Information Processing Letters 112 (2012) 604–609

Contents lists available at SciVerse ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

Linear complexity of binary sequences derived from Euler quotients with prime-power modulus

Xiaoni Du [a,b], Zhixiong Chen [c,d,*], Lei Hu [d]

[a] College of Mathematics and Information Science, Northwest Normal University, Lanzhou, Gansu 730070, PR China
[b] State Key Lab. of Integrated Service Networks, Xidian University, Xi'an, Shaanxi 710071, PR China
[c] Department of Mathematics, Putian University, Putian, Fujian 351100, PR China
[d] State Key Laboratory of Information Security, Graduate School of Chinese Academy of Sciences, Beijing 100049, PR China

ARTICLE INFO

Article history:
Received 3 February 2012
Received in revised form 16 April 2012
Accepted 23 April 2012
Available online 15 May 2012
Communicated by D. Pointcheval

Keywords:
Euler quotients
Fermat quotients
Pseudorandom binary sequences
Linear complexity
Cryptography

ABSTRACT

We extend the definition of binary threshold sequences from Fermat quotients to Euler quotients modulo p^r with odd prime p and $r \geqslant 1$. Under the condition of $2^{p-1} \not\equiv 1 \pmod{p^2}$, we present exact values of the linear complexity by defining cyclotomic classes modulo p^n for all $1 \leqslant n \leqslant r$. The linear complexity is very close to the period and is of desired value for cryptographic purpose. We also present a lower bound on the linear complexity for the case of $2^{p-1} \equiv 1 \pmod{p^2}$.

1. Introduction

For an odd prime p, integers $r \geqslant 1$ and u with $\gcd(u,p)=1$, the *Euler quotient* $Q_{p^r}(u)$ *modulo* p^r is defined as the unique integer with

$$Q_{p^r}(u) \equiv \frac{u^{\varphi(p^r)}-1}{p^r} \pmod{p^r},$$
$$0 \leqslant Q_{p^r}(u) \leqslant p^r - 1,$$

where $\varphi(-)$ is the Euler totient function, and we also define

$$Q_{p^r}(kp) = 0, \quad k \in \mathbb{Z}.$$

See, e.g., [1,5,14] for details.

If $r=1$, $Q_p(u)$ is just the *Fermat quotient* studied in [7,9,13,15–18] and references therein. More recently, Fermat quotients are studied from the viewpoint of cryptography, see [2–4,6,8,13].

Motivated by the previous work [2–4], we define a family of binary sequences (e_u) by using the Euler quotient $Q_{p^r}(u)$ by

$$e_u = \begin{cases} 0, & \text{if } 0 \leqslant Q_{p^r}(u)/p^r < \frac{1}{2}, \\ 1, & \text{if } \frac{1}{2} \leqslant Q_{p^r}(u)/p^r < 1. \end{cases} \tag{1}$$

We note that (e_u) is p^{r+1}-periodic since $Q_{p^r}(u)$ is a p^{r+1}-periodic sequence modulo p^r by the fact

$$Q_{p^r}(u+kp^r) \equiv Q_{p^r}(u) - kp^{r-1}u^{-1} \pmod{p^r} \tag{2}$$

for any integer k and u with $\gcd(u,p)=1$. In fact, for such u, we have

$$Q_{p^r}(u+kp^r) \equiv \frac{(u+kp^r)^{\varphi(p^r)}-1}{p^r}$$

* Corresponding author at: Department of Mathematics, Putian University, Putian, Fujian 351100, PR China.
E-mail addresses: ymLdxn@126.com (X. Du), ptczx@126.com (Z. Chen), hulei@gucas.ac.cn (L. Hu).

0020-0190/$ – see front matter
http://dx.doi.org/10.1016/j.ipl.2012.04.011

$$\begin{aligned}
&\equiv \frac{u^{\varphi(p^r)}-1}{p^r} + k\varphi(p^r)u^{\varphi(p^r)-1} \\
&\quad + kp^r\varphi(p^r)(\varphi(p^r)-1)u^{\varphi(p^r)-2}/2 + \cdots \\
&\quad + (kp^r)^{\varphi(p^r)-1} \\
&\equiv \frac{u^{\varphi(p^r)}-1}{p^r} + k\varphi(p^r)u^{\varphi(p^r)-1} \\
&\equiv Q_{p^r}(u) - kp^{r-1}u^{-1} \pmod{p^r}.
\end{aligned}$$

For $r = 1$, linear complexity of (e_u) defined in (1) was investigated in [2]. The linear complexity is considered as a primary quality measure for periodic sequences and plays an important role in applications of sequences in cryptography. A low linear complexity has turned out to be undesirable for cryptographical applications. 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 $\mathbb{F}_2$

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

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

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

hence

$$L((s_u)) = T - \deg(\gcd(x^T - 1, s(x))), \tag{3}$$

which is the degree of the minimal polynomial, see [11,19] for a more detailed exposition.

We will extend the result of [2] to show the following theorem.

Theorem 1. *Let (e_u) be the p^{r+1}-periodic binary sequence defined as in Eq. (1). If $2^{p-1} \not\equiv 1 \pmod{p^2}$, then the linear complexity $L((e_u))$ of (e_u) satisfies*

$$L((e_u)) = \begin{cases} p^{r+1} - p, & \text{if } p \equiv 1 \pmod 4, \\ p^{r+1} - p, & \text{if } p \equiv 3 \pmod 4 \text{ and } r \text{ is even}, \\ p^{r+1} - 1, & \text{if } p \equiv 3 \pmod 4 \text{ and } r \text{ is odd}. \end{cases}$$

2. Auxiliary lemmas

In order to prove the theorem, we will define a partition of the residue class ring modulo p^{n+1} with respect to the Euler quotient $Q_{p^n}(u)$ for $1 \leqslant n \leqslant r$. We denote by $\mathbb{Z}_{p^n} = \{0, 1, \ldots, p^n - 1\}$ the residue class ring modulo p^n and by $\mathbb{Z}^*_{p^n}$ the unit group of $\mathbb{Z}_{p^n}$ for $n \geqslant 1$. Let

$$D_l^{(n)} = \{u\colon 0 \leqslant u \leqslant p^{n+1} - 1,\ \gcd(u, p) = 1,\ Q_{p^n}(u) = l\}$$

for $l = 0, 1, \ldots, p^n - 1$ and $n \geqslant 1$. Thus, one can define (e_u) equivalently by

$$e_u = \begin{cases} 0, & \text{if } u \in D_0^{(r)} \cup \cdots \cup D^{(r)}_{(p^r-1)/2} \cup p\mathbb{Z}_{p^r}, \\ 1, & \text{if } u \in D^{(r)}_{(p^r+1)/2} \cup \cdots \cup D^{(r)}_{p^r-1}, \end{cases}$$
$$0 \leqslant u \leqslant p^{r+1} - 1,$$

where $p\mathbb{Z}_{p^r} = \{pa \pmod{p^r}\colon a = 0, 1, \ldots, p^r - 1\}$.

Lemma 1. *For all $n \geqslant 1$, let $uD_l^{(n)} = \{uv \pmod{p^{n+1}}\colon v \in D_l^{(n)}\}$. If $u \in D_{l'}^{(n)}$, then we have*

$$uD_l^{(n)} = D^{(n)}_{l+l' \pmod{p^n}},$$

where $0 \leqslant l, l' \leqslant p^n - 1$.

Proof. It is easy to get the desired result from the fact that

$$Q_{p^n}(uv) \equiv Q_{p^n}(u) + Q_{p^n}(v) \pmod{p^n} \tag{4}$$

for integers u, v with $\gcd(uv, p) = 1$, see [1]. □

Lemma 2. (i) *For $n' \geqslant n \geqslant 1$ and $0 \leqslant l' \leqslant p^{n'} - 1$, we have*

$$\{u \pmod{p^{n+1}}\colon u \in D_{l'}^{(n')}\} = D^{(n)}_{l' \pmod{p^n}}.$$

(ii) *For $n \geqslant 1$ and $0 \leqslant l \leqslant p^n - 1$, we have*

$$\{u \pmod p\colon u \in D_l^{(n)}\} = \{1, 2, \ldots, p - 1\}.$$

Proof. For all integers $n \geqslant 1$ by [1, Proposition 4.4 and Corollary 4.4], $Q_{p^n}(u)$ induces a group epimorphism

$$Q_{p^n}: \mathbb{Z}^*_{p^{n+1}} \to (\mathbb{Z}_{p^n}, +)$$

with kernel $D_0^{(n)}$ of order $p - 1$. So each $D_l^{(n)}$ has $p - 1$ elements for $1 \leqslant l < p^n$.

(i) It is sufficient to show the case of $n' = n + 1$, then the claim follows by induction.

For any $u \in D_{l'}^{(n+1)}$, by [1, Proposition 4.1] we have

$$Q_{p^n}(u) \equiv Q_{p^{n+1}}(u) \equiv l' \pmod{p^n},$$

which indicates that $u \pmod{p^{n+1}} \in D^{(n)}_{l' \pmod{p^n}}$ since p^{n+1} is a period of $Q_{p^n}(u)$. So we get

$$\{u \pmod{p^{n+1}}\colon u \in D_{l'}^{(n+1)}\} \subseteq D^{(n)}_{l' \pmod{p^n}}.$$

Then we show the cardinality of $\{u \pmod{p^{n+1}}\colon u \in D_{l'}^{(n+1)}\}$ is $p - 1$, equal to that of $D^{(n)}_{l' \pmod{p^n}}$. In fact, if $u \equiv u' \pmod{p^{n+1}}$ for $u, u' \in D_{l'}^{(n+1)}$, we suppose $u = u' + k_0 p^{n+1}$ for some $0 \leqslant k_0 < p$. We have

$$\begin{aligned}
l' &\equiv Q_{p^{n+1}}(u') \equiv Q_{p^{n+1}}(u) \equiv Q_{p^{n+1}}(u' + k_0 p^{n+1}) \\
&\equiv Q_{p^{n+1}}(u') - k_0 u^{-1} p^n \pmod{p^{n+1}},
\end{aligned}$$

which indicates that $k_0 = 0$ and $u = u'$. We prove the first result.