SHORT CHARACTER SUMS WITH FERMAT QUOTIENTS [1] [2]

Mei-Chu Chang[3]

§. Introduction.

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

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

If $p|u$, 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].) From 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.

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

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

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

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

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

---

[1] 2000 *Mathematics Subject Classification.* Primary 11L40, 11L26; Secondary 11A07, 11B75.

[2] *Key words.* character sums, Fermat quotients

[3] Research partially financed by the National Science Foundation.

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

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).

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

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*

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

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

$$N(n, G, T) \le T\, t^{\frac{2v+1}{2v(v+1)}}\, n^{-\frac{1}{2(v+1)}+\epsilon} + T^2\, t^{\frac{1}{v}}\, n^{-\frac{1}{v}+\epsilon}, \qquad (1.1)$$

where v is an arbitrary fixed integer.

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

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

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

$$\sum_{1\le x\le p^2} \big|\widehat{1}_G(x)\big|^4 \ll p^{\,\frac{9}{2}}. \qquad (1.2)$$

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 $\{1, \cdots, p-1\}$ and G by sending x to x^p.

Fact 1.3. Note that

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

§2. A distributional inequality.

Our main result is the following.

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

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

Then

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

Proof. It follows from property (ii) in Remark 1.3, we have

$$\begin{aligned} u(\xi) =& \big|\{y \in G : y \in p\,\xi + [1,p-1]\}\big| \\ \leq& \sum_{y \in G} K(y - p\,\xi), \end{aligned} \tag{2.3}$$

where $K; \mathbb{Z}/p^2\mathbb{Z} \to [0,1]$ is a smooth function mapping $[1,p]$ to the constant 1.

Hence

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

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

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

and

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

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

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

(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 $x \in G$.

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

where

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

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

Next,

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

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

$$\begin{aligned}
\sum c(t)^2 &< p\big\{p^{\,1+\epsilon}p^{\frac{3}{4}}p^{-\frac{1}{2}+\epsilon} + p^{2+2\epsilon}pp^{-2+\epsilon}\big\} \\
&< p^{\frac{9}{4}+\epsilon}
\end{aligned} \tag{2.8}$$

Combining (2.6)-(2.8), we have

$$\sum_{\xi=1}^{p} u(\xi)^2 < p^{\,\frac{11}{8}+2\epsilon}. \qquad \square$$

§3. Character sums with Fermat quotients.

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

$$\Big|\sum_{x=1}^{k} \chi\big(q_p(x)\big)\Big| \lesssim_\delta kp^{-\frac{\delta}{16}+\epsilon}.$$

Proof.

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

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

Since

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

this gives

$$\begin{aligned}
&\Big|\sum_{x=1}^{k}\chi(q_p(x)\Big| \\
=&\Big|\sum_{s=1}^{p-1}\sum_{y\le p^\delta}\chi\Big(\frac{s^{p-1}-1}{p}-s^{p-2}y\Big)\Big| \\
\le&\sum_{s=1}^{p-1}\Big|\sum_{y\le p^\delta}\chi\Big(\frac{s^p-s}{p}-y\Big)\Big| \\
=&\sum_{\xi}u(\xi)\Big|\sum_{y\le p^\delta}\chi(\xi-y)\Big|\,,
\end{aligned} \tag{3.1}$$

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

Take an integer $r\sim\frac{1}{\delta}$. By Hölder inequality and Proposition 2.1, (3.1) is bounded by

$$\begin{aligned}
&\Big[\sum_{\xi}u(\xi)^{\frac{2r}{2r-1}}\Big]^{1-\frac{1}{2r}}\Big[\sum_{\xi=1}^{p}\Big|\sum_{y\le p^\delta}\chi(\xi-y)\Big|^{2r}\Big]^{\frac{1}{2r}} \\
\le&\Big[\sum_{\xi}u(\xi)\Big]^{1-\frac{1}{r}}\Big[\sum_{\xi}u(\xi)^2\Big]^{\frac{1}{2r}}\Big[\sum_{\xi=1}^{p}\Big|\sum_{y\le p^\delta}\chi(\xi-y)\Big|^{2r}\Big]^{\frac{1}{2r}} \\
\le&\, p^{1-\frac{1}{r}}p^{\frac{11}{16r}+\epsilon}\Big[\sum_{\xi=1}^{p}\Big|\sum_{y\le p^\delta}\chi(\xi-y)\Big|^{2r}\Big]^{\frac{1}{2r}}.
\end{aligned}$$

Using Weil's bound for the last factor gives

$$\begin{aligned}
&\Big|\sum_{x=1}^{k}\chi(q_p(x)\Big| \\
\lesssim&\, p^{1-\frac{5}{16r}+\epsilon}\Big\{c(r)p^{\delta\,r}p+p^{2r\delta}c(r)\sqrt{p}\Big\}^{\frac{1}{2r}} \\
\le&\, c(r)p^{1-\frac{5}{16r}+\frac{\delta}{2}+\frac{1}{2r}+\epsilon}+c(r)p^{1-\frac{5}{16r}+\delta+\frac{1}{4r}+\epsilon} \\
=&\, c(r)k\Big\{p^{\frac{3}{16r}-\frac{\delta}{2}+\epsilon}+p^{-\frac{1}{16r}+\epsilon}\Big\} \\
=&\, c(r)kp^{-\frac{\delta}{16}+\epsilon}. \qquad\qquad \square
\end{aligned}$$

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

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

$$\Big|\sum_{x=1}^{k}\chi\Big(\frac{x^p-x}{p}\Big)\Big|\lesssim_\delta\ kp^{-\frac{\delta}{16}+\epsilon}.$$

Proof.

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

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

Then

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

We obtain

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

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

§4. Sums over primes.

In the same paper [S], Shparlinski also obtained nontrivial bound on

$$\sum_{\substack{x\leq N\\ x\ \text{prime}}}\chi\big(q_p(x)\big),$$

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 $N>p^{\frac{3}{2}+\delta}$. Then we have*

$$\sum_{\substack{x\leq N\\ x\ prime}}\chi\big(q_p(x)\big)<Np^{-\delta_1},$$

where $\delta_1=\delta^2/3$.

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 two lemmas.

Lemma 4.2. *Let η_1 and η_2 be functions defined on $\mathbb{Z}/p\mathbb{Z}$ such that*

$$\sum_{x=1}^{p} |\eta_i(x)| \leq 1 \text{ for } i = 1, 2,$$

$$\sum_{x=1}^{p} |\eta_1(x)|^2 < p^{-\frac{1}{2}-\delta}, \tag{4.1}$$

and

$$\|\eta_2\|_\infty < p^{-\delta}, \tag{4.2}$$

for some $\delta > 0$.

Let χ be a nontrivial multiplicative character mod p. Then

$$\Big| \sum \eta_1(x_1)\eta_2(x_2)\chi(x_1 + x_2) \Big| < p^{-\delta_1}$$

for some $\delta_1 > \delta^2/2$.

The proof of Lemma 4.2 is analogous to the argument used to prove Theorem 3.1.

Lemma 4.3. *For $1 \ll T < p$, define*

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

Then

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

(ii). *If $T > p^{3/4+\theta}$ with $\frac{1}{2} > \theta > 0$, 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

$$G = \{x^p \mod p^2 : 1 \leq x \leq p - 1\}.$$

Then

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

Also,

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

To prove the lemma, for Case (i), in (4.3), we take $v \sim \frac{1}{\theta}$. So $T = p^{\frac{1}{v}+\epsilon}$, and (4.3) is bounded by $T^{1+\frac{1}{2(v+1)}} < T^{1+\frac{\theta}{2}}$. For Case (ii), we take $v = 1$ in (4.3). $\square$

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.)

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

Take

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

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

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

Using Fact 1.3 and a standard argument (See e.g. Theorem 3.4 in [S].), we reduce the second sums in (4.6) to bilinear sums of the form

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

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

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

with $N^{1-\tau} < U < N$.

Since $N > p^{\frac{3}{2}+\delta}$, we may use Corollary 3.2 in [S] to bound (4.8). (In fact, the argument used in the proof of Theorem 3.1 may be adapted as well.)

To estimate (4.7), we will use Lemmas 4.2 and 4.3.

Define

$$\eta_1(x) = \frac{1}{V} \sum_{\substack{V \le v \le 2V \\ q_p(v)=x}} \beta(v),$$

and

$$\eta_2(x) = \frac{1}{U} \sum_{\substack{U \le u \le 2U \\ q_p(u)=x}} \alpha(u).$$

Recall that $U > p^\tau$ and $V > N^{\frac{1}{2}-e} > p^{\frac{3}{4}+\frac{\delta}{2}}$.

Clearly, $\sum |\eta_2(x)| \le \frac{1}{U} \sum_{U \le u \le 2U} |\alpha(u)| < p^\epsilon$ and similarly for η_1. Also, from Lemma 4.3,

$$\begin{aligned}
&\|\eta_2\|_\infty^2 \\
&\le \sum_x |\eta_2(x)|^2 \\
&\le \|\alpha\|_\infty^2 \, U^{-2} \sum_x \big|\{U \le u \le 2U : q_p(u) = x\}\big|^2 \\
&< p^\epsilon U^{-1+\frac{\tau}{2}} \\
&< p^{-\frac{\tau}{2}},
\end{aligned}$$

and

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

We rewrite (4.7) as

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

use Lemma 4.2 (replacing δ by $\min(\frac{\delta}{5}, \frac{\tau}{4})$) and get an estimate

$$UVp^{-\delta^2/2} < Np^{-\delta^2/3}. \quad \square$$

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 4.4. *Assume $N > p^{\frac{3}{2}+\delta}$. 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

$$\frac{(xy)^p - xy}{p} \equiv xy\; q_p(xy) \equiv xy\big(q_p(x)+q_p(y)\big) \mod p.$$

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

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

with $N^{1-\epsilon} < UV < N^{1+\epsilon}$, $p^{\tau} < U \le V$, $\|\alpha\|_\infty, \|\beta\|_\infty < p^\epsilon$, and

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

with $N^{1-\tau} < U < N$.

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 estimate

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

with ξ fixed, $(\xi, p) = 1$ and $X > N^{1-\epsilon} > p^{3/2}$. In fact, it suffices to assume $X > p^{1+\delta}$ since the same argument as for Theorem 3.2 is applicable.

Thus, setting

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

we have

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

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

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

Following the proof of Proposition 2.1, we have

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

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

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

and

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

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

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

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

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

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

§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 $\delta_1 < \frac{\delta}{10}$.)

Let

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

Clearly,

$$\begin{aligned} &\Big|[1,N] \setminus V\Big| \\ &\le N \prod_{\substack{p^{\,\delta_1}<\ell<p^{\,\frac{\delta}{2}} \\ \ell \text{ prime}}} \Big(1-\frac{1}{\ell}\Big) \\ &\le N \exp\Big\{ - \sum_{\substack{p^{\,\delta_1}<\ell<p^{\,\frac{\delta}{2}} \\ \ell \text{ prime}}} \frac{1}{\ell}\Big\} \lesssim N\frac{\delta_1}{\delta} \sim N(\log p)^{-1+\epsilon}. \end{aligned} \tag{5.1}$$

(The last inequality follows from Prime Number Theorem.)

We will make a further subdivision of V.

Let

$$\alpha = \delta_1 = (\log p)^{-1+\epsilon} \tag{5.2}$$

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

$$p^{\delta_1} = (1+\alpha)^{j_1}, \quad p^{\frac{\delta}{2}} = (1+\alpha)^{j_2}. \tag{5.3}$$

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

$$\begin{aligned} V_j = \big\{ n \in [1,N] : n \text{ has a single prime divisor in } P_j \\ \text{and no prime divisors in } \bigcup_{i<j} P_i \big\}. \end{aligned} \tag{5.4}$$

Clearly, from the definition,

$$\begin{aligned} & V \setminus \bigcup_{j_1 \le j \le j_2} V_j \\ & \subset \big\{ n \in [1,N] : n \text{ has two prime divisors in some } P_j, j_1 \le j \le j_2 \big\}. \end{aligned}$$

Hence, by Prime Number Theorem and that $j \le \frac{\log p}{\alpha}$,

$$\begin{aligned} & \Big| V \setminus \bigcup_{j_1 \le j \le j_2} V_j \Big| \\ & \le \sum_{j \ge j_1} \Big\{ \sum_{\ell_1,\, \ell_2 \in P_j} \frac{N}{\ell_1 \ell_2} \Big\} \\ & \le N \sum_{j \ge j_1} \Big\{ \sum_{\ell \in P_j} \frac{1}{\ell} \Big\}^2 \\ & \le N \sum_{j \ge j_1} \Big\{ \frac{|P_j|}{(1+\alpha)^j} \Big\}^2 \\ & \le N \sum_{j \ge j_1} \Big\{ \frac{1+\alpha}{(1+j)\log(1+\alpha)} - \frac{1}{j\ \log(1+\alpha)} + O\Big(e^{-\sqrt{\delta_1 \log p}}\Big) \Big\}^2 \\ & \lesssim N \sum_{j \ge j_1} \Big(\frac{1}{j} + \frac{1}{j^2 \alpha} + O\Big(e^{-\sqrt{\delta_1 \log p}}\Big) \Big)^2 \\ & \lesssim N \Big(\frac{1}{j_1} + \frac{\log p}{\alpha}\ e^{-\sqrt{\delta_1 \log p}} \Big) \\ & \lesssim \frac{N}{j_1}. < N (\log p)^{-2+\epsilon}. \end{aligned} \tag{5.5}$$

Next, denote

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

It follows from (5.4), the definition of V_j that

$$P_j \Omega_j \subset V_j$$

and

$$V_j \setminus \big(P_j\ \Omega_j\big) \subset P_j \times \Big[\frac{N}{(1+\alpha)^{j+1}}, \frac{N}{(1+\alpha)^{j}}\Big].$$

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

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

Therefore,

$$\begin{aligned}\sum_{j_1\le j\le j_2} \Big|V_j \setminus \big(P_j\ \Omega_j\big)\Big| \lesssim & N\alpha\Big[\ \log j_2 + j_2 e^{-\sqrt{\delta_1 \log p}}\ \Big] \\ & < N\Big[\alpha(\log\log p + \log\frac{1}{\alpha}) + (\log p)e^{-\sqrt{\delta_1 \log p}}\ \Big] \\ & \lesssim N(\log p)^{-1+2\epsilon}.\end{aligned} \tag{5.6}$$

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

$$P_j \times \Omega_j \longrightarrow P_j\Omega_j$$

is a one-to-one and onto.

Combining (5.1), (5.5) and (5.6), we have

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

For each j, the double sum

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

with

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

and

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

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 $\frac{N}{(1+\alpha)^j} > p^{3/4+\delta/2}$.

By inequality (4.3) $\big($with $v = 1$ for $\sum \eta_1(x)^2\big)$,

$$\begin{aligned}\sum \eta_1(x)^2 &\le N\bigg(p^2, G, \frac{N}{(1+\alpha)^j}\bigg)\\ &\le p^{\epsilon}\bigg(\frac{N}{(1+\alpha)^j}\bigg)^2\bigg\{\frac{(1+\alpha)^j}{N}\ p^{\frac14} + p^{-1}\bigg\}\\ &\le \bigg(\frac{N}{(1+\alpha)^j}\bigg)^2 p^{-\frac12-\frac{\delta}{3}}\end{aligned}$$

and

$$\begin{aligned}\sum \eta_2(y)^2 &\le N\big(p^2, G, (1+\alpha)^j\big)\\ &\le p^{\epsilon}(1+\alpha)^{2j}\min_{v\ge1}\bigg\{\frac{p^{1/\,2v(v+1)}}{(1+\alpha)^j} + p^{-1/v}\bigg\}\\ &\le p^{\epsilon}(1+\alpha)^{2j}(1+\alpha)^{-j(1-\delta/2)}\\ &< p^{-\delta_1/2}(1+\alpha)^{2j}.\end{aligned}$$

(We obtain the third inequality by taking v such that $p^{1/v} > (1+\alpha)^j \ge p^{1/(v+1)}$.)

Thus, after normalization, Lemma 4.2 can be applied with δ replaced by $\min(\frac{\delta}{3}, \frac{\delta_1}{2})$, and we obtain

$$\Big|\sum_{\ell\in P_j,\ m\in\Omega_j} \chi\big(q_p(\ell)+q_p(m)\big)\Big| < Np^{-\delta^2/2} < Np^{-c\delta_1}. \tag{5.9}$$

The theorem follows from (5.7) and (5.9). □

References

[BFKS] Bourgain J., Ford K., Konyagin S. V., Shparlinski I. E., *On the divisibility of Fermat quotients* , Michigan Math. J. Volume 59, Issue 2 (2010), 313-328.

[BKS] Bourgain J., Konyagin S. V., Shparlinski I. E., *Product sets of rationals, multiplicative translates of subgroups in residue rings and fixed points of the discrete logarithm*, Intern. Math. Research Notices, (2008), 1-29.

[COW] Chen Z., Ostafe A., Winterhof A., *Structure of Pseudorandom Numbers Derived from Fermat Quotients*, Lecture Notes in Computer Science 6087, Springer, Berlin, (2010), 7385.

[ET] Ernvall R., Metsnkyl T., *On the p-divisibility of Fermat quotients*, Math. Comp. 66 (1997), 13531365.

[F] Fouch W. L., *On the KummerMirimanoff congruences*, Q. J. Math. 37 (1986), 257261.

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

[G1] Granville A., *Some conjectures related to Fermats last theorem*, Number Theory, de Gruyter, NewYork, 1990, 177192.

[G2] ———, *On pairs of coprime integers with no large prime factors*, Expos. Math. 9 (1991), 335350.

[Hb] Heath-Brown R., *An estimate for Heilbronns exponential sum*, Analytic Number Theory: Proceeding of a Conference in Honor of Heini Halberstam, Birkhuser, Boston, 1996, 451463.

[HbK] Heath-Brown D. R., Konyagin S. V., *New bounds for Gauss sums derived from kth powers, and for Heilbronn's exponential sum*, Quart. J. Math. 51, (2000), 221-35.

[Ih] Ihara Y., *On the EulerKronecker constants of global ?elds and primes with small norms*, Algebraic Geometry and Number Theory, Progress in Mathematics 850, Birkhuser, Boston, 2006, 407451.

[IK] Iwaniec H., Kowalski E., *Analytic number theory*, Amer. Math. Soc., Providence RI, (2004).

[OS] Ostafe A., Shparlinski I. E., *Pseudorandomness and dynamics of Fermat quotients*, SIAM J. Discr. Math., (to appear).

[S1] Shparlinski I. E., *Character sums with Fermat quotients*, Quart. J. Math. 00 (2010), 1-13.

[S2] ———, *Open problems on exponential and character sums*, Number Theory: Proc. 5th China-Japan Seminar on Number Theory, Higashi-Osaka, 2008, World Scientific, (2010), 222-242.

[L] LENSTRA H. W., *miller's primality test*, Inform. Process. Lett. 8, (1979), 86-88.

Department Of Mathematics, University Of California, Riverside, CA 92521

E-mail address: mcc@math.ucr.edu