PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 140, Number 4, April 2012, Pages 1199–1206
S 0002-9939(2011)11203-6
Article electronically published on August 2, 2011

ON THE VALUE SET OF FERMAT QUOTIENTS

IGOR E. SHPARLINSKI

(Communicated by Matthew A. Papanikolas)

ABSTRACT. We obtain an upper bound $p^{463/252+o(1)}$ on the smallest L such that the set of the first L Fermat quotients modulo a prime p represents all residues modulo p.

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

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

We also define

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

Fermat quotients appear and play a major role in various questions of computational and algebraic number theory and thus their distribution modulo p has been studied in a number of works; see, for example, [1, 5, 6, 7, 8, 9, 10, 11, 13, 15, 16, 17, 18] and the references therein. In particular, the image set

$$\mathcal{I}_p(U) = \{q_p(u) \ : \ 1 \le u \le U\}$$

has been investigated in some of these works.

Let $I_p(U) = \#\mathcal{I}_p(U)$ be the cardinality of $\mathcal{I}_p(U)$. It is well known (see, for example, [6, Section 2]) that

$$I_p(p^2) = p, \tag{1}$$

which follows immediately from the congruence (4) below.

The case of $U = p$ is of special interest too. Vandiver [19] (see also [6, Section 3]) has shown that

$$\sqrt{p} - 1 \le I_p(p) \le p - \sqrt{(p-1)/2}. \tag{2}$$

The above lower bound has been improved in [16, Theorem 3.8] as

$$I_p(p) \ge (1+o(1))\frac{p}{(\log p)^2},$$

as $p \to \infty$.

It is also well known that the p-divisibility of Fermat quotients $q_p(a)$ by p is important for many applications and, in particular, the smallest value ℓ_p of $u \ge 1$

Received by the editors December 20, 2010 and, in revised form, January 2, 2011.
2000 *Mathematics Subject Classification.* Primary 11A07, 11L07.
Key words and phrases. Fermat quotients, value set, preimage.

with $q_p(u) \neq 0$, has been studied in a number of works; see [1, 6, 7, 9, 15]. Improving the previous estimate $\ell_p = O\left((\log p)^2\right)$ of Lenstra [15] (see also [7, 10, 13]) the bounds

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

(where almost all p means for all p but a set of relative density zero) have been given in [1].

Since $\mathcal{I}_p(1) = \{0\}$, one can define ℓ_p as the smallest L with $I_p(L) > 1$.

Here we study $I_p(L)$ at the other end of the spectrum and define L_p as the smallest L for which $I_p(L) = p$. We see from (2) that

$$L_p > p.$$

Here we obtain an upper bound on L_p.

In fact we estimate a more general quantity

$$\Lambda_p = \min\{L \ : \ \forall K \in \mathbb{Z} \text{ we have } \#\{q_p(K+1), \ldots, q_p(K+L)\} = p\}$$

and improve the trivial bound $\Lambda_p \le p^2$.

Theorem 1. *We have*

$$\Lambda_p \le p^{463/252+o(1)}$$

as $p \to \infty$.

Our proof is based on a combination of several results from [2, 4] on the distribution of elements of a multiplicative subgroup of the unit groups of a residue ring and with bounds on the Heilbronn exponential sums of Heath-Brown and Konyagin [12].

We also supplement it by the estimate on L such that almost all residues modulo p appear among $q_p(1), \ldots, q_p(L)$.

Theorem 2. *For any real function* $\psi(z) \to \infty$ *as* $z \to \infty$, *for* $M_p = \left\lfloor p^{3/2}\psi(p) \right\rfloor$ *we have*

$$I(M_p) = (1 + o(1))p$$

as $p \to \infty$.

2. Preparations

2.1. **General notation.** Throughout the paper, p always denotes a prime number, while k, m and n (in both the upper and lower cases) denote positive integer numbers.

We use $\mathbb{Z}_m^*$ to denote the unit group of the residue ring $\mathbb{Z}_m$ modulo m.

For a complex z, we put

$$\mathbf{e}_m(z) = \exp(2\pi i z/m).$$

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

2.2. **Basic properties of Fermat quotients.** Most of our results are based on the following two well-known properties of Fermat quotients.

For any integers k, u and v with $\gcd(uv, p) = 1$ we have

$$q_p(uv) \equiv q_p(u) + q_p(v) \pmod{p} \tag{3}$$

and

$$q_p(u + kp) \equiv q_p(u) - ku^{-1} \pmod{p}; \tag{4}$$

see, for example, [6, Equations (2) and (3)].

Let $\mathcal{G}_p$ be the group of the pth power residues modulo p^2. The congruence (3) immediately implies:

Lemma 3. *For any $u \in \mathbb{Z}$ and $w \in \mathcal{G}_p$ we have*

$$q_p(u) = q_p(uw).$$

2.3. **Gaps between the elements of multiplicative subgroups of residue rings.** Let $\mathcal{G}$ be a multiplicative subgroup of $\mathbb{Z}_m^*$.

For $\eta \in \mathbb{Z}_m^*$, we denote by $\Delta_m(\eta, \mathcal{G})$ the largest gap between the elements of the conjugacy class $\eta\mathcal{G}$, that is,

$$\Delta_m(\eta, \mathcal{G}) \quad = \quad \max\{H \ : \ \exists\, J \in \mathbb{Z}_m \text{ such that } J + j \notin \eta\mathcal{G},\ j = 1, \ldots, H\}.$$

Furthermore, for $\lambda \in \mathbb{Z}_m$ we use $M_m(\lambda, \mathcal{G}, Z)$ to denote the number of solutions to the congruence

$$\lambda \equiv zu \pmod{m}, \qquad 1 \le |z| \le Z,\ u \in \mathcal{G}.$$

(Note that λ need not be coprime to m, so that the translated subgroup $\lambda\mathcal{G}$ need not be a coset in $\mathbb{Z}_m^*$.)

Also, we define the exponential sums

$$S_m(\lambda, \mathcal{G}) = \sum_{v \in \mathcal{G}} \mathbf{e}_m(\lambda v).$$

We need the following analogue of [14, Lemma 7.1], which is given by [4, Lemma 2], that relates $\Delta_m(\eta, \mathcal{G})$ with $M_m(\lambda, \mathcal{G}, Z)$ and $S_m(\lambda, \mathcal{G})$. We note that in [4, Lemma 2] only the case $\eta = 1$ is considered, but in the case of arbitrary $\eta \in \mathbb{Z}_m^*$ the proof is identical.

Lemma 4. *Assume that $\mathcal{G}$ is of order t and that for some positive integer $Z \le m/2$ we have*

$$\sum_{\lambda \in \mathbb{Z}_m} M_m(\lambda, \mathcal{G}, Z)\, |S_m(\eta\lambda, \mathcal{G})| \le 0.5t^2.$$

Then, as $m \to \infty$,

$$\Delta_m(\eta, \mathcal{G}) \le m^{1+o(1)} Z^{-1}.$$

Also, for a real Z, let $N_m(\mathcal{G}, Z)$ be the number of solutions to the congruence

$$ux \equiv y \pmod{m}, \qquad \text{where } 0 < |x|, |y| \le Z,\ u \in \mathcal{G}.$$

We now recall [2, Theorem 1], which gives an upper bound on $N_m(\mathcal{G}, Z)$. We note that the proof given in [2] works only for $Z \ge m^{1/2}$ (which is always satisfied in the present paper); however, it is shown in [3] that the result holds without this condition too, exactly as it is formulated in [2].

Lemma 5. *Let $\nu \ge 1$ be a fixed integer and let $m \to \infty$. Assume $\#\mathcal{G} = t \gg \sqrt{m}$. Then for any positive number Z we have*

$$N_m(\mathcal{G}, Z) \le Zt^{(2\nu+1)/2\nu(\nu+1)} m^{-1/2(\nu+1)+o(1)} + Z^2 t^{1/\nu} m^{-1/\nu+o(1)}.$$

2.4. **Heilbronn sums.** Now, for a prime p and an integer λ, we define the *Heilbronn sum*

$$H_p(\lambda) = \sum_{b=1}^{p-1} \mathbf{e}_{p^2}(\lambda b^p)$$

(we note that for our purpose it is more convenient not to include $b = 0$ in the summation range). We recall the following estimate due to Heath-Brown and Konyagin [12, Theorem 2].

Lemma 6. *Uniformly over all $s \not\equiv 0 \mod p$, we have*

$$\sum_{r=1}^{p} |H_p(s + rp)|^4 \ll p^{7/2}.$$

Since $H_p(rp) = 0$ if $r \not\equiv 0 \mod p$ and $H_p(rp) = p$ if $r \equiv 0 \mod p$, we immediately derive from Lemma 6 that

$$\sum_{u=1}^{p^2} |H_p(u)|^4 \ll p^{9/2}. \tag{5}$$

3. Proof of Theorem 1

Clearly for every $g \in \mathcal{G}_p$ there is $\eta \in \mathbb{Z}_{p^2}^*$ such that the smallest positive residue modulo p^2 of ηg belongs to the interval $[1, H]$, where H is the maximum gap between the residues modulo p^2 of the conjugacy class $\eta\mathcal{G}_p$. Therefore, it follows from (1) and Lemma 3 that

$$\Lambda_p \le \max_{\eta \in \mathbb{Z}_{p^2}^*} \Delta_{p^2}(\eta, \mathcal{G}_p) + 1. \tag{6}$$

We now fix a sufficiently small $\varepsilon > 0$ and put

$$Z = \left\lfloor p^{41/252-\varepsilon} \right\rfloor.$$

By Lemma 4 we see from (6) that it is enough to show that for any ε and the above choice of Z, we have

$$\sum_{\lambda \in \mathbb{Z}_{p^2}} M_{p^2}(\lambda, \mathcal{G}_p, Z)\, |H_p(\eta\lambda)| \le 0.5(p-1)^2 \tag{7}$$

for every $\eta \in \mathbb{Z}_{p^2}^*$, where, as before, $\mathcal{G}_p$ denotes the group of the pth power residues modulo p^2.

Writing

$$\sum_{\lambda \in \mathbb{Z}_{p^2}} M_{p^2}(\lambda, \mathcal{G}_p, Z)\, |H_p(\eta\lambda)|$$

$$= \sum_{\lambda \in \mathbb{Z}_{p^2}} M_{p^2}(\lambda, \mathcal{G}_p, Z)^{1/2} \left(M_{p^2}(\lambda, \mathcal{G}_p, Z)^2\right)^{1/4} \left(|H_p(\eta\lambda)|^4\right)^{1/4},$$

by the Hölder inequality, and using that $\eta \in \mathbb{Z}_{p^2}^*$, we obtain

$$\begin{aligned}(8)\qquad &\left(\sum_{\lambda\in\mathbb{Z}_{p^2}} M_{p^2}(\lambda,\mathcal{G}_p,Z)\,|H_p(\eta\lambda)|\right)^4\\ &\qquad\le \left(\sum_{\lambda\in\mathbb{Z}_{p^2}} M_{p^2}(\lambda,\mathcal{G}_p,Z)\right)^2 \sum_{\lambda\in\mathbb{Z}_{p^2}} M_{p^2}(\lambda,\mathcal{G}_p,Z)^2 \sum_{\lambda\in\mathbb{Z}_{p^2}} |H_p(\lambda)|^4.\end{aligned}$$

Trivially, we have

$$\sum_{\lambda\in\mathbb{Z}_{p^2}} M_{p^2}(\lambda,\mathcal{G}_p,Z) \le 2Z(p-1). \tag{9}$$

We also see that

$$\sum_{\lambda\in\mathbb{Z}_{p^2}} M_{p^2}(\lambda,\mathcal{G}_p,Z)^2 = (p-1)N_{p^2}(\mathcal{G}_p,Z).$$

Hence, Lemma 5 applied with $\nu = 6$ immediately leads to the estimate

$$N_{p^2}(\mathcal{G}_p,Z) \le Zp^{13/84}(p^2)^{-1/14+o(1)} + Z^2p^{1/6}(p^2)^{-1/6+o(1)} = Zp^{1/84+o(1)}$$

(since for $Z \le p^{41/252}$ the first term dominates). Therefore

$$\sum_{\lambda\in\mathbb{Z}_{p^2}} M_{p^2}(\lambda,\mathcal{G}_p,Z)^2 \ll Zp^{85/84+o(1)}. \tag{10}$$

Substituting (5), (9) and (10) in (8), we deduce that

$$\begin{aligned}\sum_{\lambda\in\mathbb{Z}_{p^2}} M_{p^2}(\lambda,\mathcal{G}_p,Z)\,|H_p(\eta\lambda)| &\ll (Zp)^{1/2}\left(Zp^{85/84+o(1)}\right)^{1/4}(p^{9/2})^{1/4}\\ &\ll Z^{3/4}p^{631/336+o(1)} = o(p^2).\end{aligned}$$

Therefore (7) holds provided that p is large enough, which concludes the proof.

4. Proof of Theorem 2

Let $T(K,a)$ denote the number of solutions to the equation

$$q_p(u+(k_1+k_2)p) = a, \qquad 1 \le u \le p-1,\ 0 \le k_1,k_2 \le K-1.$$

For an integer a with $0 \le a < p$, we have

$$T(K,a) = \sum_{u=1}^{p-1}\sum_{k_1,k_2=0}^{K-1} \frac{1}{p}\sum_{\lambda=0}^{p-1} \mathbf{e}_p\left(\lambda\left(q_p\left(u+(k_1+k_2)p\right)-a\right)\right).$$

Changing the order of summation, separating the term $(p-1)K^2/p$ corresponding to $\lambda = 0$ and using (4), we write

$$\begin{aligned} T(K,a) - \frac{(p-1)K^2}{p} &= \frac{1}{p}\sum_{\lambda=1}^{p-1} \mathbf{e}_p(-\lambda a) \sum_{u=1}^{p-1} \mathbf{e}_p(\lambda q_p(u)) \\ &\qquad \times \sum_{k_1,k_2=0}^{K-1} \mathbf{e}_p(-\lambda(k_1+k_2)u^{-1}) \\ &= \frac{1}{p}\sum_{\lambda=1}^{p-1} \mathbf{e}_p(-\lambda a)\sigma(\lambda), \end{aligned}$$

where

$$\sigma(\lambda) = \sum_{u=1}^{p-1} \mathbf{e}_p(\lambda q_p(u)) \left(\sum_{k=0}^{K-1} \mathbf{e}_p(-\lambda k u^{-1})\right)^2.$$

Clearly, if $\gcd(\lambda, p) = 1$, then

$$|\sigma(\lambda)| \le \sum_{u=1}^{p-1} \left|\sum_{k=0}^{K-1} \mathbf{e}_p(\lambda k u^{-1})\right|^2 \le \sum_{v=0}^{p-1} \left|\sum_{k=0}^{K-1} \mathbf{e}_p(kv)\right|^2 = pK. \tag{11}$$

Furthermore,

$$\begin{aligned} \sum_{a=0}^{p-1} \left(T(K,a) - \frac{(p-1)K^2}{p}\right)^2 &= \frac{1}{p^2}\sum_{a=0}^{p-1} \sum_{\lambda_1,\lambda_2=1}^{p-1} \mathbf{e}_p(-(\lambda_1+\lambda_2)a)\sigma(\lambda_1)\sigma(\lambda_2) \\ &= \frac{1}{p^2}\sum_{\lambda_1,\lambda_2=1}^{p-1} \sum_{a=0}^{p-1} \mathbf{e}_p(-(\lambda_1+\lambda_2)a)\sigma(\lambda_1)\sigma(\lambda_2). \end{aligned}$$

Clearly,

$$\sum_{a=0}^{p-1} \mathbf{e}_p(-(\lambda_1+\lambda_2)a) = 0$$

unless $\lambda_1 \equiv -\lambda_2 \pmod p$, in which case it is equal to p. Hence,

$$\sum_{a=0}^{p-1} \left(T(K,a) - \frac{(p-1)K^2}{p}\right)^2 = \frac{1}{p}\sum_{\lambda=1}^{p-1} \sigma(\lambda)\sigma(-\lambda) = \frac{1}{p}\sum_{\lambda=1}^{p-1} |\sigma(\lambda)|^2.$$

Using (11), we derive

$$\sum_{a=0}^{p-1} \left(T(K,a) - \frac{(p-1)K^2}{p}\right)^2 < p^2K^2.$$

Therefore $T(K,a) = 0$ for at most $p^4(p-1)^{-2}K^{-2}$ values of $a = 0, \ldots, p-1$. Taking $K = \lfloor 0.5p^{1/2}\psi(p) \rfloor$ and using the inequality

$$M_p \le 2(K-1)p + p - 1,$$

we conclude the proof.

5. Comments

We remark that the bound of Theorem 1 resembles the bound $p^{463/504+o(1)}$ of [2, Theorem 7] on the largest gap between the elements of a conjugacy class of a subgroup $\mathcal{G}$ of $\mathbb{Z}_p^*$ of order $\#\mathcal{G} > p^{1/2}$. Indeed the proofs and results are quite similar, but they are based on somewhat different technical tools (on the bound on the average values of Heilbronn and Gauss sums, respectively). It is not clear whether they can be merged in a more general result which contains them as special cases.

Acknowledgement

The author is grateful to 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. MR2677624

[2] J. Bourgain, S. V. Konyagin and I. E. Shparlinski, 'Product sets of rationals, multiplicative translates of subgroups in residue rings and fixed points of the discrete logarithm', *Intern. Math. Research Notices*, **2008** (2008), Article ID rnn090, 1–29. MR2439546 (2009i:11007)

[3] J. Bourgain, S. V. Konyagin and I. E. Shparlinski, 'Corrigenda to: Product sets of rationals, multiplicative translates of subgroups in residue rings and fixed points of the discrete logarithm', *Intern. Math. Research Notices*, **2009** (2009), 3146-3147. MR2533800 (2010i:11006)

[4] J. Bourgain, S. Konyagin, C. Pomerance and I. E. Shparlinski, 'On the smallest pseudopower', *Acta Arith.*, **140** (2009), 43–55. MR2557852 (2010j:11127)

[5] Z. Chen, A. Ostafe and A. Winterhof, 'Structure of pseudorandom numbers derived from Fermat quotients', *Proc. Intern. Workshop on the Arith. of Finite Fields, Istanbul, 2010*. Lect. Notes in Comp. Sci., vol. 6087, Springer-Verlag, Berlin, 2010, 73–85.

[6] R. Ernvall and T. Metsänkylä, 'On the p-divisibility of Fermat quotients', *Math. Comp.*, **66** (1997), 1353–1365. MR1408373 (97i:11003)

[7] W. L. Fouché, 'On the Kummer-Mirimanoff congruences', *Quart. J. Math. Oxford*, **37** (1986), 257–261. MR854625 (88a:11022)

[8] D. Gomez and A. Winterhof, 'Multiplicative character sums of Fermat quotients and pseudorandom sequences', *Period. Math. Hungarica* (to appear).

[9] A. Granville, 'Some conjectures related to Fermat's Last Theorem', *Number Theory*, de Gruyter, New York, 1990, 177–192. MR1106660 (92k:11036)

[10] A. Granville, 'On pairs of coprime integers with no large prime factors', *Expos. Math.*, **9** (1991), 335–350. MR1137813 (92m:11095)

[11] D. R. Heath-Brown, 'An estimate for Heilbronn's exponential sum', *Analytic Number Theory: Proc. Conf. in Honor of Heini Halberstam*, Birkhäuser, Boston, 1996, 451–463. MR1409372 (97k:11120)

[12] 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. MR1765792 (2001h:11106)

[13] Y. Ihara, 'On the Euler-Kronecker constants of global fields and primes with small norms', *Algebraic Geometry and Number Theory*, Progress in Math., Vol. 253, Birkhäuser Boston, Boston, MA, 2006, 407–451. MR2263195 (2007h:11127)

[14] S. V. Konyagin and I. E. Shparlinski, *Character sums with exponential functions and their applications*, Cambridge Univ. Press, Cambridge, UK, 1999. MR1725241 (2000h:11089)

[15] H. W. Lenstra, 'Miller's primality test', *Inform. Process. Lett.*, **8** (1979), 86–88. MR520273 (80c:10008)

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

[17] I. E. Shparlinski, 'Character sums with Fermat quotients', *Quart. J. Math.* (to appear).
[18] I. E. Shparlinski, 'Bounds of multiplicative character sums with Fermat quotients of primes', *Bull. Aust. Math. Soc.* **83** (2011), 456–462.
[19] H. S. Vandiver, 'An aspect of the linear congruence with applications to the theory of Fermat's quotient', *Bull. Amer. Math. Soc.*, **22** (1915), 61–67. MR1559712

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