Linear complexity of binary sequences derived from polynomial quotients

Zhixiong Chen[1,2] and Domingo Gómez-Pérez[3]

[1] Department of Mathematics, Putian University,
Putian, Fujian 351100, P.R. China
[2] State Key Laboratory of Information Security, Institute of Software
Chinese Academy of Sciences, Beijing 100049, P.R. China
ptczx@126.com
[3] University of Cantabria
Avd. Los Castros, s/n, Santander, Spain
domingo.gomez@unican.es
http://personales.unican.es/gomezd

Abstract. We determine the linear complexity of p^2-periodic binary threshold sequences derived from *polynomial quotient*, which is defined by the function $(u^w - u^{wp})/p \pmod p$. When $w = (p-1)/2$ and $2^{p-1} \not\equiv 1 \pmod{p^2}$, we show that the linear complexity is equal to one of the following values $\{p^2-1,\ p^2-p,\ (p^2+p)/2+1,\ (p^2-p)/2\}$, depending whether $p \equiv 1,\ -1,\ 3,\ -3 \pmod 8$. But it seems that the method can't be applied to the case of general w.

Keywords: Fermat quotients, polynomial quotients, finite fields, pseudorandom binary sequences, linear complexity, cryptography

1 Introduction

For an odd prime p and an integer u with $\gcd(u,p) = 1$, the *Fermat quotient* $q_p(u)$ *modulo* p 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 extend the definition,

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

An alternative definition of $q_p(u)$ is given by

$$q_p(u) \equiv \frac{u^{p-1} - u^{(p-1)p}}{p} \pmod p \tag{1}$$

for all u. There are several results which involve the distribution and structure of Fermat quotients $q_p(u)$ modulo p and it has numerous applications in computational and algebraic number theory, see [1, 2]. The papers [3–6] studied character sums with Fermat quotients and [7, 8] investigated the value sets of Fermat quotients. Even recently, Fermat quotients have been studied from the viewpoint of cryptography and dynamical systems, see [9–14].

Chen and Winterhof in [4] generalized the function (1) introducing a parameter $w \in \{1, \dots p-1\}$, to define

$$F_w(u) \equiv \frac{u^w - u^{wp}}{p} \pmod p, \qquad 0 \le F_w(u) \le p-1,\ u \ge 0, \tag{2}$$

which is called a *polynomial quotient modulo p*.

Du, Klapper and Chen used the construction of [11] for Fermat quotients to define a family of *binary threshold sequences* (e_u) by

$$e_u = \begin{cases} 0, & \text{if } 0 \le F_w(u) < p/2, \\ 1, & \text{otherwise,} \end{cases} \tag{3}$$

for $u \ge 0$, see [12]. We note that (e_u) is p^2-periodic since

$$F_w(u + kp) = F_w(u) + wku^{w-1} \pmod p. \tag{4}$$

Certain interesting properties have been investigated for (e_u) under some special conditions. If $w = p-1$, Chen, Ostafe and Winterhof considered the correlation measure and linear complexity profile of (e_u) using certain exponential sums in [11]. Chen, Hu and Du determined the *linear complexity* (see below for the definition) of (e_u) if 2 is a primitive root modulo p^2 in [10].

We recall that the *linear complexity* $L((s_u))$ of a T-periodic sequence (s_u) over the binary field $\mathbb{F}_2$ is the least order L of a linear recurrence relation over $\mathbb{F}_2$

$$s_{u+L} = c_{L-1}s_{u+L-1} + \cdots + c_1 s_{u+1} + c_0 s_u \quad \text{for } u \ge 0$$

which is satisfied by (s_u) and where $c_0 = 1, c_1, \dots, c_{L-1} \in \mathbb{F}_2$. The polynomial

$$M(x) = x^L + c_{L-1}x^{L-1} + \cdots + c_0 \in \mathbb{F}_2[x]$$

is called the *minimal polynomial* of (s_u). The *generating polynomial* of (s_u) is defined by

$$s(x) = s_0 + s_1 x + s_2 x^2 + \cdots + s_{T-1}x^{T-1} \in \mathbb{F}_2[x].$$

It is easy to see that

$$M(x) = (x^T - 1)/\gcd\left(x^T - 1,\ s(x)\right),$$

hence

$$L((s_u)) = T - \deg\left(\gcd(x^T - 1,\ s(x))\right), \tag{5}$$

which is the degree of the minimal polynomial, see [15–17] for a more detailed exposition.

Du, Klapper and Chen extended the corresponding results of [10] in [12] to the case of all $w \in \{1, \dots, p-1\}$ as the following theorem.

Theorem 1. *[12] Let (e_u) be the p^2-periodic binary sequence defined as in (3). If 2 is a primitive root modulo p^2, then the linear complexity of (e_u) is*

$$L((e_u)) = \begin{cases} p^2 - p, & \text{if } p \equiv 1 \pmod 4, \\ p^2 - 1, & \text{if } p \equiv 3 \pmod 4 \text{ and } w > 1, \\ p^2 - p + 1, & \text{if } p \equiv 3 \pmod 4 \text{ and } w = 1. \end{cases}$$

We have extended Theorem 1 in [9] for the case of $w = p-1$ under a more general condition of $2^{p-1} \not\equiv 1 \pmod{p^2}$. If 2 is a primitive root modulo p^2, then we always have $2^{p-1} \not\equiv 1 \pmod{p^2}$. But the converse is not true, because there do exist such primes p, e.g., $p = 43$. We find that the idea of [9] can help us to study the linear complexity of (e_u) under the condition of $w = (p-1)/2$ and $2^{p-1} \not\equiv 1 \pmod{p^2}$, as described in the following theorem.

Theorem 2. *Let (e_u) be the p^2-periodic binary sequence defined as in (3) with $w = (p-1)/2$. Assume that $2^{p-1} \not\equiv 1 \pmod{p^2}$ then,*

$$L((e_u)) = \begin{cases} p^2 - p \ \text{ or } \ (p^2-p)/2, & \text{if } p \equiv 1 \pmod 8, \\ p^2 - 1 \ \text{ or } \ (p^2+p)/2 + 1, & \text{if } p \equiv -1 \pmod 8, \\ p^2 - p, & \text{if } p \equiv -3 \pmod 8, \\ p^2 - 1, & \text{if } p \equiv 3 \pmod 8. \end{cases}$$

In order to prove the theorem, we need to introduce the following function,

$$H_w(u) \equiv u^{-w} F_w(u) \pmod p, \text{ with } 0 \le H_w(u) \le p-1,$$

if $\gcd(u,p) = 1$ and otherwise $H_w(u) = 0$, and define the (p^2-periodic) binary sequence (h_u) by

$$h_u = \begin{cases} 0, & \text{if } 0 \le H_w(u) < p/2, \\ 1, & \text{otherwise.} \end{cases} \tag{6}$$

We will study the linear complexity of (e_u) in terms of (h_u) if $w = (p-1)/2$.

2 Auxiliary Lemmas

From (2), it is easy to check that for $\gcd(uv,p) = 1$

$$(uv)^{-w} F_w(uv) \equiv u^{-w} F_w(u) + v^{-w} F_w(v) \pmod p, \tag{7}$$

see [4]. So according to (4) and (7), we have

$$H_w(u + kp) = H_w(u) + wku^{-1} \pmod p \tag{8}$$

if $\gcd(u,p) = 1$, and

$$H_w(uv) \equiv H_w(u) + H_w(v) \pmod p \tag{9}$$

if $\gcd(uv,p)=1$. Let

$$D_l=\{u: 0\le u\le p^2-1,\ \gcd(u,p)=1,\ H_w(u)=l\}$$

for $l=0,1,\dots,p-1$ and $P=\{kp: 0\le k\le p-1\}$, one can give an equivalent definition for the sequence (h_u) in (6),

$$h_u=\begin{cases}0, & \text{if } u\in D_0\cup\cdots\cup D_{(p-1)/2}\cup P,\\ 1, & \text{if } u\in D_{(p+1)/2}\cup\cdots\cup D_{p-1},\end{cases}\qquad 0\le u\le p^2-1.$$

For $l\in\{0,\dots,p-1\}$, we define

$$Q_l=\left\{u\in D_l:\left(\frac{u}{p}\right)=1\right\}\quad\text{and}\quad N_l=\left\{u\in D_l:\left(\frac{u}{p}\right)=-1\right\},$$

here and hereafter $\left(\frac{\cdot}{p}\right)$ denotes the Legendre symbol. We use the notation $aD_l=\{ab \pmod{p^2}: b\in D_l\}$. Using (8) and (9) we have the following basic facts:

1. $aD_l=D_{l+l' \pmod p}$ if $a\in D_{l'}$.
2. $aQ_l=Q_{l+l' \pmod p}$ if $a\in Q_{l'}$.
3. $aN_l=N_{l+l' \pmod p}$ if $a\in Q_{l'}$.
4. $aQ_l=N_{l+l' \pmod p}$ if $a\in N_{l'}$.
5. $aN_l=Q_{l+l' \pmod p}$ if $a\in N_{l'}$.
6. For $l\in\{0,\dots,p-1\}$, $|D_l|$, the cardinality of D_l, is equal to $p-1$. $|Q_l|=|N_l|=(p-1)/2$.

We note that Facts 1-5 can be easily obtained from (9). Fact 1 implies that the cardinality of D_l is equal to the cardinality of $D_{l'}$, for any pair l,l'. So each D_l has $p-1$ elements for $l\in\{0,\dots,p-1\}$. On the other hand, the following equality holds

$$\{a \pmod p : a\in D_l\}=\{1,2,\dots,p-1\},\quad l\in\{0,1,\dots,p-1\}$$

by (8). In the set $\{1,2,\dots,p-1\}$, there are $(p-1)/2$ quadratic residues and $(p-1)/2$ quadratic nonresidues, respectively. So both Q_l and N_l contain $(p-1)/2$ elements.

The definition of the sets $D_l,\ Q_l,\ N_l$ allows us to show a relationship between the sequences (e_u) and (h_u) for $w=(p-1)/2$. According to the previous definitions, we have

$$e_u=\begin{cases}h_u, & \text{if } u\in P\cup D_0,\\ h_u, & \text{if } u\in Q_1\cup Q_2\cup\cdots\cup Q_{p-1},\\ h_u+1, & \text{if } u\in N_1\cup N_2\cup\cdots\cup N_{p-1}.\end{cases}$$

The reason is that when $w=(p-1)/2$, we have

$$H_{\frac{p-1}{2}}(u)\equiv\left(\frac{u}{p}\right)F_{\frac{p-1}{2}}(u)\pmod p.$$

This implies a relation between the generating polynomials of the sequences (e_u) and (h_u). Define

$$D_l(x) = \sum_{u\in D_l} x^u \in \mathbb{F}_2[x], \quad Q_l(x) = \sum_{u\in Q_l} x^u \in \mathbb{F}_2[x], \quad N_l(x) = \sum_{u\in N_l} x^u \in \mathbb{F}_2[x]$$

for $l \in \{0, \dots, p-1\}$. We see that the generating polynomial of (h_u) is

$$h(x) = \sum_{u=0}^{p^2-1} h_u x^u = \sum_{l=\frac{p+1}{2}}^{p-1} D_l(x) \in \mathbb{F}_2[x]$$

and the generating polynomial of (e_u) is

$$e(x) = \sum_{u=0}^{p^2-1} e_u x^u = h(x) + \sum_{l=1}^{p-1} N_l(x) \in \mathbb{F}_2[x].$$

Below we will consider the common roots of $e(x)$ and $x^{p^2}-1$. The number of the common roots will lead to the values of linear complexity of (e_u) by (5).

In the following, let d be the multiplicative order of 2 modulo p^2, i.e., d is the least positive integer such that $2^d \equiv 1 \pmod{p^2}$. Let $\mathbb{F}_{2^d}$ be the field of order 2^d and $\beta \in \mathbb{F}_{2^d}$ a primitive p^2-th root of unity. We note that most calculations below are mainly performed in finite fields with characteristic two. In the context, we denote by $\mathbb{Z}_p = \{0, 1, \dots, p-1\}$ (respectively $\mathbb{Z}_{p^2} = \{0, 1, \dots, p^2-1\}$) the residue class ring modulo p (respectively p^2) and by $\mathbb{Z}^*_{p^2}$ the unit group of $\mathbb{Z}_{p^2}$.

Lemma 1. *Let $\beta \in \mathbb{F}_{2^d}$ be a primitive p^2-th root of unity. We have*

$$e(\beta^n) = \begin{cases} 0, & \text{if } n = 0, \\ \frac{p-1}{2}, & \text{if } n = kp, \ k = 1, \dots, p-1. \end{cases}$$

Proof. If $n = 0$, we have $e(\beta^0) = h(1) + \sum\limits_{l=1}^{p-1} N_l(1) = \frac{(p-1)^2}{2} + \frac{(p-1)^2}{2} \equiv 0 \pmod 2$.

For $n = kp$ with $1 \le k \le p-1$, we use the following facts to find the value of the sum,

$$\{a \pmod p : a \in D_l\} = \mathbb{Z}_p \quad \text{and} \quad \{a \pmod p : a \in N_l\} = N$$

where N is the set of quadratic nonresidues of $\mathbb{Z}_p$. Using the notation $N(x) = \sum\limits_{u\in N} x^u$, we find

$$\begin{aligned} h(\beta^{kp}) = \sum_{l=\frac{p+1}{2}}^{p-1} \sum_{u\in D_l} \beta^{kpu} &= \sum_{l=\frac{p+1}{2}}^{p-1} \sum_{u\in D_l} (\beta^{pk})^u \\ &= \sum_{l=\frac{p+1}{2}}^{p-1} (\beta^{pk} + \beta^{2pk} + \cdots + \beta^{(p-1)pk}) = \frac{p-1}{2} \end{aligned}$$

and hence

$$
\begin{aligned}
e(\beta^{kp}) = h(\beta^{kp}) + \sum_{l=1}^{p-1} N_l(\beta^{kp}) &= \frac{p-1}{2} + \sum_{l=1}^{p-1} N(\beta^{kp}) \\
&= \frac{p-1}{2} + (p-1)\sum_{u\in N} \beta^{kup} = \frac{p-1}{2}.
\end{aligned}
$$

With this remark, we finish the proof.

Lemma 2. *Let $\beta \in \mathbb{F}_{2^d}$ be a primitive p^2-th root of unity. For all $n \in \mathbb{Z}_{p^2}^*$, we have $\sum\limits_{l=0}^{p-1} N_l(\beta^n) = 0$.*

Proof. If $a : 0 < a < p$ is a quadratic nonresidue modulo p, we find that $a + kp$ is also a quadratic nonresidue modulo p for all $0 \le k \le p-1$. So we have

$$
\sum_{l=0}^{p-1} N_l(\beta^n) = \sum_{\substack{a=1 \\ (\frac{a}{p})=-1}}^{p-1} \sum_{k=0}^{p-1} \beta^{n(a+kp)} = \sum_{\substack{a=1 \\ (\frac{a}{p})=-1}}^{p-1} \beta^{na} \sum_{k=0}^{p-1} \beta^{nkp}.
$$

This finishes the proof.

The next lemma is a technical lemma, which will be used in the proof of the main theorem.

Lemma 3. *Let $\beta \in \mathbb{F}_{2^d}$ be a primitive p^2-th root of unity. If $2 \in D_{\ell_0}$ for some $1 \le \ell_0 \le p-1$, we have $D_l(\beta^n) \neq 0$ for all $0 \le l \le p-1$ and $n \in \mathbb{Z}_{p^2}^*$.*

Proof. Since $2 \in D_{\ell_0}$, i.e., $H_{\frac{p-1}{2}}(2) = \ell_0$, by (9) we have $H_{\frac{p-1}{2}}(2^j) \equiv j\ell_0 \pmod p$ and hence each D_l $(0 \le l \le p-1)$ exactly contain one element $2^j \pmod{p^2}$ for $0 \le j \le p-1$.

Now we show $D_l(\beta^n) \neq 0$ for all $0 \le l \le p-1$ and $n \in \mathbb{Z}_{p^2}^*$. Suppose that there is an $n_0 \in D_{i_0}$ for some $1 \le i_0 \le p-1$ such that $D_{l_0}(\beta^{n_0}) = 0$ for some $0 \le l_0 \le p-1$. Then we have

$$
0 = (D_{l_0}(\beta^{n_0}))^{2^j} = D_{l_0}(\beta^{2^j n_0}) = D_{l_0+i_0+j\ell_0 \pmod p}(\beta)
$$

for all $0 \le j \le p-1$. That is, for all $0 \le l \le p-1$, $D_l(\beta) = 0$. This implies $D_l(\beta^n) = 0$ for all $n \in \mathbb{Z}_{p^2}^*$, which indicates that, for any $l = 0, 1, \ldots, p-1$, the polynomial $D_l(x)$ has at least $p(p-1)$ many roots. However, the proof of [9, Lemma 4] told us that at least one $D_l(x)$ has degree $< p^2 - p$, which is a contradiction. Therefore, $D_l(\beta^n) \neq 0$ for all $0 \le l \le p-1$ and $n \in \mathbb{Z}_{p^2}^*$.

Lemma 4. *Let $\beta \in \mathbb{F}_{2^d}$ be a primitive p^2-th root of unity, then*

1. *If $2 \in Q_{\ell_0}$ for some $1 \le \ell_0 \le p-1$ and $e(\beta^{n_0}) = 0$ for some $n_0 \in \mathbb{Z}_{p^2}^*$, then there exist exactly $(p^2-p)/2$ many $n \in \mathbb{Z}_{p^2}^*$ such that $e(\beta^n) = 0$.*

2. If $2 \in N_{\ell_0}$ for some $1 \le \ell_0 \le p-1$, then $e(\beta^n) \ne 0$ for all $n \in \mathbb{Z}_{p^2}^*$.

Proof. It is easy to see that for all $n \in \mathbb{Z}_{p^2}^*$

$$e(\beta^n) = h(\beta^n) + \sum_{l=1}^{p-1} N_l(\beta^n) = h(\beta^n) + N_0(\beta^n)$$

by Lemma 2. Let

$$\Delta_j(x) = \sum_{l=\frac{p+1}{2}+j}^{p-1+j} D_{l \mod p}(x) \in \mathbb{F}_2[x], \quad j \in \{0, \ldots, p-1\}.$$

Then together with Facts 1, 3 and 5, we have

$$e(\beta^n) = h(\beta^n) + N_0(\beta^n) = \begin{cases} \Delta_l(\beta) + N_l(\beta), & \text{if } n \in Q_l, \\ \Delta_l(\beta) + Q_l(\beta), & \text{if } n \in N_l, \end{cases}$$

which indicates $e(\beta^m) \ne e(\beta^n)$ for $m \in Q_l$ and $n \in N_l$ by Lemma 3.

We suppose that $n_0 \in D_{i_0}$ for some $1 \le i_0 \le p-1$. If $n_0 \in Q_{i_0}$ and $2 \in Q_{\ell_0}$, then $2^j n_0 \in Q_{j\ell_0+i_0 \pmod p}$ for $0 \le j \le p-1$. We derive

$$\begin{aligned} e(\beta^n) &= \Delta_{j\ell_0+i_0 \pmod p}(\beta) + N_{j\ell_0+i_0 \pmod p}(\beta) \\ &= e(\beta^{2^j n_0}) = (e(\beta^{n_0}))^{2^j} = 0 \end{aligned}$$

for all $n \in Q_{j\ell_0+i_0 \pmod p}$ and hence $e(\beta^n) \ne 0$ for all $n \in N_{j\ell_0+i_0 \pmod p}$. So we have for $n \in \mathbb{Z}_{p^2}^*$

$$e(\beta^n) = 0 \quad \text{iff} \quad n \in Q_0 \cup Q_1 \cup \cdots \cup Q_{p-1}.$$

Similarly, if $n_0 \in N_{i_0}$ and $2 \in Q_{\ell_0}$, we have

$$e(\beta^n) = 0 \quad \text{iff} \quad n \in N_0 \cup N_1 \cup \cdots \cup N_{p-1}.$$

Thus we conclude that there exist $p(p-1)/2$ many $n \in \mathbb{Z}_{p^2}^*$ such that $e(\beta^n) = 0$ since both Q_l and N_l contain $(p-1)/2$ elements.

For the case of $2 \in N_{\ell_0}$, i.e., $\left(\frac{2}{p}\right) = -1$, if $e(\beta^{n_0}) = 0$ for some $n_0 \in Q_{i_0}$, then we have $2^p n_0 \in N_{i_0}$ and

$$e(\beta^{2^p n_0}) = (e(\beta^{n_0}))^{2^p} = 0,$$

and so $e(\beta^n) = 0$ for all $n \in N_{i_0} \cup Q_{i_0}$ $(= D_{i_0})$, a contradiction. So in this case, $e(\beta^n) \ne 0$ for all $n \in \mathbb{Z}_{p^2}^*$. Similarly, the assumption of $e(\beta^{n_0}) = 0$ for some $n_0 \in N_{i_0}$ will also lead to a contradiction.

3 Proof of Main Theorem and Final Remarks

Proof (Proof of Theorem 2). In order to use Lemmas 3 and 4, we first prove $H_{\frac{p-1}{2}}(2) \neq 0$ if $2^{p-1} \not\equiv 1 \pmod{p^2}$. Suppose that

$$2^{p-1} \equiv 1 + zp \pmod{p^2}$$

for some $0 < z < p$. According to the definition of $F_{\frac{p-1}{2}}(u)$, we have

$$\begin{aligned} F_{\frac{p-1}{2}}(4) &\equiv \frac{4^{\frac{p-1}{2}} - 4^{\frac{p-1}{2}p}}{p} \\ &\equiv \frac{2^{p-1} - 2^{(p-1)p}}{p} \\ &\equiv \frac{(1+zp) - (1+zp)^p}{p} \\ &\equiv z \not\equiv 0 \pmod{p}. \end{aligned}$$

So we derive

$$H_{\frac{p-1}{2}}(2) \equiv 2^{-1} H_{\frac{p-1}{2}}(4) \equiv 2^{-1} \left(\frac{4}{p}\right) F_{\frac{p-1}{2}}(4) \not\equiv 0 \pmod{p}.$$

Now we suppose that $\left(\frac{2}{p}\right) = 1$. In this case, $p \equiv \pm 1 \pmod 8$. If $p \equiv 1 \pmod 8$, we have $e(\beta^n) = 0$ if $n \in \{kp : 0 \leq k \leq p-1\}$ by Lemma 1 and there are either no numbers in $\mathbb{Z}_{p^2}^*$ or $p(p-1)/2$ many $n \in \mathbb{Z}_{p^2}^*$ such that $e(\beta^n) = 0$ by Lemma 4. Then the number of the common roots of $e(x)$ and $x^{p^2} - 1$ is either p or $(p^2+p)/2$ and hence the linear complexity of (e_u) is $p^2 - p$ or $(p^2-p)/2$. For the case of $p \equiv -1 \pmod 8$, the result follows similarly.

Under the condition of $\left(\frac{2}{p}\right) = -1$, it can be proved in a similar way.

In this article, we estimate possible values of linear complexity of certain binary sequences of period p^2 defined by polynomial quotients F_w with $w = (p-1)/2$ under the condition of $2^{p-1} \not\equiv 1 \pmod{p^2}$. The results depend on whether $p \equiv \pm 1$ or $\pm 3 \pmod 8$, respectively. Our research partially extends results of linear complexity of the corresponding binary sequences when 2 is a primitive root modulo p^2 in [12]. But it seems that the method can't be applied to the case of general w. The reason is the relationship $H_{(p-1)/2}(u) \equiv \{F_{(p-1)/2}(u), -F_{(p-1)/2}(u)\} \pmod{p}$ does not hold for other values of w.

The calculation of linear complexity of (e_u) was done for all primes $p < 200$ and $\left(\frac{2}{p}\right) = 1$. The experiment results illuminate that the linear complexity only equals $p^2 - p$ or $p^2 - 1$. So we might ask that whether there exist primes p such that linear complexity equals $(p^2-p)/2$ or $(p^2+p)/2 + 1$.

We finally note that, our theorem covers most primes (possessing the property of $2^{p-1} \not\equiv 1 \pmod{p^2}$) since the primes p satisfying $2^{p-1} \equiv 1 \pmod{p^2}$ are very rare. To date the only known such primes are $p = 1093$ and $p = 3511$ and it was reported that there are no new such primes $p < 4 \times 10^{12}$, see [18].

Acknowledgements

The authors wish to thank Xiaoni Du, Gottlieb Pirsic and Arne Winterhof for valuable comments.

Z.X.C. was partially supported by the National Natural Science Foundation of China under grant No.61170246, the Program for New Century Excellent Talents in Fujian Province University of China under grant No.JK2010047 and the Open Funds of State Key Laboratory of Information Security (Chinese Academy of Sciences) under grant No.01-01-1. D. G-P was partially supported by the Spanish Ministry of Economy, Division of Innovation and Research under project No. TIN2011-27479-C04-04.

References

1. Ernvall, R., Metsänkylä, T.: On the p-divisibility of Fermat quotients. Math. Comp. **66**(219) (1997) 1353–1365
2. Granville, A.: Some conjectures related to Fermat's last theorem. In: Number theory (Banff, AB, 1988). de Gruyter, Berlin (1990) 177–192
3. Chang, M.C.: Short character sums with Fermat quotients. Acta Arith. **152**(1) (2012) 23–38
4. Chen, Z., Winterhof, A.: Additive character sums of polynomial quotients. Preprint
5. Shparlinski, I.: Character sums with Fermat quotients. Quart. J. Math. Oxford. **62**(4) (2011) 1031–1043
6. Shparlinski, I.E.: Bounds of multiplicative character sums with Fermat quotients of primes. Bull. Aust. Math. Soc. **83**(3) (2011) 456–462
7. Shparlinski, I.E.: On the value set of Fermat quotients. Proc. Amer. Math. Soc. **140**(140) (2011) 1199–1206
8. Shparlinski, I.E.: Fermat quotients: exponential sums, value set and primitive roots. Bull. Lond. Math. Soc. **43**(6) (2011) 1228–1238
9. Chen, Z., Du, X.: On the linear complexity of binary threshold sequences derived from Fermat quotients. Des. Codes Cryptogr. (In press)
10. Chen, Z., Hu, L., Du, X.: Linear complexity of some binary sequences derived from Fermat quotients. China Communications **9**(2) (2012) 105–108
11. Chen, Z., Ostafe, A., Winterhof, A.: Structure of pseudorandom numbers derived from Fermat quotients. In: Arithmetic of finite fields. Volume 6087 of Lecture Notes in Comput. Sci. Springer, Berlin (2010) 73–85
12. Du, X., Klapper, A., Chen, Z.: Linear complexity of pseudorandom sequences generated by Fermat quotients and their generalizations. Inf. Proc. Letters **112**(6) (2012) 233 – 237
13. Gomez, D., Winterhof, A.: Multiplicative character sums of fermat quotients and pseudorandom sequences. Period. Math. Hungar. (In press)
14. Ostafe, A., Shparlinski, I.E.: Pseudorandomness and dynamics of Fermat quotients. SIAM J. Discrete Math. **25**(1) (2011) 50–71
15. Lidl, R., Niederreiter, H.: Finite fields. Second edn. Volume 20 of Encyclopedia of Mathematics and its Applications. Cambridge University Press, Cambridge (1997)
16. Meidl, W., Niederreiter, H.: Linear complexity, k-error linear complexity, and the discrete Fourier transform. J. Complexity **18**(1) (2002) 87–103

17. Winterhof, A.: A note on the linear complexity profile of the discrete logarithm in finite fields. In: Coding, cryptography and combinatorics. Volume 23 of Progr. Comput. Sci. Appl. Logic. Birkhäuser, Basel (2004) 359–367
18. Crandall, R., Dilcher, K., Pomerance, C.: A search for Wieferich and Wilson primes. Math. Comp. **66**(217) (1997) 433–449