Publ. Math. Debrecen
94/1-2 (2019), 55–74
DOI: 10.5486/PMD.2019.8222

Pseudo-random subsets constructed by using Fermat quotients

By HUANING LIU (Xi'an) and GUOTUO ZHANG (Xi'an)

Abstract. Let p be a prime, and let n be an arbitrary integer with $(n,p) = 1$. The Fermat quotient $q_p(n)$ is defined as the unique integer with

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

We also define $q_p(kp) = 0$ for $k \in \mathbb{Z}$. In this paper, we study the pseudo-randomness of subsets constructed by Fermat quotients, by using the estimates for exponential sums and character sums with Fermat quotients.

1. Introduction

For a prime p and an integer n with $(n,p) = 1$, the Fermat quotient $q_p(n)$ is defined as

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

We also define $q_p(kp) = 0$, $k \in \mathbb{Z}$. It is easy to show that $q_p(u) = q_p(p^2 \pm u)$ for $p > 2$, and

$$q_p(a + kp) \equiv q_p(a) - ka^{-1} \pmod p \tag{1.1}$$

Mathematics Subject Classification: 11K38, 11K45, 11A07, 11T23, 11T24, 11T71.
Key words and phrases: Fermat quotient, pseudo-random subset, exponential sum, character sum.
This work is supported by National Natural Science Foundation of China under Grant No. 11571277, and the Science and Technology Program of Shaanxi Province of China under Grant Nos. 2014KJXX-61, 2016GY-080 and 2016GY-077.

for any $a, k \in \mathbb{Z}$ with $(a, p) = 1$. Fermat quotients arose from the study of the first case of Fermat's Last Theorem, which claimed that the equation

$$x^n + y^n + z^n = 0, \qquad 2 \nmid n, \qquad (n, xyz) = 1, \qquad n > 1 \tag{$(1)_n$}$$

has no solutions in integers x, y and z.

In 1823, Sophie Germain proved that if n and $2n+1$ are both prime, then $(1)_n$ has no solutions in integers. In 1909, Wieferich showed that if $(1)_p$ has solutions in integers x, y and z, then $q_p(2) = 0$. Shortly later, Mirimanoff extended the result to $q_p(3) = 0$. In 1917, Pollaczek proved that if prime p is sufficiently large and $(1)_p$ has solutions in integers x, y and z, then $q_p(u) = 0$ for each prime $u \leq 31$. In 1988, Granville and Monagan showed that if $(1)_p$ has solutions in integers x, y and z, then $q_p(u) = 0$ for all primes $u \leq 89$. See [13] for an excellent survey of the first case of Fermat's Last Theorem.

Fermat quotients have numerous applications in computational and algebraic number theory (see [1]–[2], [4], [6], [12], [16]–[19]). For example, we define the sets

$$\begin{aligned}
I_p(N) &= \left|\{q_p(u) : 1 \leq u \leq N, (u, p) = 1\}\right|, \\
M(p) &= \left|\{q_p(u) : 1 \leq u \leq p - 1\}\right|, \\
F(p) &= \left|\{u : 0 \leq u \leq p - 1, q_p(u) = u\}\right|, \\
R(p, a) &= \left|\{u : 0 \leq u \leq p - 1, q_p(u) = a\}\right|, \\
\vartheta(p) &= \frac{1}{p^2} \cdot \left|\{(u, v) : 0 \leq u, v \leq p - 1, q_p(u) = q_p(v)\}\right|, \\
U(p; k, h) &= \left|\{u : 0 \leq u \leq p - 1, q_p(u) \equiv z \pmod{p} \text{ for } z \in [k + 1, \ldots, k + h]\}\right|.
\end{aligned}$$

Vandiver [20] showed that $\sqrt{p} - 1 \leq M(p) \leq p - \sqrt{\frac{p-1}{2}}$. Fouché [11] proved $R(p, a) \leq p^{1/2+o(1)}$. Ostafe and Shparlinski [16] obtained the following estimations:

$$\begin{aligned}
M(p) &\geq (1 + o(1)) \frac{p}{(\log p)^2}, \qquad & F(p) &\ll p^{11/12+o(1)}, \\
\vartheta(p) &\leq p^{-3/4+o(1)}, & U(p; k, h) &\leq h^{1/2} p^{1/2+o(1)}.
\end{aligned}$$

Chen and Winterhof [6] gave certain generalization and improvement on Ostafe and Shparlinski's result.

Proposition 1.1. *Let $P(x) \in \mathbb{F}_p[x]$ be of degree $1 \leq d < p$. Then we have*

$$\#\left\{u : 1 \leq u \leq p - 1, q_p(u) = P(u)\right\} \ll \begin{cases} d^{1/4} p^{5/6}, & 1 \leq d \leq p^{1/3}, \\ d^{1/8} p^{7/8}, & d > p^{1/3}, \end{cases}$$

as $p \to \infty$.

Shparlinski [17] proved some lower bounds on the image size $I_p(N)$.

Proposition 1.2. *For every p and $N < p$, we have*

$$I_p(N) \geq (1 + o(1)) \frac{N^2}{p(\log N)^2}.$$

For every p and arbitrary fixed $\epsilon > 0$, there exists some $\delta > 0$ such that, for $p^\epsilon < N < p$, we have $I_p(N) \geq p^\delta$.

Shparlinski [17] also studied the primitive roots and power non-residues among the values of the Fermat quotients.

Proposition 1.3. *For every p, there exists $n \leq p^{3/4+o(1)}$ such that $q_p(n)$ is a primitive root modulo p. For every p and positive integer $d \mid p-1$, there exists $n \leq p^{3/4+o(1)}$ such that $q_p(n)$ is a d-th power non-residue modulo p.*

In this paper, we further study the pseudo-randomness of subsets constructed by using Fermat quotients. Let $\mathcal{R} \subset \{1, 2, \ldots, N\}$, and define the sequence

$$E_N = E_N(\mathcal{R}) = \{e_1, e_2, \ldots, e_N\} \in \left\{1 - \frac{|\mathcal{R}|}{N},\ -\frac{|\mathcal{R}|}{N}\right\}^N$$

by

$$e_n = \begin{cases} 1 - \frac{|\mathcal{R}|}{N}, & \text{for } n \in \mathcal{R}, \\ -\frac{|\mathcal{R}|}{N}, & \text{for } n \notin \mathcal{R}. \end{cases}$$

Dartyge and Sárközy [8] introduced the measures of pseudo-randomness: The *well-distribution measure* of the subset $\mathcal{R}$ is defined by

$$W(\mathcal{R}, N) = \max_{a,b,t} \left| \sum_{j=0}^{t-1} e_{a+jb} \right|,$$

where the maximum is taken over all a, b, $t \in \mathbb{N}$ with $1 \leq a \leq a + (t-1)b \leq N$. The *correlation measure of order k* of the subset $\mathcal{R}$ is defined by

$$C_k(\mathcal{R}, N) = \max_{M,D} \left| \sum_{n=1}^{M} e_{n+d_1} \cdots e_{n+d_k} \right|,$$

where the maximum is taken over all $D = (d_1, \ldots, d_k)$ and M with $0 \leq d_1 < \cdots < d_k \leq N - M$.

The subset $\mathcal{R}$ is considered as a pseudo-random subset if both $W(\mathcal{R}, N)$ and $C_k(\mathcal{R}, N)$ (at least for small k) are "small" in terms of N. Later many pseudo-random subsets were given and studied. For example, Dartyge, Mosaki and Sárközy [7] proved the following results.

Proposition 1.4. *Assume that p is an odd prime number, $f(x) \in \mathbb{F}_p[x]$ is of degree $d \geq 2$. Let $r \in \mathbb{Z}, s \in \mathbb{N}, s < p/2$. Define $\mathcal{R} \subset \{1, \dots, p\}$ by*

$$\mathcal{R} = \{n : 1 \leq n \leq p,\ \exists h \in \{r, r+1, \dots, r+s-1\} \text{ with } f(n) \equiv h \pmod{p}\}.$$

Then we have

$$W(\mathcal{R}, p) < 2d\sqrt{p}(\log p)^2.$$

And for $2 \leq k \leq d-1$, we have

$$C_k(\mathcal{R}, p) < 2d\sqrt{p}(1 + \log p)^{k+1}.$$

Dartyge and Sárközy [9] presented large families of pseudo-random subsets formed by power residues.

Proposition 1.5. *Let $p \geq 2$ be a prime number, $d \mid p-1$ and $f \in \mathbb{F}_p[x]$ of degree k. Define*

$$\mathcal{R} = \left\{x \in \mathbb{F}_p : \exists y \in \mathbb{F}_p^* \text{ with } f(x) \equiv y^d \pmod{p}\right\}.$$

Write $f = f_1^{\alpha_1} \cdots f_r^{\alpha_r}$ for the factorization into irreducible factors in $\overline{\mathbb{F}}_p$, and suppose that $(d, \alpha_1, \dots, \alpha_r) = 1$. Then

$$W(\mathcal{R}, p) \leq 20k\sqrt{p}\log p.$$

Let f be a polynomial of degree k with no multiple roots in $\overline{\mathbb{F}}_p$, and let $k, l \in \mathbb{N}$ such that one of the following conditions is satisfied:

(i) *l=2;*

(ii) *d is a prime divisor of $p-1$, and $(4l)^k < p$;*

(iii) *the polynomial $x^{p-1} + \cdots + x + 1$ is irreducible in $\mathbb{F}_d[x]$ and $\max(k, l) < p$.*

Then we have

$$C_l(\mathcal{R}, p) \leq lk\left(1 + \frac{20k\log p}{\sqrt{p}}\right)^l + 9\left(\frac{d-1}{d}\right)^l\left(1 + \frac{10k\log p}{\sqrt{p}}\right)^l lk\sqrt{p}\log p.$$

Dartyge, Sárközy and Szalay [10] studied the pseudo-randomness of certain subsets related to primitive roots.

Proposition 1.6. *Let p be an odd prime, $k, r \in \mathbb{N}$, $f(x) \in \mathbb{F}_p[x]$ of degree D. Let*

$$\mathcal{G}_p = \{g_1, g_2, \dots, g_{\phi(p-1)}\}, \qquad (0 < g_1 < g_2 < \cdots < g_{\phi(p-1)} < p)$$

be the set of the primitive roots modulo p. Define the subset $\mathcal{R} \subset \mathbb{F}_p$ by

$$\mathcal{R} = \{g^k : g \in \mathcal{G}_p, \exists x \in \mathbb{F}_p^* \text{ with } f(g^k) = x^r\}.$$

If $f(x)$ is irreducible over $\mathbb{F}_p$, then we have

$$W(\mathcal{R}, p) \ll D 2^{\omega(\frac{p-1}{k})} p^{1/2} \log p.$$

Moreover, if we also assume that $D \geq 2$ or $D = r = 1$, we also have

$$C_K(\mathcal{R}, p) \ll KD \left((1 + O(Dp^{-1/2})) 2^{\omega(\frac{p-1}{k})} \right)^K p^{1/2} \log p.$$

Chen [3] constructed a family of pseudo-random subsets modulo pq, where p, q are two distinct primes satisfying "RSA type" with $2 < p < q < 2p$, and studied the well-distribution and correlation measures. Liu and Song [15] further studied the correlation measures of the subsets.

In this paper, we study the pseudo-random subsets constructed by using Fermat quotients. Our results are the following.

Theorem 1.1. *Let p be an odd prime number, and let $r, s \in \mathbb{N}$ with $1 \leq r < r + s - 1 \leq p - 1$. Define $\mathcal{R} \subset \{1, \ldots, p^2\}$ by*

$$\mathcal{R} = \left\{ n : 1 \leq n \leq p^2,\ \exists h \in \{r, r+1, \ldots, r+s-1\} \text{ with } q_p(n) \equiv h \pmod{p} \right\}.$$

Then we have

$$W\left(\mathcal{R}, p^2\right) \ll p (\log p)^2,$$

and

$$C_2\left(\mathcal{R}, p^2\right) \ll p (\log p)^3.$$

Furthermore, if $s = o(p)$, then

$$C_3\left(\mathcal{R}, p^2\right) \ll s^2 + p^{\frac{3}{2}} (\log p)^3.$$

While $s = \left[\frac{p}{3}\right]$, we have

$$C_3\left(\mathcal{R}, p^2\right) \geq \frac{1}{54} p^2 + O\left(p (\log p)^4\right).$$

Theorem 1.2. *Let p be an odd prime number, and $d \mid p-1$. Define $\mathcal{R} \subset \left\{1, \ldots, p^2\right\}$ by*

$$\mathcal{R} = \left\{n : 1 \leq n \leq p^2,\ \exists\, y \text{ such that } 1 \leq y \leq p-1 \text{ and } q_p(n) \equiv y^d \pmod p\right\}.$$

Then we have

$$W\left(\mathcal{R}, p^2\right) \ll p^{\frac{3}{2}} \log p,$$

and

$$C_k\left(\mathcal{R}, p^2\right) \ll k p^{\frac{5}{3}},$$

where the implied constant depends on d.

Theorem 1.3. *Let p be an odd prime number, and let $\mathcal{G}_p$ be the set of the primitive roots modulo p. Define $\mathcal{R} \subset \left\{1, \ldots, p^2\right\}$ by*

$$\mathcal{R} = \left\{n : 1 \leq n \leq p^2, q_p(n) \in \mathcal{G}_p\right\}.$$

Then we have

$$W\left(\mathcal{R}, p^2\right) \ll 2^{\omega(p-1)} p^{\frac{3}{2}} \log p.$$

and

$$C_k\left(\mathcal{R}, p^2\right) \ll k 2^{k\omega(p-1)} p^{\frac{5}{3}}.$$

Remark 1.1. Our results show that the subsets in Theorems 1.2 and 1.3 enjoy good pseudo-random properties. However, the subset in Theorem 1.1 is not pseudo-random.

2. Exponential sums and character sums with Fermat quotients

The exponential sums with Fermat quotients have been studied by many authors. Write $e(y) = \mathrm{e}^{2\pi i y}$. Heath-Brown [14] proved the following estimation by using the Pólya–Vinogradov bound and the Burgess bound.

Proposition 2.1. *For any integer a coprime to p, we have*

$$\sum_{\substack{M < n \leq M+N \\ p \nmid n}} e\left(\frac{a q_p(n)}{p}\right) \ll N^{1/2} p^{3/8},$$

uniformly for $M, N \geq 1$. In particular,

$$\sum_{n=1}^{p-1} e\left(\frac{a q_p(n)}{p}\right) \ll p^{7/8},$$

uniformly for $p \nmid a$.

Ostafe and Shparlinski [16] obtained a non-trivial bound of exponential sums with linear combinations of Fermat quotients.

Proposition 2.2. *For any integer $s \geq 1$, we have*

$$\max_{(a_0,\dots,a_s,p)=1} \left| \sum_{u=M+1}^{M+N} e\left(\frac{\sum_{j=0}^{s-1} a_j q_p(u+j)}{p}\right)\right| \ll sp\log p,$$

uniformly over M and $p^2 > N \geq 1$.

Using Proposition 2.2, they studied the distribution of the points

$$\left(\frac{q_p(u)}{p}, \dots, \frac{q_p(u+s-1)}{p}\right), \qquad u = M+1, \dots, M+N,$$

in the s-dimensional cube. Moreover, Chen, Ostafe and Winterhof [5] gave the following generalization.

Proposition 2.3. *Let $d_0, d_1, \dots, d_{s-1}$ be integers with $0 \leq d_0 < d_1 < \dots < d_{s-1} < p^2$. Suppose that no triple (d_l, d_h, d_t) satisfies $d_l \equiv d_h \equiv d_t \pmod p$ for $0 \leq l < h < t < s$. We have*

$$\max_{(a_0,\dots,a_s,p)=1} \left| \sum_{u=1}^{N} e\left(\frac{\sum_{j=0}^{s-1} a_j q_p(u+d_j)}{p}\right)\right| \ll s\max\left\{p\log p, Np^{-\frac{1}{2}}\right\}$$

for $1 \leq N \leq p^2$. If $s = 2$ or $d_{s-1} < p$, the stronger bound $sp\log p$ holds.

Now, we give the following identities on certain exponential sums of Fermat quotients.

Theorem 2.1. *Let $p > 2$ be a prime, and let u be an integer with $(u,p) = 1$. For any integer z, we have*

$$\left|\sum_{n=1}^{p^2} e\left(\frac{uq_p(n)}{p}\right) e\left(\frac{zn}{p^2}\right)\right| = p.$$

Proof. Write $n = a + bp$, we get

$$\sum_{n=1}^{p^2} e\left(\frac{uq_p(n)}{p}\right) e\left(\frac{zn}{p^2}\right) = \sum_{a=1}^{p}\sum_{b=0}^{p-1} e\left(\frac{uq_p(a+bp)}{p}\right) e\left(\frac{z(a+bp)}{p^2}\right)$$
$$= \sum_{a=1}^{p-1}\sum_{b=0}^{p-1} e\left(\frac{uq_p(a+bp)}{p}\right) e\left(\frac{z(a+bp)}{p^2}\right) + \sum_{b=0}^{p-1} e\left(\frac{z(1+b)}{p}\right).$$

Assume that $p \nmid z$. By (1.1), we have

$$\sum_{n=1}^{p^2} e\left(\frac{uq_p(n)}{p}\right) e\left(\frac{zn}{p^2}\right) = \sum_{a=1}^{p-1}\sum_{b=0}^{p-1} e\left(\frac{uq_p(a+bp)}{p}\right) e\left(\frac{z(a+bp)}{p^2}\right)$$
$$= \sum_{a=1}^{p-1}\sum_{b=0}^{p-1} e\left(\frac{u\left(q_p(a) - ba^{-1}\right)}{p}\right) e\left(\frac{z(a+bp)}{p^2}\right)$$
$$= \sum_{a=1}^{p-1} e\left(\frac{uq_p(a)}{p}\right) e\left(\frac{za}{p^2}\right) \sum_{b=0}^{p-1} e\left(\frac{b(z-ua^{-1})}{p}\right)$$
$$= p \sum_{\substack{a=1 \\ z\equiv ua^{-1} \ (\mathrm{mod}\ p)}}^{p-1} e\left(\frac{uq_p(a)}{p}\right) e\left(\frac{za}{p^2}\right)$$

Hence,

$$\left|\sum_{n=1}^{p^2} e\left(\frac{uq_p(n)}{p}\right) e\left(\frac{zn}{p^2}\right)\right| = p.$$

Suppose that $p \mid z$. By (1.1), we get

$$\sum_{n=1}^{p^2} e\left(\frac{uq_p(n)}{p}\right) e\left(\frac{zn}{p^2}\right) = \sum_{a=1}^{p-1}\sum_{b=0}^{p-1} e\left(\frac{uq_p(a+bp)}{p}\right) e\left(\frac{z(a+bp)}{p^2}\right) + p$$
$$= \sum_{a=1}^{p-1}\sum_{b=0}^{p-1} e\left(\frac{u\left(q_p(a) - ba^{-1}\right)}{p}\right) e\left(\frac{z(a+bp)}{p^2}\right) + p$$
$$= \sum_{a=1}^{p-1} e\left(\frac{uq_p(a)}{p}\right) e\left(\frac{za}{p^2}\right) \sum_{b=0}^{p-1} e\left(-\frac{bua^{-1}}{p}\right) + p = p.$$

This proves Theorem 2.1. $\square$

Theorem 2.2. *Let $p > 2$ be a prime, and let u_1, u_2, u_3 be integers with $(u_1u_2u_3, p) = 1$. Let d_1, k_2, k_3 and M be integers such that $0 \le d_1 < d_1 + k_2p < d_1 + k_3p \le p^2 - M$. Then we have*

$$\sum_{n=1}^{M} e\left(\frac{u_1q_p(n+d_1) + u_2q_p(n+d_1+k_2p) + u_3q_p(n+d_1+k_3p)}{p}\right)$$
$$= \begin{cases} M, & \text{if } u_1+u_2+u_3 \equiv 0 \pmod p \text{ and } u_2k_2+u_3k_3 \equiv 0 \pmod p, \\ O(p), & \text{if } u_1+u_2+u_3 \equiv 0 \pmod p \text{ and } u_2k_2+u_3k_3 \not\equiv 0 \pmod p, \\ O(p\log p), & \text{if } u_1+u_2+u_3 \not\equiv 0 \pmod p. \end{cases}$$

Proof. We may suppose that $M \ge p$, since otherwise the claim is trivial. By (1.1), we get

$$\sum_{n=1}^{M} e\left(\frac{u_1q_p(n+d_1) + u_2q_p(n+d_1+k_2p) + u_3q_p(n+d_1+k_3p)}{p}\right)$$
$$= \sum_{\substack{n=1 \\ (n+d_1,p)=1}}^{M} e\left(\frac{u_1q_p(n+d_1)+u_2q_p(n+d_1+k_2p)+u_3q_p(n+d_1+k_3p)}{p}\right) + \sum_{\substack{n=1 \\ (n+d_1,p)>1}}^{M} 1$$
$$= \sum_{\substack{n=1 \\ (n+d_1,p)=1}}^{M} e\left(\frac{(u_1+u_2+u_3)q_p(n+d_1)-(u_2k_2+u_3k_3)(n+d_1)^{-1}}{p}\right) + \sum_{\substack{n=1 \\ (n+d_1,p)>1}}^{M} 1.$$

Case 1. $u_1 + u_2 + u_3 \equiv 0 \pmod p$ and $u_2k_2 + u_3k_3 \equiv 0 \pmod p$. We have

$$\sum_{n=1}^{M} e\left(\frac{u_1q_p(n+d_1) + u_2q_p(n+d_1+k_2p) + u_3q_p(n+d_1+k_3p)}{p}\right) = M.$$

Case 2. $u_1 + u_2 + u_3 \equiv 0 \pmod p$ and $u_2k_2 + u_3k_3 \not\equiv 0 \pmod p$. It is not hard to show that

$$\sum_{n=1}^{M} e\left(\frac{u_1q_p(n+d_1) + u_2q_p(n+d_1+k_2p) + u_3q_p(n+d_1+k_3p)}{p}\right)$$
$$= \sum_{\substack{n=1 \\ (n+d_1,p)=1}}^{M} e\left(-\frac{(u_2k_2+u_3k_3)(n+d_1)^{-1}}{p}\right) + \sum_{\substack{n=1 \\ (n+d_1,p)>1}}^{M} 1 =$$

$$= \sum_{0\le k\le\left[\frac{M}{p}\right]-1} \sum_{\substack{v=1\\(v+d_1,p)=1}}^{p} e\left(-\frac{(u_2k_2+u_3k_3)(kp+v+d_1)^{-1})}{p}\right) + O(p)$$

$$= \sum_{0\le k\le\left[\frac{M}{p}\right]-1} \sum_{\substack{v=1\\(v+d_1,p)=1}}^{p} e\left(-\frac{(u_2k_2+u_3k_3)(v+d_1)^{-1})}{p}\right) + O(p) \ll p.$$

Case 3. $u_1+u_2+u_3 \not\equiv 0 \pmod p$. By (1.1) and the properties of residue systems, we have

$$\begin{aligned}
&\sum_{n=1}^{M} e\left(\frac{u_1q_p(n+d_1)+u_2q_p(n+d_1+k_2p)+u_3q_p(n+d_1+k_3p)}{p}\right)\\
&= \sum_{\substack{n=1\\(n+d_1,p)=1}}^{M} e\left(\frac{(u_1+u_2+u_3)q_p(n+d_1)-(u_2k_2+u_3k_3)(n+d_1)^{-1})}{p}\right) + \sum_{\substack{n=1\\(n+d_1,p)>1}}^{M} 1\\
&= \sum_{0\le k\le\left[\frac{M}{p}\right]-1} \sum_{\substack{v=1\\(v+d_1,p)=1}}^{p} e\left(\frac{(u_1+u_2+u_3)q_p(kp+v+d_1)}{p}\right.\\
&\qquad\qquad \left. -\frac{(u_2k_2+u_3k_3)(kp+v+d_1)^{-1})}{p}\right) + O(p)\\
&= \sum_{\substack{v=1\\(v+d_1,p)=1}}^{p} e\left(\frac{(u_1+u_2+u_3)q_p(v+d_1)-(u_2k_2+u_3k_3)(v+d_1)^{-1})}{p}\right)\\
&\quad \times \sum_{0\le k\le\left[\frac{M}{p}\right]-1} e\left(-\frac{(u_1+u_2+u_3)(v+d_1)^{-1}k}{p}\right) + O(p)\\
&\ll \sum_{\substack{v=1\\(v+d_1,p)=1}}^{p} \left| \sum_{0\le k\le\left[\frac{M}{p}\right]-1} e\left(-\frac{(u_1+u_2+u_3)(v+d_1)^{-1}k}{p}\right)\right| + p\\
&\ll \sum_{\substack{v=1\\(v+d_1,p)=1}}^{p} \frac{1}{\left\langle -\frac{(u_1+u_2+u_3)(v+d_1)^{-1}}{p}\right\rangle} + p \ll \sum_{0<|v|\le\frac{p-1}{2}} \frac{1}{\left\langle \frac{v}{p}\right\rangle} + p \ll p\log p,
\end{aligned}$$

where $\langle\alpha\rangle$ denotes the distance of the real number α to the nearest integer.

This completes the proof of Theorem 2.2. □

On the other hand, character sums with Fermat quotients have also been studied by many authors. For example, from [12] we know that

$$\sum_{u=0}^{N-1} \chi\left(q_p(au+b)\right) \ll N^{1-\frac{1}{v}} p^{\frac{5v+1}{4v^2}} (\log p)^{\frac{1}{v}}, \tag{2.1}$$

for $1 \le N \le p^2$ and every fixed integer $v \ge 1$, where χ is a non-trivial multiplicative character modulo p, and a, b are integers with $(a,p^2) \ne p^2$. Gomez and Winterhof [12] further studied the following character sums.

Proposition 2.4. *Let $\chi_1, \chi_2, \ldots, \chi_l$ be nontrivial multiplicative characters modulo p. Then we have*

$$\sum_{u=0}^{N-1} \chi_1\left(q_p\left(u+d_1\right)\right) \cdots \chi_l\left(q_p\left(u+d_l\right)\right) \ll \max\left\{\frac{lN}{p^{\frac{1}{3}}},\ lp^{\frac{3}{2}}\log p\right\},$$

for any integers $0 \le d_1 < \cdots < d_l \le p^2-1$ and $1 \le N \le p^2$.

3. Proof of Theorem 1.1

For integer h with $(h,p)=1$, by (1.1), we get

$$\begin{aligned}\sum_{\substack{n=1\\ q_p(n)\equiv h\ (\mathrm{mod}\ p)}}^{p^2} 1 &= \sum_{\substack{n=1\\ (n,p)=1\\ q_p(n)\equiv h\ (\mathrm{mod}\ p)}}^{p^2} 1 = \sum_{\substack{a=1\\ q_p(a+kp)\equiv h\ (\mathrm{mod}\ p)}}^{p-1}\sum_{k=0}^{p-1} 1\\ &= \sum_{\substack{a=1\\ q_p(a)-ka^{-1}\equiv h\ (\mathrm{mod}\ p)}}^{p-1}\sum_{k=0}^{p-1} 1 = \sum_{a=1}^{p-1}\sum_{\substack{k=0\\ ka^{-1}\equiv q_p(a)-h\ (\mathrm{mod}\ p)}}^{p-1} 1 = p-1.\end{aligned}$$

Suppose that $\mathcal{A} \subset \{1,2,\ldots,p-1\}$. Then

$$\sum_{\substack{n=1\\ q_p(n)\in\mathcal{A}}}^{p^2} 1 = |\mathcal{A}|\cdot(p-1). \tag{3.1}$$

Noting that $1 \le r < r+s-1 \le p-1$, we have

$$|\mathcal{R}| = s(p-1).$$

It is easy to show that, for $1 \le n \le p^2$,

$$\frac{1}{p}\sum_{h=r}^{r+s-1}\sum_{|u|\le\frac{p-1}{2}} e\left(\frac{u(q_p(n)-h)}{p}\right) = \begin{cases}1, & n\in\mathcal{R},\\ 0, & n\notin\mathcal{R}.\end{cases}$$

Hence,

$$\begin{aligned} e_n &= \frac{1}{p}\sum_{h=r}^{r+s-1}\sum_{|u|\le\frac{p-1}{2}} e\left(\frac{u(q_p(n)-h)}{p}\right) - \frac{|\mathcal{R}|}{p^2} \\ &= \frac{1}{p}\sum_{1\le|u|\le\frac{p-1}{2}}\left(\sum_{h=r}^{r+s-1} e\left(-\frac{uh}{p}\right)\right) e\left(\frac{uq_p(n)}{p}\right) + O\left(\frac{1}{p}\right), \end{aligned} \tag{3.2}$$

where the term $\frac{|\mathcal{R}|}{p^2}$ is compensated by the contribution of $u=0$.

For a, b, $t\in\mathbb{N}$ with $1\le a\le a+(t-1)b\le p^2$, from (3.2) and Theorem 2.1, we get

$$\begin{aligned} \sum_{j=0}^{t-1} e_{a+jb} &= \frac{1}{p}\sum_{1\le|u|\le\frac{p-1}{2}}\left(\sum_{h=r}^{r+s-1} e\left(-\frac{uh}{p}\right)\right)\sum_{j=0}^{t-1} e\left(\frac{uq_p(a+jb)}{p}\right) + O(p) \\ &= \frac{1}{p^3}\sum_{1\le|u|\le\frac{p-1}{2}}\left(\sum_{h=r}^{r+s-1} e\left(-\frac{uh}{p}\right)\right)\sum_{n=1}^{p^2} e\left(\frac{uq_p(n)}{p}\right)\sum_{j=0}^{t-1} \\ &\quad\times\sum_{z=1}^{p^2} e\left(\frac{z(n-(a+jb))}{p^2}\right) + O(p) \\ &= \frac{1}{p^3}\sum_{1\le|u|\le\frac{p-1}{2}}\left(\sum_{h=r}^{r+s-1} e\left(-\frac{uh}{p}\right)\right)\sum_{z=1}^{p^2}\left(\sum_{j=0}^{t-1} e\left(-\frac{z(a+jb)}{p^2}\right)\right) \\ &\quad\times\sum_{n=1}^{p^2} e\left(\frac{uq_p(n)}{p}\right) e\left(\frac{zn}{p^2}\right) + O(p) \ll p(\log p)^2. \end{aligned}$$

Hence,

$$W\left(\mathcal{R}, p^2\right) \ll p(\log p)^2.$$

For integers d_1, d_2 and M with $0\le d_1 < d_2 \le p^2 - M$, from (3.2) and Proposition 2.3, we get

$$\sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} = \sum_{n=1}^{M} \left(\frac{1}{p} \sum_{1 \le |u_1| \le \frac{p-1}{2}} \left(\sum_{h_1=r}^{r+s-1} e\left(-\frac{u_1 h_1}{p}\right)\right) e\left(\frac{u_1 q_p(n+d_1)}{p}\right) + O\left(\frac{1}{p}\right)\right)$$
$$\times \left(\frac{1}{p} \sum_{1 \le |u_2| \le \frac{p-1}{2}} \left(\sum_{h_2=r}^{r+s-1} e\left(-\frac{u_2 h_2}{p}\right)\right) e\left(\frac{u_2 q_p(n+d_2)}{p}\right) + O\left(\frac{1}{p}\right)\right)$$
$$= \frac{1}{p^2} \sum_{1 \le |u_1| \le \frac{p-1}{2}} \left(\sum_{h_1=r}^{r+s-1} e\left(-\frac{u_1 h_1}{p}\right)\right) \sum_{1 \le |u_2| \le \frac{p-1}{2}} \left(\sum_{h_2=r}^{r+s-1} e\left(-\frac{u_2 h_2}{p}\right)\right)$$
$$\times \sum_{n=1}^{M} e\left(\frac{u_1 q_p(n+d_1) + u_2 q_p(n+d_2)}{p}\right) + O\left(p \log p\right) \ll p(\log p)^3.$$

Therefore,

$$C_2\left(\mathcal{R}, p^2\right) \ll p(\log p)^3.$$

For integers d_1, d_2, d_3 and M with $0 \le d_1 < d_2 < d_3 \le p^2 - M$, by (3.2), we have

$$\sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} e_{n+d_3}$$
$$= \sum_{n=1}^{M} \left(\frac{1}{p} \sum_{1 \le |u_1| \le \frac{p-1}{2}} \left(\sum_{h_1=r}^{r+s-1} e\left(-\frac{u_1 h_1}{p}\right)\right) e\left(\frac{u_1 q_p(n+d_1)}{p}\right) + O\left(\frac{1}{p}\right)\right)$$
$$\times \left(\frac{1}{p} \sum_{1 \le |u_2| \le \frac{p-1}{2}} \left(\sum_{h_2=r}^{r+s-1} e\left(-\frac{u_2 h_2}{p}\right)\right) e\left(\frac{u_2 q_p(n+d_2)}{p}\right) + O\left(\frac{1}{p}\right)\right)$$
$$\times \left(\frac{1}{p} \sum_{1 \le |u_3| \le \frac{p-1}{2}} \left(\sum_{h_3=r}^{r+s-1} e\left(-\frac{u_3 h_3}{p}\right)\right) e\left(\frac{u_3 q_p(n+d_3)}{p}\right) + O\left(\frac{1}{p}\right)\right)$$
$$= \frac{1}{p^3} \sum_{1 \le |u_1| \le \frac{p-1}{2}} \left(\sum_{h_1=r}^{r+s-1} e\left(-\frac{u_1 h_1}{p}\right)\right) \sum_{1 \le |u_2| \le \frac{p-1}{2}} \left(\sum_{h_2=r}^{r+s-1} e\left(-\frac{u_2 h_2}{p}\right)\right)$$
$$\times \sum_{1 \le |u_3| \le \frac{p-1}{2}} \left(\sum_{h_3=r}^{r+s-1} e\left(-\frac{u_3 h_3}{p}\right)\right)$$
$$\times \sum_{n=1}^{M} e\left(\frac{u_1 q_p(n+d_1) + u_2 q_p(n+d_2) + u_3 q_p(n+d_3)}{p}\right) + O\left(p\left(\log p\right)^2\right).$$

We consider d_1, d_2, d_3 in two cases.

Case 1. $d_1 \equiv d_2 \equiv d_3 \pmod p$ does not hold. Then from Proposition 2.3, we get

$$\sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} e_{n+d_3} \ll p^{\frac{3}{2}} (\log p)^3.$$

Case 2. $d_1 \equiv d_2 \equiv d_3 \pmod p$. Write $d_2 = d_1 + k_2 p$, $d_3 = d_1 + k_3 p$, where $0 < k_2 < k_3 < p$. Then from Theorem 2.2, we have

$$\begin{aligned}
\sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} e_{n+d_3} &= \frac{M}{p^3} \sum_{1 \le |u_1| \le \frac{p-1}{2}} \sum_{1 \le |u_2| \le \frac{p-1}{2}} \sum_{\substack{1 \le |u_3| \le \frac{p-1}{2} \\ u_1+u_2+u_3 \equiv 0 \,(\mathrm{mod}\ p) \\ u_2 k_2 + u_3 k_3 \equiv 0 \,(\mathrm{mod}\ p)}} \left(\sum_{h_1=r}^{r+s-1} e\left(-\frac{u_1 h_1}{p}\right)\right) \\
&\quad \times \left(\sum_{h_2=r}^{r+s-1} e\left(-\frac{u_2 h_2}{p}\right)\right) \left(\sum_{h_3=r}^{r+s-1} e\left(-\frac{u_3 h_3}{p}\right)\right) + O\left(p (\log p)^4\right) \\
&= \frac{M}{p^3} \sum_{h_1=r}^{r+s-1} \sum_{h_2=r}^{r+s-1} \sum_{h_3=r}^{r+s-1} \sum_{1 \le |u| \le \frac{p-1}{2}} \\
&\quad \times e\left(\frac{u\left((1-k_3 k_2^{-1}) h_1 + k_3 k_2^{-1} h_2 - h_3\right)}{p} \right) + O\left(p (\log p)^4\right). \qquad (3.3)
\end{aligned}$$

Assume that $s = o(p)$. Then

$$\begin{aligned}
\sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} e_{n+d_3} &= \frac{M}{p^2} \sum_{h_1=r}^{r+s-1} \sum_{h_2=r}^{r+s-1} \sum_{\substack{h_3=r \\ (1-k_3 k_2^{-1}) h_1 + k_3 k_2^{-1} h_2 - h_3 \equiv 0 \,(\mathrm{mod}\ p)}}^{r+s-1} 1 - \frac{M s^3}{p^3} + O\left(p (\log p)^4\right) \\
&\ll \frac{M s^2}{p^2} + p (\log p)^4 .
\end{aligned}$$

Therefore,

$$C_3\left(\mathcal{R}, p^2\right) \ll s^2 + p^{\frac{3}{2}} (\log p)^3 .$$

Now taking $M = p^2 - 2p$, $d_1 = 0$, $d_2 = p$ and $d_3 = 2p$ in (3.3), we have

$$\begin{aligned}
&\sum_{n=1}^{p^2-2p} e_{n+d_1} e_{n+d_2} e_{n+d_3} \\
&= \frac{p^2-2p}{p^3} \sum_{h_1=r}^{r+s-1} \sum_{h_2=r}^{r+s-1} \sum_{h_3=r}^{r+s-1} \sum_{1 \le |u| \le \frac{p-1}{2}} e\left(\frac{u\,(2h_2 - h_1 - h_3)}{p} \right) + O\left(p (\log p)^4\right) =
\end{aligned}$$

$$= \frac{p^2-2p}{p^3} \sum_{h_1=0}^{s-1} \sum_{h_2=0}^{s-1} \sum_{h_3=0}^{s-1} \sum_{1 \le |u| \le \frac{p-1}{2}} e\left(\frac{u\,(2h_2-h_1-h_3)}{p}\right) + O\left(p\,(\log p)^4\right)$$

$$= \frac{p^2-2p}{p^2} \sum_{\substack{h_1=0\ h_2=0\ h_3=0 \\ h_1+h_3=2h_2}}^{s-1}\ \sum^{s-1} \sum^{s-1} 1 - \frac{p^2-2p}{p^3} s^3 + O\left(p\,(\log p)^4\right).$$

Noting that

$$\sum_{h_1=0}^{s-1} \sum_{h_2=0}^{s-1} \sum_{\substack{h_3=0 \\ h_1+h_3=2h_2}}^{s-1} 1 = \sum_{h_2=0}^{s-1} \sum_{h_1=0}^{s-1} \sum_{\substack{h_3=0 \\ h_1+h_3=2h_2}}^{s-1} 1$$

$$= \sum_{0 \le 2h_2 \le s-1} (2h_2+1) + \sum_{s \le 2h_2 \le 2s-2} (2s-1-2h_2)$$

$$= \sum_{\substack{1 \le t \le s \\ 2 \nmid t}} t + \sum_{\substack{1 \le t \le s-1 \\ 2 \nmid t}} t = \begin{cases} \dfrac{s^2+1}{2}, & \text{if } 2 \nmid s, \\ \dfrac{s^2}{2}, & \text{if } 2 \mid s. \end{cases}$$

Thus we have

$$\sum_{n=1}^{p^2-2p} e_{n+d_1} e_{n+d_2} e_{n+d_3} = \frac{s^2}{2} - \frac{s^3}{p} + O\left(p\,(\log p)^4\right).$$

Assume that $s = \left[\frac{p}{3}\right]$. We immediately get

$$\sum_{n=1}^{p^2-2p} e_{n+d_1} e_{n+d_2} e_{n+d_3} = \frac{1}{54} p^2 + O\left(p\,(\log p)^4\right).$$

Therefore,

$$C_3\left(\mathcal{R}, p^2\right) \ge \frac{1}{54} p^2 + O\left(p\,(\log p)^4\right).$$

This proves Theorem 1.1.

4. Proof of Theorem 1.2

From (3.1), we get

$$|\mathcal{R}| = \frac{(p-1)^2}{d}.$$

On the other hand, we denote by χ_0 the principal character modulo p. Assume that $q_p(n) \neq 0$. By the orthogonality of characters of order d, we have

$$\frac{1}{d} \sum_{\substack{\chi^d=\chi_0 \\ \chi \bmod p}} \chi\left(q_p(n)\right) = \begin{cases} 1, & \text{if } \exists\, y \text{ such that } 1 \le y \le p-1 \text{ and } q_p(n) \equiv y^d (\text{mod } p), \\ 0, & \text{otherwise}, \end{cases}$$

$$= \begin{cases} 1, & n \in \mathcal{R}, \\ 0, & n \notin \mathcal{R}. \end{cases}$$

Hence,

$$e_n = \frac{1}{d} \sum_{\substack{\chi^d=\chi_0 \\ \chi \bmod p}} \chi\left(q_p(n)\right) - \frac{|\mathcal{R}|}{p^2} = \frac{1}{d} \sum_{\substack{\chi^d=\chi_0 \\ \chi\neq\chi_0 \\ \chi \bmod p}} \chi\left(q_p(n)\right) + O\left(\frac{1}{p}\right). \tag{4.1}$$

For a, b, $t \in \mathbb{N}$ with $1 \le a \le a + (t-1)b \le p^2$, from (4.1) and (2.1), we get

$$\sum_{j=0}^{t-1} e_{a+jb} = \sum_{j=0}^{t-1} \left(\frac{1}{d} \sum_{\substack{\chi^d=\chi_0 \\ \chi\neq\chi_0 \\ \chi \bmod p}} \chi\left(q_p(a+jb)\right) + O\left(\frac{1}{p}\right) \right)$$

$$= \frac{1}{d} \sum_{\substack{\chi^d=\chi_0 \\ \chi\neq\chi_0 \\ \chi \bmod p}} \sum_{j=0}^{t-1} \chi\left(q_p(a+jb)\right) + O\left(p\right) \ll p^{\frac{3}{2}} \log p.$$

Therefore,

$$W\left(\mathcal{R}, p^2\right) \ll p^{\frac{3}{2}} \log p.$$

For integers $d_1, d_2, \ldots, d_k$ and M with $0 \le d_1 < d_2 < \cdots < d_k \le p^2 - M$, from (4.1) and Proposition 2.4, we have

$$\sum_{n=1}^{M} e_{n+d_1} \cdots e_{n+d_k}$$

$$= \sum_{n=1}^{M} \left(\frac{1}{d} \sum_{\substack{\chi_1^d=\chi_0 \\ \chi_1\neq\chi_0 \\ \chi_1 \bmod p}} \chi_1\left(q_p(n+d_1)\right) + O\left(\frac{1}{p}\right) \right) \times \cdots$$

$$\times \left(\frac{1}{d} \sum_{\substack{\chi_k^d = \chi_0 \\ \chi_k \neq \chi_0 \\ \chi_k \bmod p}} \chi_k \left(q_p(n+d_k) \right) + O\left(\frac{1}{p}\right) \right)$$

$$= \frac{1}{d^k} \sum_{\substack{\chi_1^d = \chi_0 \\ \chi_1 \neq \chi_0 \\ \chi_1 \bmod p}} \cdots \sum_{\substack{\chi_k^d = \chi_0 \\ \chi_k \neq \chi_0 \\ \chi_k \bmod p}} \sum_{n=1}^{M} \chi_1 \left(q_p(n+d_1) \right) \cdots \chi_k \left(q_p(n+d_k) \right) + O\left(kp\right) \ll kp^{\frac{5}{3}}.$$

Hence,

$$C_k \left(\mathcal{R}, p^2 \right) \ll kp^{\frac{5}{3}}.$$

This completes the proof of Theorem 1.2.

5. Proof of Theorem 1.3

By (3.1), we have

$$|\mathcal{R}| = (p-1)\phi(p-1).$$

Suppose that $q_p(n) \neq 0$. Noting that

$$\frac{\phi(p-1)}{p-1} \sum_{s|p-1} \frac{\mu(s)}{\phi(s)} \sum_{\substack{\text{ord } \chi = s \\ \chi \bmod p}} \chi(q_p(n)) = \begin{cases} 1, & \text{if } q_p(n) \text{ is a primitive root modulo } p, \\ 0, & \text{otherwise,} \end{cases}$$

$$= \begin{cases} ll1, & n \in \mathcal{R}, \\ 0, & n \notin \mathcal{R}. \end{cases}$$

Thus, we have

$$e_n = \frac{\phi(p-1)}{p-1} \sum_{s|p-1} \frac{\mu(s)}{\phi(s)} \sum_{\substack{\text{ord } \chi = s \\ \chi \bmod p}} \chi\left(q_p(n)\right) - \frac{|\mathcal{R}|}{p^2}$$

$$= \frac{\phi(p-1)}{p-1} \sum_{\substack{s|p-1 \\ s>1}} \frac{\mu(s)}{\phi(s)} \sum_{\substack{\text{ord } \chi = s \\ \chi \bmod p}} \chi\left(q_p(n)\right) + O\left(\frac{1}{p}\right). \tag{5.1}$$

For a, b, $t \in \mathbb{N}$ with $1 \leq a \leq a+(t-1)b \leq p^2$, from (5.1) and (2.1), we get

$$\begin{aligned}\sum_{j=0}^{t-1} e_{a+jb} &= \sum_{j=0}^{t-1}\left(\frac{\phi(p-1)}{p-1}\sum_{\substack{s\mid p-1\\ s>1}}\frac{\mu(s)}{\phi(s)}\sum_{\substack{\mathrm{ord}\ \chi=s\\ \chi \bmod p}}\chi\left(q_p(a+jb)\right)+O\left(\frac{1}{p}\right)\right)\\ &= \frac{\phi(p-1)}{p-1}\sum_{\substack{s\mid p-1\\ s>1}}\frac{\mu(s)}{\phi(s)}\sum_{\substack{\mathrm{ord}\ \chi=s\\ \chi \bmod p}}\sum_{j=0}^{t-1}\chi\left(q_p(a+jb)\right)+O\left(p\right)\\ &\ll 2^{\omega(p-1)}p^{\frac{3}{2}}\log p.\end{aligned}$$

Therefore,

$$W\left(\mathcal{R},p^2\right) \ll 2^{\omega(p-1)}p^{\frac{3}{2}}\log p.$$

For integers $d_1, d_2, \cdots, d_k$ and M with $0 \leq d_1 < d_2 < \cdots < d_k \leq p^2-M$, from (5.1) and Proposition 2.4 we have

$$\begin{aligned}&\sum_{n=1}^{M} e_{n+d_1}\cdots e_{n+d_k}\\ &= \sum_{n=1}^{M}\left(\frac{\phi(p-1)}{p-1}\sum_{\substack{s_1\mid p-1\\ s_1>1}}\frac{\mu(s_1)}{\phi(s_1)}\sum_{\substack{\mathrm{ord}\ \chi_1=s_1\\ \chi_1\neq\chi_0\\ \chi_1 \bmod p}}\chi_1\left(q_p(n+d_1)\right)+O\left(\frac{1}{p}\right)\right)\times\cdots\\ &\quad\times\left(\frac{\phi(p-1)}{p-1}\sum_{\substack{s_k\mid p-1\\ s_k>1}}\frac{\mu(s_k)}{\phi(s_k)}\sum_{\substack{\mathrm{ord}\ \chi_k=s_k\\ \chi_k\neq\chi_0\\ \chi_k \bmod p}}\chi_k\left(q_p(n+d_k)\right)+O\left(\frac{1}{p}\right)\right)\\ &= \frac{\phi^k(p-1)}{(p-1)^k}\sum_{\substack{s_1\mid p-1\\ s_1>1}}\frac{\mu(s_1)}{\phi(s_1)}\sum_{\substack{\mathrm{ord}\ \chi_1=s_1\\ \chi_1\neq\chi_0\\ \chi_1 \bmod p}}\cdots\sum_{\substack{s_k\mid p-1\\ s_k>1}}\frac{\mu(s_k)}{\phi(s_k)}\sum_{\substack{\mathrm{ord}\ \chi_k=s_k\\ \chi_k\neq\chi_0\\ \chi_k \bmod p}}\\ &\quad\times\sum_{n=1}^{M}\chi_1\left(q_p(n+d_1)\right)\cdots\chi_k\left(q_p(n+d_k)\right)+O\left(k2^{k\omega(p-1)}p\right) \ll k2^{k\omega(p-1)}p^{\frac{5}{3}}.\end{aligned}$$

Hence,

$$C_k\left(\mathcal{R},p^2\right) \ll k2^{k\omega(p-1)}p^{\frac{5}{3}}.$$

This completes the proof of Theorem 1.3.

Acknowledgements. The authors express their gratitude to the referees for their helpful and detailed comments.

References

[1] H. Aly and A. Winterhof, Boolean functions derived from Fermat quotients, *Cryptogr. Commun.* **3** (2011), 165–174.

[2] M.-C. Chang, Short character sums with Fermat quotients, *Acta Arith.* **152** (2012), 23–38.

[3] Z. Chen, Large families of pseudo-random subsets formed by generalized cyclotomic classes, *Monatsh. Math.* **161** (2010), 161–172.

[4] Z. Chen and X. Du, On the linear complexity of binary threshold sequences derived from Fermat quotients, *Des. Codes Cryptogr.* **67** (2013), 317–323.

[5] 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, Vol. **6087**, *Springer-Verlag*, *Berlin*, 2010, 73–85.

[6] Z. Chen and A. Winterhof, Interpolation of Fermat quotients, *SIAM J. Discrete Math.* **28** (2014), 1–7.

[7] C. Dartyge, E. Mosaki and A. Sárközy, On large families of subsets of the set of the integers not exceeding N, *Ramanujan J.* **18** (2009), 209–229.

[8] C. Dartyge and A. Sárközy, On pseudo-random subsets of the set of the integers not exceeding N, *Period. Math. Hungar.* **54** (2007), 183–200.

[9] C. Dartyge and A. Sárközy, Large families of pseudorandom subsets formed by power residues, *Unif. Distrib. Theory* **2** (2007), 73–88.

[10] C. Dartyge, A. Sárközy and M. Szalay, On the pseudo-randomness of subsets related to primitive roots, *Combinatorica* **30** (2010), 139–162.

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

[12] D. Gomez and A. Winterhof, Multiplicative character sums of Fermat quotients and pseudorandom sequences, *Period. Math. Hungar.* **64** (2012), 161–168.

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

[14] D. R. Heath-Brown, An estimate for Heilbronn's exponential sum, In: Analytic Number Theory, Vol. 2, *Birkhäuser Boston*, *Boston , MA*, 1996, 451–463.

[15] H. Liu and E. Song, A note on pseudorandom subsets formed by generalized cyclotomic classes, *Publ. Math. Debrecen* **85** (2014), 257–271.

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

[17] I. E. Shparlinski, Fermat quotients: exponential sums, value set and primitive roots, *Bull. Lond. Math. Soc.* **43** (2011), 1228–1238.

[18] I. E. Shparlinski, Character sums with Fermat quotients, *Q. J. Math.* **62** (2011), 1031–1043.

[19] I. E. Shparlinski, Bounds of multiplicative character sums with Fermat quotients of primes, *Bull. Aust. Math. Soc.* **83** (2011), 456–462.

[20] 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.

HUANING LIU
SCHOOL OF MATHEMATICS
NORTHWEST UNIVERSITY
XI'AN 710127, SHAANXI
P. R. CHINA

E-mail: hnliumath@hotmail.com

GUOTUO ZHANG
SCHOOL OF MATHEMATICS
NORTHWEST UNIVERSITY
XI'AN 710127, SHAANXI
P. R. CHINA

E-mail: 18700845764@163.com

(Received January 3, 2018; revised July 30, 2018)