This is the published version of:


**Access to the published version:**

http://dx.doi.org/10.1017/S000497271000198X

**Copyright:**

Copyright 2011 Australian Mathematical Publishing Association Inc. Published by Cambridge University Press.
CLUS OF MULTIPLICATIVE CHARACTER SUMS WITH FERMAT QUOTIENTS OF PRIMES

IGOR E. SHPARLINSKI

(Received 14 August 2010)

Abstract

Given a prime $p$, the Fermat quotient $q_p(u)$ of $u$ with $\gcd(u, p) = 1$ is defined by the conditions

$$q_p(u) \equiv \frac{u^{p-1} - 1}{p} \mod p, \quad 0 \leq q_p(u) \leq p - 1.$$ 

We derive a new bound on multiplicative character sums with Fermat quotients $q_p(\ell)$ at prime arguments $\ell$.


Keywords and phrases: Fermat quotients, character sums, Vaughan identity.

1. Introduction

For a prime $p$ and an integer $u$ with $\gcd(u, p) = 1$ the Fermat quotient $q_p(u)$ is defined as the unique integer with

$$q_p(u) \equiv \frac{u^{p-1} - 1}{p} \mod p, \quad 0 \leq q_p(u) \leq p - 1.$$ 

We also put

$$q_p(kp) = 0, \quad k \in \mathbb{Z}.$$ 

Fermat quotients $q_p(u)$ appear and have numerous applications in computational and algebraic number theory and have been studied in a number of works; see, for example, [1, 4, 5, 8, 9, 12, 14] and references therein. The study of their distribution modulo $p$ is especially important. This has motivated a number of works [2, 7, 11, 15, 16] where bounds on various exponential and multiplicative character sums with Fermat quotients are given. For example, Heath-Brown [11, Theorem 2] has given a nontrivial upper bound on exponential sums with $q_p(u)$, $u = M + 1, \ldots, M + N$, for any integers $M$ and $N$ provided that $N \geq p^{3/4+\varepsilon}$ for...
some fixed $\varepsilon > 0$ and $p \to \infty$. Furthermore, using the full power of the Burgess bound, one can obtain a nontrivial estimate already for $N \geq p^{1/2+\varepsilon}$; see [4, Section 4]. For longer intervals of length $N \geq p^{1+\varepsilon}$, a nontrivial bound of exponential sums with linear combinations of $s \geq 1$ consecutive values $q_p(u), \ldots, q_p(u+s-1)$ has been given in [15]; see also [2].

Several one-dimensional and bilinear multiplicative character sums have recently been estimated in [16]; see also [7]. Moreover, in [16, Corollary 4.2] the following multiplicative character sums over primes:

$$T_p(N; \chi) = \sum_{\ell \leq N \text{ prime}} \chi(q_p(\ell))$$

are estimated as

$$|T_p(N; \chi)| \leq (Np^{-1/2} + N^{6/7} p^{3/7})N^{o(1)}, \quad (1)$$
as $N \to \infty$.

Here we use an idea of Garaev [6] and derive a new upper bound on the sums $T_p(N; \chi)$ which, as in [16], nontrivial provided that $N \geq p^{3+\varepsilon}$, for some fixed $\varepsilon > 0$, but improves (1).

As in [16], we first estimate related sums with the von Mangoldt function

$$\Lambda(n) = \begin{cases} \log \ell & \text{if } n \text{ is a power of a prime } \ell, \\ 0 & \text{otherwise.} \end{cases}$$

**Theorem 1.** For any integer $N \geq 1$ and nonprincipal multiplicative character $\chi$ modulo $p$,

$$\left| \sum_{n \leq N} \Lambda(n)\chi(q_p(n)) \right| \leq (Np^{-1/2} + N^{5/6} p^{1/2})N^{o(1)},$$
as $N \to \infty$.

Via partial summation, we immediately derive the following corollary.

**Corollary 2.** For any integer $N \geq 1$ and nonprincipal multiplicative character $\chi$ modulo $p$,

$$|T_p(N; \chi)| \leq (Np^{-1/2} + N^{5/6} p^{1/2})N^{o(1)},$$
as $N \to \infty$.

Throughout the paper, $\ell$ and $p$ always denote prime numbers, while $k, m$ and $n$ (in both upper and lower case) denote positive integer numbers.

The implied constants in the symbols ‘$O$’ and ‘$\ll$’ may occasionally depend on the integer parameter $\nu \geq 1$ and are absolute otherwise. We recall that the notations $U = O(V)$ and $U \ll V$ are both equivalent to the assertion that the inequality $|U| \leq cV$ holds for some constant $c > 0$. 
2. Vaughan identity

We use the following result of Vaughan [17] in the form given in [3, Ch. 24].

**Lemma 3.** For any complex-valued function $f(n)$ and any real numbers $U, V > 1$ with $UV \leq N$,

$$\sum_{n \leq N} \Lambda(n) f(n) \ll \Sigma_1 + \Sigma_2 + \Sigma_3 + \Sigma_4,$$

where

$$\Sigma_1 = \left| \sum_{n \leq U} \Lambda(n) f(n) \right|,$$

$$\Sigma_2 = (\log UV) \sum_{k \leq UV} \left| \sum_{m \leq N/k} f(km) \right|,$$

$$\Sigma_3 = (\log N) \sum_{k \leq V} \max_{w \geq 1} \left| \sum_{w \leq m \leq N/k} f(km) \right|,$$

$$\Sigma_4 = \left| \sum_{k \leq N \atop k > V, m > U} \Lambda(m) \sum_{d \mid k, d \leq V} \mu(d) f(km) \right|.$$

We apply this identity with $f(n) = \chi(n)$ for a nonprincipal multiplicative character $\chi$ modulo $p$.

3. Sums with consecutive integers

We need some estimates of single and double character sums from [16]. First we recall a special case of [16, Theorem 3.1].

**Lemma 4.** For every fixed integer $\nu \geq 1$, for any integers $M \geq 1$, nonprincipal multiplicative character $\chi$ modulo $p$,

$$\left| \sum_{m=1}^{M} \chi(q_p(km)) \right| \leq M^{1-1/\nu} p^{(5\nu+1)/4\nu^2+o(1)}$$

as $p \to \infty$, uniformly over all integers $k$ with $\gcd(k, p) = 1$.

Next we present the following special case of [16, Theorem 3.3].

**Lemma 5.** Given two positive integers $K$ and $M$ and two sequences $\alpha_k$, $1 \leq k \leq K$, and $\beta_m$, $1 \leq m \leq M$, of complex numbers with

$$A = \max_{1 \leq k \leq K} |\alpha_k| \quad \text{and} \quad B = \max_{1 \leq m \leq M} |\beta_m|,$$

for any nonprincipal multiplicative character $\chi$ modulo $p$,

$$\sum_{k \leq K} \sum_{m \leq M} \alpha_k \beta_m \chi(q_p(km)) \ll AB\left(\frac{K}{p} + K^{1/2}\right)\left(\frac{M}{p} + M^{1/2}\right) p^{3/2}.$$
We now use the idea of [6] to derive a version of Lemma 5 for the case where the summation limit over \( m \) depends on \( k \).

**Lemma 6.** Given two integers \( K \) and \( M \), a sequence of positive integers \( M_k \) with \( M_k \leq M \), \( 1 \leq k \leq K \), and two sequences \( \alpha_k \), \( K < k \leq 2K \), and \( \beta_m \), \( 1 \leq m \leq M \), of complex numbers with

\[
A = \max_{1 \leq k \leq K} |\alpha_k| \quad \text{and} \quad B = \max_{1 \leq m \leq M} |\beta_m|,
\]

for any nonprincipal multiplicative character \( \chi \) modulo \( p \),

\[
\sum_{k \leq K} \sum_{m \leq M_k} \alpha_k \beta_m \chi(q_p(km)) \ll AB \left( \frac{K}{p} + K^{1/2} \right) \left( \frac{M}{p} + M^{1/2} \right)^{3/2} p^{o(1)}.
\]

**Proof.** For a complex \( z \) we define \( e_M(z) = \exp(2\pi i z/M) \). We have

\[
\sum_{m \leq M_k} \alpha_k \beta_m \chi(q_p(km))
\]

\[
= \sum_{m \leq M} \alpha_k \beta_m \chi(q_p(km)) \frac{1}{M} \sum_{-(M-1)/2 \leq s \leq M/2} \sum_{w \leq M_k} e_M(s(m-w))
\]

\[
= \frac{1}{M} \sum_{-(M-1)/2 \leq s \leq M/2} \sum_{w \leq M_k} e_M(-sw) \sum_{m \leq M} \alpha_k \beta_m e_M(sm) \chi(q_p(km)).
\]

Since for \( |s| \leq M/2 \) we have

\[
\sum_{w \leq M_k} e_M(-sw) = \eta_{k,s} \frac{M}{|s|+1},
\]

for some complex numbers \( \eta_{k,s} \ll 1 \), see [13, Bound (8.6)], we conclude that for \( |s| \leq M/2 \) and \( k \leq K \) there are some complex numbers \( \gamma_{k,s} = \eta_{k,s} \alpha_k \) such that

\[
\sum_{k \leq K} \sum_{m \leq M_k} \alpha_k \beta_m \chi(q_p(km))
\]

\[
= \sum_{-(M-1)/2 \leq s \leq M/2} \frac{1}{|s|+1} \sum_{k \leq K} \sum_{m \leq M} \gamma_{k,s} \beta_m e_M(sm) \chi(q_p(km)).
\]

Using Lemma 5, we derive the desired result. \( \square \)

As in [16], our main technical tool is an estimate of different double sums with a ‘hyperbolic’ area of summation. We now derive a stronger version of [16, Theorem 3.4].

**Lemma 7.** Given real numbers \( X, Y, Z \) with \( Z > Y > X \geq 2 \) and two sequences \( \alpha_k \), \( X < k \leq Y \), and \( \beta_m \), \( 1 \leq m \leq Z/X \), of complex numbers with

\[
A = \max_{X < k \leq Y} |\alpha_k| \quad \text{and} \quad B = \max_{1 \leq m \leq Z/X} |\beta_m|,
\]
for any nonprincipal multiplicative character \( \chi \) modulo \( p \),
\[
\sum_{X < k \leq Y} \sum_{m \leq Z/k} \alpha_k \beta_m \chi(q_p(km)) \ll AB(Zp^{-2} + Y^{1/2}Z^{1/2}p^{-1} + X^{-1/2}Zp^{-1} + Z^{1/2})p^{3/2}Z^{o(1)}.
\]

**Proof.** Defining some values of \( \alpha_k \) as zeros, we write
\[
\sum_{X < k \leq Y} \sum_{m \leq Z/k} \alpha_k \beta_m \chi(q_p(km)) = \sum_{j = 1}^{J} \sum_{e_j \leq k \leq e_j + 1} \sum_{m \leq Z/k} \alpha_k \beta_m \chi(q_p(km)),
\]
where \( I = \lfloor \log X \rfloor \) and \( J = \lfloor \log Y \rfloor \). So, by Lemma 6,
\[
\sum_{X < k \leq Y} \sum_{m \leq Z/k} \alpha_k \beta_m \chi(q_p(km)) \ll ABp^{3/2}Z^{o(1)} \sum_{j = 1}^{J} \left( \frac{e_j}{p} + e_j^{1/2} \right) \left( \frac{Ze^{-j}}{p} + Z^{1/2}e^{-j/2} \right) \ll ABp^{3/2}Z^{o(1)} \left( JZp^{-2} + e^{1/2}Z^{1/2}p^{-1} + e^{-1/2}Zp^{-1} + JZ^{1/2} \right).
\]
Since \( X \ll e^I \leq e^J \ll Y \), we immediately obtain the desired result. \( \square \)

4. **Proof of Theorem 1**

Since the bound is trivial for \( N < p^3 \), we assume that \( N \geq p^3 \).

Let us fix some \( U, V > 1 \) with \( UV \leq N \) and apply Lemma 3 with the function \( f(n) = \chi(q_p(n)) \).

We estimate \( \Sigma_1 \) trivially by the prime number theorem,

\[
\Sigma_1 = \sum_{1 \leq n \leq U} \Lambda(n) f(n) \ll \sum_{1 \leq n \leq U} \Lambda(n) \ll U.
\]

To bound \( \Sigma_2 \) we fix some parameter \( W \) and write
\[
\Sigma_2 = (\Sigma_{2,1} + \Sigma_{2,2})N^{o(1)},
\]
where
\[
\Sigma_{2,1} = \sum_{k \leq W} \sum_{m \leq N/k} \chi(q_p(km)) \quad \text{and} \quad \Sigma_{2,2} = \sum_{W < k \leq UV} \sum_{m \leq N/k} \chi(q_p(km)).
\]
We now estimate the inner sum in $\Sigma_{2,1}$ by Lemma 4 (with $v = 1$) if $\gcd(k, p) = 1$ and also use the trivial bound $O(N/k)$ for $p|k$, getting

$$\Sigma_{2,1} \leq \sum_{1 \leq k \leq W \overline{\gcd(k,p) = 1}} p^{3/2+o(1)} + \sum_{1 \leq k \leq W} \frac{N^{1+o(1)}}{k} \leq WP^{3/2+o(1)} + N^{1+o(1)}p^{-1}. \quad (4)$$

To estimate $\Sigma_{2,2}$, we apply Lemma 7. Thus

$$\Sigma_{2,2} \leq (Np^{-1/2} + N^{1/2}U^{1/2}V^{1/2}p^{1/2} + NW^{-1/2}p^{1/2} + N^{1/2}p^{3/2})N^{o(1)}. \quad (5)$$

Clearly, all the term $N^{1+o(1)}p^{-1}$ in the bound (4) is dominated by the term $N^{1+o(1)}p^{-1/2}$ in (5), thus choosing $W = N^{2/3}p^{-2/3}$, we see from (3) that

$$\Sigma_2 \leq (Np^{-1/2} + N^{1/2}U^{1/2}V^{1/2}p^{1/2} + N^{2/3}p^{5/6} + N^{1/2}p^{3/2})N^{o(1)}.$$ 

Since $N^{1/2}p^{3/2} \geq N^{2/3}p^{5/6}$ for $N \leq p^4$ and $Np^{-1/2} \geq N^{2/3}p^{5/6}$ for $N \geq p^4$, this bound simplifies as

$$\Sigma_2 \ll (Np^{-1/2} + N^{1/2}U^{1/2}V^{1/2}p^{1/2} + N^{1/2}p^{3/2})N^{o(1)}. \quad (6)$$

Similarly to (4), we also obtain

$$\Sigma_3 \ll (V p^{3/2} + Np^{-1})N^{o(1)}. \quad (7)$$

It remains only to estimate

$$\Sigma_4 = \left| \sum_{V < k \leq N/U} \sum_{U < m \leq N/k} \Lambda(m) \sum_{d | k, d \leq V} \sum_{d | k} \mu(d) \chi(q_p(km)) \right|.$$ 

Since

$$\left| \sum_{d | k, d \leq V} \mu(d) \right| \leq \sum_{d | k} 1 = k^{o(1)} \quad \text{and} \quad \Lambda(m) \leq \log m,$$

see [10, Theorem 315], Lemma 7 yields

$$\Sigma_4 \leq (Np^{-2} + N^{1/2}(N/U)^{1/2}p^{-1} + NV^{-1/2}p^{-1} + N^{1/2})p^{3/2}N^{o(1)}$$

$$\leq (Np^{-1/2} + NU^{-1/2}p^{1/2} + NV^{-1/2}p^{1/2} + N^{1/2}p^{3/2})N^{o(1)}. \quad (8)$$

We now choose $U$ and $V$ to satisfy

$$U = V \quad \text{and} \quad N^{1/2}U^{1/2}V^{1/2}p^{1/2} = NU^{-1/2}p^{1/2}$$

in order to balance the terms that depend on $U$ and $V$ in the bounds (6) and (8), that is,

$$U = V = N^{1/3}.$$ 

With this choice recalling also (2) and (7), we obtain

$$\sum_{n \leq N} \Lambda(n)\chi(q_p(n)) \ll (Np^{-1/2} + N^{5/6}p^{1/2} + N^{1/2}p^{3/2})N^{o(1)}.$$ 

Clearly the result is trivial for $N < p^3$. On the other hand, $N^{5/6}p^{1/2} \geq N^{1/2}p^{3/2}$ for $N \geq p^3$. The result now follows.
References


IGOR E. SHPARLINSKI, Department of Computing, Macquarie University, Sydney, NSW 2109, Australia
e-mail: igor.shparlinski@mq.edu.au
Australian Mathematical Society. Bulletin

 ISSN: 0004-9727
Title: Australian Mathematical Society. Bulletin
Publishing Body: Cambridge University Press
Country: United Kingdom
Status: Active
Start Year: 1969
Frequency: 6 times a year
Annual Term: In 2 vols; 3 nos. per vol.
Document Type: Journal; Academic/Scholarly
Refereed: Yes
Abstracted/Indexed: Yes
Media: Print
Alternate Edition ISSN: 1755-1633
Language: Text in English
Price: GBP 250, USD 477 combined subscription per year to institutions (Print & Online Eds.) (effective 2010)
Subject: MATHEMATICS
Dewey #: 510
LC#: QA1
CODEN: ALNBAB
Article Index: Index Available
Pages per Issue: 176
Editor(s): Donald E Taylor (Editor-in-Chief)
E-Mail: bulletin@austms.org.au
URL: http://journals.cambridge.org/action/displayJournal?jid=BAZ
Description: Aims at quick publication of original research in all branches of mathematics.

Request this title:
I’d like to request this title.
Corrections:
Submit corrections to Ulrich’s about this title.
Publisher of this title?
If yes, click GO! to contact Ulrich’s about updating your title listings in the Ulrich’s database.