcal{J} = J \leqslant t/N$ produces a valid partition $u \in \mathcal{P}_{a,n}$, where $u_j = 1$ if $j \in \mathcal{J}$ and $u_j = 0$ otherwise. Thus we obtain

$$\#\mathcal{P}_{a,n} \geqslant \sum_{J \leqslant t/N} \binom{\#\mathcal{S}_{a,n}(N)}{J}.$$

It remains to estimate $\#\mathcal{S}_{a,n}(N)$ and choose suitable a and N.

It is well known (see, for example, [21, Lemma 2.1]) that

$$\#\{j : 1 \leqslant j \leqslant N, \gcd(j, n) = 1\} = N\varphi(n)/n + O(n^{o(1)}).$$

https://doi.org/10.1017/S0004972719001187 Published online by Cambridge University Press

Among the cosets of $\langle 2\rangle \subseteq (\mathbb{Z}/n\mathbb{Z})^*$ at least one must have at least the average number of representatives in $[1, N]$, so there exists an integer a, prime to n, for which

$$\begin{aligned}\#\mathcal{S}_{a,n}(N) &\geqslant \frac{t}{\varphi(n)} \cdot \#\{j : 1 \leqslant j \leqslant N, \gcd(j, n) = 1\} \\ &= \frac{t}{\varphi(n)}(N\varphi(n)/n + O(n^{o(1)})) = (1 + o(1))\frac{tN}{n}\end{aligned}$$

as $n \to \infty$, provided $N \geqslant n^{\varepsilon}$ for some fixed $\varepsilon > 0$.

Choose $N = \lfloor \sqrt{2n} \rfloor$. Since $t \geqslant n^{1/2+\varepsilon}$,

$$\#\mathcal{S}_{a,n}(N) \geqslant \frac{tN}{n} + O(n^{o(1)}) = (2 + o(1))\frac{t}{N}.$$

By the Stirling formula,

$$\#\mathcal{P}_{a,n} \geqslant \sum_{J \leqslant t/N} \binom{\#\mathcal{S}_{a,n}(N)}{J} \geqslant \binom{\#\mathcal{S}_{a,n}(N)}{\lfloor t/N \rfloor} \geqslant \exp\left((2\log 2 + o(1))\frac{t}{N}\right).$$

Thus we have proved the following result.

Corollary 3.3. *Suppose that n is odd and t is the multiplicative order of two modulo n. Then*

$$P(n) \geqslant \exp\left[(\log 4 + o(1))\frac{t}{\sqrt{2n}}\right].$$

In particular, if $n = p^k$, then it is easy to show that $t \geqslant c(p)p^k$, where $c(p) > 0$ depends only on p, and hence Corollary 3.3 gives a version of Corollary 3.2 in the form

$$P(n) \geqslant \exp(c(p)\sqrt{n}).$$

We remark that the condition $t > \sqrt{2n}$ of Corollary 3.3 corresponds to the limits of our method. Indeed, there are about $\varphi(n)/t$ distinct cosets $\mathcal{S}_{a,n}$ and, since $\varphi(n) = n^{1+o(1)}$, each of them is expected to contain very few elements from the interval $[1, t]$, which are the only suitable elements that can be used in the construction of the set $\mathcal{P}_{a,n}$ given by (2.1).

Since

$$\frac{\log 4}{\sqrt{2}} \approx 0.98025 \quad \text{and} \quad \frac{\pi}{\sqrt{3}} \approx 1.8138,$$

in the case of $t \approx n$ we recover a result similar to Corollaries 3.1 and 3.2, but with a smaller constant in the exponent.

Our lower bounds are quite small compared with the upper bounds $P(n) \leqslant B_1(n) \sim 2^t$ and $P(n) \leqslant B_2(n) \sim n2^{t/2}$ (see (1.1)), which follow from Theorem 1.1. On the other hand, they are typically much stronger than the linear and quadratic in n lower bounds which one can extract from Theorem 1.2.

https://doi.org/10.1017/S0004972719001187 Published online by Cambridge University Press

4. Numerical results

It is interesting to compare the lower bound of Theorem 2.1 with actual values of $P(n)$. Table 1 shows numerical values of $P(n)$ and $\#\mathcal{P}_{a,n}$ for odd $n \leqslant 101$ and a

TABLE 1. Values of $P(n)$ and $\#\mathcal{P}_{a,n}$ for odd $n \leqslant 101$.

n	$P(n)$	t	a	$\#\mathcal{P}_{a,n}$
3	3	2	1	2
5	15	4	1	5
7	7	3	1	3
—	—	—	3	1
9	63	6	1	7
11	341	10	1	33
13	819	12	1	55
15	15	4	1	4
—	—	—	7	1
17	255	8	1	8
—	—	—	3	5
19	9709	18	1	207
21	63	6	1	6
—	—	—	5	2
23	2047	11	1	28
—	—	—	5	4
25	25575	20	1	190
27	13797	18	1	79
29	475107	28	1	1261
31	31	5	1	5
—	—	—	3	2
—	—	—	5	1
—	—	—	7	1
—	—	—	11	1
—	—	—	15	1
33	1023	10	1	10
—	—	—	5	3
35	4095	12	1	16
—	—	—	3	4
37	3233097	36	1	4310
39	4095	12	1	22
—	—	—	7	2
41	41943	20	1	70
—	—	—	3	25
43	5461	14	1	17
—	—	—	3	10
—	—	—	7	4
45	4095	12	1	12
—	—	—	7	3
47	8388607	23	1	241
—	—	—	5	14
49	2097151	21	1	53
—	—	—	3	27
51	255	8	1	8
—	—	—	5	3
—	—	—	11	1
—	—	—	19	1
53	3556769739	52	1	35680
55	1048575	20	1	66
—	—	—	3	8
57	29127	18	1	33
—	—	—	5	8
59	31675383749	58	1	72503
61	65498251203	60	1	91103
63	63	6	1	6
—	—	—	5	2
—	—	—	11	1
—	—	—	13	1
—	—	—	23	1
—	—	—	31	1
65	4095	12	1	12
—	—	—	3	4
—	—	—	7	3
—	—	—	11	2
67	575525617597	66	1	176945
69	4194303	22	1	31
—	—	—	5	17
71	34359738367	35	1	1427
—	—	—	7	35
73	511	9	1	9
—	—	—	3	3
—	—	—	5	3
—	—	—	9	1
—	—	—	11	1
—	—	—	13	1
—	—	—	17	1
—	—	—	25	1
75	1048575	20	1	24
—	—	—	7	6
77	1073741823	30	1	100
—	—	—	3	70
79	549755813887	39	1	1028
—	—	—	3	106
81	10871635887	54	1	6159
83	182518930210733	82	1	911361
85	255	8	1	8
—	—	—	3	3
—	—	—	7	2
—	—	—	9	1
—	—	—	13	1
—	—	—	21	1
—	—	—	29	1
—	—	—	37	1
87	268435455	28	1	154
—	—	—	5	9
89	2047	11	1	11
—	—	—	3	6
—	—	—	5	3
—	—	—	9	2
—	—	—	11	1
—	—	—	13	1
—	—	—	19	1
—	—	—	33	1
91	4095	12	1	12
—	—	—	3	8
—	—	—	9	2
—	—	—	11	2
—	—	—	17	1
—	—	—	19	1
93	1023	10	1	10
—	—	—	5	2
—	—	—	7	2
—	—	—	11	1
—	—	—	17	1
—	—	—	23	1
95	22906492245	36	1	905
—	—	—	7	17
97	1627389855	48	1	2216
—	—	—	5	283
99	3243933	30	1	49
—	—	—	5	32
101	37905296863701641	100	1	4827382

https://doi.org/10.1017/S0004972719001187 Published online by Cambridge University Press

representative a for each coset of the factor group $(\mathbb{Z}/n\mathbb{Z})^*/\langle 2\rangle$. These values were computed using Sage. Unsurprisingly, the largest value of $\#\mathcal{P}_{a,n}$ is achieved for $a = 1$ in these small cases, due to the presence of small powers of two in $\mathcal{S}_{1,n}$. However, when $n = 109$, we find that

$$\#\mathcal{P}_{1,109} = 99 < 178 = \#\mathcal{P}_{3,109} = \max_{\gcd(a,109)=1} \#\mathcal{P}_{a,109}.$$

5. Lower bounds on multiplicative orders

Since the quality of our bounds depends rather dramatically on the multiplicative order of two modulo n, here we give a short outline of known results.

First, we observe that the applicability of Corollary 3.1 for infinitely many prime $n = p$ is equivalent to *Artin's conjecture* (see [17] for an exhaustive survey). On the other hand, we are not aware of any conditional (let alone unconditional) results or well-established conjectures towards a version of Artin's conjecture for the non-Wieferich primes which appear in Corollary 3.2. It is natural to expect that there are infinitely many such primes but known results are scarce [22].

Primes p and integers n for which t is large, in particular, exceeding $\sqrt{p}$, have been studied in many different contexts, but most commonly in the theory of *pseudorandom number generators*. These results originate from the work of Erdős and Murty [10] and are conveniently summarised in [14]. For example, for any function $\psi(n) \to 0$ as $n \to \infty$, we have $t \geqslant n^{1/2+\psi(n)}$ for almost all (in a sense of relative density) primes $p = n$ (see [10, Theorem 1]) and odd integers n (see [14, Theorem 11]). Furthermore, for a positive proportion of primes $p = n$ (see [14, Lemma 19])) and odd integers n (see [14, Theorem 21]) we have $t \geqslant n^{0.677}$.

Acknowledgement

The first author thanks the Alexander–von-Humboldt Foundation for support, the Universität Heidelberg for hospitality and Hannes Breuer for interesting discussions.

The authors are grateful to the organisers of the the *Sixth Number Theory Down Under* Conference (NTDU-6), Canberra, 24–27 September, 2018, for creating a very encouraging and collaborative atmosphere, which has led to this work.

References

[1] O. Ahmadi, I. E. Shparlinski and J. F. Voloch, 'Multiplicative order of Gauss periods', *Internat. J. Number Theory* **6** (2010), 877–882.
[2] G. E. Andrews, *The Theory of Partitions* (Addison-Wesley, New York, 1976).
[3] F. Breuer, 'Periods of Ducci sequences and odd solutions to a Pellian equation', *Bull. Aust. Math. Soc.* **100** (2019), 201–205.
[4] F. Breuer, E. Lötter and A. B. van der Merwe, "Ducci sequences and cyclotomic polynomials', *Finite Fields Appl.* **13** (2007), 293–304.
[5] R. Brown and J. L. Merzel, 'The number of Ducci sequences with given period', *Fibonacci Quart.* **45** (2007), 115–121.

https://doi.org/10.1017/S0004972719001187 Published online by Cambridge University Press

[6] N. J. Calkin, J. G. Stevens and D. M. Thomas, 'A characterization for the length of cycles of the n-number Ducci game', *Fibonacci Quart.* **43** (2005), 53–59.
[7] C. Ciamberlini and A. Marengoni, 'Su una interessante curiosità numerica', *Periodiche di Matematiche* **17** (1937), 25–30.
[8] A. Clausing, 'Ducci matrices', *Amer. Math. Monthly* **125** (2018), 901–921.
[9] A. Ehrlich, 'Periods of Ducci's N-number game of differences', *Fibonacci Quart.* **28** (1990), 302–305.
[10] P. Erdős and M. R. Murty, 'On the order of a(mod p)', in: *Proc. 5th Canadian Number Theory Association Conf.* (American Mathematical Society, Providence, RI, 1999), 87–97.
[11] J. von zur Gathen and I. E. Shparlinski, 'Orders of Gauss periods in finite fields', *Appl. Algebra Engrg. Comm. Comput.* **9** (1998), 15–24.
[12] H. Glaser and G. Schöffl, 'Ducci-sequences and Pascal's triangle', *Fibonacci Quart.* **33** (1995), 313–324.
[13] P. Hagis, 'On a class of partitions with distinct summands', *Trans. Amer. Math. Soc.* **112** (1964), 401–415.
[14] P. Kurlberg and C. Pomerance, 'On the period of the linear congruential and power generators', *Acta Arith.* **119** (2005), 149–169.
[15] A. L. Ludington, 'Cycles of differences of integers', *J. Number Theory* **13** (1981), 255–261.
[16] M. Misiurewicz, J. G. Stevens and D. M. Thomas, 'Iterations of linear maps over finite fields', *Linear Algebra Appl.* **413** (2006), 218–234.
[17] P. Moree, 'Artin's primitive root conjecture – a survey', *Integers* **12A** (2012), 1–100; Paper A13.
[18] The On-line Encyclopedia of Integer Sequences, entry #A038553. https://oeis.org/A038553.
[19] R. Popovych, 'Elements of high order in finite fields of the form $\mathbb{F}_q[x]/\Phi_r(x)$', *Finite Fields Appl.* **18**(4) (2012), 700–710.
[20] R. Popovych, 'Sharpening of the explicit lower bounds for the order of elements in finite field extensions based on cyclotomic polynomials', *Ukrainian Math. J.* **66**(6) (2014), 916–927.
[21] I. E. Shparlinski, 'Linear equations with rational fractions of bounded height and stochastic matrices', *Q. J. Math.* **69** (2018), 487–499.
[22] J. H. Silverman, 'Wieferich's criterion and the abc-conjecture', *J. Number Theory* **30** (1988), 226–237.
[23] S. Solak and M. Bahşi, 'Some properties of circulant matrices with Ducci sequences', *Linear Algebra Appl.* **542** (2018), 557–568.

FLORIAN BREUER, School of Mathematical and Physical Sciences,
University of Newcastle, Newcastle, NSW 2308, Australia
e-mail: florian.breuer@newcastle.edu.au

IGOR E. SHPARLINSKI, School of Mathematics and Statistics,
University of New South Wales, Sydney, NSW 2052, Australia
e-mail: igor.shparlinski@unsw.edu.au

https://doi.org/10.1017/S0004972719001187 Published online by Cambridge University Press