I. E. SHPARLINSKI
KODAI MATH. J.
36 (2013), 99–108

ON VANISHING FERMAT QUOTIENTS AND A BOUND OF THE IHARA SUM

Igor E. Shparlinski

Abstract

We improve an estimate of A. Granville (1987) on the number of vanishing Fermat quotients $q_p(\ell)$ modulo a prime p when ℓ runs through primes $\ell \le N$. We use this bound to obtain an unconditional improvement of the conditional (under the Generalised Riemann Hypothesis) estimate of Y. Ihara (2006) on a certain sum, related to vanishing Fermat quotients. In turn this sum appears in the study of the index of certain subfields of cyclotomic fields $\mathbf{Q}(\exp(2\pi i/p^2))$.

1. Introduction

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

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

We also define $q_p(u) = 0$ for $u \equiv 0 \pmod p$.

Fermat quotients appear and play a major role in various questions of computational and algebraic number theory and thus have been studied in a number of works: see, for example, [1, 2, 3, 5, 6, 8, 10, 12] and references therein. Understanding the vanishing of Fermat quotients $q_p(a)$ is important for many applications and in particular, the smallest value ℓ_p of $u \ge 1$ with $q_p(u) \ne 0$, has been investigated in [1, 2, 3, 5, 10]. For example, in [1], improving the previous estimate $\ell_p = O((\log p)^2)$ of Lenstra [10] (see also [3, 6, 8]), the following bounds have been given:

$$\ell_p \le \begin{cases} (\log p)^{463/252+o(1)} & \text{for all primes } p, \\ (\log p)^{5/3+o(1)} & \text{for almost all primes } p, \end{cases}$$

(where "almost all primes p" means for all primes p but a set of relative density zero).

2000 *Mathematics Subject Classification*. 11A07, 11N25, 11R04.
Key words and phrases. Fermat quotient, Ihara sum, cyclotomic field.
Received September 16, 2011; revised April 13, 2012.

For integers $M \ge 0$ and $N \ge 1$ we consider the sets

$$\mathcal{Q}_p(M,N) = \{M+1 \le n \le M+N : q_p(n) = 0\},$$
$$\mathcal{R}_p(M,N) = \{M+1 \le \ell \le M+N : \ell \text{ prime}, \ q_p(\ell) = 0\},$$

and also put

$$\mathcal{Q}_p(N) = \mathcal{Q}_p(0,N) \quad \text{and} \quad \mathcal{R}_p(N) = \mathcal{R}_p(0,N).$$

Here we use some results of [1], combined with the approach of Granville [4] and some other arguments, to obtain new estimates on the cardinalities of these sets.

For example, for small N our estimates on $\#\mathcal{Q}_p(N)$ and $\#\mathcal{R}_p(N)$ improve those of [4]. We apply these improvements to study the sums

$$S_p = \sum_{n \in \mathcal{Q}_p(p)} \frac{\Lambda(n)}{n}$$

introduced by Ihara [8], where, as usual,

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

denotes the *von Mangoldt function*.

We note that in [8, Corollary 7], under the *Generalised Riemann Hypothesis*, the bound

$$S_p \le 2 \log\log p + 2 + o(1) \tag{1}$$

as $p \to \infty$, has been obtained. Here we give an unconditional proof of a stronger bound.

Throughout the paper, the implied constants in the symbols 'O', and '$\ll$' may occasionally depend on the real positive parameter α and are absolute otherwise (we recall that the notation $U \ll V$ is equivalent to $U = O(V)$).

2. Preparations

We recall that for any integers m and n with $\gcd(mn, p) = 1$ we have

$$q_p(mn) \equiv q_p(m) + q_p(n) \pmod p, \tag{2}$$

see, for example, [2, Equation (2)].

Let $\mathcal{G}_p$ be the group of the pth power residues in the unit group $\mathbf{Z}_{p^2}^*$ of the residue ring $\mathbf{Z}_{p^2}$ modulo p^2.

LEMMA 1. *For any $u \in \mathbf{Z}_{p^2}^*$ the conditions $q_p(u) = 0$ and $u \in \mathcal{G}_p$ are equivalent.*

Proof. Clearly $q_p(u) = 0$ for $u \in \mathbf{Z}_{p^2}^*$ is equivalent to $u^{p-1} \equiv 1 \pmod{p^2}$, which in turn is equivalent to $u \in \mathcal{G}_p$. □

For integers $M \geq 0$ and $N \geq 1$ Let $T_p(M, N)$ be the number of $w \in [M+1, M+N]$ such that their residues modulo p^2 belong to $\mathcal{G}_p$. Clearly,

$$\#\mathcal{Q}_p(M, N) = T_p(M, N) + O(N/p + 1), \tag{3}$$

(the term $O(N/p + 1)$ comes from $w \equiv 0 \pmod{p}$). The following estimate follows immediately from [1, Equation (12)] (we also note that although the proof of [1, Equation (12)], given only for initial intervals it works without any changes for any interval).

Lemma 2. *For any fixed*

$$\alpha > \frac{463}{252},$$

and

$$N \geq p^{\alpha}$$

we have

$$T_p(M, N) \ll N/p.$$

Furthermore, we need the following estimate which is derived by Heath-Brown and Konyagin [7, Section 2] from [7, Lemma 4] (more general results are given by Malykhin [11, Theorems 1 and 2]).

Lemma 3. *We have*

$$W_p \ll p^{5/2},$$

where

$$W_p = \#\{w_1, w_2, w_3, w_4 \in \mathcal{G}_p : w_1 + w_2 \equiv w_3 + w_4 \pmod{p^2}\}.$$

Let $\tau_s(n)$ be the number of representations of n as a product of s positive integers:

$$\tau_s(n) = \#\{(n_1, \ldots, n_s) \in \mathbf{N}^s \mid n = n_1 n_2 \cdots n_s\}.$$

We also need the following upper bound from [13]:

Lemma 4. *Uniformly over n and s we have*

$$\tau_s(n) \leq \exp\left(\frac{(\log n)(\log s)}{\log\log n}\left(1 + O\left(\frac{\log\log\log n + \log s}{\log\log n}\right)\right)\right).$$

In particular, we have:

Corollary 5. *If $s = (\log n)^{o(1)}$ then*

$$\tau_s(n) \leq n^{o(1)}.$$

as $n \to \infty$.

3. Distribution of vanishing Fermat quotients

Here we estimate the cardinality of the sets $\mathcal{Q}_p(M;N)$ and $\mathcal{R}_p(M;N)$. For large values of N, namely for $N \geq p^{\alpha}$ with some fixed $\alpha > 463/252$ an essentially optimal bound $\#\mathcal{Q}_p(M,N) \ll N/p$ follows from (3) and Lemma 2. Hence, for $N \leq p^{463/252}$ we have

$$\#\mathcal{Q}_p(M,N) \ll \min\{N, p^{211/252+o(1)}\}, \qquad (4)$$

as $p \to \infty$.

Here we consider the case of smaller values of N.

We start with the case of $M = 0$, that is, with the sets $\mathcal{Q}_p(N)$ and $\mathcal{R}_p(N)$. In this case, Granville [4] has given a nontrivial bound on the cardinality of the set $\mathcal{R}_p(N)$. Namely, it is shown in [4] that for $u = 1, 2, \dots$

$$\#\mathcal{R}_p(p^{1/u}) \leq up^{1/2u}. \qquad (5)$$

We note that the argument used in the proof of (5) can be used to estimate $\#\mathcal{R}_p(p^{1/u})$ for any real $u \geq 1$.

We derive now upper bounds on $\#\mathcal{Q}_p(N)$ and $\#\mathcal{R}_p(N)$ that improve (5).

Theorem 6. *For any fixed*

$$\alpha > \frac{463}{252},$$

for $1 \leq u = (\log p)^{o(1)}$, *where*

$$u = \frac{\log p}{\log N},$$

we have

$$\#\mathcal{Q}_p(N) \ll Np^{-(1+o(1))/\lceil \alpha u \rceil}$$

as $p \to \infty$.

Proof. We put

$$s = \lceil \alpha u \rceil.$$

We consider $(\#\mathcal{Q}_p(N))^s$ products $n = n_1 \cdots n_s$ where $(n_1, \dots, n_s) \in \mathcal{Q}_p(N)^s$. By (2) we see that

$$q_p(n) \equiv q_p(n_1) + \cdots + q_p(n_s) \equiv 0 \pmod p,$$

thus $q_p(n) = 0$.

Furthermore, using Corollary 5 we see that each $n \leq N^s < p^{\alpha+1}$ has at most

$$\tau_s(n) = p^{o(1)}$$

such representations. We also note that $N^s \ge p^\alpha$. Therefore, combining Lemmas 1 and 2, we derive

$$(\#\mathcal{Q}_p(N))^s \le T_p(N^s)p^{o(1)} \le N^s p^{-1+o(1)},$$

which implies the desired result. □

Corollary 7. *If*

$$\frac{\log p}{\log N} = (\log p)^{o(1)} \quad and \quad \frac{\log p}{\log N} \to \infty$$

then

$$\#\mathcal{Q}_p(N) \le N^{211/463+o(1)}$$

as $p \to \infty$.

For the set $\mathcal{R}_p(N)$ we have a bound in a wider range of u.

Theorem 8. *For any fixed*

$$\alpha > \frac{463}{252},$$

for $u \ge 1$, *where*

$$u = \frac{\log p}{\log N},$$

we have

$$\#\mathcal{R}_p(N) \ll uNp^{-1/\lceil \alpha u \rceil}$$

as $p \to \infty$.

Proof. The proof is the same as that of Theorem 6 except that instead of Corollary 5 we note that there are at most $s!$ products of s primes $\ell_1 \cdots \ell_s$ that take the same value. So, we derive

$$(\#\mathcal{R}_p(N))^s \ll s! T_p(N^s) \ll s! N^s p^{-1},$$

and the result now follows. □

Corollary 9. *If* $N = p^{o(1)}$ *then*

$$\#\mathcal{R}_p(N) \le N^{211/463+o(1)} \log p$$

as $p \to \infty$.

The method that has been used in Theorems 6 and 8 does not apply to shifted intervals. To estimate $\mathcal{Q}_p(M, N)$ for an arbitrary M we use a different method.

THEOREM 10. *We have,*

$$\#\mathcal{Q}_p(M,N) \ll N^{1/4}p^{5/8}.$$

Proof. We may assume that $N < 0.5p^2$ as otherwise the bound is trivial. Let

$$V_p(\lambda) = \#\{w_1, w_2 \in \mathcal{G}_p : w_1 + w_2 \equiv \lambda \pmod{p^2}\}.$$

Clearly

$$\sum_{\lambda \in [2M, 2M+2N]} V_p(\lambda) \geq T_p(M,N)^2. \tag{6}$$

Furthermore, by the Cauchy inequality

$$\left(\sum_{\lambda \in [2M, 2M+2N]} V_p(\lambda)\right)^2 \leq N \sum_{\lambda \in [2M, 2M+2N]} V_p(\lambda)^2 \leq N \sum_{\lambda=1}^{p^2} V_p(\lambda)^2 = NW_p, \tag{7}$$

where W_p is as in Lemma 3.

Combining the inequalities (6) and (7) and using Lemma 3, we obtain $T_p(M,N) \ll N^{1/4}p^{5/8}$. Recalling (3), and verifying that $N^{1/4}p^{5/8} \geq N/p$ for $N \leq 0.5p^2$, we obtain the desired result. □

Clearly, the bound of Theorem 10 improves the bound (4) for

$$p^{5/6} \leq N \leq p^{107/126}.$$

4. Ihara sums

First we consider approximations of S_p by partial sums

$$S_p(N) = \sum_{n \in \mathcal{Q}_p(N)} \frac{\Lambda(n)}{n}.$$

THEOREM 11. *For $N = p^{o(1)}$ we have*

$$S_p = S_p(N) + O(N^{-252/463+o(1)} \log p)$$

as $p \to \infty$.

Proof. Clearly, we have

$$S_p - S_p(N) = \sum_{\substack{\ell > N \\ \ell \in \mathcal{R}_p(p)}} \frac{\log \ell}{\ell} + O(N^{-1} \log N). \tag{8}$$

We now see from Corollary 9 that for any

$$L < N^3$$

we have

$$\sum_{\substack{2L \ge \ell > L \\ \ell \in \mathcal{R}_p(p)}} \frac{\log \ell}{\ell} \le \frac{\log L}{L} \sum_{\ell \in \mathcal{R}_p(2L)} 1 \tag{9}$$

$$\le \frac{\log L}{L} L^{211/463+o(1)} \log p = L^{-252/463+o(1)} \log p.$$

For

$$p \ge L > N^3$$

we choose

$$\alpha = \frac{463}{251}$$

and note that for $u \ge 1$ we have

$$\lceil \alpha u \rceil \le \frac{3}{2} \alpha u.$$

Thus Theorem 8 implies the bound

$$\#\mathcal{R}_p(L) \ll L^{1-2/3\alpha} \log p \ll L^{2/3} \log p.$$

Hence in the above range, we have

$$\sum_{\substack{2L \ge \ell > L \\ \ell \in \mathcal{R}_p(p)}} \frac{\log \ell}{\ell} \le \frac{\log L}{L} \sum_{\ell \in \mathcal{R}_p(2L)} 1 \tag{10}$$

$$\le \frac{\log L}{L} L^{2/3} \log p = L^{-1/3+o(1)} \log p.$$

Thus covering the range $[N, p]$ by dyadic intervals of the form $[L, 2L]$ and using the bounds (9), and (10) we derive

$$\sum_{\substack{\ell > N \\ \ell \in \mathcal{R}_p(p)}} \frac{\log \ell}{\ell} \le N^{-252/463+o(1)} \log p,$$

which after the substituting it in (8) implies the desired estimate. □

Since by the Mertens formula (see, for example, [9, Equation (2.14)])

$$S_p(N) \le \sum_{n \le N} \frac{\Lambda(n)}{n} = \log N + O(1),$$

we derive from Theorem 11:

Corollary 12. *For $N = p^{o(1)}$ we have*

$$S_p \le \log N + O(N^{-252/463+o(1)} \log p + 1)$$

as $p \to \infty$.

We now obtain an unconditional improvement of the conditional estimate (1).

Corollary 13. *We have*

$$S_p \le (463/252 + o(1)) \log\log p$$

as $p \to \infty$.

Proof. Taking $N = \lceil (\log p)^{\alpha} \rceil$ with $\alpha > 463/252$ in the bound of Corollary 12 leads to the estimate

$$S_p \le \alpha \log\log p + O(1).$$

Since α is arbitrary, the result now follows. □

5. Index of some subfields of cyclotomic fields

We recall that the index $I(\mathbf{K})$ of an algebraic number field $\mathbf{K}$ is the greatest common divisor of indexes $[\mathcal{O}_{\mathbf{K}} : \mathbf{Z}[\xi]]$ taken over all $\xi \in \mathcal{O}_{\mathbf{K}}$, where $\mathcal{O}_{\mathbf{K}}$ is the ring of integers of $\mathbf{K}$.

As in [8], we denote by I_p the index of the field $\mathbf{K}_p$, which is the unique cyclic extension of degree p over $\mathbf{Q}$ that is contained in the cyclotomic field $\mathbf{Q}(\exp(2\pi i/p^2))$.

It has been shown in [8, Proposition 4 (i)] that under the Generalised Riemann Hypothesis the bound

$$\log I_p \le (1 + o(1)) p^2 \log\log p \tag{11}$$

holds as $p \to \infty$. Also [8, Proposition 5] gives an unconditional but weaker bound

$$\log I_p \le (1/4 + o(1)) p^2 \log p.$$

We use Corollary 13 to obtain an unconditional improvement of (11).

Theorem 14. *We have*

$$\log I_p \le \left(\frac{463}{504} + o(1)\right) p^2 \log\log p$$

as $p \to \infty$.

Proof. By [8, Equation (2.4.1)] we have

$$\log I_p = \sum_{n \in \mathcal{Q}_p(p)} \alpha_p(n) \Lambda(n), \tag{12}$$

where

$$\alpha_p(n) = \left\lfloor \frac{p}{n} \right\rfloor \left(p - \frac{1}{2}n - \frac{1}{2}\left\lfloor \frac{p}{n} \right\rfloor n \right).$$

Since

$$\alpha_p(n) = \left\lfloor \frac{p}{n} \right\rfloor \left(p - \frac{1}{2}n\left(1 + \left\lfloor \frac{p}{n} \right\rfloor\right)\right) \le \left\lfloor \frac{p}{n} \right\rfloor \frac{p}{2} \le \frac{p^2}{2n},$$

we see from (12) that

$$\log I_p \le \frac{p^2}{2} S_p.$$

Using Corollary 13, we conclude the proof. □

One certainly expects that I_p is much smaller than the bound given in Theorem 14, however no unconditional lower bound seems to be known. However, Ihara [8, Proposition 4 (ii)] gives a conditional lower bound of the type

$$\log I_p \gg p^{3/2},$$

with an explicit value of the implied constant.

Acknowledgement. The author is very grateful to Andrew Granville, Yasutaka Ihara, Sergei Konyagin and Arne Winterhof for their comments.

During the preparation of this work the author was supported in part by the Australian Research Council Grant DP1092835.

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] R. Ernvall and T. Metsänkylä, On the p-divisibility of Fermat quotients, Math. Comp. **66** (1997), 1353–1365.

[3] W. L. Fouché, On the Kummer-Mirimanoff congruences, Quart. J. Math. Oxford **37** (1986), 257–261.

[4] A. Granville, Diophantine equations with varying exponents, PhD Thesis, Queenís University, Kingston, Ontario, Canada, 1987.

[5] A. Granville, Some conjectures related to Fermat's last theorem, Number theory, Walter de Gruyter, NY, 1990, 177–192.

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

[7] D. R. Heath-Brown and S. V. Konyagin, New bounds for Gauss sums derived from kth powers, and for Heilbronn's exponential sum, Quart. J. Math. **51** (2000), 221–235.

[8] Y. Ihara, On the Euler-Kronecker constants of global fields and primes with small norms, Algebraic geometry and number theory, Progress in math. **850**, Birkhäuser, Boston, Cambridge, MA, 2006, 407–451.

[9] H. Iwaniec and E. Kowalski, Analytic number theory, Amer. Math. Soc., Providence, RI, 2004.

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

[11] Y. V. Malykhin, Bounds for exponential sums modulo p^2, J. Math. Sci. **116** (2006), 5686–5696 (translated from Fundame. Prikl. Matem. **11**(6) (2005), 81–94).

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

[13] L. P. Usol'tsev, On an estimate for a multiplicative function, Additive problems in number theory, Kuybyshev. Gos. Ped. Inst., Kuybyshev, 1985, 34–37 (in Russian).

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