Bull. Aust. Math. Soc. **83** (2011), 456–462
doi:10.1017/S000497271000198X

BOUNDS 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

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

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

2010 *Mathematics subject classification*: primary 11A07; secondary 11L40, 11N25.
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

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

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 $N \ge p^{3/4+\varepsilon}$ for

The author was supported in part by Australian Research Council Grant DP1092835.

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:

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

are estimated as

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

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 is, 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 χ 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 χ 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, ℓ 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 $c > 0$.

https://doi.org/10.1017/S000497271000198X Published online by Cambridge University Press

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 $UV \le N$,*

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

where

$$\Sigma_1 = \bigg|\sum_{n\le U} \Lambda(n) f(n)\bigg|,$$

$$\Sigma_2 = (\log UV) \sum_{k\le UV}\bigg|\sum_{m\le N/k} f(km)\bigg|,$$

$$\Sigma_3 = (\log N) \sum_{k\le V}\max_{w\ge 1}\bigg|\sum_{w\le m\le N/k} f(km)\bigg|,$$

$$\Sigma_4 = \bigg|\sum_{\substack{km\le N\\ k>V, m>U}} \Lambda(m) \sum_{d\mid k, d\le V} \mu(d) f(km)\bigg|.$$

We apply this identity with $f(n) = \chi(n)$ for a nonprincipal multiplicative character χ 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 $\nu \ge 1$, for any integers $M \ge 1$, nonprincipal multiplicative character χ modulo p,*

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

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 α_k, $1 \le k \le K$, and β_m, $1 \le m \le M$, of complex numbers with*

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

for any nonprincipal multiplicative character χ modulo p,

$$\sum_{k\le K}\sum_{m\le M} \alpha_k\beta_m\chi(q_p(km)) \ll AB\Big(\frac{K}{p} + K^{1/2}\Big)\Big(\frac{M}{p} + M^{1/2}\Big)p^{3/2}.$$

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 $M_k \le M$, $1 \le k \le K$, and two sequences α_k, $K < k \le 2K$, and β_m, $1 \le m \le M$, of complex numbers with*

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

for any nonprincipal multiplicative character χ modulo p,

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

PROOF. For a complex z we define $\mathbf{e}_M(z) = \exp(2\pi i z/M)$. We have

$$\begin{aligned}\sum_{m\le M_k} &\alpha_k\beta_m\chi(q_p(km)) \\ &= \sum_{m\le M} \alpha_k\beta_m\chi(q_p(km))\frac{1}{M}\sum_{-(M-1)/2\le s\le M/2}\ \sum_{w\le M_k} \mathbf{e}_M(s(m-w)) \\ &= \frac{1}{M}\sum_{-(M-1)/2\le s\le M/2}\ \sum_{w\le M_k}\mathbf{e}_M(-sw)\sum_{m\le M}\alpha_k\beta_m\mathbf{e}_M(sm)\chi(q_p(km)).\end{aligned}$$

Since for $|s| \le M/2$ we have

$$\sum_{w\le M_k}\mathbf{e}_M(-sw) = \eta_{k,s}\frac{M}{|s|+1},$$

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

$$\begin{aligned}\sum_{k\le K}\sum_{m\le M_k} &\alpha_k\beta_m\chi(q_p(km)) \\ &= \sum_{-(M-1)/2\le s\le M/2}\frac{1}{|s|+1}\sum_{k\le K}\sum_{m\le M}\gamma_{k,s}\beta_m\mathbf{e}_M(sm)\chi(q_p(km)).\end{aligned}$$

Using Lemma 5, we derive the desired result. □

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 $Z > Y > X \ge 2$ and two sequences α_k, $X < k \le Y$, and β_m, $1 \le m \le Z/X$, of complex numbers with*

$$A = \max_{X<k\le Y} |\alpha_k| \quad \text{and} \quad B = \max_{1\le m\le Z/X} |\beta_m|,$$

https://doi.org/10.1017/S000497271000198X Published online by Cambridge University Press

for any nonprincipal multiplicative character χ *modulo* p*,*

$$\sum_{X<k\le Y}\sum_{m\le Z/k}\alpha_k\beta_m\chi(q_p(km)) \ll AB(Zp^{-2}+Y^{1/2}Z^{1/2}p^{-1}+X^{-1/2}Zp^{-1}+Z^{1/2})p^{3/2}Z^{o(1)}.$$

PROOF. Defining some values of α_k as zeros, we write

$$\sum_{X<k\le Y}\sum_{m\le Z/k}\alpha_k\beta_m\chi(q_p(km)) = \sum_{j=I}^{J}\sum_{e^j\le k\le e^{j+1}}\sum_{m\le Z/k}\alpha_k\beta_m\chi(q_p(km)),$$

where $I=\lfloor \log X\rfloor$ and $J=\lfloor \log Y\rfloor$. So, by Lemma 6,

$$\begin{aligned}\sum_{X<k\le Y}\sum_{m\le Z/k}&\alpha_k\beta_m\chi(q_p(km))\\ &\ll ABp^{3/2}Z^{o(1)}\sum_{j=I}^{J}\Big(\frac{e^j}{p}+e^{j/2}\Big)\Big(\frac{Ze^{-j}}{p}+Z^{1/2}e^{-j/2}\Big)\\ &\ll ABp^{3/2}Z^{o(1)}(JZp^{-2}+e^{J/2}Z^{1/2}p^{-1}+e^{-I/2}Zp^{-1}+JZ^{1/2}).\end{aligned}$$

Since $X\ll e^I\le e^J\ll Y$, we immediately obtain the desired result. □

4. Proof of Theorem 1

Since the bound is trivial for $N<p^3$, we assume that $N\ge p^3$.

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

We estimate Σ_1 trivially by the prime number theorem,

$$\Sigma_1=\Big|\sum_{1\le n\le U}\Lambda(n)f(n)\Big|\le\sum_{1\le n\le U}\Lambda(n)\ll U. \tag{2}$$

To bound Σ_2 we fix some parameter W and write

$$\Sigma_2=(\Sigma_{2,1}+\Sigma_{2,2})N^{o(1)}, \tag{3}$$

where

$$\Sigma_{2,1}=\sum_{k\le W}\Big|\sum_{m\le N/k}\chi(q_p(km))\Big|,$$

$$\Sigma_{2,2}=\sum_{W<k\le UV}\Big|\sum_{m\le N/k}\chi(q_p(km))\Big|.$$

https://doi.org/10.1017/S000497271000198X Published online by Cambridge University Press

We now estimate the inner sum in $\Sigma_{2,1}$ by Lemma 4 (with $\nu = 1$) if $\gcd(k, p) = 1$ and also use the trivial bound $O(N/k)$ for $p|k$, getting

$$\Sigma_{2,1} \le \sum_{\substack{1\le k\le W \\ \gcd(k,p)=1}} p^{3/2+o(1)} + \sum_{\substack{1\le k\le W \\ p|k}} \frac{N^{1+o(1)}}{k} \le Wp^{3/2+o(1)} + N^{1+o(1)}p^{-1}. \qquad (4)$$

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

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

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

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

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

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

Similarly to (4), we also obtain

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

It remains only to estimate

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

Since

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

see [10, Theorem 315], Lemma 7 yields

$$\begin{aligned} \Sigma_4 &\le (Np^{-2} + N^{1/2}(N/U)^{1/2}p^{-1} + NV^{-1/2}p^{-1} + N^{1/2})p^{3/2}N^{o(1)} \\ &\le (Np^{-1/2} + NU^{-1/2}p^{1/2} + NV^{-1/2}p^{1/2} + N^{1/2}p^{3/2})N^{o(1)}. \end{aligned} \qquad (8)$$

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

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

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

https://doi.org/10.1017/S000497271000198X Published online by Cambridge University Press

References

[1] J. Bourgain, K. Ford, S. V. Konyagin and I. E. Shparlinski, 'On the divisibility of Fermat quotients', *Michigan Math. J.* **59** (2010), 313–328.

[2] Z. Chen, A. Ostafe and A. Winterhof, 'Structure of pseudorandom numbers derived from Fermat quotients', in: *Arithmetic of Finite Fields*, Lecture Notes in Computer Science, 6087 (eds. M. Anwar Hasan and Tor Helleseth) (Springer, Berlin, 2010), pp. 73–85.

[3] H. Davenport, *Multiplicative Number Theory*, 2nd edn (Springer, New York, 1980).

[4] R. Ernvall and T. Metsänkylä, 'On the p-divisibility of Fermat quotients', *Math. Comp.* **66** (1997), 1353–1365.

[5] W. L. Fouché, 'On the Kummer–Mirimanoff congruences', *Q. J. Math. Oxford* **37** (1986), 257–261.

[6] M. Z. Garaev, 'An estimate of Kloosterman sums with prime numbers and an application', *Mat. Zametki* **88**(3) (2010), 365–373 (in Russian).

[7] D. Gomez and A. Winterhof, 'Multiplicative character sums of Fermat quotients and pseudorandom sequences', *Period. Math. Hungar.*, to appear.

[8] A. Granville, 'Some conjectures related to Fermat's last theorem', in: *Number Theory* (W. de Gruyter, New York, 1990), pp. 177–192.

[9] A. Granville, 'On pairs of coprime integers with no large prime factors', *Expo. Math.* **9** (1991), 335–350.

[10] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers* (Oxford University Press, Oxford, 1979).

[11] R. Heath-Brown, 'An estimate for Heilbronn's exponential sum', in: *Analytic Number Theory: Proc. Conf. in Honor of Heini Halberstam* (Birkhäuser, Boston, 1996), pp. 451–463.

[12] Y. Ihara, 'On the Euler–Kronecker constants of global fields and primes with small norms', in: *Algebraic Geometry and Number Theory*, Progress in Mathematics, 850 (Birkhäuser, Boston, 2006), pp. 407–451.

[13] H. Iwaniec and E. Kowalski, *Analytic Number Theory* (American Mathematical Society, Providence, RI, 2004).

[14] H. W. Lenstra, 'Miller's primality test', *Inform. Process. Lett.* **8** (1979), 86–88.

[15] A. Ostafe and I. E. Shparlinski, 'Pseudorandomness and dynamics of Fermat quotients', *SIAM J. Discrete Math.* **25** (2011), 50–71.

[16] I. E. Shparlinski, 'Character sums with Fermat quotients', *Q. J. Math.*, to appear.

[17] R. C. Vaughan, 'An elementary method in prime number theory', *Acta Arith.* **37** (1980), 111–115.

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

https://doi.org/10.1017/S000497271000198X Published online by Cambridge University Press