ACTA ARITHMETICA
152.1 (2012)

Short character sums with Fermat quotients

by

Mei-Chu Chang (Riverside, CA)

0. Introduction. Let p be a prime and u an integer coprime with p. The *Fermat quotient* $q_p(u)$ is the unique integer satisfying

$$(0.1)\qquad q_p(u) \equiv \frac{u^{p-1}-1}{p} \bmod p \quad \text{and} \quad 0 \le q_p(u) \le p-1.$$

If $p \mid u$, we set $q_p(u) = 0$.

The distribution of Fermat quotients and related sequences is interesting from several perspectives. First, there are several applications, in particular to algebraic number theory and computer science. Fermat quotients play for instance a role in primality testing (see [L]) and are well-studied as model for generating pseudo-random numbers (see [COW]). On the analytical side, establishing discrepancy bounds for those sequences relies on the theory of exponential sums. Those methods provide nontrivial results, but there is nevertheless often a large gap between what can be proven and the conjectured truth. Some other papers related to Fermat quotients are [S3], [S4] and [S5].

Exponential sum estimates for partial sequences $q_p(u)$, $u = n+1, \dots, n+N$, appear in the work of Heath-Brown [Hb]. Our interest in the present paper is in incomplete character sums, following up on the paper [S1]. More precisely, we obtain nontrivial estimates on sums of the type

$$\sum_{u=1}^{N} \chi(q_p(u)) \qquad \text{(Theorem 3.1)},$$

$$\sum_{u=1}^{N} \chi(uq_p(u)) \qquad \text{(Theorem 3.2)}$$

2010 *Mathematics Subject Classification*: Primary 11L40, 11L26; Secondary 11A07, 11B75.
Key words and phrases: character sums, Fermat quotients.

DOI: 10.4064/aa152-1-3

for $N > p^{1+\delta}$ ($\delta > 0$ arbitrary) and also for sums over primes

$$\sum_{\substack{l\le N\\ l\,\text{prime}}} \chi(q_p(l)) \qquad \text{(Theorem 4.1)}$$

for $N > p^{3/2+\delta}$.

Thus the restriction on N is weaker than those imposed in [S1]. Our results contribute to some of the problems put forward in [S2].

For shorter range ($N > p^{3/4+\delta}$), we have the following result (the saving on the bound is only logarithmic):

$$\Big|\sum_{u\le N} \chi(q_p(u))\Big| \lesssim_\delta N(\log N)^{-1+\epsilon} \qquad \text{(Theorem 5.1).}$$

With respect to Theorems 3.1 and 3.2, the statements remain valid for general intervals $[M, M+N]$ as in [S1].

The method is based on a new result on the distribution (mod$p$) of the sequence $uq_p(u)$ for $u = 1, \dots, p$ (see Proposition 2.1), which is another issue brought up in [S1]. Its proof relies on the Heilbronn exponential sum bound from [Hb] and [HBK], which is combined with combinatorial estimates from [BKS].

1. Preliminaries

Theorem 1.1 ([BKS]). *Let G be a multiplicative subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$. For $T \in \mathbb{Z}_+$, denote*

$$N(n,G,T) = |\{(x,y) : 0 < |x|, |y| < T,\ xy^{-1} \in G\}|.$$

Then for $t = \max\{|G|, \sqrt{n}\}$ and T arbitrary, we have

$$N(n,G,T) < c_{v,\epsilon}\{Tt^{(2v+1)/(2v(v+1))}n^{-1/(2(v+1))+\epsilon} + T^2\, t^{1/v}n^{-1/v+\epsilon}\}, \tag{1.1}$$

where v is an arbitrary integer.

Theorem 1.2 ([HBK]). *Let $G < (\mathbb{Z}/p^2\mathbb{Z})^*$ be the subgroup of p-powers, i.e.*

$$G = \{x^p \bmod p^2 : (x,p) = 1\},$$

and let 1_G be the indicator function of G. Then

$$\sum_{1\le x\le p^2} |\widehat{1}_G(x)|^4 \ll p^{9/2}. \tag{1.2}$$

Remark 1.2.1. The subgroup G in Theorem 1.2 has the following properties:

(i) $|G| = p - 1$.

(ii) There is a one-to-one correspondence between $\{1, \dots, p-1\}$ and G by sending x to x^p.

FACT 1.3. Note that

$$q_p(xy) = q_p(x) + q_p(y). \tag{1.3}$$

For later use, we also specify a bilinear character sum estimate. The result is well-known. We include the proof here, since there is a need to specify the role of small parameters in the final estimate.

THEOREM 1.4. *Let η_1, η_2 be functions defined on $\mathbb{Z}/p\mathbb{Z}$ such that*

$$\sum_{x=1}^{p} |\eta_i(x)| \le 1 \quad \textit{for } i = 1, 2, \tag{1.4}$$

$$\sum_{x=1}^{p} |\eta_1(x)|^2 < p^{-1/2-\delta_1}, \tag{1.5}$$

$$\|\eta_2\|_\infty < p^{-\delta_2} \tag{1.6}$$

for some $\delta_1, \delta_2 > 0$. Let χ be a nontrivial multiplicative character modulo p. Then

$$\Big|\sum_{x_1,x_2} \eta_1(x_1)\eta_2(x_2)\chi(x_1+x_2)\Big| < c\delta_2^{-1} p^{-\delta_1\delta_2/2}, \tag{1.7}$$

where c is a constant.

Proof. Using the high moment method originating from Burgess' work ([Bu]), we let $r \in \mathbb{Z}_+$ (to be specified) and estimate the left hand side of (1.7) by

$$\begin{aligned} &\sum_{x_1=1}^{p} |\eta_1(x_1)| \Big|\sum_{x_2} \eta_2(x_2)\chi(x_1+x_2)\Big| \\ &\le \Big[\sum_{x_1=1}^{p} |\eta_1(x_1)|^{2r/(2r-1)}\Big]^{1-1/2r} \Big[\sum_{x_1=1}^{p} \Big|\sum_{x_2} \eta_2(x_2)\chi(x_1+x_2)\Big|^{2r}\Big]^{1/2r} \\ &\le \Big[\sum_{x_1=1}^{p} |\eta_1(x_1)|\Big]^{1-1/r} \Big[\sum_{x_1=1}^{p} |\eta_1(x_1)|^2\Big]^{1/2r} M^{1/2r} < p^{(1/2+\delta_1)/2r} M^{1/2r}, \end{aligned} \tag{1.8}$$

where we used Hölder's inequality, (1.4) and (1.5), and defined

$$M = \sum_{x=1}^{p} \Big|\sum_{y} \eta_2(y)\chi(x+y)\Big|^{2r}.$$

Then

$$\begin{aligned} M &< cr\sqrt{p}\Big(\sum |\eta_2(y)|\Big)^{2r} + p\binom{2r}{r} r^r \Big(\sum |\eta_2(y)|\Big)^{r} \|\eta_2\|_\infty^r \\ &< cr\sqrt{p} + (4r)^r p^{1-r\delta_2}, \end{aligned} \tag{1.9}$$

where the first term comes from an application of Weil's character sum bound to polynomials $(x+y_1)\cdots(x+y_r)(x+y_{r+1})^{p-2}\cdots(x+y_{2r})^{p-2}$ with at least one single root, and the second term from the remaining contributions.

Substitution of (1.9) into (1.8) gives the estimate

$$crp^{(1/2+\delta_1)/2r}(p^{1/4r}+p^{1/2r-\delta_2/2}) < crp^{-\delta_1\delta_2/4} \tag{1.10}$$

by taking $1/\delta_2 < r < 2/\delta_2$. ■

2. A distributional inequality. Our main result is the following.

Proposition 2.1. *For $\xi \in \mathbb{Z}/p\mathbb{Z}$, define*

$$u(\xi) = |\{x \in [1,p] : x^p - x \equiv p\xi \bmod p^2\}|. \tag{2.1}$$

Then, for any $\epsilon > 0$ and any p sufficiently large,

$$\sum_{\xi=1}^{p} u(\xi)^2 < p^{11/8+\epsilon}. \tag{2.2}$$

Proof. It follows from property (ii) in Remark 1.2.1 that

$$u(\xi) = |\{y \in G : y \in p\xi + [1,p-1]\}| \le \sum_{y\in G} K(y-p\xi), \tag{2.3}$$

where we define $K(x) = \phi(x/p)$ for $|x| < \frac{1}{2}p^2$ with ϕ a smooth function such that $\phi(u) = 1$ for $|u| \le 1$ and $\phi(u) = 0$ for $|u| \ge 2$.

Hence

$$|\widehat{K}(\lambda)| < p^{-100} \quad \text{for } \lambda > p^{1+\epsilon}, \tag{2.4}$$

where

$$\widehat{K}(\lambda) = \sum_{x=1}^{p^2} K(x)e_{p^2}(\lambda x).$$

Putting (2.3) and (2.4) together, we have

$$u(\xi) \le \frac{1}{p^2}\sum_{\lambda=1}^{p^2} \widehat{K}(\lambda)e_p(\lambda\xi)\,\widehat{1}_G(-\lambda),$$

and

$$\begin{aligned}
&\sum_{\xi=1}^{p} u(\xi)^2 \\
&\quad\le \frac{1}{p^4}\sum_{\lambda_1,\lambda_2=1}^{p^2} \widehat{K}(\lambda_1)\overline{\widehat{K}(\lambda_2)}\Big[\sum_{\xi=1}^{p} e_p(\xi(\lambda_1-\lambda_2))\Big]\,\widehat{1}_G(-\lambda_1)\,\overline{\widehat{1}_G(-\lambda_2)} \\
&\quad\le \frac{1}{p^3}\sum_{\substack{\lambda_1,\lambda_2=1\\ \lambda_1\equiv\lambda_2 \bmod p}}^{p^2} |\widehat{K}(\lambda_1)|\,|\widehat{K}(\lambda_2)|\,|\widehat{1}_G(-\lambda_1)|\,|\widehat{1}_G(-\lambda_2)|.
\end{aligned} \tag{2.5}$$

Since $|\widehat{K}(\lambda)| \lesssim p$ and (2.4) holds, we have

$$\begin{aligned}(2.6)\qquad \sum_{\xi=1}^{p} u(\xi)^2 &\lesssim \frac{1}{p} \sum_{\substack{|\lambda_i|<p^{1+\epsilon}\\ \lambda_1\equiv\lambda_2 \bmod p}} |\widehat{1}_G(\lambda_1)|\,|\widehat{1}_G(\lambda_2)| \lesssim \frac{p^\epsilon}{p} \sum_{|\lambda|<p^{1+\epsilon}} |\widehat{1}_G(\lambda)|^2 \\ &\lesssim \frac{|G|^2}{p^{1-\epsilon}} + \frac{1}{p^{1-\epsilon}} \sum_{0<|\lambda|<p^{1+\epsilon}} |\widehat{1}_G(\lambda)|^2.\end{aligned}$$

(The second inequality is by Cauchy–Schwarz.)

To bound $\sum_{0<|\lambda|<p^{1+\epsilon}} |\widehat{1}_G(\lambda)|^2$, we will use Theorems 1.1 and 1.2 and an argument from [KS].

First, we note that $\widehat{1}_G(\lambda) = \widehat{1}_G(\lambda x)$ for $x \in G$. Hence

$$\begin{aligned}(2.7)\qquad \sum_{0<|\lambda|<p^{1+\epsilon}} |\widehat{1}_G(\lambda)|^2 &= \frac{1}{p-1} \sum_{\substack{x\in G\\ 0<|\lambda|<p^{1+\epsilon}}} |\widehat{1}_G(x\lambda)|^2 \\ &= \frac{1}{p-1} \sum_{0<j<p^2} c(j)|\widehat{1}_G(j)|^2 \\ &\le \frac{1}{p-1}\Big[\sum c(j)^2\Big]^{1/2}\Big[\sum |\widehat{1}_G(j)|^4\Big]^{1/2} \\ &\ll p^{5/4}\Big[\sum c(j)^2\Big]^{1/2},\end{aligned}$$

where

$$c(j) = |\{(x,\lambda) \in G \times [0 < |\lambda| < p^{1+\epsilon}] : x\lambda \equiv j \bmod p^2\}|.$$

(The first inequality is by Cauchy–Schwarz, and the second inequality by Theorem 1.2.)

Next,

$$\begin{aligned}\sum c(j)^2 &= |\{(x_1,x_2,\lambda_1,\lambda_2) \in G^2 \times [0<|\lambda| < p^{1+\epsilon}]^2 : x_1\lambda_1 = x_2\lambda_2 \bmod p^2\}| \\ &= (p-1)|\{(x,\lambda_1,\lambda_2) \in G \times [0<|\lambda| < p^{1+\epsilon}]^2 : x\lambda_1 = \lambda_2 \bmod p^2\}|.\end{aligned}$$

Applying Theorem 1.1 with $n = p^2$, $T = p^{1+\epsilon}$, $v = 1$, $t = p$, we have

$$(2.8)\qquad \sum c(j)^2 < (p-1)\{p^{1+\epsilon}p^{3/4}p^{-1/2+\epsilon} + p^{2+2\epsilon}pp^{-2+\epsilon}\} < p^{9/4+\epsilon}.$$

Combining (2.6)–(2.8), we get

$$\sum_{\xi=1}^{p} u(\xi)^2 < p^{11/8+2\epsilon}. \ \blacksquare$$

3. Character sums with Fermat quotients

Theorem 3.1. *Let χ be a nontrivial multiplicative character modulo p and $k = p^{1+\delta}$, with $1 \geq \delta > 0$. Then for p sufficiently large,*

$$\Big|\sum_{x=1}^{k} \chi(q_p(x))\Big| < ckp^{-\delta/33}.$$

Proof. For $\gcd(x,p) = 1$, we write

$$x = s + py \quad \text{with } 1 \leq s \leq p-1 \text{ and } y \leq p^{\delta}.$$

Since

$$(s+py)^{p-1} \equiv s^{p-1} + p(p-1)s^{p-2}y \equiv s^{p-1} - ps^{p-2}y \bmod p^2,$$

this gives

$$\text{(3.1)} \quad \Big|\sum_{x=1}^{k} \chi(q_p(x)\Big| = \Big|\sum_{s=1}^{p-1} \sum_{y \leq p^{\delta}} \chi\Big(\frac{s^{p-1}-1}{p} - s^{p-2}y\Big)\Big|$$
$$\leq \sum_{s=1}^{p-1} \Big|\sum_{y \leq p^{\delta}} \chi\Big(\frac{s^p - s}{p} - y\Big)\Big| = \sum_{\xi} u(\xi)\Big|\sum_{y \leq p^{\delta}} \chi(\xi - y)\Big|,$$

where the inequality uses the fact that $s^{p-1} \equiv 1 \bmod p$, and $u(\xi)$ is defined as in Proposition 2.1.

We estimate (3.1) by applying Theorem 1.4, taking

$$\eta_1 = \frac{1}{p}u, \qquad \eta_2 = p^{-\delta} 1_{[0,p^{\delta}]}.$$

Thus, from (2.2) in Proposition 2.1, we may take $\delta_1 = 1/8 - \epsilon$ in (1.5) and deduce from (1.7) that

$$\Big|\sum_{x=1}^{k} \chi(q_p(x))\Big| < c\delta^{-1}p^{1+\delta-\delta\delta_1/4} < ckp^{-\delta/33}$$

as claimed. ∎

The same approach applies to $\sum_{x=1}^{k} \chi((x^p - x)/p)$.

Theorem 3.2. *Let χ be a nontrivial multiplicative character modulo p and $k = p^{1+\delta}$, with $1 \geq \delta > 0$. Then*

$$\Big|\sum_{x=1}^{k} \chi\Big(\frac{x^p - x}{p}\Big)\Big| < ckp^{-\delta/33+\epsilon}.$$

Proof. As in the proof of Theorem 3.1, for $\gcd(x,p) = 1$, we set

$$x = s + py \quad \text{with } 1 \leq s \leq p-1 \text{ and } 0 \leq y \leq p^{\delta}.$$

Then

$$\frac{x^p - x}{p} \equiv \frac{s^p - s}{p} - y \bmod p.$$

We obtain

$$\Big|\sum_{x=1}^{k} \chi\Big(\frac{x^p - x}{p}\Big)\Big| \le \sum_{s=1}^{p-1} \Big|\sum_{y \le p^\delta} \chi\Big(\frac{s^p - s}{p} - y\Big)\Big|.$$

This is (3.1) in the proof of Theorem 3.1. ■

4. Sums over primes. In [S1], Shparlinski also obtained a nontrivial bound on

$$\sum_{\substack{x \le N\\ x \text{ prime}}} \chi(q_p(x)), \tag{4.1}$$

the character sums with Fermat quotients over primes, for $N > p^{3+\epsilon}$. In the next theorem, we improve his result.

THEOREM 4.1. *Assume $N > p^{3/2+\delta}$. Then*

$$\sum_{\substack{x \le N\\ x \text{ prime}}} \chi(q_p(x)) < Np^{-\delta_1}, \tag{4.2}$$

where $\delta_1 \sim \delta$.

REMARK 4.1.1. The analysis in the proof of Theorem 4.1 can be made more precise to give a better dependence of δ_1 on δ but we only want to get a nontrivial bound under the weakest possible assumption on N.

We will use the following lemma.

LEMMA 4.2. *For $1 \ll T$, define*

$$\sigma(z) = |\{x \in [1, T] : q_p(x) = z\}|.$$

Then for $0 < \theta < 1/2$ and p large enough:

(i) *If $p > T > p^\theta$ with $\theta > 0$, then $\sum \sigma(z)^2 < T^{3/2+\epsilon}$.*
(ii) *If $T > p^{3/4+\theta}$ with $1/2 > \theta > 0$, then $\sum \sigma(z)^2 < T^2 p^{-1/2-\theta/2}$.*

Proof. In Theorem 1.1, we take $n = p^2$, $t = p$ and

$$G = \{x^p \bmod p^2 : 1 \le x \le p-1\}.$$

Then

$$N(p^2, G, T) < c_{v,\epsilon}(Tp^{1/(2v(v+1))+\epsilon} + T^2 p^{-1/v+\epsilon}). \tag{4.3}$$

Also,

$$\begin{aligned}\sum_{z<T}\sigma(z)^2 &= |\{(x_1,x_2)\in[1,T]^2 : q_p(x_1)=q_p(x_2)\}|\\ &= |\{(x_1,x_2)\in[1,T]^2 : x_1^{p-1}\equiv x_2^{p-1} \bmod p\}|\\ &= |\{(x_1,x_2)\in[1,T]^2 : x_1\in x_2G\}|\\ &\le N(p^2,G,T).\end{aligned}$$

To prove the lemma, for case (i), in (4.3), we take $v\in\mathbb{Z}_+$ such that $p^{1/(v+1)} < T \lesssim p^{1/v}$. Hence (4.3) is bounded by $T^{1+1/2v+\epsilon} < T^{3/2+\epsilon}$. For case (ii), we take $v=1$ in (4.3). ∎

Proof of Theorem 4.1. We follow the usual procedure, estimating

$$\sum_{n\le N}\Lambda(n)\chi\big(q_p(n)\big) \tag{4.4}$$

using Vaughan's identity (see [IK, Prop. 13.4])

$$\Lambda(n)=\sum_{\substack{b|n\\ b\le y}}\mu(b)\log\frac{n}{b}-\sum\sum_{\substack{bc|n\\ b\le y,\,c\le z}}\mu(b)\Lambda(c)+\sum\sum_{\substack{bc|n\\ b>y,\,c>z}}\mu(b)\Lambda(c). \tag{4.5}$$

Take

$$y=z=2\sqrt{N}$$

so that the last term in (4.5) can be omitted. We obtain

$$\begin{aligned}&\sum_{n\le N}\Lambda(n)\chi\big(q_p(n)\big)\\ &\le\Big|\sum_{\substack{b\le y\\ bd\le N}}\mu(b)\log(d)\chi(q_p(bd))\Big|+\Big|\sum_{\substack{b\le y,\,c\le z\\ bcd\le N}}\mu(b)\Lambda(c)\chi\big(q_p(bcd)\big)\Big|.\end{aligned} \tag{4.6}$$

Using Fact 1.3 and a standard argument (see e.g. Theorem 3.4 in [S1]), we reduce both sums in the right-hand side of (4.6) to bilinear sums of the form

$$\Big|\sum_{\substack{U\le u\le 2U\\ V\le v\le 2V}}\alpha(u)\beta(v)\chi(q_p(u)+q_p(v))\Big| \tag{4.7}$$

with $N\lesssim UV<N$, $N^{1/20}<U\le V$, $\|\alpha\|_\infty$, $\|\beta\|_\infty<p^\epsilon$, and linear sums

$$\Big|\sum_{U\le u\le 2U}\chi\big(q_p(\xi u)\big)\Big| \tag{4.8}$$

with $N^{9/10}<U<N$.

Bounding (4.8) is straightforward. Since $N>p^3/2$ and $U>p^{27/20}>p^{5/4}$, we may use Corollary 3.2 of [S1]. (In fact, the argument used in the proof of Theorem 3.1 may be adapted as well.)

To estimate (4.7), we will use Theorem 1.4 and Lemma 4.2.

Define

$$\eta_1(x) = \frac{1}{V} \sum_{\substack{V \le v \le 2V \\ q_p(v)=x}} \beta(v), \qquad \eta_2(x) = \frac{1}{U} \sum_{\substack{U \le u \le 2U \\ q_p(u)=x}} \alpha(u).$$

Recall that $U > N^{1/20} > p^{3/40}$ and $V \gtrsim N^{1/2} \gtrsim p^{3/4+\delta/2}$.

Clearly, $\sum |\eta_2(x)| \le U^{-1} \sum_{U \le u \le 2U} |\alpha(u)| < p^{\epsilon}$ and similarly for η_1. From Lemma 4.2,

$$\begin{aligned} \|\eta_2\|_\infty^2 \le \sum_x |\eta_2(x)|^2 \le \|\alpha\|_\infty^2 U^{-2} \sum_x |\{U \le u \le 2U : q_p(u) = x\}|^2 \\ < p^{\epsilon} U^{-1/2+\epsilon} < p^{-3/80+\epsilon} < p^{-1/27}, \end{aligned}$$

and

$$\begin{aligned} \sum_x |\eta_1(x)|^2 \le \|\beta\|_\infty^2 \, V^{-2} \sum_x |\{V \le v \le 2V : q_p(v) = x\}|^2 \\ < p^{-1/2-\delta/4+\epsilon} < p^{-1/2-\delta/5}. \end{aligned}$$

We rewrite (4.7) as

$$UV \Big| \sum_{x_1, x_2} \eta_1(x_1) \eta_2(x_2) \chi(x_1 + x_2) \Big|,$$

and use Theorem 1.4 to get the estimate

$$UVp^{-\delta/270} < Np^{-\delta/270}. \ \blacksquare$$

An argument similar to the one above can be used to treat the sums

$$\sum_{\substack{n \le N \\ n \, \text{prime}}} \chi\Big(\frac{n^p - n}{p}\Big)$$

from Problem 46 in [S2].

Theorem 4.3. *Assume $N > p^{3/2+\delta}$. Then there is $\delta' = \delta'(\delta) > 0$ such that*

$$\Big| \sum_{\substack{n \le N \\ n \, \text{prime}}} \chi\Big(\frac{n^p - n}{p}\Big) \Big| < Np^{-\delta'}.$$

Proof. First, we note that

$$\frac{(xy)^p - xy}{p} \equiv xyq_p(xy) \equiv xy(q_p(x) + q_p(y)) \bmod p.$$

Thus, instead of (4.7) and (4.8), we have

$$\Big|\sum_{\substack{U\le u\le 2U\\ V\le v\le 2V}}\alpha(u)\beta(v)\chi(u)\chi(v)\chi(q_p(u)+q_p(v))\Big| \tag{4.9}$$

with $UV\sim N$, $N^{1/20}<U\le V$, $\|\alpha\|_\infty, \|\beta\|_\infty < p^\epsilon$, and

$$\Big|\sum_{U\le u\le 2U}\chi(u)\chi(q_p(\xi u))\Big| \tag{4.10}$$

with $N^{9/10}<U<N$.

For (4.9), we define $\alpha_1(u)=\alpha(u)\chi(u)$ and $\beta_1(v)=\beta(v)\chi(v)$. We obtain the same bound as for (4.7).

Bounding (4.10) amounts to estimating

$$\sum_{x\le X}\chi\bigg(\frac{(\xi x)^p-\xi x}{p}\bigg) \tag{4.11}$$

with ξ fixed, $(\xi,p)=1$ and $X>N^{9/10}>p^{27/20}$. In fact, it suffices to assume $X>p^{1+\delta}$ since the same argument as for Theorem 3.2 is applicable.

Thus, setting

$$x=s+py \quad \text{with } 1\le s\le p-1 \text{ and } 0\le y\le p^\delta,$$

we have

$$\frac{(\xi x)^p-\xi x}{p}\equiv\frac{(\xi s)^p-\xi s}{p}-\xi y \bmod p. \tag{4.12}$$

Following the same argument, we need the analogue of Proposition 2.1 with u on $\mathbb{Z}/p\mathbb{Z}$ defined as

$$u(z)=|\{s\in[1,p-1]:(\xi s)^p-\xi s\equiv p\, z\xi \bmod p^2\}|.$$

Following the proof of Proposition 2.1, we have

$$\begin{aligned}u(z)&=|\{y\in G:\xi^p y\in pz\xi+\xi[1,p-1]\bmod p^2\}|\\ &=|\{y\in G:\xi^{p-1}y\in pz+[1,p-1]\bmod p^2\}|.\end{aligned}$$

Let K be as in the proof of Proposition 2.1. Then

$$u(z)\le\sum_{y\in G}K(\xi^{p-1}y-pz)\le\frac{1}{p^2}\sum_{\lambda=1}^{p^2}\widehat{K}(\lambda)e_p(\lambda z)\,\widehat{1}_G(-\xi^{p-1}\lambda),$$

and

$$\sum_{z=1}^{p}u(z)^2\le\frac{1}{p^3}\sum_{\substack{\lambda_1,\lambda_2=1\\ \lambda_1\equiv\lambda_2 \bmod p}}^{p^2}|\widehat{K}(\lambda_1)|\,|\widehat{K}(\lambda_2)|\,|\widehat{1}_G(-\xi^{p-1}\lambda_1)|\,|\widehat{1}_G(-\xi^{p-1}\lambda_2)|.$$

As for (2.5), we need to estimate

$$\sum_{0<|\lambda|<p^{1+\epsilon}} |\widehat{1}_G(\xi^{p-1}\lambda)|^2 = \frac{1}{p} \sum_{0<t<p^2} c(t)|\widehat{1}_G(t)|^2,$$

where

$$\begin{aligned} c(t) &= |\{(x,\lambda) \in G \times [0<|\lambda|<p^{1+\epsilon}] : x\xi^{p-1}\lambda \equiv t \bmod p^2\}| \\ &= |\{(x,\lambda) \in G \times [0<|\lambda|<p^{1+\epsilon}] : x\lambda \equiv \xi_1^{p-1} t \bmod p^2\}| \end{aligned}$$

with $\xi\xi_1 \equiv 1 \bmod p^2$.

The argument is completed exactly as in Proposition 2.1 and we obtain

$$\sum_{z=1}^{p} u(z)^2 < p^{11/8+\epsilon}. \ \blacksquare$$

5. Shorter ranges. We return to Problem 45 in [S2]. It is in fact possible to obtain a nontrivial bound on

$$\sum_{n\le N} \chi\Big(\frac{n^{p-1}-1}{p}\Big)$$

for N as small as $p^{3/4+\delta}$, but the saving on the bound is only logarithmic.

THEOREM 5.1. *For $N > p^{3/4+\delta}$ with $\delta > 0$, we have*

$$\Big|\sum_{n\le N} \chi\Big(\frac{n^{p-1}-1}{p}\Big)\Big| \lesssim_\delta N(\log N)^{-1+\epsilon}.$$

Proof. We will remove subintervals (where we use the trivial bounds on the character sums) until Lemma 4.2 is applicable.

We fix

$$\delta_1 = (\log p)^{-1+\epsilon}.$$

(Note that $\delta_1 < \delta/10$.) Let

$$V = \{n \in [1,N] : n \text{ has a prime divisor in } [p^{\delta_1}, p^{\delta/2}]\}.$$

To estimate $|[1,N] \setminus V|$, rather than a reference we give the following standard argument.

Defining $X_l = \{n < N : l \mid n\}$, we have

$$[1,N]\setminus V = \bigcap_{\substack{p^{\delta_1}<l<p^{\delta/2} \\ l\,\text{prime}}} ([1,N]\setminus X_l) \subset \bigcap_{\substack{p^{\delta_1}<l<p^{\delta_2} \\ l\,\text{prime}}} ([1,N]\setminus X_l)$$

with $\delta_1 < \delta_2 < \delta/2$ to be specified. Take an even integer r such that $r\delta_2 < 3/4$. From the inclusion-exclusion principle and the Prime Number

Theorem,

$$
\begin{aligned}
(5.1)\quad & |[1,N]\setminus V| \\
&\le N - \sum_{\substack{p^{\delta_1}<l<p^{\delta_2}\\ l\,\text{prime}}} |X_l| + \sum_{\substack{p^{\delta_1}<l_1,l_2<p^{\delta_2}\\ l_i\,\text{prime}}} |X_{l_1l_2}| - \cdots + \sum_{\substack{p^{\delta_1}<l_1,\dots,l_r<p^{\delta_2}\\ l_i\,\text{prime}}} |X_{l_1\cdots l_r}| \\
&\le N - \sum_l \frac{N}{l} + \sum_{l_1,l_2} \frac{N}{l_1l_2} - \cdots + \sum_{l_1,\dots,l_r} \frac{N}{l_1\cdots l_r} + p^{r\delta_2} \\
&\le N \prod_{\substack{p^{\delta_1}<l<p^{\delta_2}\\ l\,\text{prime}}} \left(1-\frac{1}{l}\right) + N\sum_{s>r}\frac{1}{s!}\Bigg(\sum_{\substack{p^{\delta_1}<l<p^{\delta_2}\\ l\,\text{prime}}} \frac{1}{l}\Bigg)^s + p^{r\delta_2} \\
&\lesssim N\frac{\delta_1}{\delta_2} + N\left(\frac{e}{r}\log\frac{\delta_2}{\delta_1}\right)^r,
\end{aligned}
$$

provided $r > \frac{1}{2}\log(\delta_2/\delta_1)$.

We take $r \sim \log(1/\delta_1)$ and $\delta_2 \sim 1/r$. Then (5.1) implies that

$$
(5.2)\qquad |[1,N]\setminus V| \lesssim N\delta_1 \log\frac{1}{\delta_1} < N(\log p)^{-1+\epsilon}.
$$

We will make a further subdivision of V.

Let

$$
\alpha = \delta_1 = (\log p)^{-1+\epsilon}
$$

be a small parameter. We choose j_1, j_2 such that

$$
(5.3)\qquad p^{\delta_1} \sim (1+\alpha)^{j_1}, \quad p^{\delta/2} \sim (1+\alpha)^{j_2}.
$$

Let P_j be the set of primes in $[(1+\alpha)^j, (1+\alpha)^{j+1}]$ and let

$$
(5.4)\qquad V_j = \Big\{ n \in [1,N] : n \text{ has a single prime divisor in } P_j \text{ and no prime divisors in } \bigcup_{i<j} P_i \Big\}.
$$

Clearly, from the definition,

$$
(5.7)\qquad V \setminus \bigcup_{j_1\le j\le j_2} V_j \subset \{n \in [1,N] : n \text{ has two prime divisors in some } P_j,\ j_1 \le j \le j_2\}.
$$

Hence, by the Prime Number Theorem and since $j \le (\log p)/\alpha$,

$$
\begin{aligned}
(5.5)\quad & \Big| V \setminus \bigcup_{j_1\le j\le j_2} V_j \Big| \\
&\le \sum_{j\ge j_1} \Big\{ \sum_{l_1,l_2\in P_j} \frac{N}{l_1l_2} \Big\} \le N \sum_{j\ge j_1} \Big\{ \sum_{l\in P_j} \frac{1}{l} \Big\}^2 \le N \sum_{j\ge j_1} \Big\{ \frac{|P_j|}{(1+\alpha)^j} \Big\}^2
\end{aligned}
$$

$$\le N \sum_{j \ge j_1} \left\{ \frac{1+\alpha}{(1+j)\log(1+\alpha)} - \frac{1}{j\log(1+\alpha)} + O(e^{-\sqrt{\delta_1 \log p}}) \right\}^2$$

$$\lesssim N \sum_{j \ge j_1} \left(\frac{1}{j} + \frac{1}{j^2\alpha} + O(e^{-\sqrt{\delta_1 \log p}}) \right)^2 \lesssim N\left(\frac{1}{j_1} + \frac{\log p}{\alpha} e^{-\sqrt{\delta_1 \log p}} \right)$$

$$\lesssim \frac{N}{j_1} \lesssim \frac{N}{\log p}.$$

Next, denote

$$\Omega_j = \left\{ m \in \left[1, \frac{N}{(1+\alpha)^{j+1}}\right] : m \text{ has no prime divisors in } \bigcup_{i \le j} P_i \right\}.$$

It follows from the definition (5.4) of V_j that

$$P_j \Omega_j \subset V_j \quad \text{and} \quad V_j \setminus (P_j\ \Omega_j) \subset P_j \times \left[\frac{N}{(1+\alpha)^{j+1}}, \frac{N}{(1+\alpha)^j} \right].$$

Hence, using the bound on $|P_j|$ obtained in (5.5), we have

$$|V_j \setminus (P_j\ \Omega_j)| \le |P_j| \frac{N\alpha}{(1+\alpha)^{j+1}} \lesssim N\alpha\left[\frac{1}{j} + O(e^{-\sqrt{\delta_1 \log p}}) \right].$$

Therefore,

$$\sum_{j_1 \le j \le j_2} |V_j \setminus (P_j \Omega_j)| \lesssim N\alpha[\log j_2 + j_2 e^{-\sqrt{\delta_1 \log p}}] \tag{5.6}$$

$$< N\left[\alpha\left(\log\log p + \log\frac{1}{\alpha} \right) + (\log p) e^{-\sqrt{\delta_1 \log p}} \right]$$

$$\lesssim N(\log p)^{-1+2\epsilon}.$$

Note also that from the definition of Ω_j, the product map

$$P_j \times \Omega_j \to P_j \Omega_j$$

is one-to-one and onto.

Combining (5.2), (5.5) and (5.6), we have

$$\Big| \sum_{n \le N} \chi(q_p(n)) \Big| \lesssim N(\log p)^{-1+2\epsilon} + \sum_{j_1 \le j \le j_2} \Big| \sum_{l \in P_j,\, m \in \Omega_j} \chi(q_p(l) + q_p(m)) \Big|. \tag{5.7}$$

For each j, the double sum satisfies

$$\sum_{l \in P_j,\, m \in \Omega_j} \chi(q_p(l) + q_p(m)) = \sum \eta_1(x)\eta_2(y)\chi(x+y) \tag{5.8}$$

with

$$\eta_1(x) = |\{m \in \Omega_j : q_p(m) = x\}| \le |\{m \le N/(1+\alpha)^j : q_p(m) = x\}|,$$

$$\eta_2(y) = |\{l \in P_j : q_p(l) = y\}| \le |\{l \le (1+\alpha)^{j+1} : q_p(l) = y\}|.$$

We will use Lemma 4.2 and Theorem 1.1 to estimate (5.8).

Recall that $p^{\delta_1} \le (1+\alpha)^j \le p^{\delta/2}$. Hence $N/(1+\alpha)^j > p^{3/4+\delta/2}$. By inequality (4.3) (with $v = 1$),

$$\sum \eta_1(x)^2 \le N\left(p^2, G, \frac{N}{(1+\alpha)^j}\right) \le p^\epsilon \left(\frac{N}{(1+\alpha)^j}\right)^2 \left\{\frac{(1+\alpha)^j}{N} p^{1/4} + p^{-1}\right\}$$
$$\le \left(\frac{N}{(1+\alpha)^j}\right)^2 p^{-1/2-\delta/3}.$$

Since Theorem 1.1 as formulated cannot be applied for the very short range $T = (1+\alpha)^{j+1}$, to estimate $\sum \eta_2(y)^2$ we include a separate argument. Clearly,

$$\sum \eta_2(y)^2 = |\{(l_1, l_2) \in P_j \times P_j : l_1 \in l_2 G\}| \le |P_j| \max_l |P_j \cap lG|. \tag{5.9}$$

Take $r \in \mathbb{Z}_+$ such that $T^r < p^2 \le T^{r+1}$. Then the map $\pi_{p^2} : \mathbb{Z} \to \mathbb{Z}/p^2\mathbb{Z}$ when restricted to the r-fold product set $P_j^r \subset \mathbb{Z}$ will be one-to-one. In particular,

$$p - 1 = |G| \ge \frac{1}{r!} |P_j \cap lG|^r,$$

which implies

$$|P_j \cap lG| < rp^{1/r} < rT^{(r+1)/2r} < \frac{1}{\delta_1} T^{2/3}.$$

Hence (5.9) is bounded by

$$c(1+\alpha)^{2j} \log p \, p^{-\delta_1/3} < (1+\alpha)^{2j} p^{-\delta_1/4}, \tag{5.10}$$

from the choice of δ_1.

From Theorem 1.4, we have

$$\Big| \sum_{l \in P_j,\, m \in \Omega_j} \chi(q_p(l) + q_p(m)) \Big| < N p^{-\delta\delta_1/24} < N e^{-c\delta(\log p)^\epsilon}.$$

The theorem follows from (5.7) and (5.10). ■

Acknowledgments. The author would like to thank the referee for many helpful comments. The author would also like to thank the mathematics department of University of California at Berkeley for its hospitality.

This research was partially financed by the National Science Foundation.

References

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

[BKS] 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*, Int. Math. Res. Notices 2008, art. ID rnn 090, 29 pp.

[Bu] D. A. Burgess, *On character sums and primitive roots*, Proc London Math. Soc. (3) 12 (1962), 179–192.

[COW] Z. Chen, A. Ostafe and A. Winterhof, *Structure of pseudorandom numbers derived from Fermat quotients*, in: Lecture Notes in Comput. Sci. 6087, Springer, Berlin, 2010, 73–85.

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

[F] W. L. Fouché, *On the Kummer–Mirimanoff congruences*, Quart. J. Math. Oxford Ser. (2) 37 (1986), 257–261.

[GW] D. Gomez and A. Winterhof, *Multiplicative character sums of Fermat quotients and pseudorandom sequences*, preprint, 2010.

[G1] A. Granville, *Some conjectures related to Fermat's last theorem*, in: Number Theory, de Gruyter, NewYork, 1990, 177–192.

[G2] —, *On pairs of coprime integers with no large prime factors*, Expo. Math. 9 (1991), 335–350.

[Hb] D. R. Heath-Brown, *An estimate for Heilbronn's exponential sum*, in: Analytic Number Theory, Proc. Conf. in Honor of Heini Halberstam, Vol. 2, Birkhäuser, Boston, 1996, 451–463.

[HBK] 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.

[Ih] Y. Ihara, *On the Euler–Kronecker constants of global fields and primes with small norms*, in: Algebraic Geometry and Number Theory, Progr. Math. 253, Birkhäuser, Boston, 2006, 407–451.

[IK] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, Amer. Math. Soc., Providence, RI, 2004.

[KS] S. V. Konyagin and I. E. Shparlinski, *Character Sums with Exponential Functions and Their Applications*, Cambridge Univ. Press, Cambridge, 1999.

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

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

[S1] I. E. Shparlinski, *Character sums with Fermat quotients*, Quart. J. Math., to appear.

[S2] —, *Open problems on exponential and character sums*, in: Number Theory. Dreaming in Dreams (Higashi-Osaka, 2008), World Sci., Hackensack, NJ, 2010, 222–242.

[S3] —, *Fermat quotients: Exponential sums, value set and primitive roots*, Bull. London Math. Soc., to appear.

[S4] —, *On the value set of Fermat quotients*, Proc. Amer. Math. Soc., to appear.

[S5] I. E. Shparlinski, *On vanishing Fermat quotients and a bound of the Ihara sum*, preprint.

Mei-Chu Chang
Department of Mathematics
University of California
Riverside, CA 92521, U.S.A.
E-mail: mcc@math.ucr.edu

Received on 6.1.2011
and in revised form on 27.7.2011 (6597)