Math. J. Okayama Univ. **54** (2012), 1–32

SOME REMARKS ON LUCAS PSEUDOPRIMES

Noriyuki Suwa

Abstract. We present a way of viewing Lucas pseudoprimes, Euler-Lucas pseudoprimes and strong Lucas pseudoprimes in the context of group schemes. This enables us to treat the Lucas pseudoprimalities in parallel to establish pseudoprimes, Euler pseudoprimes and strong pseudoprimes.

Introduction

Let p be a prime > 2. Then, as is well known, we have the following assertions:
(1)(Fermat) If a is an integer prime to p, then $a^{p-1} \equiv 1 \mod p$;
(2)(Euler) If a is an integer prime to p, then $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \mod p$;
(3) Put $p-1 = 2^s m$ with $(m,2) = 1$. If a is an integer prime to p, then either $a^m \equiv 1 \mod p$ or $a^{2^k m} \equiv -1 \mod p$ for some $k < s$.

These facts provide us with a convenient way to prove that an odd integer n is composite. That is to say, n is verified to be composite if a statement fails for n among those above mentioned. The repeated squaring method is very effective to perform the required exponentiation. In particular, the assertion (3) is a basis for the Strong Probale Prime Test or the Miller-Rabin Test ([8],[10]), which is recognized as rapid and accurate enough to generate an industrial-grade prime ([3, Ch.III, 5]). Examining the accuracy of probable prime tests, we arrive at the notion of pseudoprimality.

Let n be an odd composite and a an integer prime to n.
(1) n is called a *pseudoprime* base to a if $a^{n-1} \equiv 1 \mod n$;
(2) n is called an *Euler pseudoprime* base to a if $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \mod n$;
(3) Put $n-1 = 2^s m$ with $(m,2) = 1$. Then n is called a *strong pseudoprime* base to a if either $a^m \equiv 1 \mod n$ or $a^{2^k m} \equiv -1 \mod n$ for some $k < s$.

Besides the Miller-Rabin Test, there are proposed several probable prime tests and defined several notions of pseudoprimality. In this article, we reformulate Lucas pseudoprimes, Euler-Lucas pseudoprimes and strong Lucas pseudoprimes in the context of group schemes. It would be profitable to

Mathematics Subject Classification. Primary 11Y11; Secondary 14L15.
Key words and phrases. primality test, group scheme.
Partially supported by The Research on Security and Reliability in Electronic Society, Chuo University 21st Century COE Program.

view these pseudoprimalities using the language of group schemes because the ideas then seem much clearer, to use a phrase at the beginning of [3, Ch.III, 6]: it is profitable to view this pseudoprime construct using the language of finite fields, not just to be fashionable, but because the ideas then seem less ad hoc. It would narrow a way to reject the language of group schemes though it is not so popular yet. We use here only elementary facts on affine group schemes, for example, the contents in the first two chapters of the introductory book [Waterhouse, 13].

The main result is stated as Theorem 3.4, and the following assertion is the key for our argument.

Corollary 2.8. *Let P, Q and D be non zero integers, and let n be an odd integer > 1 with $(n, DQ) = 1$ and $P^2 - 4Q \equiv D \mod n$. Put*

$$\xi = \Big(\frac{D+2Q}{2Q}, \frac{P}{2Q}\Big) \in U(D)(\mathbb{Z}/n\mathbb{Z}).$$

Then:
(1) *n is a Lucas pseudoprime with respect to (P, Q) if and only if $\xi^{n-\varepsilon(n)} = I$ in $U(D)(\mathbb{Z}/n\mathbb{Z})$;*
(2) *n is an Euler-Lucas pseudoprime with respect to (P, Q) if and only if either $\Big(\frac{Q}{n}\Big) = 1$ and $\xi^{\frac{n-\varepsilon(n)}{2}} = I$, or $\Big(\frac{Q}{n}\Big) = -1$ and $\xi^{\frac{n-\varepsilon(n)}{2}} = -I$ in $U(D)(\mathbb{Z}/n\mathbb{Z})$;*
(3) *n is a strong Lucas pseudoprime with respect to (P, Q) if and only if $\xi^m = I$ or $\xi^{2^k m} = -I$ for some $k < s$ in $U(D)(\mathbb{Z}/n\mathbb{Z})$. Here $n - \varepsilon(n) = 2^s m$ with $(m, 2) = 1$.*
(A definition of $U(D)(\mathbb{Z}/n\mathbb{Z})$ is mentioned in 2.1. We denote by I the unit of the group $U(D)(\mathbb{Z}/n\mathbb{Z})$.)

Now we explain the organization of the article. The description is expository and self-contained for the reader's convenience. In the Section 1, we recall elementary facts on Lucas sequences and the definition of Lucas pseudoprimes, Euler-Lucas pseudoprimes and strong Lucas pseudoprimes. In the Section 2, we introduce some affine group schemes and refomulate the Lucas pseudoprimalities by the language of group schemes. The main theorem is stated in the Section 3, and proved in the Section 4. It should be mentioned that the main theorem is a reformulation of results in the preceding works [1], [2], [15] except the formula for $|\tilde{B}_{e\ell psp}|$. However it would be allowed to emphasize that the arguments in the preceding works are unified by the language of one-dimensional tori. In the Section 5, several consequences are presented for the main result.

We conclude the article, mentioning relations between Lucas pseudoprimes and Frobenius pseudoprimes defined by Grantham ([4], [5]) in the

Section 6. For example, the following assertion would reveal a part of interesting relations among various pseudoprimalities, some of which Grantham investigated in [5].

Proposition 6.7. *Let P, Q be integers $\neq 0$ with $D = P^2 - 4Q$ not a square, and let n be an odd composite with $(n, DQ) = 1$. Assume that n is a Frobenius pseudoprime with respect to (P, Q). Then n is an Euler pseudoprime to base Q if and only if n is an Euler-Lucas pseudoprime with respect to (P, Q).*

It would be worth while to verify in our context the probable prime tests proposed by Kida [7], to examine the deterministic prime tests proposed by Gurevich-Kunyavskii [6] and to analyze the Frobenius pseudoprimalities defined by Grantham [4], [5]. We refer to original papers [1], [2], [4], [5], [15] and monographs [3], [11] for further topics on the Lucas pseudoprimalities, for example, the distribution of Lucas pseudoprimes and the accuracy of probable prime tests related with the Lucas pseudoprimalities.

Notation

For a positive odd integer n and an integer a prime to n, $\left(\frac{a}{n}\right)$ denotes the Jacobi symbol.

$\mathbb{G}_{m,\mathbb{Z}}$**:** the multiplicative group scheme over $\mathbb{Z}$
G_D**,** $U(D)$**:** defined in 2.1
$\tilde{B}_{\ell psp}(n, D)$**,** $\tilde{B}_{e\ell psp}(n, D)$**,** $\tilde{B}_{s\ell psp}(n, D)$**:** defined in 3.3
$B_{psp}(n)$**,** $B_{epsp}(n)$**,** $B_{spsp}(n)$**:** defined in [9] and recalled in 3.7

For a group scheme G and a commutative ring R, $G(R)$ denotes the group of R-valued points of G. In particular, $R^\times = \mathbb{G}_m(R)$ stands for the multiplicative group of invertible elements of R.

1. Recall: Lucas pseudoprimalities

In the section, we fix non-zero integers P, Q with $P^2 - 4Q \neq 0$ and put $D = P^2 - 4Q$.

Definition 1.1. Let P, Q be integers $\neq 0$, and put $D = P^2 - 4Q$. We assume that $D \neq 0$. Let α, β denote the roots of the quadratic equation $t^2 - Pt + Q = 0$. We define sequences $\{U_n\}_{n\geq 0}$ and $\{V_n\}_{n\geq 0}$ by

$$U_n = U_n(P, Q) = \frac{\alpha^n - \beta^n}{\alpha - \beta},\ V_n = V_n(P, Q) = \alpha^n + \beta^n.$$

The sequence $\{U_n\}_{n\geq 0}$, $\{V_n\}_{n\geq 0}$ are called *Lucas sequences* associated to (P, Q).

The following assertions are verified immediately from the definition.

(1) $U_0 = 0$, $U_1 = 1$, $U_{n+2} - PU_{n+1} + QU_n = 0$, $V_0 = 2$, $V_1 = P$, $V_{n+2} - PV_{n+1} + QV_n = 0$.
(2) $V_n^2 - DU_n^2 = 4Q^n$.
(3) $2V_{n+m} = V_nV_m + DU_nU_m$, $2U_{n+m} = U_nV_m + V_nU_m$.
In particular,
(4) $V_{2n} = \frac{1}{2}(V_n^2 + DU_n^2) = V_n^2 - 2Q^n = DU_n^2 + 2Q^n$, $U_{2n} = U_nV_n$.

Moreover, the following assertion is concluded readily from the recurrence relations (1):

(5) Let p be a prime, and assume that $p \mid Q$. If $p \mid P$, then $p \mid U_n$ and $p \mid V_n$ for any $n > 1$. On the other hand, if $p \nmid P$, then $p \nmid U_n$ and $p \nmid V_n$ for any $n \geq 1$.

Lemma 1.2. *Let n be an odd integer > 1 with $(n, D) = 1$. If there exists $k > 1$ such that $U_k \equiv 0 \mod n$, then n is prime to Q.*

Proof. Assume that $(n, Q) > 1$. Let p be a prime divisor of (n, Q). By 1.1(5), if $p \nmid P$, then $p \nmid U_k$ for any $k > 1$, which is a contradiction to the assumption. On the other hand, if $p \mid P$, then $p \mid D$, which is a contradiction to $(n, D) = 1$.

The following statement is well known.

Theorem 1.3. *Let p be a prime > 2 with $p \nmid DQ$. Then:*

(1) *If $\left(\frac{D}{p}\right) = 1$, then $U_{p-1} \equiv 0 \mod p$ and $V_{p-1} \equiv 2 \mod p$. Furthermore, $U_{\frac{p-1}{2}} \equiv 0 \mod p$ if and only if $\left(\frac{Q}{p}\right) = 1$. Moreover, $V_{\frac{p-1}{2}} \equiv 0 \mod p$ if and only if $\left(\frac{Q}{p}\right) = -1$.*

(2) *If $\left(\frac{D}{p}\right) = -1$, then $U_{p+1} \equiv 0 \mod p$ and $V_{p+1} \equiv 2Q \mod p$. Furthermore, $U_{\frac{p+1}{2}} \equiv 0 \mod p$ if and only if $\left(\frac{Q}{p}\right) = 1$. Moreover, $V_{\frac{p+1}{2}} \equiv 0 \mod p$ if and only if $\left(\frac{Q}{p}\right) = -1$.*

Notation 1.4. For an odd integer $n > 1$ with $(n, D) = 1$, we put $\varepsilon(n) = \left(\frac{D}{n}\right)$.

Definition 1.5.([2, sec.1]) An odd composite n is called a *Lucas pseudoprime* with respect to (P, Q) if $(n, D) = 1$ and $U_{n-\varepsilon(n)} \equiv 0 \mod n$.

By Lemma 1.2, if n is a Lucas pseudoprime with respect to (P,Q), then n is prime to Q.

Definition 1.6.([2, sec.3]) An odd composite n is called an *Euler-Lucas pseudoprime* with respect to (P,Q) if $(n,DQ)=1$ and either $\left(\frac{Q}{n}\right)=1$, $U_{\frac{n-\varepsilon(n)}{2}}\equiv 0 \mod n$ or $\left(\frac{Q}{n}\right)=-1$, $V_{\frac{n-\varepsilon(n)}{2}}\equiv 0 \mod n$.

By the formula (4) in 1.1 and Lemma 1.2, we obtain the following assertion:

Proposition 1.7. *If n is an Euler-Lucas pseudoprime with respect to (P,Q), then n is a Lucas pseudoprime with respect to (P,Q).*

Lemma 1.8. *Let p be a prime >2 and $p\nmid D$. Let $p-\varepsilon(p)=2^s m$ with $(m,2)=1$. Then $U_m\equiv 0 \mod p$ or $V_{2^k m}\equiv 0 \mod p$ for some $k<s$.*

Proof. Combining the formulas $U_m V_m V_{2m}\cdots V_{2^{s-1}m}=U_{2^s m}$ and $U_{2^s m}=U_{p-\varepsilon(p)}\equiv 0 \mod p$, we obtain the result.

Definition 1.9.([2, sec.3]) An odd composite n is called a *strong Lucas pseudoprime* with respect to (P,Q) if either $U_m\equiv 0 \mod n$ or $V_{2^k m}\equiv 0 \mod n$ for some $k<s$. Here $n-\varepsilon(n)=2^s m$ with $(m,2)=1$.

Proposition 1.10.([2, Th.3]) *If n is a strong Lucas pseudoprime with respect to (P,Q), then n is an Euler-Lucas pseudoprime with respect to (P,Q).*

Proposition 1.11. *Let n be an odd integer >1 with $(n,Q)=1$. Assume that D is a square. Then there exists $a\in\mathbb{Z}$ such that $\beta a\equiv\alpha \mod n$. Furthermore, if n is a Lucas pseudoprime (resp. an Euler-Lucas pseudoprime, a strong Lucas pseudoprime) with respect to (P,Q), then n is a pseudoprime (resp. an Euler pseudoprime, a strong pseudoprime) to base a.*

Proof. By the assumption, we have $(\alpha,n)=(\beta,n)=1$ since $\alpha\beta=Q$. To verify the last statement, it is sufficient to note that

$$U_k\equiv 0 \mod n \Leftrightarrow \alpha^k\equiv\beta^k \mod n \Leftrightarrow a^k\equiv 1 \mod n;$$
$$V_k\equiv 0 \mod n \Leftrightarrow \alpha^k\equiv-\beta^k \mod n \Leftrightarrow a^k\equiv -1 \mod n.$$

2. Group schemes G_D, $U(D)$ and $G_{(D)}$

Throughout the sections hereafter, we fix a non-zero integer D. For an odd integer n prime to D, we put $\varepsilon(n)=\left(\frac{D}{n}\right)$. We adopt standard notations in [13] concerning to affine group schemes.

Definition 2.1. Let $D \in \mathbb{Z}$, and put

$$A_D = \mathbb{Z}[t]/(t^2 - D),$$

$$G_D = \prod_{A_D/\mathbb{Z}} \mathbb{G}_{m,A_D} = \operatorname{Spec} \mathbb{Z}[X, Y, \frac{1}{X^2 - DY^2}].$$

The group law of G_D is given by

$$\begin{aligned} \Delta &: (X, Y) \mapsto (X \otimes X + DY \otimes Y, X \otimes Y + Y \otimes X), \\ \varepsilon &: (X, Y) \mapsto (1, 0), \\ S &: (X, Y) \mapsto \big(\frac{X}{X^2 - DY^2}, \frac{-Y}{X^2 - DY^2}\big). \end{aligned}$$

Furthermore, a homomorphism of affine group schemes

$$\mathrm{Nr} : G_D = \operatorname{Spec} \mathbb{Z}[X, Y, \frac{1}{X^2 - DY^2}] \to \mathbb{G}_{m,\mathbb{Z}} = \operatorname{Spec} \mathbb{Z}[T, \frac{1}{T}]$$

is defined by

$$T \mapsto X^2 - DY^2 : \mathbb{Z}[T, \frac{1}{T}] \to \mathbb{Z}[X, Y, \frac{1}{X^2 - DY^2}].$$

Put now $U(D) = \operatorname{Ker}[\mathrm{Nr} : G_D \to \mathbb{G}_{m,\mathbb{Z}}]$. More precisely,

$$U(D) = \operatorname{Spec} \mathbb{Z}[X, Y]/(X^2 - DY^2 - 1),$$

and the group law of $U(D)$ is given by

$$\begin{aligned} \Delta &: (X, Y) \mapsto (X \otimes X + DY \otimes Y, X \otimes Y + Y \otimes X), \\ \varepsilon &: (X, Y) \mapsto (1, 0), \\ S &: (X, Y) \mapsto \big(\frac{X}{X^2 - DY^2}, \frac{-Y}{X^2 - DY^2}\big). \end{aligned}$$

The group scheme $U(D)$ is a torus over $\mathbb{Z}[\frac{1}{2D}]$.

In fact, put $A = \mathbb{Z}[\sqrt{D}, \frac{1}{2D}]$. Then an isomorphism of group schemes over A

$$U(D)_A = \operatorname{Spec} A[X, Y]/(X^2 - DY^2 - 1) \xrightarrow{\sim} \mathbb{G}_{m,A} = \operatorname{Spec} A[U, \frac{1}{U}]$$

is given by

$$U \mapsto X + \sqrt{D}Y : A[U, \frac{1}{U}] \to A[X, Y]/(X^2 - DY^2 - 1).$$

Furthermore the sequence of group schemes

$$0 \longrightarrow U(D) \longrightarrow G_D \xrightarrow{\mathrm{Nr}} \mathbb{G}_{m,\mathbb{Z}} \longrightarrow 0$$

is exact over $\mathbb{Z}[\frac{1}{2D}]$.

For the convenience, here is given a more concrete description of 2.1.

2.2. Let R be a commutative ring. Then we have

$$G_D(R) = (R[t]/(t^2 - D))^\times = \{(a, b) \in R^2 \ ; \ a^2 - Db^2 \text{ is invertible in } R\},$$

and the multiplication of $G_D(R)$ is given by

$$(a, b)(a', b') = (aa' + Dbb', ab' + a'b).$$

The unit of $G_D(R)$ is given by $(1, 0)$, and we have

$$(a, b)^{-1} = \big(\frac{a}{a^2 - Db^2}, -\frac{b}{a^2 - Db^2}\big).$$

Furthermore, for $\eta = (a, b) \in G_D(R)$, we have

$$\mathrm{Nr}(\eta) = a^2 - Db^2,$$

and

$$U_D(R) = \mathrm{Ker}[\mathrm{Nr} : G_D(R) \to \mathbb{G}_m(R) = R^\times] = \{(a, b) \in R^2 \ ; \ a^2 - Db^2 = 1\}.$$

Notation 2.3. Let R be a commutative ring. We shall denote the unit $(1, 0) \in U(D)(R) \subset G_D(R)$ by I. For $\eta = (a, b) \in G_D(R)$ and $c \in R^\times$, we denote $(ca, cb) \in G_D(R)$ by $c\eta$. In particular, $(-a, -b) \in G_D(R)$ is denoted by $-\eta$.

Let $\xi \in U(D)(R)$ and $c \in R^\times$. Then $c\xi \in U(D)(R)$ if and only if $c^2 = 1$.

2.4. The correspondence $c \mapsto cI$ defines an embedding of multiplicative groups $i_R : R^\times \to (R[t]/(t^2 - D))^\times$. The map i_R is represented by the homomorphism of group schemes

$$i : \mathbb{G}_{m,\mathbb{Z}} = \mathrm{Spec}\, \mathbb{Z}[T, \frac{1}{T}] \to G_D = \mathrm{Spec}\, \mathbb{Z}[X, Y, \frac{1}{X^2 - DY^2}]$$

defined by

$$(X, Y) \mapsto (T, 0) : \mathbb{Z}[X, Y, \frac{1}{X^2 - DY^2}] \to \mathbb{Z}[T, \frac{1}{T}].$$

A homomorphism of group schemes

$$\gamma : G_D = \mathrm{Spec}\, \mathbb{Z}[X, Y, \frac{1}{X^2 - DY^2}] \to U(D) = \mathrm{Spec}\, \mathbb{Z}[X, Y]/(X^2 - DY^2 - 1)$$

is defined by

$$(X, Y) \mapsto \Big(\frac{X^2 + DY^2}{X^2 - DY^2}, \frac{2XY}{X^2 - DY^2}\Big) :$$
$$\mathbb{Z}[X, Y]/(X^2 - DY^2 - 1) \to \mathbb{Z}[X, Y, \frac{1}{X^2 - DY^2}].$$

The sequence of group schemes

$$0 \longrightarrow \mathbb{G}_{m,\mathbb{Z}} \xrightarrow{i} G_D \xrightarrow{\gamma} U(D) \longrightarrow 0$$

is exact over $\mathbb{Z}[\frac{1}{2D}]$. Furthermore the composite of the embedding $U(D) \to G_D$ and $\gamma : G_D \to U(D)$ is the square map.

An endomorphism σ of group schemes $G_D = \operatorname{Spec} \mathbb{Z}[X, Y, \frac{1}{X^2 - DY^2}]$ is defined by

$$(X, Y) \mapsto (X, -Y) : \mathbb{Z}[X, Y, \frac{1}{X^2 - DY^2}] \to \mathbb{Z}[X, Y, \frac{1}{X^2 - DY^2}].$$

Let R be a ring and $\eta = (a, b) \in G_D(R)$. Then we have $\sigma(\eta) = (a, -b)$. By convention we denote $\sigma(\eta)$ also by $\bar{\eta}$. It is readily seen that $\eta\bar{\eta} = \operatorname{Nr}(\eta)\, I$. Furthermore, we have

$$\gamma(\eta) = \Big(\frac{a^2 + Db^2}{a^2 - Db^2}, \frac{2ab}{a^2 - Db^2}\Big) = \operatorname{Nr}(\eta)^{-1}\, \eta^2 = \eta\bar{\eta}^{-1}.$$

Lemma 2.5. *Let R be a commutative ring and $\eta \in G_D(R)$. Then:*
(1) *$\gamma(\eta) = I$ if and only if $\bar{\eta} = \eta$.*
(2) *$\gamma(\eta) = -I$ if and only if $\bar{\eta} = -\eta$.*

Proof. The assertion is a direct consequence of the formula $\gamma(\eta) = \eta\bar{\eta}^{-1}$.

Example 2.6. Let P, Q be integers $\neq 0$ with $D = P^2 - 4Q \neq 0$. Let $\{U_n\}_{n\geq 0}$, $\{V_n\}_{n\geq 0}$ denote the Lucas sequences associated to (P, Q). Then

$$\Big(\frac{V_k}{2}, \frac{U_k}{2}\Big) \in G_D(\mathbb{Z}[\frac{1}{2Q}])$$

since $V_k^2 - DU_k^2 = 4Q^k$. Moreover, we have

$$\Big(\frac{V_k}{2}, \frac{U_k}{2}\Big)\Big(\frac{V_l}{2}, \frac{U_l}{2}\Big) = \Big(\frac{V_{k+l}}{2}, \frac{U_{k+l}}{2}\Big)$$

in $G_D(\mathbb{Z}[\frac{1}{2Q}])$. In particular,

$$\Big(\frac{V_k}{2}, \frac{U_k}{2}\Big) = \Big(\frac{V_1}{2}, \frac{U_1}{2}\Big)^k = \Big(\frac{P}{2}, \frac{1}{2}\Big)^k.$$

Furthermore, we have

$$\gamma\Big(\frac{V_k}{2}, \frac{U_k}{2}\Big) = \Big(\frac{V_k^2 + DU_k^2}{4Q^k}, \frac{2V_kU_k}{4Q^k}\Big) = \Big(\frac{V_{2k}}{2Q^k}, \frac{U_{2k}}{2Q^k}\Big),$$

and therefore,

$$\Big(\frac{V_{2k}}{2Q^k}, \frac{U_{2k}}{2Q^k}\Big) = \Big(\frac{V_2}{2Q}, \frac{U_2}{2Q}\Big)^k = \Big(\frac{D + 2Q}{2Q}, \frac{P}{2Q}\Big)^k$$

in $U(D)(\mathbb{Z}[\frac{1}{2Q}])$.

Lemma 2.7. *Let P, Q and D be integers $\neq 0$, and let n be an odd integer > 1 with $(n, Q) = 1$ and $P^2 - 4Q \equiv D \mod n$. Put*

$$\xi = \Big(\frac{D+2Q}{2Q}, \frac{P}{2Q}\Big) \in U(D)(\mathbb{Z}/n\mathbb{Z}).$$

Then:

(1) $U_k \equiv 0 \mod n$ *if and only if* $\xi^k = I$ *in* $U(D)(\mathbb{Z}/n\mathbb{Z})$;

(2) $V_k \equiv 0 \mod n$ *if and only if* $\xi^k = -I$ *in* $U(D)(\mathbb{Z}/n\mathbb{Z})$.

Proof. Put $\eta = (P/2, 1/2) \in G_D(\mathbb{Z}/n\mathbb{Z})$. Then we have $\xi = \gamma(\eta)$. Combining Lemma 2.5 and the equality $\eta^k = (V_k/2, U_k/2)$ in $G_D(\mathbb{Z}/n\mathbb{Z})$, we can obtain the result.

Corollary 2.8. *Under the notation above, we assume that $(n, DQ) = 1$. Then*:

(1) *n is a Lucas pseudoprime with respect to (P, Q) if and only if $\xi^{n-\varepsilon(n)} = I$ in $U(D)(\mathbb{Z}/n\mathbb{Z})$;*

(2) *n is an Euler-Lucas pseudoprime with respect to (P, Q) if and only if either $\Big(\frac{Q}{n}\Big) = 1$ and $\xi^{\frac{n-\varepsilon(n)}{2}} = I$ or $\Big(\frac{Q}{n}\Big) = -1$ and $\xi^{\frac{n-\varepsilon(n)}{2}} = -I$ in $U(D)(\mathbb{Z}/n\mathbb{Z})$;*

(3) *n is a strong Lucas pseudoprime with respect to (P, Q) if and only if either $\xi^m = I$ or $\xi^{2^k m} = -I$ for some $k < s$ in $U(D)(\mathbb{Z}/n\mathbb{Z})$. Here $n - \varepsilon(n) = 2^s m$ with $(m, 2) = 1$.*

Remark 2.9. Let P, Q be integers $\neq 0$ with $D = P^2 - 4Q \neq 0$. Put

$$\eta = \Big(\frac{P}{2}, \frac{1}{2}\Big) \text{ and } \xi = \gamma(\eta) = \Big(\frac{P+2Q}{2Q}, \frac{P}{2Q}\Big).$$

Then:

(1) $Q^k \equiv 1 \mod n$ if and only if $\eta^{2k} = \xi^k$.

(2) $Q^k \equiv -1 \mod n$ if and only if $\eta^{2k} = -\xi^k$.

We conclude the section, giving a description on the group $U(D)(\mathbb{Z}/p^\alpha\mathbb{Z})$ for a prime power p^α. Corollary 2.11 has an importance in the proof of the main theorem.

Lemma 2.10. *Let p be a prime with $(p, 2D) = 1$. Then the sequence*

$$0 \to \mathrm{Ker}[U(D)(\mathbb{Z}_p) \to U(D)(\mathbb{F}_p)] \to U(D)(\mathbb{Z}_p) \to U(D)(\mathbb{F}_p) \to 0$$

is a splitting exact sequence, and $\mathrm{Ker}[U(D)(\mathbb{Z}_p) \to U(D)(\mathbb{F}_p)]$ *is isomorphic to the additive group $\mathbb{Z}_p$. Moreover,*

(1) *If* $\left(\frac{D}{p}\right) = 1$, *then* $U(D)(\mathbb{F}_p)$ *is a cyclic group of order* $p-1$.

(2) *If* $\left(\frac{D}{p}\right) = -1$, *then* $U(D)(\mathbb{F}_p)$ *is a cyclic group of order* $p+1$.

Proof. If $\left(\frac{D}{p}\right) = 1$, then $U(D) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is isomorphic to the multiplicative group $\mathbb{G}_{m,\mathbb{Z}_p}$. This implies the assertion.

On the other hand, if $\left(\frac{D}{p}\right) = -1$, then we have

$$U(D)(\mathbb{Z}_p) = \{\alpha \in \mathbb{Z}_p[\sqrt{D}]^\times \ ; \ \mathrm{Nr}_{\mathbb{Q}_p(\sqrt{D})/\mathbb{Q}_p}(\alpha) = 1\}.$$

Let $a \in p\mathbb{Z}_p$. Then we have

$$\exp a\sqrt{D} \in 1 + p\mathbb{Z}_p[\sqrt{D}]$$

and

$$\mathrm{Nr}_{\mathbb{Q}_p(\sqrt{D})/\mathbb{Q}_p}(\exp a\sqrt{D}) = 1.$$

Moreover the correspondence $a \mapsto \exp a\sqrt{D}$ gives rise to an isomorphism of groups

$$p\mathbb{Z}_p \xrightarrow{\sim} \mathrm{Ker}[U(D)(\mathbb{Z}_p) \to U(D)(\mathbb{F}_p)].$$

On the other hand, we have

$$U(D)(\mathbb{F}_p) = \{\alpha \in \mathbb{F}_p(\sqrt{D})^\times \ ; \ \mathrm{Nr}_{\mathbb{F}_p(\sqrt{D})/\mathbb{F}_p}(\alpha) = 1\}.$$

Hence $U(D)(\mathbb{F}_p)$ is a cyclic group of order $p+1$. Futhermore, since the quadratic extension $\mathbb{Q}_p(\sqrt{D})/\mathbb{Q}_p$ is unramified, the Teichmüller lifting gives a section of the reduction map $U(D)(\mathbb{Z}_p) \to U(D)(\mathbb{F}_p)$.

Corollary 2.11.([1, Th.3.1]) *Let* p *be a prime with* $(p, 2D) = 1$ *and* α *a positive integer. Then*:

(1) *If* $\left(\frac{D}{p}\right) = 1$, *then* $U(D)(\mathbb{Z}/p^\alpha\mathbb{Z})$ *is a cyclic group of order* $(p-1)p^{\alpha-1}$;

(2) *If* $\left(\frac{D}{p}\right) = -1$, *then* $U(D)(\mathbb{Z}/p^\alpha\mathbb{Z})$ *is a cyclic group of order* $(p+1)p^{\alpha-1}$.

Notation 2.12.([1, Sec.2]) For a positive integer n with $(n, 2D) = 1$, we define

$$\varphi_D(n) = \begin{cases} 1 & \text{if } n = 1 \\ |U(D)(\mathbb{Z}/n\mathbb{Z})| & \text{if } n > 1. \end{cases}$$

If $(n,m)=1$, then $\varphi_D(nm)=\varphi_D(n)\varphi_D(m)$. Moreover, if p is a prime, then

$$\varphi_D(p^\alpha)=\begin{cases}(p-1)p^{\alpha-1} & \text{if } \left(\frac{D}{p}\right)=1\\ (p+1)p^{\alpha-1} & \text{if } \left(\frac{D}{p}\right)=-1.\end{cases}$$

Hence, if D is a square, $\varphi_D(n)$ is nothing but the Euler function $\varphi(n)$ for n with $(n,2D)=1$.

Remark 2.13. (cf. [14]) Let D be an integer $\neq 0$. Then an affine group scheme $G_{(D)}$ is defined by

$$G_{(D)}=\operatorname{Spec}\mathbb{Z}[X,Y]/(X^2-DY^2-Y)$$

with the group structure:

$$\begin{aligned}\Delta &: X\mapsto X\otimes 1+1\otimes X+2DX\otimes Y+2DY\otimes X,\\ &\quad Y\mapsto Y\otimes 1+1\otimes Y+2DY\otimes Y+2X\otimes X,\\ \varepsilon &: X\mapsto 0,\ Y\mapsto 0,\\ S &: X\mapsto -X,\ Y\mapsto Y.\end{aligned}$$

The group scheme $G_{(D)}$ is smooth over $\mathbb{Z}$.

A surjective homomorphism of group schemes

$$\beta : G_D=\operatorname{Spec}\mathbb{Z}[X,Y,\frac{1}{X^2-DY^2}]\to G_{(D)}=\operatorname{Spec}\mathbb{Z}[X,Y]/(X^2-DY^2-Y)$$

is defined by

$$X\mapsto\frac{XY}{X^2-DY^2},\ Y\mapsto\frac{Y^2}{X^2-DY^2}:$$
$$\mathbb{Z}[X,Y]/(X^2-DY^2-Y)\to\mathbb{Z}[X,Y,\frac{1}{X^2-DY^2}].$$

Moreover,

$$X\mapsto T,\ Y\mapsto 0:\mathbb{Z}[X,Y,\frac{1}{X^2-DY^2}]/(XY,Y^2)\to\mathbb{Z}[T,\frac{1}{T}]$$

gives rise to an isomorphism

$$\begin{aligned}\mathbb{G}_{m,\mathbb{Z}}&=\operatorname{Spec}\mathbb{Z}[T,\frac{1}{T}]\\ &\xrightarrow{\sim}\operatorname{Ker}[\beta : G_D\to G_{(D)}]=\operatorname{Spec}\mathbb{Z}[X,Y,\frac{1}{X^2-DY^2}]/(XY,Y^2).\end{aligned}$$

Furthermore, a homomorphism of affine group schemes

$$\alpha : G_{(D)}=\operatorname{Spec}\mathbb{Z}[X,Y]/(X^2-DY^2-Y)$$

$$\to U(D) = \operatorname{Spec} \mathbb{Z}[X,Y]/(X^2 - DY^2 - 1)$$

is defined by

$$X \mapsto 2DY + 1,\ Y \mapsto 2X :$$
$$\mathbb{Z}[X,Y]/(X^2 - DY^2 - 1) \to \mathbb{Z}[X,Y]/(X^2 - DY^2 - Y).$$

Hence $\alpha : G_{(D)} \to U(D)$ is an isomorphism over $\mathbb{Z}[\frac{1}{2D}]$.

The homomorphism $\gamma : G_D \to U(D)$ is nothing but the composite of $\beta : G_D \to G_{(D)}$ and $\alpha : G_{(D)} \to U(D)$.

It would be suitable to define the function $\varphi_D(n)$ by

$$\varphi_D(n) = \begin{cases} 1 & \text{if } n = 1 \\ |G_{(D)}(\mathbb{Z}/n\mathbb{Z})| & \text{if } n > 1. \end{cases}$$

since the reduction map $G_{(D)}(\mathbb{Z}_p) \to G_{(D)}(\mathbb{Z}/p^\alpha\mathbb{Z})$ is surjective for any prime p and any $\alpha \geq 1$. This definition respects Arnault [1] since the homomorphism $\alpha : G_{(D)} \to U(D)$ is isomorphic over $\mathbb{Z}/n\mathbb{Z}$ with $(n, 2D) = 1$. Moreover, if p is a prime divisor of $2D$, then we have $\varphi_D(p^\alpha) = p^\alpha$.

It is also verified that:
(1) If $2 \nmid D$, then $G_{(D)}(\mathbb{Z}/2^\alpha\mathbb{Z})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-1}\mathbb{Z}$;
(2) If $D \equiv -3 \mod 9$, then $G_{(D)}(\mathbb{Z}/3^\alpha\mathbb{Z})$ is isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3^{\alpha-1}\mathbb{Z}$;
(3) If p is a prime divisor of D, then $G_{(D)}(\mathbb{Z}/p^\alpha\mathbb{Z})$ is isomorphic to $\mathbb{Z}/p^\alpha\mathbb{Z}$ except the case (2).

3. Statement of the theorem

Notation 3.1. Let D be an integer $\neq 0$ and p a prime > 2 with $(p, D) = 1$. For $\xi \in U(D)(\mathbb{F}_p)$, we define a symbol $\left[\frac{\xi}{p}\right]$ by

$$\left[\frac{\xi}{p}\right] = \begin{cases} 1 & \text{if } \xi^{\frac{p-\varepsilon(p)}{2}} = I, \\ -1 & \text{if } \xi^{\frac{p-\varepsilon(p)}{2}} = -I. \end{cases}$$

We have gotten an exact sequence

$$1 \longrightarrow \{\pm I\} \longrightarrow U(D)(\mathbb{F}_p) \overset{\text{square}}{\longrightarrow} U(D)(\mathbb{F}_p) \overset{[\frac{-}{p}]}{\longrightarrow} \{\pm 1\} \longrightarrow 1.$$

since $U(D)(\mathbb{F}_p)$ is a cyclic group of order $p - \varepsilon(p)$. Moreover, let n be an odd integer > 1 with $(n, D) = 1$. For $\xi \in U(D)(\mathbb{Z}/n\mathbb{Z})$, we define a symbol $\left[\frac{\xi}{n}\right]$ by

$$\left[\frac{\xi}{n}\right] = \prod_{p|n} \left[\frac{\xi}{p}\right]^{\operatorname{ord}_p n}.$$

Example 3.2. Let D be an integer $\neq 0$ and n an odd integer > 1 with $(n, D) = 1$. Let $P,\ Q \in \mathbb{Z}$. Assume that $(n, Q) = 1$ and $P^2 - 4Q \equiv D \mod n$. Put

$$\xi = \Big(\frac{D+2Q}{2Q}, \frac{P}{2Q}\Big).$$

As is noticed in Example 2.6, we have

$$\xi^k = \Big(\frac{V_{2k}}{2Q^k}, \frac{U_{2k}}{2Q^k}\Big).$$

Hence Theorem 1.3 implies that

$$\Big[\frac{\xi}{p}\Big] = \Big(\frac{Q}{p}\Big)$$

for each prime divisor p of n, and therefore,

$$\Big[\frac{\xi}{n}\Big] = \Big(\frac{Q}{n}\Big).$$

We shall introduce notations after Monier [9].

Definition 3.3. Let D be an integer $\neq 0$ and n an odd integer > 1 with $(n, D) = 1$. Let $n - \varepsilon(n) = 2^s m$ with $(m, 2) = 1$. We put:

$$\tilde{B}_{\ell psp}(n, D) = \{\xi \in U(D)(\mathbb{Z}/n\mathbb{Z})\ ;\ \xi^{n-\varepsilon(n)} = I\},$$

$$\tilde{B}_{e\ell psp}(n, D) = \left\{ \xi \in U(D)(\mathbb{Z}/n\mathbb{Z})\ ;\ \begin{array}{l} \Big[\frac{\xi}{n}\Big] = 1 \text{ and } \xi^{\frac{n-\varepsilon(n)}{2}} = I, \\ \text{or } \Big[\frac{\xi}{n}\Big] = -1 \text{ and } \xi^{\frac{n-\varepsilon(n)}{2}} = -I \end{array} \right\},$$

$$\tilde{B}_{s\ell psp}(n, D) = \{\xi \in U(D)(\mathbb{Z}/n\mathbb{Z})\ ;\ \xi^m = I, \text{ or } \xi^{2^k m} = -I \text{ for some } k < m\}.$$

We denote often $\tilde{B}_{\ell psp}(n, D)$, $\tilde{B}_{e\ell psp}(n, D)$, $\tilde{B}_{s\ell psp}(n, D)$ by $\tilde{B}_{\ell psp}$, $\tilde{B}_{e\ell psp}$, $\tilde{B}_{s\ell psp}$, respectively, when (n, D) is fixed.

Now we can state the main theorem.

Theorem 3.4. *Let D be an integer $\neq 0$ and n an odd integer > 1 with $(n, D) = 1$. Let r denote the number of distinct prime divisors of n, and put $n - \varepsilon(n) = 2^s m$ with $(m, 2) = 1$ and $\nu = \min_{p|n} \mathrm{ord}_2(p - \varepsilon(p))$. Then:*

(1) $\tilde{B}_{\ell psp} \supset \tilde{B}_{e\ell psp} \supset \tilde{B}_{s\ell psp}$.

(2) *$\tilde{B}_{\ell psp}$ is a subgroup of $U(D)(\mathbb{Z}/n\mathbb{Z})$ and*

$$|\tilde{B}_{\ell psp}| = \prod_{p|n} (n - \varepsilon(n), p - \varepsilon(p));$$

(3) $\tilde{B}_{e\ell psp}$ *is a subgroup of* $U(D)(\mathbb{Z}/n\mathbb{Z})$ *and*

$$|\tilde{B}_{e\ell psp}(n,D)|=\begin{cases} 2\prod_{p|n}\big(\frac{n-\varepsilon(n)}{2},p-\varepsilon(p)\big) & \text{if } s=\nu \\ \prod_{p|n}\big(\frac{n-\varepsilon(n)}{2},p-\varepsilon(p)\big) & \text{if } s>\nu \text{ and } \mathrm{ord}_p n\equiv 0 \mod 2 \text{ for any } p|n \text{ with } \mathrm{ord}_2(p-\varepsilon(p))<s \\ \frac{1}{2}\prod_{p|n}\big(\frac{n-\varepsilon(n)}{2},p-\varepsilon(p)\big) & \text{if } s>\nu \text{ and } \mathrm{ord}_p n\equiv 1 \mod 2 \text{ for some } p|n \text{ with } \mathrm{ord}_2(p-\varepsilon(p))<s. \end{cases}$$

(4) $|\tilde{B}_{s\ell psp}|=\Big(1+\dfrac{2^{r\nu}-1}{2^r-1}\Big)\prod_{p|n}(m,p-\varepsilon(p))$.

Example 3.5. Let p be a prime >2 and $n=p^\alpha$. Then $\tilde{B}_{\ell psp}=\tilde{B}_{e\ell psp}=\tilde{B}_{s\ell psp}$ and its order is equal to $p-\varepsilon(p)$. The first case of (3) occurs when α is odd, and the second when α is even.

Remark 3.6. Let n be an odd integer >1 and $n-\varepsilon(n)=2^s m$ with $(m,2)=1$. Since $(m,2)=1$, $(-I)^m=-I$, and therefore $\{\pm I\}\subset\tilde{B}_{s\ell psp}\subset\tilde{B}_{e\ell psp}\subset\tilde{B}_{\ell psp}$.

Remark 3.7. Assume that D is a square. Put $D=d^2$. Then an isomorphism of group schemes over $\mathbb{Z}[\frac{1}{2D}]$

$$\tilde{s}:U(D)_{\mathbb{Z}[\frac{1}{2D}]}=\mathrm{Spec}\,\mathbb{Z}[\frac{1}{2D}][X,Y]/(X^2-DY^2-1)\xrightarrow{\sim}\mathbb{G}_{m,\mathbb{Z}[\frac{1}{2D}]}=\mathrm{Spec}\,\mathbb{Z}[\frac{1}{2D}][U,\frac{1}{U}]$$

is defined by

$$U\mapsto X+dY:\mathbb{Z}[\frac{1}{2D}][U,\frac{1}{U}]\to\mathbb{Z}[\frac{1}{2D}][X,Y]/(X^2-DY^2-1).$$

Then for an odd integer n with $(n,D)=1$, an isomorphism of groups $\tilde{s}:U(D)(\mathbb{Z}/n\mathbb{Z})\xrightarrow{\sim}(\mathbb{Z}/n\mathbb{Z})^\times$ is given by $\xi=(a,b)\mapsto a+db$. Moreover $\tilde{s}$ induces isomorphisms

$$\tilde{B}_{\ell psp}(n,D)\xrightarrow{\sim}B_{psp}(n),$$
$$\tilde{B}_{e\ell psp}(n,D)\xrightarrow{\sim}B_{epsp}(n)$$

and a bijection

$$\tilde{B}_{s\ell psp}(n,D)\xrightarrow{\sim}B_{spsp}(n).$$

Here

$$B_{psp}(n) = \{a \in (\mathbb{Z}/n\mathbb{Z})^\times \ ; \ a^{n-1} = 1\},$$
$$B_{epsp}(n) = \{a \in (\mathbb{Z}/n\mathbb{Z})^\times \ ; \ a^{\frac{n-1}{2}} = \left(\frac{a}{n}\right)\},$$
$$B_{spsp}(n) = \{a \in (\mathbb{Z}/n\mathbb{Z})^\times \ ; \ a^m = 1, \text{ or } a^{2^k m} = -1 \text{ for some } k < m\}.$$

Definition 3.8. Let D be an integer $\neq 0$. An odd composite n is called a *Carmichael-Lucas number* to base D if n is prime to D and $\tilde{B}_{\ell psp}(n, D) = U(D)(\mathbb{Z}/n\mathbb{Z})$. The Carmichael-Lucas numbers to base 1 are nothing but the Carmichael numbers.

Corollary 3.9.([15, Th.4]) *A Carmichael-Lucas number is square-free. Furthermore put $n = p_1 p_2 \cdots p_r$, where $p_1, p_2, \ldots, p_r$ are distinct primes. Then n is a Carmichael-Lucas number to base $D \neq 0$ if and only if $r \geq 2$ and $n - \varepsilon(n)$ is a common multiple of $p_1 - \varepsilon(p_1), p_2 - \varepsilon(p_2), \ldots, p_r - \varepsilon(p_r)$.*

Proof. By (2) of Theorem 3.4, n is a Carmichael-Lucas number to base D if and only if $\varphi_D(n) = \prod_{p|n}(n - \varepsilon(n), p - \varepsilon(p))$. Furthermore, by Corollary 2.11, $\varphi_D(n) = \prod_{p|n}(p - \varepsilon(p))$ if and only if n is square-free. Therefore it is sufficient to note that $\prod_{p|n}(p - \varepsilon(p)) = \prod_{p|n}(n - \varepsilon(n), p - \varepsilon(p))$ if and only if $(p - \varepsilon(p))|(n - \varepsilon(n))$ for each prime divisor p of n.

4. Proof of the theorem

Lemma 4.1. *Let D be an integer $\neq 0$, n an odd integer > 1 with $(n, D) = 1$ and d a divisor of $n - \varepsilon(n)$. Put*

$$H = \{\xi \in U(D)(\mathbb{Z}/n\mathbb{Z}) \ ; \ \xi^d = I\}.$$

Then H is a subgroup of $U(D)(\mathbb{Z}/n\mathbb{Z})$ and $|H| = \prod_{p|n}(d, p - \varepsilon(p))$.

Proof. Put $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, where $p_1, p_2, \ldots, p_r$ are distinct primes, and $\xi_i = \xi \mod p_i^{e_i}$ for each i. Then the correspondence $\xi \mapsto (\xi_1, \xi_2, \ldots, \xi_r)$ gives rise to an isomorphism

$$U(D)(\mathbb{Z}/n\mathbb{Z}) \xrightarrow{\sim} U(D)(\mathbb{Z}/p_1^{e_1}\mathbb{Z}) \times U(D)(\mathbb{Z}/p_2^{e_2}\mathbb{Z}) \times \cdots \times U(D)(\mathbb{Z}/p_r^{e_r}\mathbb{Z}).$$

We obtain the result, noting that $\mathrm{Ker}[d : U(D)(\mathbb{Z}/p_i^{e_i}\mathbb{Z}) \to U(D)(\mathbb{Z}/p_i^{e_i}\mathbb{Z})]$ is a cyclic group of order $(d, p_i - \varepsilon(p_i))$ since $U(D)(\mathbb{Z}/p_i^{e_i}\mathbb{Z})$ is a cyclic group of order $\varphi_D(p_i^{e_i}) = (p_i - \varepsilon(p_i))p^{e_i - 1}$ and d is prime to p_i.

Lemma 4.2. *Let n be an odd integer > 1 and k an integer ≥ 1. Put $\nu = \min_{p|n} \mathrm{ord}_2(p - \varepsilon(p))$. Then there exists $\xi \in U(D)(\mathbb{Z}/n\mathbb{Z})$ such that $\xi^{2^k} = -I$ if and only if $k \leq \nu - 1$.*

Proof. Put $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, where $p_1, p_2, \ldots, p_r$ are distinct primes. Let $\xi \in U(D)(\mathbb{Z}/n\mathbb{Z})$. Then we have $\xi^{2^k} = -I$ if and only if $\xi^{2^k} \equiv -I \mod p_i^{e_i}$ for each i. There exists $\xi_i \in U(D)(\mathbb{Z}/p_i^{e_i}\mathbb{Z})$ such that $\xi_i^{2^k} = -I$ if and only if $p_i - \varepsilon(p_i)$ is divisible by 2^{k+1}, since $U(D)(\mathbb{Z}/p_i^{e_i}\mathbb{Z})$ is a cyclic group of order $\varphi_D(p_i^{e_i}) = (p_i - \varepsilon(p_i))p^{e_i - 1}$ and 2 is prime to p_i. Hence we obtain the result.

Lemma 4.3. *Let n be an odd integer > 1. Put $s = \mathrm{ord}_2(n - \varepsilon(n))$ and $\nu = \min_{p|n} \mathrm{ord}_2(p - \varepsilon(p))$. Then we have $s \geq \nu$.Furthermore,*

$$s = \nu \;\Leftrightarrow \sum_{\substack{p|n \\ \mathrm{ord}_2(p-\varepsilon(p))=\nu}} \mathrm{ord}_p n \equiv 1 \mod 2,$$

$$s > \nu \;\Leftrightarrow \sum_{\substack{p|n \\ \mathrm{ord}_2(p-\varepsilon(p))=\nu}} \mathrm{ord}_p n \equiv 0 \mod 2.$$

Proof. Let p be a prime divisor of n. Noting that

$$\mathrm{ord}_2(p - \varepsilon(p)) = \nu \;\Leftrightarrow\; p \equiv \varepsilon(p) + 2^\nu \mod 2^{\nu+1},$$
$$\mathrm{ord}_2(p - \varepsilon(p)) > \nu \;\Leftrightarrow\; p \equiv \varepsilon(p) \mod 2^{\nu+1},$$

we obtain

$$\begin{aligned} n &\equiv \prod_{p|n} \varepsilon(p)^{\mathrm{ord}_p n} + \Big(\sum_{\substack{p|n \\ \mathrm{ord}_2(p-\varepsilon(p))=\nu}} \varepsilon(p)\mathrm{ord}_p n \Big) 2^\nu \\ &\equiv \varepsilon(n) + \Big(\sum_{\substack{p|n \\ \mathrm{ord}_2(p-\varepsilon(p))=\nu}} \mathrm{ord}_p n \Big) 2^\nu \mod 2^{\nu+1}. \end{aligned}$$

Corollary 4.4. *Let n be an odd integer > 1. Put $s = \mathrm{ord}_2(n - \varepsilon(n))$ and $\nu = \min_{p|n} \mathrm{ord}_2(p - \varepsilon(p))$. Then:*

(1) *For any prime divisor p of n we have $s \leq \mathrm{ord}_2(p - \varepsilon(p))$ if and only if $s = \nu$;*

(2) *There exists a prime divisor p of n such that $s > \mathrm{ord}_2(p - \varepsilon(p))$ if and only if $s > \nu$.*

Corollary 4.5. *Let D be an integer $\neq 0$ and n an odd integer > 1 with $(n, D) = 1$. Put $s = \mathrm{ord}_2(n - \varepsilon(n))$ and $\nu = \min_{p|n} \mathrm{ord}_2(p - \varepsilon(p))$. Let $\xi \in U(D)(\mathbb{Z}/n\mathbb{Z})$. Then*:

(1) *If $\xi^{2^{\nu-1}} = I$, then $\left[\frac{\xi}{n}\right] = 1$;*

(2) *If $\xi^{2^{\nu-1}} = -I$ and $s > \nu$, then $\left[\frac{\xi}{n}\right] = 1$;*

(3) *If $\xi^{2^{\nu-1}} = -I$ and $s = \nu$, then $\left[\frac{\xi}{n}\right] = -1$.*

Proof. First assume that $\xi^{2^{\nu-1}} = I$. Then for each prime divisor p of n we have

$$\xi^{\frac{p-\varepsilon(p)}{2}} = (\xi^{2^{\nu-1}})^{\frac{p-\varepsilon(p)}{2^\nu}} \equiv I \mod p,$$

which implies that $\left[\frac{\xi}{p}\right] = 1$. Hence we obtain the first assertion.

Now we assume that $\xi^{2^{\nu-1}} = -I$. Then we have

$$\xi^{\frac{p-\varepsilon(p)}{2}} \equiv \begin{cases} I \mod p & \text{if } \mathrm{ord}_2(p-\varepsilon(p)) > \nu \\ -I \mod p & \text{if } \mathrm{ord}_2(p-\varepsilon(p)) = \nu, \end{cases}$$

and therefore,

$$\left[\frac{\xi}{p}\right] = \begin{cases} 1 & \text{if } \mathrm{ord}_2(p-\varepsilon(p)) > \nu \\ -1 & \text{if } \mathrm{ord}_2(p-\varepsilon(p)) = \nu. \end{cases}$$

Hence we obtain

$$\left[\frac{\xi}{n}\right] = (-1)^e,$$

where

$$e = \sum_{\substack{p|n \\ \mathrm{ord}_2(p-\varepsilon(p))=\nu}} \mathrm{ord}_p n.$$

Therefore the last two assertions follow from Lemma 4.3.

4.6. Proof of Theorem 3.4.
(1) Assume first that $\xi \in \tilde{B}_{e\ell psp}$. Then by definition we have $\xi^{\frac{n-\varepsilon(n)}{2}} = \pm I$, which implies that $\xi^{n-\varepsilon(n)} = I$, that is, $\xi \in \tilde{B}_{\ell psp}$.

Assume now that $\xi \in \tilde{B}_{s\ell psp}$. Then by definition and by Lemma 4.2, we have $\xi^m = I$ or $\xi^{2^k m} = -I$ for some $k \leq \nu - 1$.
Case (a): $s = \nu$. Then we have

$$\xi^{\frac{n-\varepsilon(n)}{2}} = \xi^{2^{\nu-1}m} = \pm I.$$

Furthermore, by Corollary 4.5 we have

$$\Big[\frac{\xi}{n}\Big] = \Big[\frac{\xi^m}{n}\Big] = \begin{cases} 1 & \text{if } \xi^{2^{\nu-1}m} = I \\ -1 & \text{if } \xi^{2^{\nu-1}m} = -I, \end{cases}$$

since m is odd. This implies that $\xi \in \tilde{B}_{e\ell psp}$.
Case (b): $s > \nu$. We have

$$\xi^{\frac{n-\varepsilon(n)}{2}} = \xi^{2^{s-1}m} = (\xi^{2^{\nu-1}m})^{2^{s-\nu}} = I.$$

On the other hand, by Corollary 4.5, we have $\Big[\frac{\xi}{n}\Big] = 1$, which implies that $\xi \in \tilde{B}_{e\ell psp}$.

(2) Applying Lemma 4.1 to $d = n - \varepsilon(n)$, we obtain the assertion.

(3) Put $C = \{\xi \in U(D)(\mathbb{Z}/n\mathbb{Z}) \ ; \ \xi^{\frac{n-\varepsilon(n)}{2}} = I\}$. Then C is a subgroup of $U(D)(\mathbb{Z}/n\mathbb{Z})$. Furthermore, by Lemma 4.1 we have

$$|C| = \prod_{p|n} \Big(\frac{n-\varepsilon(n)}{2}, p - \varepsilon(p)\Big).$$

Case (a): $s = \nu$. If $\xi \in C$, then $\xi^{2^{\nu-1}m} = I$. Hence by Corollary 4.5, we obtain $\Big[\frac{\xi}{n}\Big] = \Big[\frac{\xi^m}{n}\Big] = 1$, which implies that $\xi \in \tilde{B}_{e\ell psp}$

On the other hand, by Lemma 4.2 there exists $\xi \in U(D)(\mathbb{Z}/n\mathbb{Z})$ such that $\xi^{2^{\nu-1}} = -I$. Then it follows from Corollary 4.5 that $\Big[\frac{\xi}{n}\Big] = -1$ and that $\xi \in \tilde{B}_{e\ell psp}(n, D)$.

It follows that the homomorphism $\tilde{B}_{e\ell psp} \to \{\pm 1\}$ defined by $\xi \mapsto \Big[\frac{\xi}{n}\Big]$ is surjective and that $\mathrm{Ker}[\tilde{B}_{e\ell psp} \to \{\pm 1\}] = C$, and therefore C is a subgroup of $\tilde{B}_{e\ell psp}$ of index 2.
Case (b): $s > \nu$. By Lemma 4.2, there does not exist $\xi \in U(D)(\mathbb{Z}/n\mathbb{Z})$ such that $\xi^{\frac{n-\varepsilon(n)}{2}} = \xi^{2^{s-1}m} = -I$, which implies that $\tilde{B}_{e\ell psp} \subset C$.

Now let $\xi \in C$. Let p be a prime divisor of n. If $\mathrm{ord}_2(p - \varepsilon(p)) \geq s$, then $\Big[\frac{\xi}{p}\Big] = 1$.Indeed, we have

$$\xi^{\frac{p-\varepsilon(p)}{2}} \equiv (\xi^{\frac{p-\varepsilon(p)}{2}})^m = (\xi^{2^{s-1}m})^{\frac{p-\varepsilon(p)}{2^s}} \equiv I \mod p$$

since $\xi^{\frac{n-\varepsilon(n)}{2}} \equiv I \mod p$ and $(m, 2) = 1$.

Hence, if $\mathrm{ord}_p n \equiv 0 \mod 2$ for any prime divisor p of n with $\mathrm{ord}_2(p - \varepsilon(p)) < s$, then we have $\Big[\frac{\xi}{n}\Big] = 1$ for all $\xi \in C$. It follows that $\tilde{B}_{e\ell psp} = C$.

On the other hand, assume that there exists a prime divisor p of n such that $\mathrm{ord}_2(p-\varepsilon(p)) < s$ and $\mathrm{ord}_p n \equiv 1 \mod 2$. Put $n = p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$, where $p_1, p_2, \ldots, p_r$ are distinct primes and $p_1 = p$. Take $\xi_1 \in U(D)(\mathbb{Z}/p^{e_1}\mathbb{Z})$ so that $\left[\frac{\xi_1}{p_1}\right] = -1$. Then we have $\xi_1^{\frac{p_1-\varepsilon(p_1)}{2}} \equiv -I \mod p_1$. By Lemma 2.7, replacing ξ_1 by $\xi_1^{p_1^{e_1-1}}$, we may assume that $\xi_1^{\frac{p_1-\varepsilon(p_1)}{2}} \equiv -I \mod p_i^{e_i}$. Furthermore, we put $s_1 = \mathrm{ord}_2(p_1 - \varepsilon(p_1))$. Then we obtain

$$\left[\frac{\xi_1^{\frac{p_1-\varepsilon(p_1)}{2^{s_1}}}}{p_1}\right] = \left[\frac{\xi_1}{p_1}\right]^{\frac{p_1-\varepsilon(p_1)}{2^{s_1}}} = -1$$

since $\dfrac{p_1-\varepsilon(p_1)}{2^{s_1}} \equiv 1 \mod 2$. Repalcing ξ_1 by $\xi_1^{\frac{p_1-\varepsilon(p_1)}{2^{s_1}}}$, we may assume that $\xi_1^{2^{s_1-1}} \equiv -I \mod p_i^{e_i}$. Since $s_1 - 1 < s - 1$, we obtain $\xi_1^{2^{s-1}} \equiv I \mod p_i^{e_i}$, and therefore $\xi_1^{\frac{n-\varepsilon(n)}{2}} \equiv I \mod p_i^{e_i}$. Hence, if we take $\xi \in U(D)(\mathbb{Z}/n\mathbb{Z})$ so that

$$\xi \equiv \xi_1 \mod p_1^{e_1},\ \xi \equiv I \mod p_2^{e_2}, \ldots,\ \xi \equiv I \mod p_r^{e_r},$$

we have $\xi^{\frac{n-\varepsilon(n)}{2}} \equiv I \mod n$. On the other hand, we have $\left[\frac{\xi}{n}\right] = -1$ since $e_1 \equiv 1 \mod 2$ and

$$\left[\frac{\xi}{p_1}\right] = -1,\ \left[\frac{\xi}{p_2}\right] = 1, \ldots,\ \left[\frac{\xi}{p_r}\right] = 1.$$

It follows that the homomorphism $C \to \{\pm 1\}$ defined by $\xi \mapsto \left[\frac{\xi}{n}\right]$ is surjective and that $\mathrm{Ker}[C \to \{\pm 1\}] = \tilde{B}_{e\ell psp}$, and therefore $\tilde{B}_{e\ell psp}$ is a subgroup of C of index 2.

(4) Put $C_k = \{\xi \in U(D)(\mathbb{Z}/n\mathbb{Z})\ ;\ \xi^{2^k m} = I\}$ for each $k \geq 0$. Then C_k is a subgroup of $U(D)(\mathbb{Z}/n\mathbb{Z})$ and

$$|C_k| = \prod_{p|n}(2^k m, p - \varepsilon(p))$$

by Lemma 4.1. Moreover, if $k \leq \nu$, then

$$\prod_{p|n}(2^k m, p-\varepsilon(p)) = 2^{rk}\prod_{p|n}(m, p-\varepsilon(p)).$$

Put now $B_k = \{\xi \in U(D)(\mathbb{Z}/n\mathbb{Z})\ ;\ \xi^{2^k m} = -I\}$ for each $k \geq 0$. Then $B_k \neq \emptyset$ if and only if there exists $\xi \in U(D)(\mathbb{Z}/n\mathbb{Z})$ such that $\xi^{2^k} = -I$, since $(m, 2) = 1$. Furthermore, if $B_k \neq \emptyset$, then the correspondence $\eta \mapsto \xi\eta$ gives rise to a bijection $C_k \xrightarrow{\sim} B_k$, where $\xi \in B_k$. By Lemma 4.2, there exists

$\xi \in U(D)(\mathbb{Z}/n\mathbb{Z})$ such that $\xi^{2^k} = -I$ if and only if $k+1 \le \nu$. Hence, if $k \ge \nu$, then $B_k = \emptyset$. Hence we obtain a partition of $\tilde{B}_{s\ell psp}$

$$\tilde{B}_{s\ell psp} = C_0 \cup B_0 \cup B_1 \cup \cdots \cup B_{\nu-1},$$

and therefore

$$\begin{aligned}|\tilde{B}_{s\ell psp}| &= (1 + 1 + 2^r + \cdots + 2^{r(\nu-1)}) \prod_{p|n} (m, p - \varepsilon(p)) \\ &= \Big(1 + \frac{2^{r\nu} - 1}{2^r - 1}\Big) \prod_{p|n} (m, p - \varepsilon(p)).\end{aligned}$$

Remark 4.7. Under the notations of Theorem 3.4, let $\tilde{C}$ denote the subgroup of $U(D)(\mathbb{Z}/n\mathbb{Z})$ generated by $\tilde{B}_{s\ell psp}$. As is verified in 4.6, we have $\tilde{B}_{s\ell psp} = C_0 \cup B_0 \cup B_1 \cup \cdots \cup B_{\nu-1}$ and $C_{\nu-1} \supset C_0 \cup B_0 \cup B_1 \cup \cdots \cup B_{\nu-2}$. Hence we obtain

$$\tilde{C} = C_{\nu-1} \cup B_{\nu-1},$$

and therefore

$$|\tilde{C}| = 2|C_{\nu-1}| = 2^{r(\nu-1)+1} \prod_{p|n} (m, p - \varepsilon(p)).$$

In particular, $\tilde{B}_{s\ell psp}$ is a subgroup of $U(D)(\mathbb{Z}/n\mathbb{Z})$ if and only if $C_{\nu-1} = C_0 \cup B_0 \cup B_1 \cup \cdots \cup B_{\nu-2}$. This is the case only when $r = 1$ or $\nu = 1$.

Remark 4.8. Let $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ be an odd number, where $p_1, p_2, \ldots, p_r$ are distinct primes. Put $n - \varepsilon(n) = 2^s m$ with $(m, 2) = 1$ and $p_i - \varepsilon(p_i) = 2^{s_i} m_i$ with $(m_i, 2) = 1$ for each i, and put $\nu = \min\limits_{1 \le i \le r} s_i$. Then we have

$$\operatorname{ord}_2 \varphi_D(n) = \sum_{i=1}^{r} s_i$$

and, by Theorem 3.4,

$$\operatorname{ord}_2 |\tilde{B}_{\ell psp}| = \sum_{i=1}^{r} \min(s, s_i),$$

$$\operatorname{ord}_2 |\tilde{B}_{e\ell psp}| = \begin{cases} 1 + r(s-1) & \text{if } s = \nu \\ \displaystyle\sum_{i=1}^{r} \min(s-1, s_i) & \text{if } s > \nu \text{ and } e_i \equiv 0 \mod 2 \\ & \text{for any } i \text{ with } s_i < s \\ \displaystyle -1 + \sum_{i=1}^{r} \min(s-1, s_i) & \text{if } s > \nu \text{ and } e_i \equiv 1 \mod 2 \\ & \text{for some } i \text{ with } s_i < s \end{cases}$$

and

$$\mathrm{ord}_2|\tilde{C}| = 1 + r(\nu - 1).$$

Furthermore, $|\tilde{B}_{\ell psp}|$, $|\tilde{B}_{e\ell psp}|$ and $|\tilde{C}|$ are equal to $\prod_{i=1}^{r}(m, m_i)$ up to powers of 2.

5. Some consequences of the theorem

Proposition 5.1. *Let D be an integer $\neq 0$ and n an odd integer > 1 with $(n, D) = 1$. Then $\tilde{B}_{\ell psp}(n, D) = \tilde{B}_{e\ell psp}(n, D)$ if and only if either n is a prime power, or n is a square and $\mathrm{ord}_2(p - \varepsilon(p)) < \mathrm{ord}_2(n - \varepsilon(n))$ for each prime divisor p of n.*

Proof. By Remark 4.8, $|\tilde{B}_{\ell psp}| = |\tilde{B}_{e\ell psp}|$ up to powers of 2. It follows that $\tilde{B}_{\ell psp} = \tilde{B}_{e\ell psp}$ if and only if $\mathrm{ord}_2|\tilde{B}_{\ell psp}| = \mathrm{ord}_2|\tilde{B}_{e\ell psp}|$.

Put now $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, where $p_1, p_2, \ldots, p_r$ are distinct primes, and $n - \varepsilon(n) = 2^s m$ with $(m, 2) = 1$. Put $p_i - \varepsilon(p_i) = 2^{s_i} m_i$ with $(m_i, 2) = 1$ for each i, and $\nu = \min_{1 \le i \le r} s_i$.

Case (a): $s = \nu$. By Remark 4.8 we have

$$\mathrm{ord}_2|\tilde{B}_{\ell psp}| = \sum_{i=1}^{r} \min(s, s_i) = rs,$$

$$\mathrm{ord}_2|\tilde{B}_{e\ell psp}| = 1 + \sum_{i=1}^{r} \min(s - 1, s_i) = 1 + r(s - 1).$$

Hence $\mathrm{ord}_2|\tilde{B}_{\ell psp}| = \mathrm{ord}_2|\tilde{B}_{e\ell psp}|$ if and only if $r = 1$.

Case (b): $s > \nu$ and $e_i \equiv 0 \mod 2$ for any i with $s_i < s$. By Remark 4.9 we have

$$\mathrm{ord}_2|\tilde{B}_{\ell psp}| = \sum_{i=1}^{r} \min(s, s_i),\ \mathrm{ord}_2|\tilde{B}_{e\ell psp}| = \sum_{i=1}^{r} \min(s - 1, s_i).$$

Hence $\mathrm{ord}_2|\tilde{B}_{\ell psp}| = \mathrm{ord}_2|\tilde{B}_{e\ell psp}|$ if and only if $s_i < s$ for each i. If this is the case, then n is a square by the condition on e_i.

Case (c): $s > \nu$ and $e_i \equiv 1 \mod 2$ for some i with $s_i < s$. By Remark 4.8 we have

$$\mathrm{ord}_2|\tilde{B}_{\ell psp}| = \sum_{i=1}^{r} \min(s, s_i) > \mathrm{ord}_2|\tilde{B}_{e\ell psp}| = -1 + \sum_{i=1}^{r} \min(s - 1, s_i).$$

Corollary 5.2. *Let D be an integer $\neq 0$ and n an odd composite with $(n, D) = 1$. Then $|\tilde{B}_{e\ell psp}| \leq \varphi_D(n)/2$.*

Proof. It is sufficient to prove that $\tilde{B}_{e\ell psp} \neq U(D)(\mathbb{Z}/n\mathbb{Z})$ since $\tilde{B}_{e\ell psp}$ is a subgroup of $U(D)(\mathbb{Z}/n\mathbb{Z})$. If n is not a Carmichael-Lucas number to base D, then $|\tilde{B}_{e\ell psp}| \leq |\tilde{B}_{\ell psp}| < \varphi_D(n)$. On the other hand, if n is a Carmichael-Lucas number to base D, then $|\tilde{B}_{e\ell psp}| < |\tilde{B}_{\ell psp}|$ since n is neither a prime power nor a square.

Lemma 5.3. *Let D be an integer $\neq 0$ and n an odd integer > 1 with $(n, D) = 1$. Put $s = \mathrm{ord}_2(n - \varepsilon(n))$ and $\nu = \min_{p|n} \mathrm{ord}_2(p - \varepsilon(p))$. Let $\tilde{C}$ denote the subgroup of $U(D)(\mathbb{Z}/n\mathbb{Z})$ generated by $\tilde{B}_{s\ell psp}$. Then $\tilde{C} = \tilde{B}_{e\ell psp}$ if and only if either $s = \nu$, or n is a prime power, or $n = p^\alpha q^\beta$, where p, q are distinct primes with $\mathrm{ord}_2(p - \varepsilon(p)) = \mathrm{ord}_2(q - \varepsilon(q))$ and $\alpha \equiv \beta \equiv 1 \mod 2$.*

Proof. By Remark 4.8, $|\tilde{C}| = |\tilde{B}_{e\ell psp}|$ up to powers of 2. It follows that $\tilde{B}_{e\ell psp} = \tilde{C}$ if and only if $\mathrm{ord}_2|\tilde{B}_{e\ell psp}| = \mathrm{ord}_2|\tilde{C}|$.

Put now $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, where $p_1, p_2, \ldots, p_r$ are distinct primes, and $n - \varepsilon(n) = 2^s m$. Put $p_i - \varepsilon(p_i) = 2^{s_i} m_i$ with $(m_i, 2) = 1$ for each i.

Case (a): $s = \nu$. By Remark 4.8 we have

$$\mathrm{ord}_2|\tilde{B}_{e\ell psp}| = 1 + r(\nu - 1) = \mathrm{ord}_2|\tilde{C}| = 1 + r(\nu - 1).$$

Case (b): $s > \nu$ and $e_i \equiv 0 \mod 2$ for any i with $s_i < s$. By Remark 4.8 we have

$$\mathrm{ord}_2|\tilde{B}_{e\ell psp}| = \sum_{i=1}^{r} \min(s - 1, s_i) \geq r\nu,\ \mathrm{ord}_2|\tilde{C}| = 1 + r(\nu - 1).$$

Hence $\mathrm{ord}_2|\tilde{B}_{e\ell psp}| = \mathrm{ord}_2|\tilde{C}|$ if and only if $r = 1$.

Case (c): $s > \nu$ and $e_i \equiv 1 \mod 2$ for some i with $s_i < s$. In this case, we have $r \geq 2$ as is remarked in Example 3.5. By Remark 4.8 we have

$$\mathrm{ord}_2|\tilde{B}_{e\ell psp}| = -1 + \sum_{i=1}^{r} \min(s - 1, s_i) \geq r\nu - 1,\ \mathrm{ord}_2|\tilde{C}| = 1 + r(\nu - 1).$$

Hence if $\mathrm{ord}_2|\tilde{B}_{e\ell psp}| = \mathrm{ord}_2|\tilde{C}|$, then we have $r = 2$. We may assume that $s_1 \leq s_2$. Then we obtain $\min(s - 1, s_2) = \nu$. If $s_2 > s - 1 = \nu$, then we would have $e_1 \equiv 0 \mod 2$ by Lemma 4.3. This contradicts to the condition on e_i.

Hence $\mathrm{ord}_2|\tilde{B}_{e\ell psp}| = \mathrm{ord}_2|\tilde{C}| = \nu$ if and only if $r = 2$, $s_1 = s_2 = \nu$. Furthermore, if this is the case, then $e_1 \equiv e_2 \equiv 1 \mod 2$, since e_1 or e_2 is odd and $e_1 + e_2 \equiv 0 \mod 2$ by Lemma 4.3.

Proposition 5.4. *Let D be an integer $\neq 0$ and n an odd integer > 1 with $(n, D) = 1$. Then $\tilde{B}_{e\ell psp} = \tilde{B}_{s\ell psp}$ if and only if either $n - \varepsilon(n) \equiv 2 \mod 4$, or n is a prime power, or $n = p^\alpha q^\beta$, where p, q are distinct primes with $p - \varepsilon(p) \equiv q - \varepsilon(q) \equiv 2 \mod 4$ and $\alpha \equiv \beta \equiv 1 \mod 2$.*

Proof. Let $\tilde{C}$ be a subgroup of $U(D)(\mathbb{Z}/n\mathbb{Z})$ generated by $\tilde{B}_{s\ell psp}$. Then $\tilde{B}_{e\ell psp} = \tilde{B}_{s\ell psp}$ if and only if $\tilde{B}_{e\ell psp} = \tilde{C}$ and $\tilde{C} = \tilde{B}_{s\ell psp}$. Therefore, combining Lemma 5.3 and Remark 4.7, we obtain the result.

Proposition 5.5. *Let D be an integer $\neq 0$ and n an odd integer > 1 with $(n, D) = 1$. Then $|\tilde{B}_{e\ell psp}| = \varphi_D(n)/2$ if and only if n is a Carmichael-Lucas number to base D and $\mathrm{ord}_2(p-\varepsilon(p)) < \mathrm{ord}_2(n-\varepsilon(n))$ for each prime divisor p of n.*

Proof. Assume that $|\tilde{B}_{e\ell psp}| = \varphi_D(n)/2$. Then it follows from Theorem 3.4 that n is square-free. Put $n = p_1 p_2 \cdots p_r$, where $p_1, p_2, \ldots, p_r$ are distinct primes, and $n - \varepsilon(n) = 2^s m$ with $(m, 2) = 1$. Put $p_i - \varepsilon(p_i) = 2^{s_i} m_i$ with $(m_i, 2) = 1$ for each i, and $\nu = \min_{1 \le i \le r} s_i$. Then again by Theorem 3.4 we have $r \geq 2$ and $m_i | m$ for each i.

Case (a): $s = \nu$. By Remark 4.8, we have

$$\mathrm{ord}_2 |\tilde{B}_{e\ell psp}| = 1 + r(s-1), \ \mathrm{ord}_2 \varphi_D(n) = \sum_{i=1}^{r} s_i,$$

which implies that

$$1 + r(s-1) = -1 + \sum_{i=1}^{r} s_i,$$

and therefore

$$\sum_{i=1}^{r} (s_i - s + 1) = 2.$$

Since $s_i - s + 1 \geq 1$ for each i, we have $r = 2$ and $s_1 = s_2 = s$. It follows from Lemma 4.3 that $s > \nu$, which contradicts to $s = \nu$.

Case (b): $s > \nu$. By Remark 4.8 we have

$$\mathrm{ord}_2 |\tilde{B}_{e\ell psp}| = -1 + \sum_{i=1}^{r} \min(s-1, s_i)$$

since n is square-free. This implies that

$$-1 + \sum_{i=1}^{r} \min(s-1, s_i) = -1 + \sum_{i=1}^{r} s_i,$$

and therefore

$$\sum_{i=1}^{r} \min(s-1, s_i) = \sum_{i=1}^{r} s_i.$$

It follows that $s_i \leq s-1$ for each i. Hence it is concluded by Corollary 3.9 that n is a Carmichael-Lucas number to base D, since $m_i | m$ for each i.

Conversely, let $n = p_1 p_2 \cdots p_r$ be a Carmichael-Lucas number to base D, where $p_1, p_2, \ldots, p_r$ are distinct primes. Assume that we have $\mathrm{ord}_2(p_i - \varepsilon(p_i)) < \mathrm{ord}_2(n - \varepsilon(n))$ for each i. Then by Corollary 3.9 we obtain $(p_i - \varepsilon(p_i)) | \dfrac{n-\varepsilon(n)}{2}$ for each i. It follows from Theorem 3.4 that

$$|\tilde{B}_{e\ell psp}| = \frac{1}{2}\prod_{i=1}^{r}\left(\frac{n-\varepsilon(n)}{2}, p_i - \varepsilon(p_i)\right) = \frac{1}{2}\prod_{i=1}^{r}(p_i - \varepsilon(p_i)) = \frac{\varphi_D(n)}{2}$$

since $s > \nu = \min\limits_{1 \leq i \leq r} s_i$ and n is square-free.

Example 5.6. When $D = 5$, the first three examples with $|\tilde{B}_{e\ell psp}| = \varphi_D(n)/2$ are given by $323 = 17 \times 19$, $6721 = 11 \times 13 \times 47$ and $11663 = 107 \times 109$.

Corollary 5.7. *Let D be a non-square and n an odd composite with $(n, D) = 1$. Then $|\tilde{B}_{s\ell psp}| \leq \varphi_D(n)/2$. In particular, $|\tilde{B}_{s\ell psp}| = \varphi_D(n)/2$ if and only if $n = pq$ is a Carmichael-Lucas number to base D with $q = p + 2$, $\varepsilon(p) = -1$, $\varepsilon(q) = 1$, $p \equiv 1 \mod 4$.*

Proof. Combining Propositions 5.5 and 5.4, we obtain the result.

Example 5.8. When $D = 5$, the first three examples with $|\tilde{B}_{s\ell psp}| = \varphi_D(n)/2$ are given by $323 = 17 \times 19$, $19043 = 137 \times 139$ and $39203 = 197 \times 199$.

Remark 5.9. Let D be a square and n an odd composite with $(n, D) = 1$ and $n \neq 9$. Then, as is well known, $|\tilde{B}_{s\ell psp}| \leq \varphi(n)/4$ ([9], [10]). In particular, $|\tilde{B}_{s\ell psp}| = \varphi(n)/4$ if and only if either $n = pq$, where p, q are primes with $p \equiv 3 \mod 4$ and $q = 2p - 1$, or $n = p_1 p_2 p_3$ is a Carmaichael number, where p_1, p_2, p_3 are different primes with $p_1 \equiv p_2 \equiv p_3 \equiv 3 \mod 4$.

Remark 5.10. Let D be an integer $\neq 0$, n an odd integer > 1 with $(n, D) = 1$. Put $n - \varepsilon(n) = 2^s m$ with $(m, 2) = 1$ and $\nu = \min\limits_{p|n} \mathrm{ord}_2(p - \varepsilon(p))$. Then:
(1) $\tilde{B}_{e\ell psp} = \{\pm I\}$ if and only if either n is a power of 3 and $D \equiv 1 \mod 3$, or $n - \varepsilon(n) \equiv 2 \mod 4$ and $(m, p - \varepsilon(p)) = 1$ for each prime divisor p of n,

or $n = p^\alpha q^\beta$, where p, q are distinct primes with $p - \varepsilon(p) \equiv q - \varepsilon(q) \equiv 2 \mod 4$, $(m, p - \varepsilon(p)) = (m, q - \varepsilon(q)) = 1$ and $\alpha \equiv \beta \equiv 1 \mod 2$.
(2) $\tilde{B}_{s\ell psp} = \{\pm I\}$ if and only if $\nu = 1$ and $(m, p - \varepsilon(p)) = 1$ for each prime divisor p of n.

Hereafter we mention several remarks with relation to preceding works [1], [2] and [15].

Definition 5.11. Let D be an integer $\neq 0$ and n an odd integer > 1 with $(n, D) = 1$. We put:

$$B_{\ell psp}(n, D) =$$
$$\left\{ P \in \mathbb{Z}/n\mathbb{Z}\,; \begin{array}{l} \text{there exist } Q \in \mathbb{Z}/n\mathbb{Z} \text{ such that } P^2 - 4Q = D \text{ and} \\ n \text{ is a Lucas pseudoprime with respect to } (P, Q) \end{array} \right\},$$
$$B_{e\ell psp}(n, D) =$$
$$\left\{ P \in \mathbb{Z}/n\mathbb{Z}\,; \begin{array}{l} \text{there exists } Q \in (\mathbb{Z}/n\mathbb{Z})^\times \text{ such that } P^2 - 4Q = D \text{ and} \\ n \text{ is an Euler-Lucas pseudoprime with respect to } (P, Q) \end{array} \right\},$$
$$B_{s\ell psp}(n, D) =$$
$$\left\{ P \in \mathbb{Z}/n\mathbb{Z}\,; \begin{array}{l} \text{there exists } Q \in \mathbb{Z}/n\mathbb{Z} \text{ such that } P^2 - 4Q = D \text{ and} \\ n \text{ is a strong Lucas pseudoprime with respect to } (P, Q) \end{array} \right\}.$$

Notation 5.12. Let D be an integer $\neq 0$. Put

$$V_D = \operatorname{Spec} \mathbb{Z}[T, \frac{1}{T^2 - D}].$$

Then V_D is an open subscheme of the affine line $\mathbb{A}^1_{\mathbb{Z}}$ over $\mathbb{Z}$.

A morphism of affine schemes

$$\pi : V_D = \operatorname{Spec} \mathbb{Z}[T, \frac{1}{T^2 - D}] \to U(D) = \operatorname{Spec} \mathbb{Z}[X, Y]/(X^2 - DY^2 - 1)$$

is defined by

$$X \mapsto \frac{T^2 + D}{T^2 - D},\ Y \mapsto \frac{2T}{T^2 - D} : \mathbb{Z}[X, Y]/(X^2 - DY^2 - 1) \to \mathbb{Z}[T, \frac{1}{T^2 - D}].$$

Moreover, put

$$\tilde{V}_D = \mathbb{Z}[X, Y, \frac{1}{X - 1}]/(X^2 - DY^2 - 1).$$

$\tilde{V}_D$ is an open subscheme of $U(D)$. Moreover, π induces an isomorphism

$$\pi_{\mathbb{Z}[\frac{1}{2D}]} : V_{D, \mathbb{Z}[\frac{1}{2D}]} \xrightarrow{\sim} \tilde{V}_{D, \mathbb{Z}[\frac{1}{2D}]}$$

over $\mathbb{Z}[\frac{1}{2D}]$. In fact, the correspondence

$$T \mapsto \frac{DY}{X-1} : \mathbb{Z}[T, \frac{1}{T^2-D}] \to \mathbb{Z}[X, Y, \frac{1}{X-1}]/(X^2 - DY^2 - 1)$$

defines the inverse of $\pi_{\mathbb{Z}[\frac{1}{2D}]}$.

Example 5.13. Let D be an integer $\neq 0$, n an odd integer > 1 with $(n, D) = 1$ and $P \in V_D(\mathbb{Z}/n\mathbb{Z})$. Put $Q = (P^2 - D)/4 \in \mathbb{Z}/n\mathbb{Z}$. Then Q is invertible in $\mathbb{Z}/n\mathbb{Z}$, and

$$\pi(P) = \Big(\frac{P^2 + D}{P^2 - D}, \frac{2P}{P^2 - D}\Big) = \Big(\frac{D + 2Q}{2Q}, \frac{P}{2Q}\Big).$$

Lemma 5.14. *Let D be an integer $\neq 0$ and n an odd integer > 1 with $(n, D) = 1$. Then the morphism $\pi : V_D \to U(D)$ induces bijections*

$$B_{\ell psp}(n, D) \xrightarrow{\sim} \tilde{V}_D(\mathbb{Z}/n\mathbb{Z}) \cap \tilde{B}_{\ell psp}(n, D),$$
$$B_{e\ell psp}(n, D) \xrightarrow{\sim} \tilde{V}_D(\mathbb{Z}/n\mathbb{Z}) \cap \tilde{B}_{e\ell psp}(n, D),$$
$$B_{s\ell psp}(n, D) \xrightarrow{\sim} \tilde{V}_D(\mathbb{Z}/n\mathbb{Z}) \cap \tilde{B}_{s\ell psp}(n, D).$$

Proof. The assertion follows from Corollary 2.8 and Example 5.13.

Lemma 5.15. *Let D be an integer $\neq 0$, n an odd integer > 1 with $(n, D) = 1$ and $\xi \in U(D)(\mathbb{Z}/n\mathbb{Z})$. Then $\xi \in V_D \Leftrightarrow \xi \not\equiv I \mod p$ for each prime divisor p of n.*

Proof. Let $\xi \in U(D)(\mathbb{Z}/n\mathbb{Z})$. Then, by definition, $\xi \in \tilde{V}_D(\mathbb{Z}/n\mathbb{Z})$ if and only if $a - 1$ is invertible in $\mathbb{Z}/n\mathbb{Z}$, which means that $a \not\equiv 1 \mod p$ for each prime divisor p of n. On the other hand, $a \equiv 1 \mod p$ if and only if $\xi \equiv I \mod p$, since $a^2 - Db^2 \equiv 1 \mod p$.

Corollary 5.16. *Let D be an integer $\neq 0$ and n an odd integer > 1 with $(n, D) = 1$. Then the group $U(D)(\mathbb{Z}/n\mathbb{Z})$ is genarated by $\tilde{V}_D(\mathbb{Z}/n\mathbb{Z})$.*

Proof. First let p be a prime and θ a generator of $U(D)(\mathbb{Z}/p^\alpha\mathbb{Z})$. Observe that, except in the case of $p = 3$ and $\varepsilon(p) = 1$, we have $\xi \not\equiv \pm I \mod p$. On the other hand, if $p = 3$ and $\varepsilon(p) = 1$, then we have $\tilde{V}_D(\mathbb{Z}/p^\alpha\mathbb{Z}) = \{\xi \in U(D)(\mathbb{Z}/p^\alpha\mathbb{Z}) \ ; \ \xi \equiv -I \mod p\}$, and therefore, $|\tilde{V}_D(\mathbb{Z}/p^\alpha\mathbb{Z})| = |U(D)(\mathbb{Z}/p^\alpha\mathbb{Z})|/2$.

Put now $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, where $p_1, p_2, \ldots, p_r$ are distinct primes. Then the correspondence $\xi \mapsto (\xi \mod p^{e_1}, \xi \mod p^{e_2}, \ldots, \xi \mod p^{e_r})$ gives rise to an isomorphism

$$U(D)(\mathbb{Z}/n\mathbb{Z}) \xrightarrow{\sim} U(D)(\mathbb{Z}/p_1^{e_1}\mathbb{Z}) \times U(D)(\mathbb{Z}/p_2^{e_2}\mathbb{Z}) \times \cdots \times U(D)(\mathbb{Z}/p_r^{e_r}\mathbb{Z}).$$

Let H denote the subgroup of $U(D)(\mathbb{Z}/n\mathbb{Z})$ genarated by $\tilde{V}_D(\mathbb{Z}/n\mathbb{Z})$. Take a generator θ_i of $U(D)(\mathbb{Z}/p_i^{e_i}\mathbb{Z})$. Except in the case of $p_i = 3$ and $\varepsilon(p_i) = 1$, we have

$$(-I, \ldots, -I, -\theta_i, -I, \ldots, -I) \in \tilde{V}_D(\mathbb{Z}/n\mathbb{Z}),$$

which implies

$$(I, \ldots, I, \theta_i, I, \ldots, I) = -(-I, \ldots, -I, -\theta_i, -I, \ldots, -I) \in H.$$

Hence we obtain $|U(D)(\mathbb{Z}/n\mathbb{Z}) : H| < 2$, and therefore $U(D)(\mathbb{Z}/n\mathbb{Z}) = H$.

Corollary 5.17. *Let D be an integer $\neq 0$ and n an odd integer > 1 with $(n, D) = 1$. Then:*
(1) *$\tilde{B}_{\ell psp}(n, D) = U(D)(\mathbb{Z}/n\mathbb{Z})$ if and only if $B_{\ell psp}(n, D) = V_D(\mathbb{Z}/n\mathbb{Z})$.*
(2)([15, Th.7]) *$B_{e\ell psp}(n, D) \neq V_D(\mathbb{Z}/n\mathbb{Z})$.*

Remark 5.18. Williams [15] defines an odd composite n to be a Carmichael-Lucas number to base D if n is prime to D and $B_{\ell psp}(n, D) = V_D(\mathbb{Z}/n\mathbb{Z})$. The first assertion of Corollary 5.17 assures that Definition 3.8 is equivalent to Williams'.

Remark 5.19. Lemma 5.14 allows us to deduce formulas for $|B_{\ell psp}|$, $|B_{e\ell psp}|$ and $|B_{s\ell psp}|$ from those for $|\tilde{B}_{\ell psp}|$, $|\tilde{B}_{e\ell psp}|$ and $|\tilde{B}_{s\ell psp}|$, respectively. This is done indeed by Baillie and Wagstaff [2, Th.2] for $B_{\ell psp}$, and by Arnault [1, Th.1.5] for $B_{s\ell psp}$.

6. Frobenius pseudoprime

Grantham ([4], [5]) defines the notion of Frobenius pseudoprimes and strong Frobenius pseudoprimes with respect to a polynomial $f(t) \in \mathbb{Z}[t]$. We adopt here the definition given in [3] for a quadratic polynomial.

Definition 6.1.[3, Def.3.6.5] Let P, Q be integers $\neq 0$, and put $D = P^2 - 4Q$. Assume that D is not a square. An odd composite n is called a *Frobenius pseudoprime* with respect to (P, Q) if n is prime to QD and

$$t^n = \begin{cases} t & \text{if } \varepsilon(n) = 1 \\ P - t & \text{if } \varepsilon(n) = -1 \end{cases}$$

in the residue ring $\mathbb{Z}[t]/(n, t^2 - Pt + Q)$.

Remark 6.2. The correspondence $t \mapsto \dfrac{P + \sqrt{D}}{2}$ gives rise to an isomorphism of rings

$$\mathbb{Z}[\frac{1}{2}][t]/(t^2 - Pt + Q) \xrightarrow{\sim} \mathbb{Z}[\frac{1}{2}][\sqrt{D}].$$

Under this identification, we have $P - t = \dfrac{P - \sqrt{D}}{2}$. This implies the following assertion.

Let n be an odd composite with $(n, DQ) = 1$, and put $\eta = (P/2, 1/2) \in G_D(\mathbb{Z}/n\mathbb{Z})$. Then n is a Frobenius pseudoprime with respect to (P, Q) if and only if

$$\eta^n = \begin{cases} \eta & \text{if } \varepsilon(n) = 1 \\ \bar{\eta} & \text{if } \varepsilon(n) = -1. \end{cases}$$

Proposition 6.3. *Let P, Q be integers $\neq 0$ with $D = P^2 - 4Q$ not a square, and let n be an odd composite with $(n, DQ) = 1$. Assume that n is a Frobenius pseudoprime with respect to (P, Q). Then:*
(1)([5, Th.4.9]) *n is a Lucas pseudoprime with respect to (P, Q).*
(2) *n is a pseudoprime to base Q.*

Proof. Put

$$\eta = \Big(\frac{P}{2}, \frac{1}{2}\Big) \text{ and } \xi = \gamma(\eta) = \Big(\frac{D + 2Q}{2Q}, \frac{P}{2Q}\Big).$$

(1) In the case of $\varepsilon(n) = 1$, we have $\eta^n = \eta$ in $G_{(D)}(\mathbb{Z}/n\mathbb{Z})$, and therefore $\xi^n = \xi$ in $U(D)(\mathbb{Z}/n\mathbb{Z})$, which implies $\xi^{n-1} = I$.

On the other hand, in the case of $\varepsilon(n) = -1$, we have $\eta^n = \bar{\eta}$ in $G_{(D)}(\mathbb{Z}/n\mathbb{Z})$. Hence we obtain $\xi^n = \xi^{-1}$ in $U(D)(\mathbb{Z}/n\mathbb{Z})$ since $\gamma(\bar{\eta}) = \xi^{-1}$. This implies $\xi^{n+1} = I$.
(2) In both the cases we obtain $Q^n = Q$ in $\mathbb{Z}/n\mathbb{Z}$ from the fact $\mathrm{Nr}(\eta) = \mathrm{Nr}(\bar{\eta}) = Q$.

Remark 6.4. The second assertion of Proposition 6.3 is a special case of Grantham [5, Th. 4.3]) .

Remark 6.5. Let $\{U_n\}_{n\geq 0}$, $\{V_n\}_{n\geq 0}$ denote the Lucas sequences associated to (P, Q). Then we have

$$\Big(\frac{V_k}{2}, \frac{U_k}{2}\Big) = \Big(\frac{P}{2}, \frac{1}{2}\Big)^k$$

in $G_{(D)}(\mathbb{Z}[\dfrac{1}{2Q}])$, as is remarked in Example 2.6. This implies the following assertion.

Let n be an odd composite with $(n, DQ) = 1$. Then n is a Frobenius pseudoprime with respect to (P, Q) if and only if

$$U_{n-\varepsilon(n)} \equiv 0 \mod n \text{ and } V_{n-\varepsilon(n)} \equiv \begin{cases} 2 & \text{if } \varepsilon(n) = 1 \\ 2Q & \text{if } \varepsilon(n) = -1 \end{cases}$$

([3, Th.3.6.6]).

Remark 6.6. Let P, Q be integers $\neq 0$ with $D = P^2 - 4Q$ not a square, and let n be an odd composite with $(n, DQ) = 1$. Put $\eta = (P/2, 1/2) \in G_D(\mathbb{Z}/n\mathbb{Z})$. Then $\gamma(\eta) \in \tilde{B}_{\ell psp}(n, D)$ and $Q = \mathrm{Nr}(\eta) \in B_{psp}(n)$ if and only if $\eta^{n-\varepsilon(n)} = aI$, where $a \in \mathbb{Z}/n\mathbb{Z}$ with

$$a^2 = \begin{cases} 1 & \text{if } \varepsilon(n) = 1 \\ Q^2 & \text{if } \varepsilon(n) = -1. \end{cases}$$

In fact, if $\gamma(\eta) \in \tilde{B}_{\ell psp}(n, D)$, then $\gamma(\eta^{n-\varepsilon(n)}) = I$, and therefore, $\eta^{n-\varepsilon(n)} = aI$ for some $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. It follows that $a^2 = \mathrm{Nr}(\eta^{n-\varepsilon(n)}) = Q^{n-\varepsilon(n)} = Q^{n-1}Q^{1-\varepsilon(n)}$. Hence, if $Q \in B_{psp}(n)$, then we obtain $a^2 = Q^{1-\varepsilon(n)}$.

Conversely, assume that there exists $a \in \mathbb{Z}/n\mathbb{Z}$ such that $\eta^{n-\varepsilon(n)} = aI$ and $a^2 = Q^{1-\varepsilon(n)}$. Then we obtain $\gamma(\eta)^{n-\varepsilon(n)} = I$ and $Q^{n-\varepsilon(n)} = \mathrm{Nr}(\eta)^{n-\varepsilon(n)} = a^2$, and therefore $Q^{n-1} = 1$.

Proposition 6.7. *Let P, Q be integers $\neq 0$ with $D = P^2 - 4Q$ not a square, and let n be an odd composite with $(n, DQ) = 1$. Assume that n is a Frobenius pseudoprime with respect to (P, Q). Then n is an Euler pseudoprime to base Q if and only if n is an Euler-Lucas pseudoprime with respect to (P, Q).*

Proof. Put $\eta = (P/2, 1/2) \in G_D(\mathbb{Z}/n\mathbb{Z})$ and $\xi = \gamma(\eta) = \eta\bar{\eta}^{-1}$. Then we have

$$\eta^n = \begin{cases} \eta & \text{if } \varepsilon(n) = 1 \\ \bar{\eta} & \text{if } \varepsilon(n) = -1 \end{cases}$$

since n is a Frobenius pseudoprime with respect to (P, Q). Assume that n is an Euler pseudoprime to base Q, that is to say, $Q^{\frac{n-1}{2}} \equiv \left(\frac{Q}{n}\right) \mod n$. Then, by Remark 2.9, we have $\xi^{\frac{n-1}{2}} = \left(\frac{Q}{n}\right)\eta^{n-1}$. If $\varepsilon(n) = 1$, then we obtain

$$\xi^{\frac{n-\varepsilon(n)}{2}} = \left(\frac{Q}{n}\right)I.$$

If $\varepsilon(n) = -1$, then we obtain

$$\xi^{\frac{n-\varepsilon(n)}{2}} = \left(\frac{Q}{n}\right)\eta^{n-1}\xi = \left(\frac{Q}{n}\right)\eta^{n-1}(\eta\bar{\eta}^{-1}) = \left(\frac{Q}{n}\right)\eta^n\bar{\eta}^{-1} = \left(\frac{Q}{n}\right)I.$$

Therefore n is an Euler-Lucas pseudoprime with respect to (P, Q).

Conversely, assume that n is an Euler-Lucas pseudoprime with respect to (P, Q). Then we have

$$\xi^{\frac{n-\varepsilon(n)}{2}} = \left(\frac{Q}{n}\right)I.$$

If $\varepsilon(n) = -1$, we have

$$\xi^{\frac{n-1}{2}}(\eta\bar{\eta}^{-1}) = \xi^{\frac{n+1}{2}} = \Big(\frac{Q}{n}\Big)I = \Big(\frac{Q}{n}\Big)\eta^n\bar{\eta}^{-1}.$$

Hence in both the cases, we obtain $\xi^{\frac{n-1}{2}} = \Big(\frac{Q}{n}\Big)\eta^{n-1}$. It follows from Remark 2.9 that $Q^{\frac{n-1}{2}} \equiv \Big(\frac{Q}{n}\Big) \mod n$.

Remark 6.8. The if-part of Proposition 6.7 is proved by Baillie and Wagstaff [2, Th.5].

Corollary 6.9. *Let P be an integers $\neq 0$, $Q = \pm 1$ with $D = P^2 - 4Q$ not a square, and let n be an odd composite with $(n, D) = 1$. Then n is a Frobenius pseudoprime with respect to (P, Q) if and only if n is an Euler-Lucas pseudoprime with respect to (P, Q).*

Proof. Assume that n is a Frobenius pseudoprime with respect to (P, Q). It follows from Proposition 6.7 that n is an Euler-Lucas pseudoprime with respect to (P, Q) since n is an Euler pseudoprime to base $Q = \pm 1$.

Conversely, assume that n is an Euler-Lucas pseudoprime with respect to (P, Q). Put $\eta = (P/2, 1/2) \in G_D(\mathbb{Z}/n\mathbb{Z})$ and $\xi = \eta\bar{\eta}^{-1}$. As is remarked at the end of 2.4, we have

$$\eta\bar{\eta} = \mathrm{Nr}(\eta)I = \begin{cases} I & \text{if } Q = 1 \\ -I & \text{if } Q = -1, \end{cases}$$

and therefore

$$\eta^2 = \begin{cases} \xi & \text{if } Q = 1 \\ -\xi & \text{if } Q = -1. \end{cases}$$

In the case of $Q = 1$, we have $\eta^{n-\varepsilon(n)} = \xi^{\frac{n-\varepsilon(n)}{2}} = I$ by Corollary 2.8, which implies

$$\eta^n = \eta^{\varepsilon(n)} = \begin{cases} \eta & \text{if } \varepsilon(n) = 1 \\ \bar{\eta} & \text{if } \varepsilon(n) = -1. \end{cases}$$

In the case of $Q = -1$ and $n \equiv 1 \mod 4$, we have $\eta^{n-\varepsilon(n)} = (-\xi)^{\frac{n-\varepsilon(n)}{2}} = (-1)^{\frac{n-\varepsilon(n)}{2}} I$ by Corollary 2.8, which implies

$$\eta^n = (-1)^{\frac{n-\varepsilon(n)}{2}}\eta^{\varepsilon(n)} = \begin{cases} \eta & \text{if } \varepsilon(n) = 1 \\ -(-\bar{\eta}) = \bar{\eta} & \text{if } \varepsilon(n) = -1. \end{cases}$$

In the case of $Q = -1$ and $n \equiv 3 \mod 4$, we have $\eta^{n-\varepsilon(n)} = (-\xi)^{\frac{n-\varepsilon(n)}{2}} = (-1)^{\frac{n-\varepsilon(n)}{2}}(-I)$ by Corollary 2.8, which implies

$$\eta^n = (-1)^{\frac{n-\varepsilon(n)}{2}+1}\eta^{\varepsilon(n)} = \begin{cases} \eta & \text{if } \varepsilon(n) = 1 \\ -(-\bar{\eta}) = \bar{\eta} & \text{if } \varepsilon(n) = -1. \end{cases}$$

ACKOWLEDGEMENT

This article was finished during the author's stay at Torre Archimede of Università degli studi di Padova. He would like to express his hearty thanks to its hospitality. In particular he is very grateful to Marco Garuti and Alessandro Languasco for their helpful advices and notices, often accompanied with caffè normale. Finally he highly appreciates it that the referee has read the manuscript very carefully.

References

[1] F. Arnault, The Rabin-Monier theorem for Lucas pseudoprimes. Math. Comp. 66 (1997) 869–881
[2] R. Baillie, S. S. Wagstaff, Lucas pseudo-primes. Math. Comp. 35 (1980) 1391–1417
[3] R. Crandall, R. Pomerance, *Prime numbers, a computational perspective. 2nd ed.* Springer-Verlag, 2005.
[4] J. Grantham, A probable prime test with high confidence. J. Number Theory 72 (1998) 32–47
[5] J. Grantham, Frobenius pseudoprimes. Math. Comp. 70 (2001) 873–891
[6] A. Gurevich, B. Kunyavskii, Primality testing through algebraic groups. Arch. Math. 93 (2009) 555–564
[7] M. Kida, Primality tests using algebraic groups. Exp. Math. 13 (2004) 421-427
[8] G. L. Miller, Riemann's hypothesis and a test for primality. J. Comput. and System Sci. 13 (1976) 300–317
[9] L. Monier, Evaluation and comparison of two efficient probabilistic primality testing algorithms. Theoret. Comput. Sci. 12 (1980) 97–108
[10] M. O. Rabin, Probabilistic algorithm for testing primality. J. Number Theory 12 (1980) 128–138
[11] P. Ribenboim, *The little book of big primes*. Springer-Verlag, 1991.
[12] R. Solovay, V. Strassen, A fast Monte-Carlo test for primality. SIAM J. Comput. 6 (1977) 84–85
[13] W. C. Waterhouse, *Introduction to affine group schemes*. Springer-Verlag, 1979.
[14] W. C. Waterhouse, B. Weisfeiler, One-dimensional affine group schemes. J. Algebra 66 (1980) 550–568
[15] H. C. Williams, On numbers analogous to the Carmichael numbers. Canad. Math. Bull. 20 (1977) 133–143

Noriyuki Suwa
Department of Mathematics,
Faculty of Science and Engineerings
Chuo University
1-13-27 Kasuga, Bunkyo-ku, Tokyo 112-8551 Japan
e-mail address: suwa@math.chuo-u.ac.jp

(*Received August 6, 2010*)
(*Revised December 25, 2010*)