中央大学理工学研究所論文集　第10号　2004年
Journal of the Institute of Science and Engineering. Chuo University

擬素数，Euler擬素数，強擬素数に関する幾つかの注意

諏訪紀幸*，新宮領貞治†

本論では擬素数，Euler擬素数，強擬素数に関して知られている結果を整理し，多少の知見を加える．論述が完結するように周知のことでも証明を与えた．また，寄与については各節の最後で明記した．

記号．

n を整数 >1 とする．素数 p に対して n の素因数分解における p の指数を $\mathrm{ord}_p n$ で記す．また，n が奇数のとき，$n-1=2^s m$ (m は奇数) とおき，

$$B_{psp}=\{a\in(\mathbb{Z}/n\mathbb{Z})^\times\ ;\ a^{n-1}=1\},$$
$$B_{epsp}=\left\{a\in(\mathbb{Z}/n\mathbb{Z})^\times\ ;\ a^{\frac{n-1}{2}}=\left(\frac{a}{n}\right)\right\},$$
$$B_{spsp}=\left\{a\in(\mathbb{Z}/n\mathbb{Z})^\times\ ;\ a^m=1 \text{ または } a^{2^k m}=-1 \text{ となる } 0\le k<s \text{ が存在する}\right\}$$

と定義する．

１．用語と定理

命題 1.1. n を整数 >1 とする．$a^{n-1}\not\equiv 1 \mod n$, $(a,n)=1$ となるような整数 a が存在するなら，n は合成数．

証明．p が素数で $p\nmid a$ なら，Fermat の定理から $a^{p-1}\equiv 1 \mod p$.

定義 1.2. n を奇数 >1，a を n と素な整数とする．$a^{n-1}\equiv 1 \mod n$ となるとき，n は a を底とする擬素数であるという．

命題 1.3. n を奇数 >1 とする．$a^{\frac{n-1}{2}}\not\equiv\left(\frac{a}{n}\right) \mod n$, $(a,n)=1$ となるような整数 a が存在するなら，n は合成数．

証明．p が素数 >2 で $p\nmid a$ なら，Euler の規準から $a^{\frac{p-1}{2}}\equiv\left(\frac{a}{p}\right) \mod p$.

定義 1.4. n を奇数 >1，a を n と素な整数とする．$a^{\frac{n-1}{2}}\equiv\left(\frac{a}{n}\right) \mod n$ となるとき，n は a を底とするEuler 擬素数であるという．

命題 1.5. n を奇数 >1 とし，$n-1=2^s m$, $2\nmid m$ とする．$a^m\not\equiv\pm1 \mod n$, $a^{2^k m}\not\equiv -1 \mod n$ $(1\le k<s)$, $(a,n)=1$ となるような整数 a が存在するなら，n は合成数．

証明．p が素数 >2, $p-1=2^s m$, $2\nmid m$, $p\nmid a$ なら，

$$(a^m-1)(a^m+1)(a^{2m}+1)\cdots(a^{2^{s-1}m}+1)=a^{2^s m}-1\equiv 0 \mod p$$

*中央大学理工学部
†ソフトバンク BB

なので，$a^m \equiv 1 \mod p$ または $a^{2^k m} \equiv -1 \mod p$ となる $k < s$ が存在する．

定義 1.6. n を奇数 > 1，$n-1 = 2^s m$，$(m, 2) = 1$ とし，a を n と素な整数とする．n が合成数で $a^m \equiv 1 \mod n$ または $a^{2^k m} \equiv -1 \mod n$ となる $k < s$ が存在するとき，n は a を底とする強擬素数であるという．

定理 1.7. n を奇数 > 1 とし，$n-1 = 2^s m$，$(m, 2) = 1$ と表わす．また，r を n の相異なる素因数の個数，$\nu = \min_{p|n} \mathrm{ord}_2(p-1)$ とする．このとき，
(1) $B_{psp} \supset B_{epsp} \supset B_{spsp}$.
(2) B_{psp} は $(\mathbb{Z}/n\mathbb{Z})^\times$ の部分群で，B_{psp} の位数は

$$\prod_{p|n}(n-1, p-1)$$

で与えられる．
(3) B_{epsp} は $(\mathbb{Z}/n\mathbb{Z})^\times$ の部分群で，B_{epsp} の位数は
(a) $s = \nu$ のとき，

$$2\prod_{p|n}(\frac{n-1}{2}, p-1)$$

(b) $s > \nu$ で $\mathrm{ord}_2(p-1) < s$ となる任意の p に対して $\mathrm{ord}_p n$ が偶数のとき，

$$\prod_{p|n}(\frac{n-1}{2}, p-1)$$

(c) $s > \nu$ で $\mathrm{ord}_2(p-1) < s$，$\mathrm{ord}_p n$ が奇数となるような n の素因数 p が存在するとき，

$$\frac{1}{2}\prod_{p|n}(\frac{n-1}{2}, p-1)$$

で与えられる．
(4) B_{spsp} の基数は

$$\Big(1 + \frac{2^{r\nu}-1}{2^r-1}\Big)\prod_{p|n}(m, p-1)$$

で与えられる．

例 1.8. p を素数 > 2，$n = p^\alpha$ とする．このとき，$B_{psp} = B_{epsp} = B_{spsp}$ で位数は $p-1$ に等しい．

補註 1.9. n を奇数 > 1 とし，$n-1 = 2^s m$，$(m, 2) = 1$ と表わす．このとき，m は奇数なので，$(-1)^m = -1$. したがって，$\{\pm 1\} \subset B_{spsp} \subset B_{epsp} \subset B_{psp}$.

定義 1.10. n を奇数 > 1 とする．n が合成数で $B_{psp} = (\mathbb{Z}/n\mathbb{Z})^\times$ が成立するとき，n は Carmichael 数であるという．

系 1.11. Carmichael 数は平方因子を持たない．また，$n = p_1 p_2 \cdots p_r$ ($p_1, p_2, \ldots, p_r$ は相異なる素数) と表わせば，n が Carmichael 数 $\Leftrightarrow r \geq 3$ で $n-1$ が $p_1 - 1$, $p_2 - 1, \ldots, p_r - 1$ の公倍数.
証明．定理 1.7(2) から，n が Carmichael 数 $\Leftrightarrow \varphi(n) = \prod_{p|n}(n-1, p-1)$．ここで，$\varphi(n) = \prod_{p|n}(p-1) \Leftrightarrow$ n が平方因子を持たない．また，$\prod_{p|n}(p-1) = \prod_{p|n}(n-1, p-1) \Leftrightarrow n$ の各素因数 p に対して $n-1$ が $p-1$ の倍数.

さらに，$r=2$, $n=pq$ $(p<q)$ と仮定すれば，$n-1=(p-1)q+(q-1)$ で $(q-1)|(n-1)$ なので，$(q-1)|(p-1)$．これは $p<q$ に反する．

覚書 1.12. 定理 1.7(1) は Pomerance, Selfridge, Wagstaff と Monier による ([10, Th.3], [9, Th.9])．また，(2) は Baillie, Wagstaff と Monier に ([2,Th.1], [9,Th.1 への追記])，(3) は Monier に ([9, Prop.3])，(4) は Monier による ([9, Prop.1])．(2)(3)(4) で述べられた公式を本稿では Monier の公式と総称することにする．Ribenboim [12, Ch.2.VIII] では

$$
\begin{aligned}
B_{psp} &= \#\{a \in \mathbb{Z}/n\mathbb{Z}\,;\, a^{n-1}=1,\ a\neq 1\},\\
B_{epsp} &= \#\Big\{a \in (\mathbb{Z}/n\mathbb{Z})^\times\,;\, a^{\frac{n-1}{2}}=\Big(\frac{a}{n}\Big),\ a\neq 1\Big\},\\
B_{spsp} &= \#\big\{a \in \mathbb{Z}/n\mathbb{Z}\,;\, a^m=1 \text{ または } a^{2^k m}=-1 \text{ となる } k<s \text{ が存在する},\ a\neq 1\big\}
\end{aligned}
$$

と記号を定義しているが，本論ではそれぞれに 1 を含めて $(\mathbb{Z}/n\mathbb{Z})^\times$ の部分集合を表わす記号として定義を改定した．

命題 1.1，命題 1.3，命題 1.5 は確率的素数判定法の根拠となっている．計算量の評価や実験結果については [2], [7], [9], [10], [11], [14] を参照のこと．Miller [7] は拡張 Riemann 予想を仮定すれば桁数の確定的多項式時間である素数判定のアルゴリズムを提案したが，命題 1.5 を判定法の根拠としている．Rabin [11] は Miller のアルゴリズムを確率的素数判定法として捉え直した．なお，Miller [7] では強擬素数という言葉は定義していないが，$a^{n-1}\equiv 1 \mod n$ で各 $k<s$ に対して $(a^{2^k m}-1,n)=1$ または n が成立するとき，n は a を底とする強擬素数であると定義していると読み取れる．また，Rabin [11] も Miller の定式化に従っている．

系 1.11 は Korselt [6] と Carmichael [3] による．Carmichel 数が無限に存在することが Alford, Granville, Pomerance [1] によって証明された．

２．定理の証明

補題 2.1. n を奇数 >1，d を $n-1$ の約数とする．$H=\{a\in(\mathbb{Z}/n\mathbb{Z})^\times\,;\, a^d\equiv 1 \mod n\}$ と定義すれば，H は $(\mathbb{Z}/n\mathbb{Z})^\times$ の部分群で，H の位数は $\displaystyle\prod_{p|n}(d,p-1)$ で与えられる．

証明．$n=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$ $(p_1,p_2,\dots,p_r$ は相異なる素数) とし，各 i に対して $a_i=a \mod p_i^{e_i}$ とおけば，対応 $a\mapsto(a_1,a_2,\dots,a_r)$ は同型 $(\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\sim} (\mathbb{Z}/p_1^{e_1}\mathbb{Z})^\times\times(\mathbb{Z}/p_2^{e_2}\mathbb{Z})^\times\times\cdots\times(\mathbb{Z}/p_r^{e_r}\mathbb{Z})^\times$ を誘導する．これから，

$$
\begin{aligned}
& a^d\equiv 1 \mod n\\
\Leftrightarrow\ & \text{各 } i \text{ に対して } a^d\equiv 1 \mod p_i^{e_i}\\
\Leftrightarrow\ & \text{各 } i \text{ に対して } a \text{ の } (\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times \text{ における位数が } d \text{ の約数}\\
\Leftrightarrow\ & \text{各 } i \text{ に対して } a \text{ の } (\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times \text{ における位数が } (d,\varphi(p_i^{e_i})) \text{ の約数}.
\end{aligned}
$$

ここで，d が $n-1$ の約数なので，d と p_i は互いに素．したがって，$(d,\varphi(p_i^{e_i}))=(d,(p_i-1)p_i^{e_i-1})=(d,p_i-1)$．また，$(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times$ が巡回群なので，位数が (d,p_i-1) の約数であるような $(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times$ の元の個数は (d,p_i-1) に等しい．

補題 2.2. n を奇数 >1，k を整数 ≥ 1 とし，$\nu=\min_{p|n}\operatorname{ord}_2(p-1)$ とおく．このとき，$a^{2^k}\equiv -1 \mod n$ となるような $a\in\mathbb{Z}$ が存在する $\Leftrightarrow k\leq\nu-1\Leftrightarrow n$ の各素因数 p に対して $p-1$ が 2^{k+1} で割り切れる．

証明.　$n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ ($p_1, p_2, \ldots, p_r$ は相異なる素数) とする．このとき,

$$\begin{aligned} & a^{2^k} \equiv -1 \mod n \\ \Leftrightarrow\ & \text{各 } i \text{ に対して } a^{2^k} \equiv -1 \mod p_i^{e_i} \\ \Leftrightarrow\ & \text{各 } i \text{ に対して } a \text{ の } (\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times \text{ における位数が } 2^{k+1} \text{ に等しい.} \end{aligned}$$

ここで，$(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times$ が巡回群なので,

$$(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times \text{ が位数 } 2^{k+1} \text{ の元を持つ } \Leftrightarrow\ 2^{k+1} | \varphi(p_i^{e_i}) \ \Leftrightarrow\ 2^{k+1} | (p_i - 1).$$

これから結論を得る.

補題 2.3. n を奇数 > 1 とし，$\nu = \min_{p|n} \mathrm{ord}_2(p-1)$ とおく．このとき，$\mathrm{ord}_2(n-1) \geq \nu$．さらに,

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

$$\mathrm{ord}_2(n-1) > \nu \ \Leftrightarrow \sum_{\substack{p|n \\ \mathrm{ord}_2(p-1)=\nu}} \mathrm{ord}_p n \equiv 0 \mod 2.$$

証明.　p を n の素因数とする．このとき,

$$\begin{aligned} & \mathrm{ord}_2(p-1) = \nu \ \Leftrightarrow\ p \equiv 1 + 2^\nu \mod 2^{\nu+1}, \\ & \mathrm{ord}_2(p-1) > \nu \ \Leftrightarrow\ p \equiv 1 \mod 2^{\nu+1}. \end{aligned}$$

これから

$$n \equiv 1 + \Big(\sum_{\substack{p|n \\ \mathrm{ord}_2(p-1)=\nu}} \mathrm{ord}_p n \Big) 2^\nu \mod 2^{\nu+1}$$

を得る.

系 2.4. n を奇数 > 1 とし，$\nu = \min_{p|n} \mathrm{ord}_2(p-1)$ とおく．このとき,

任意の n の素因数 p に対して $\mathrm{ord}_2(p-1) \geq \mathrm{ord}_2(n-1)$ が成立する $\Leftrightarrow\ \mathrm{ord}_2(n-1) = \nu$,
$\mathrm{ord}_2(p-1) < \mathrm{ord}_2(n-1)$ となるような n の素因数 p が存在する $\Leftrightarrow\ \mathrm{ord}_2(n-1) > \nu$.

系 2.5. n を奇数 > 1，a を整数とし，$\nu = \min_{p|n} \mathrm{ord}_2(p-1)$ とおく．このとき,

(1) $a^{2^{\nu-1}} \equiv 1 \mod n$ なら $\left(\dfrac{a}{n}\right) = 1$;

(2) $a^{2^{\nu-1}} \equiv -1 \mod n$ で $\mathrm{ord}_2(n-1) > \nu$ なら $\left(\dfrac{a}{n}\right) = 1$;

(3) $a^{2^{\nu-1}} \equiv -1 \mod n$ で $\mathrm{ord}_2(n-1) = \nu$ なら $\left(\dfrac{a}{n}\right) = -1$.

証明. $a^{2^{\nu-1}} \equiv 1 \mod n$ と仮定する．Euler の判定法から n の各素因数 p に対して

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} = (a^{2^{\nu-1}})^{\frac{p-1}{2^\nu}} \equiv 1 \mod p.$$

これから，$\left(\frac{a}{n}\right) = 1$.

一方，$a^{2^{\nu-1}} \equiv -1 \mod n$ と仮定すれば，

$$\frac{p-1}{2^\nu} \equiv 0 \mod 2 \Leftrightarrow \mathrm{ord}_2(p-1) > \nu,$$
$$\frac{p-1}{2^\nu} \equiv 1 \mod 2 \Leftrightarrow \mathrm{ord}_2(p-1) = \nu$$

なので，

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \mathrm{ord}_2(p-1) > \nu \\ -1 & \mathrm{ord}_2(p-1) = \nu. \end{cases}$$

したがって，

$$e = \sum_{\substack{p|n \\ \mathrm{ord}_2(p-1)=\nu}} \mathrm{ord}_p n$$

とおけば，

$$\left(\frac{a}{n}\right) = (-1)^e.$$

ここで，補題 2.3 から

$$e \equiv 0 \mod 2 \Leftrightarrow \mathrm{ord}_2(n-1) > \nu,$$
$$e \equiv 1 \mod 2 \Leftrightarrow \mathrm{ord}_2(n-1) = \nu.$$

2.6. 定理 1.7 の証明.

(1) $a \in B_{epsp}$ とすれば，定義から $a^{\frac{n-1}{2}} \equiv \pm 1 \mod n$. したがって，$a^{n-1} \equiv (\pm 1)^2 = 1 \mod n$. これから，$a \in B_{psp}$.

次に，$a \in B_{spsp}$ とする．このとき，補題 2.2 から $a^m \equiv 1 \mod n$ または $a^{2^k m} \equiv -1 \mod n$ となるような $k \leq \nu - 1$ が存在する.

$s = \nu$ の場合，

$$a^{\frac{n-1}{2}} = a^{2^{\nu-1}m} \equiv \pm 1 \mod n.$$

したがって，系 2.5 から

$$\left(\frac{a}{n}\right) = \begin{cases} 1 & a^{2^{\nu-1}m} \equiv 1 \mod n \\ -1 & a^{2^{\nu-1}m} \equiv -1 \mod n. \end{cases}$$

これから，$a \in B_{epsp}$.

$s > \nu$ の場合，

$$a^{\frac{n-1}{2}} = a^{2^{s-1}m} = (a^{2^{\nu-1}m})^{2^{s-\nu}} \equiv 1 \mod n.$$

したがって，系 2.5 から $\left(\frac{a}{n}\right) = 1$. これから，$a \in B_{epsp}$.

(2) 補題 2.1 を $d = n - 1$ に適用して結論を得る.

(3) $C=\{a\in\mathbb{Z}/n\mathbb{Z}\,;\,a^{\frac{n-1}{2}}=1\}$ とおけば，C は $(\mathbb{Z}/n\mathbb{Z})^\times$ の部分群．さらに，補題 2.1 から C の位数は $\prod_{p|n}(\frac{n-1}{2},p-1)$ に等しい．

(a) $s=\nu$ の場合．$a\in C$ なら $a^{2^{\nu-1}m}\equiv 1 \mod n$ で m が奇数なので，系 2.5 から

$$\Big(\frac{a}{n}\Big)=\Big(\frac{a}{n}\Big)^m=\Big(\frac{a^m}{n}\Big)=1.$$

したがって，$a\in B_{epsp}$.

一方，補題 2.2 から $a^{2^{\nu-1}}\equiv -1 \mod n$ となるような $a\in\mathbb{Z}$ が存在する．このとき，系 2.5 から，$\Big(\frac{a}{n}\Big)=-1$．これから，$a\in B_{epsp}$.

以上のことから，$a\mapsto\Big(\frac{a}{n}\Big)$ によって定義される準同型 $B_{epsp}\to\{\pm1\}$ は全射で，その核は C に一致する．これから，C は B_{epsp} の指数 2 の部分群．

(b)(c) $s>\nu$ の場合．補題 2.2 から $a^{\frac{n-1}{2}}=a^{2^{s-1}m}\equiv -1 \mod n$ となるような $a\in\mathbb{Z}$ は存在しない．したがって，$B_{epsp}\subset C$.

ここで，$a^{\frac{n-1}{2}}\equiv 1 \mod n$, p が n の素因数で $\mathrm{ord}_2(p-1)\geq s$ なら $\Big(\frac{a}{p}\Big)=1$．実際，$a^{\frac{p-1}{2}}\equiv\pm1 \mod p$ で m が奇数なので，

$$\Big(\frac{a}{p}\Big)\equiv a^{\frac{p-1}{2}}\equiv(a^{\frac{p-1}{2}})^m=(a^{2^{s-1}m})^{\frac{p-1}{2^s}}\equiv 1 \mod p.$$

したがって，$\mathrm{ord}_2(p-1)<s$ となる n の各素因数 p に対して $\mathrm{ord}_p n$ が偶数なら，任意の $a\in C$ に対して $\Big(\frac{a}{n}\Big)=1$ が成立する．これから，$B_{epsp}=C$.

一方，$\mathrm{ord}_p n$ が奇数で $\mathrm{ord}_2(p-1)<s=\mathrm{ord}_2(n-1)$ となるような n の素因数 p が存在すると仮定する．$n=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$ $(p_1,p_2,\dots,p_r$ は相異なる素数，$p_1=p)$ と表わし，$\Big(\frac{a_1}{p_1}\Big)=-1$ となるような a_1 を取る．このとき，$a_1^{\frac{p_1-1}{2}}\equiv -1 \mod p_1$．$a_1$ を $a_1^{p_1^{e_1-1}}$ に置き換えることによって，$a_1^{\frac{p_1-1}{2}}\equiv -1 \mod p_1^{e_1}$ と仮定してよい．さらに，$s_1=\mathrm{ord}_2(p_1-1)$ とおけば，$\frac{p_1-1}{2^{s_1}}$ が奇数なので，

$$\Big(\frac{a_1^{\frac{p_1-1}{2^{s_1}}}}{p_1}\Big)=\Big(\frac{a_1}{p_1}\Big)^{\frac{p_1-1}{2^{s_1}}}=-1.$$

したがって，a_1 を $a_1^{\frac{p_1-1}{2^{s_1}}}$ で置き換えることによって，$a_1^{2^{s_1-1}}\equiv -1 \mod p_1^{e_1}$ と仮定してよい．このとき，$s_1-1<s-1$ なので，$a_1^{2^{s-1}}\equiv 1 \mod p_1^{e_1}$．したがって，$a_1^{\frac{n-1}{2}}\equiv 1 \mod p_1^{e_1}$．したがって，$a$ を

$$a\equiv a_1 \mod p_1^{e_1},\ a\equiv 1 \mod p_2^{e_2},\dots,\ a\equiv 1 \mod p_r^{e_r}$$

となるように取れば，$a^{\frac{n-1}{2}}\equiv 1 \mod n$．一方，

$$\Big(\frac{a}{p_1}\Big)=-1,\ \Big(\frac{a}{p_2}\Big)=1,\dots,\ \Big(\frac{a}{p_r}\Big)=1$$

で e_1 が奇数なので，$\Big(\frac{a}{n}\Big)=-1$.

以上のことから，$a\mapsto\Big(\frac{a}{n}\Big)$ によって定義される準同型 $C\to\{\pm1\}$ は全射で，その核は B_{epsp} に一致する．したがって，B_{epsp} は C の指数 2 の部分群．

(4) 各 $k\geq 0$ に対して $C_k=\{a\in(\mathbb{Z}/n\mathbb{Z})^\times\,;\,a^{2^k m}=1\}$ とおけば，C_k は $(\mathbb{Z}/n\mathbb{Z})^\times$ の部分群．さらに，補題 2.1 から C_k の位数は $\prod_{p|n}(2^k m,p-1)$ に等しい．また，$k\leq\nu$ なら

$$\prod_{p|n}(2^k m,p-1)=2^{rk}\prod_{p|n}(m,p-1).$$

ここで，各 $k \geq 0$ に対して $B_k = \{a \in (\mathbb{Z}/n\mathbb{Z})^\times\ ;\ a^{2^k m} = -1\}$ とおけば，m が奇数なので，

$$B_k \neq \emptyset \ \Leftrightarrow\ c^{2^k} \equiv -1 \mod n \text{ となるような } c \text{ が存在する．}$$

さらに，$B_k \neq \emptyset$ なら $a \mapsto ca$ は双射 $C_k \xrightarrow{\sim} B_k$ を与える．ここで，補題 2.2 から，$c^{2^k} \equiv -1 \mod n$ となるような c が存在する $\Leftrightarrow k+1 \leq \nu$．したがって，$k \geq \nu$ なら $B_k = \emptyset$．これから，B_{spsp} の分割

$$B_{spsp} = C_0 \cup B_0 \cup B_1 \cup \cdots \cup B_{\nu-1}$$

を得る．以上のことから，

$$|B_{spsp}| = (1 + 1 + 2^r + \cdots + 2^{r(\nu-1)}) \prod_{p|n} (m, p-1) = \Big(1 + \frac{2^{r\nu}-1}{2^r - 1}\Big) \prod_{p|n} (m, p-1)$$

を得る．

補註 2.8. n を奇数 > 1 とし，$n - 1 = 2^s m,\ (m, 2) = 1$ と表わす．また，r を n の相異なる素因数の個数，$\nu = \min\limits_{p|n} \operatorname{ord}_2(p-1)$ とする．このとき，B_{spsp} が $(\mathbb{Z}/n\mathbb{Z})^\times$ の部分群 $\Leftrightarrow r = 1$ または $\nu = 1$.

実際，$(n-1, p-1)$ は $(m, p-1)$ と 2 巾を除いて等しいので，$|B_{psp} : C_0|$ は 2 の巾．したがって，B_{spsp} が $(\mathbb{Z}/n\mathbb{Z})^\times$ の部分群なら $|B_{spsp} : C_0|$ は 2 の巾．ここで，$|B_{spsp} : C_0| = 1 + 1 + 2^r + \cdots + 2^{(\nu-1)r}$ が 2 の巾 $\Leftrightarrow r = 1$ または $\nu = 1$.

補註 2.9. n を奇数 > 1 とし，$n-1 = 2^s m,\ (m, 2) = 1$ と表わす．また，$\nu = \min\limits_{p|n} \operatorname{ord}_2(p-1)$，$\tilde{C}$ を B_{spsp} によって生成される $(\mathbb{Z}/n\mathbb{Z})^\times$ の部分群とする．このとき，$\tilde{C} = C_{\nu-1} \cup B_{\nu-1}$ で $C_{\nu-1} \supset C_0 \cup B_0 \cup B_1 \cup \cdots B_{\nu-2}$．したがって，

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

補註 2.10. n を奇数 > 1 とし，$n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ ($p_1, p_2, \ldots, p_r$ は相異なる素数) を n の素因数分解とする．また，$n - 1 = 2^s m,\ (m, 2) = 1$ と表わす．さらに，各 i に対して $p_i - 1 = 2^{s_i} m_i,\ (m_i, 2) = 1$ と表わし，$\nu = \min\limits_{1 \leq i \leq r} s_i$ とおく．このとき，

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

また，

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

$$\operatorname{ord}_2 |B_{epsp}| = \begin{cases} 1 + r(s-1) & s = \nu \\ \displaystyle\sum_{i=1}^{r} \min(s-1, s_i) & s > \nu \text{ で } s_i < s \text{ となる任意の } i \text{ に対して } e_i \text{ が偶数} \\ \displaystyle -1 + \sum_{i=1}^{r} \min(s-1, s_i) & s > \nu \text{ で } s_i < s,\ e_i \text{ が奇数となるような } i \text{ が存在する} \end{cases}$$

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

が成立する．さらに，$|B_{psp}|$，$|B_{epsp}|$，$\tilde{C}$ は 2 巾を除いて $\prod_{i=1}^{r}(m, m_i)$ に等しい．

覚書 2.11. 補註 2.8 は Koblitz [5], 第 5 章 1 節の章末問題 23 で述べられている．

３．幾つかの帰結

命題 3.1. n を奇数 > 1 とする．このとき，$B_{psp} = B_{epsp} \Leftrightarrow n$ は素数の巾，または，n は平方数で n の各素因数 p に対して $\mathrm{ord}_2(p-1) < \mathrm{ord}_2(n-1))$ が成立する．

証明．$n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ ($p_1, p_2, \ldots, p_r$ は相異なる素数) とし，$n - 1 = 2^s m$，$(m, 2) = 1$ と表わす．また，各 i に対して $p_i - 1 = 2^{s_i} m_i$，$(m_i, 2) = 1$ と表わし，$\nu = \min_{1 \le i \le r} s_i$ とおく．補註 2.10 から，$|B_{psp}|$ は $|B_{epsp}|$ に 2 巾を除いて等しいので，$B_{psp} = B_{epsp} \Leftrightarrow \mathrm{ord}_2|B_{psp}| = \mathrm{ord}_2|B_{epsp}|$.

$s > \nu$ で $s_i < s$ で e_i が奇数となるような i が存在する場合，

$$\mathrm{ord}_2|B_{psp}| = \sum_{i=1}^{r} \min(s, s_i) > -1 + \sum_{i=1}^{r} \min(s-1, s_i) = \mathrm{ord}_2|B_{epsp}|$$

なので，$B_{psp} \neq B_{epsp}$.

また，$s > \nu$ で $s_i < s$ となる任意の i に対して e_i が偶数である場合，

$$\mathrm{ord}_2|B_{psp}| = \sum_{i=1}^{r} \min(s, s_i),\ \mathrm{ord}_2|B_{epsp}| = \sum_{i=1}^{r} \min(s-1, s_i)$$

なので，

$$B_{psp} = B_{epsp} \ \Leftrightarrow\ \sum_{i=1}^{r} \min(s, s_i) = \sum_{i=1}^{r} \min(s-1, s_i) \ \Leftrightarrow\ \text{各 } i \text{ に対して } s_i < s.$$

さらに，このとき，e_i に関する条件から n は平方数.

また，$s = \nu$ の場合，

$$\mathrm{ord}_2|B_{psp}| = \sum_{i=1}^{r} \min(s, s_i) = rs,\ \mathrm{ord}_2|B_{epsp}| = 1 + \sum_{i=1}^{r} \min(s-1, s_i) = 1 + r(s-1)$$

なので，

$$B_{psp} = B_{epsp} \ \Leftrightarrow\ rs = 1 + r(s-1) \ \Leftrightarrow\ r = 1.$$

系 3.2. n を奇の合成数とする．このとき，$|B_{epsp}| \le \varphi(n)/2$.

証明．B_{epsp} が $(\mathbb{Z}/n\mathbb{Z})^\times$ の部分群なので，$B_{epsp} \neq (\mathbb{Z}/n\mathbb{Z})^\times$ を示せばよい．n が Carmichael 数でなければ，$|B_{epsp}| \le |B_{psp}| < \varphi(n)$．また，$n$ が Carmichael 数なら，n は素数巾でも平方数でもないので，$|B_{epsp}| < |B_{psp}|$.

補題 3.3. n を奇数 > 1 とし，$s = \mathrm{ord}_2(n-1)$，$\nu = \min_{p|n} \mathrm{ord}_2(p-1))$ とおく．また，$\tilde{C}$ を B_{spsp} によって生成される $(\mathbb{Z}/n\mathbb{Z})^\times$ の部分群とする．このとき，$\tilde{C}$ が B_{epsp} に一致する $\Leftrightarrow s = \nu$，または，n が素数の巾，または，$n = p^\alpha q^\beta$ (p, q は相異なる素数で $\mathrm{ord}_2(p-1) = \mathrm{ord}_2(q-1)$，$\alpha \equiv \beta \equiv 1 \mod 2$).

証明．$n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ ($p_1, p_2, \ldots, p_r$ は相異なる素数) とし，$n - 1 = 2^s m$，$(m, 2) = 1$ と表わす．また，各 i に対して $p_i - 1 = 2^{s_i} m_i$，$(m_i, 2) = 1$ と表わせば，$\nu = \min_{1 \le i \le r} s_i$．補註 2.10 から，$|\tilde{C}|$ は $|B_{epsp}|$ に 2 巾を除いて等しいので，$B_{epsp} = \tilde{C} \Leftrightarrow \mathrm{ord}_2|B_{epsp}| = \mathrm{ord}_2|\tilde{C}|$．また，$\mathrm{ord}_2|\tilde{C}| = 1 + r(\nu - 1)$.

$s=\nu$ の場合，

$$\mathrm{ord}_2|B_{epsp}| = 1 + r(\nu - 1)$$

なので，$B_{epsp} = \tilde{C}$.

また，$s > \nu$ で $s_i < s$ となる任意の i に対して e_i が偶数である場合，

$$\mathrm{ord}_2|B_{epsp}| = \sum_{i=1}^{r} \min(s-1, s_i)$$

で各 i に対して $\min(s-1, s_i) \geq \nu$ なので，

$$B_{epsp} = \tilde{C} \ \Leftrightarrow \ \sum_{i=1}^{r} \min(s-1, s_i) = 1 + r(\nu - 1) \ \Leftrightarrow \ r = 1.$$

一方，$s > \nu$ で $s_i < s$ で e_i が奇数となるような i が存在する場合，

$$\mathrm{ord}_2|B_{epsp}| = -1 + \sum_{i=1}^{r} \min(s-1, s_i)$$

で各 i に対して $\min(s-1, s_i) \geq \nu$ なので，

$$B_{epsp} = \tilde{C} \ \Leftrightarrow \ -1 + \sum_{i=1}^{r} \min(s-1, s_i) = 1 + r(\nu - 1) \ \Leftrightarrow \ r = 2,\ s_1 = s_2 = \nu.$$

さらに，このとき，$e_1 \equiv e_2 \mod 2$ で e_1, e_2 のどちらかが奇数なので，$e_1 \equiv e_2 \equiv 1 \mod 2$.

命題 3.4. n を奇数 > 1 とする．このとき，$B_{epsp} = B_{spsp} \Leftrightarrow n \equiv 3 \mod 4$，または，$n$ が素数の巾，または，$n = p^\alpha q^\beta$ (p, q は相異なる素数で $p \equiv q \equiv 3 \mod 4$, $\alpha \equiv \beta \equiv 1 \mod 2$).

証明．$n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ ($p_1, p_2, \ldots, p_r$ は相異なる素数) とし，$n - 1 = 2^s m$, $(m, 2) = 1$ と表わす．さらに，各 i に対して $p_i - 1 = 2^{s_i} m_i$, $(m_i, 2) = 1$ と表わし，$\nu = \min\limits_{1 \leq i \leq r} s_i$ とおく．

$\tilde{C}$ を B_{spsp} によって生成される $(\mathbb{Z}/n\mathbb{Z})^\times$ の部分群とすれば，$B_{epsp} = B_{spsp} \Leftrightarrow B_{epsp} = \tilde{C}$ で $\tilde{C} = B_{spsp}$. ここで，補題 3.3 から

$$B_{epsp} = \tilde{C} \ \Leftrightarrow \ s = \nu, \text{ または, } \ r = 1, \text{ または, } \ r = 2,\ s_1 = s_2 = \nu,\ e_1 \equiv e_2 \equiv 1 \mod 2.$$

また，補註 2.8 から

$$\tilde{C} = B_{spsp} \ \Leftrightarrow \ r = 1, \text{ または, } \ \nu = 1.$$

両者を組み合わせて

$$B_{epsp} = B_{spsp} \ \Leftrightarrow \ s = 1, \text{ または, } \ r = 1, \text{ または, } \ r = 2,\ s_1 = s_2 = 1,\ e_1 \equiv e_2 \equiv 1 \mod 2$$

を得る．

命題 3.5. n を奇数 > 1 とする．このとき，
(1) $|B_{epsp}| = \varphi(n)/2 \Leftrightarrow n$ は Carmichael 数で n の各素因数 p に対して $\mathrm{ord}_2(p-1) < \mathrm{ord}_2(n-1)$ が成立する．
(2) $|B_{epsp}| = \varphi(n)/4 \Leftrightarrow n = pq$ (p, q は素数で $q = 2p - 1$)，または，n は $p_1 p_2 p_3$ (p_1, p_2, p_3 は相異なる素数で $\mathrm{ord}_2(p_1 - 1) = \mathrm{ord}_2(p_2 - 1) = \mathrm{ord}_2(p_3 - 1)$) の形の Carmaichael 数，または，$n$ は Carmichael 数

で一つの素因数 p に対して $\mathrm{ord}_2(p-1)=\mathrm{ord}_2(n-1)$ で他の素因数 q に対して $\mathrm{ord}_2(q-1)<\mathrm{ord}_2(n-1)$ が成立する．

証明．$n=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$ ($p_1,p_2,\ldots,p_r$ は相異なる素数) とし，$n-1=2^sm,\ (m,2)=1$ と表わす．さらに，各 i に対して $p_i-1=2^{s_i}m_i,\ (m_i,2)=1$ と表わし，$\nu=\min\limits_{1\le i\le r}s_i$ とおく．このとき，$\mathrm{ord}_2\varphi(n)=\sum\limits_{i=1}^{r}s_i$.

(1) $|B_{epsp}|=\varphi(n)/2$ と仮定する．このとき，n は平方因子を持たず，各 i に対して $m_i|m$ が成立する．また，$r\ge 2$.

$s=\nu$ の場合，補註 2.10 から $\mathrm{ord}_2|B_{epsp}|=1+r(s-1)$ なので，

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

したがって，

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

ここで，各 i に対して $s_i-s+1\ge 1$ なので，$r=2,\ s_1=s_2=s$．したがって，補題 2.3 から $s>\nu$．これは $s=\nu$ に反する．

次に，$s>\nu$ の場合，n は平方因子を持たないので，補註 2.10 から $\mathrm{ord}_2|B_{epsp}|=-1+\sum\limits_{i=1}^{r}\min(s-1,s_i)$.

したがって，

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

したがって，

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

これから各 i に対して $s_i\le s-1$ が成立することが従う．さらに，各 i に対して $m_i|m$ なので，n は Carmichael 数.

逆に，n が Carmichael 数で各 i に対して $s_i<s$ が成立すると仮定する．このとき，各 i に対して $(p_i-1)|\dfrac{n-1}{2}$．さらに，$s>\nu$ で n は平方因子を持たないので，補註 2.10 から

$$|B_{epsp}|=\frac{1}{2}\prod_{i=1}^{r}(\frac{n-1}{2},p_i-1)=\frac{1}{2}\prod_{i=1}^{r}(p_i-1)=\frac{\varphi(n)}{2}.$$

(2) $|B_{epsp}|=\varphi(n)/4$ と仮定する．このとき，n は平方因子を持たず，各 i に対して $m_i|m$ が成立する．また，$r\ge 2$.

$s=\nu$ の場合，補註 2.10 から $\mathrm{ord}_2|B_{epsp}|=1+r(s-1)$ なので，

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

したがって，

$$\sum_{i=1}^{r}(s_i-s+1)=3.$$

ここで，各 i に対して $s_i - s + 1 \geq 1$ なので，$r = 2,\ s_1 = s, s_2 = s+1$，または，$r = 3,\ s_1 = s_2 = s_3 = s$.
(a) $r = 2,\ s_1 = s, s_2 = s+1$ の場合，$m_1|m$ なので，$(p_1-1)|(n-1)$．ここで，$n-1 = (p_1-1)p_2+(p_2-1)$ なので，$(p_1-1)|(p_2-1)$．また，$m_2|m$ なので，$(p_2-1)|2(n-1)$．ここで，$2(n-1) = 2(p_2-1)p_1+2(p_1-1)$ なので，$(p_2-1)|2(p_1-1)$．以上のことから，$p_2 - 1 = 2(p_1-1)$.
(b) $r = 3,\ s_1 = s_2 = s_3 = s$ の場合，各 i に対して $(m, m_i) = m_i$ なので，n は Carmichael 数.

次に，$s > \nu$ の場合，n は平方因子を持たないので，補註 2.10 から $\mathrm{ord}_2|B_{epsp}| = -1+\sum_{i=1}^{r}\min(s-1, s_i)$.
したがって，

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

したがって，

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

これから，$s_i = s$ となるような i が唯一つ存在し，$j \neq i$ なら $s-1 \geq s_i$ が成立することが従う．さらに，各 i に対して $m_i|m$ なので，n は Carmichael 数.

逆に，$n = p_1p_2$ で $p_2 - 1 = 2(p_1-1)$ と仮定する．このとき，

$$p_1 - 1 = 2^{s_1}m_1,\ p_2 - 1 = 2^{s_1+1}m_1,\ n - 1 = 2^{s_1}m_1(3 + 2^{s_1+1}m_1)$$

なので，$s_2 = s_1 + 1,\ m_2 = m_1,\ s = s_1,\ m_1|m$．したがって，補註 2.10 から

$$\mathrm{ord}_2|B_{epsp}| = 1 + 2(s-1) = -2 + (s_1 + s_2) = -2 + \mathrm{ord}_2\,\varphi(n).$$

次に，n が $p_1p_2p_3$ $(s_1 = s_2 = s_3)$ の形の Carmaichael 数とする．このとき，補題 2.3 から $s = \nu$ なので，補註 2.10 から

$$\mathrm{ord}_2|B_{epsp}| = 1 + 3(s-1) = -2 + (s_1 + s_2 + s_3) = -2 + \mathrm{ord}_2\,\varphi(n).$$

また，n が Carmichael 数で，$s_1 = s$ で各 $i \geq 2$ に対して $s_i < s$ が成立すると仮定する．このとき，$s > \nu$ で n は平方因子を持たないので，補註 2.10 から

$$\mathrm{ord}_2|B_{epsp}| = -1 + \sum_{i=1}^{r}\min(s-1, s_i) = -1 + (s_1 - 1) + \sum_{i=2}^{r} s_i = -2 + \sum_{i=1}^{r} s_i = -2 + \mathrm{ord}_2\,\varphi(n).$$

これから，いずれの場合も，$|B_{epsp}| = \varphi(n)/4$.

例 3.6. (1) $|B_{epsp}| = \varphi(n)/2$ となる $n < 10^5$.

$1729 = 7 \times 13 \times 19$
$2465 = 5 \times 17 \times 29$
$15841 = 7 \times 31 \times 73$
$41041 = 7 \times 11 \times 13 \times 41$
$46657 = 13 \times 37 \times 97$
$75361 = 11 \times 13 \times 17 \times 31$

(2) $|B_{epsp}| = \varphi(n)/4$ となる $n < 10^5$.

第 1 の型

$15 = 3 \times 5$
$91 = 7 \times 13$
$703 = 19 \times 37$
$1891 = 31 \times 61$
$2701 = 37 \times 73$
$12403 = 79 \times 157$
$18721 = 97 \times 193$
$38503 = 139 \times 277$
$49141 = 157 \times 313$
$79003 = 199 \times 397$
$88831 = 211 \times 421$

第 2 の型
$8911 = 7 \times 19 \times 67$
$29341 = 13 \times 37 \times 61$
$561 = 3 \times 11 \times 17$

第 3 の型
$1105 = 5 \times 13 \times 17$
$2821 = 7 \times 13 \times 31$
$6601 = 7 \times 23 \times 41$
$10585 = 5 \times 29 \times 73$
$52633 = 7 \times 73 \times 103$
$62745 = 3 \times 5 \times 47 \times 89$

系 3.7. n を奇の合成数とする．このとき，

(1) $n \neq 9$ なら $|B_{spsp}| \leq \varphi(n)/4$.

(2) $|B_{spsp}| = \varphi(n)/4 \Leftrightarrow n = pq$ (p, q は素数で $p \equiv 3 \mod 4$, $q = 2p-1$), または, n は $p_1p_2p_3$ (p_1, p_2, p_3 は相異なる素数で $p_1 \equiv p_2 \equiv p_3 \equiv 3 \mod 4$) の形の Carmaichael 数.

証明. $n = p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$ ($p_1, p_2, \ldots, p_r$ は相異なる素数) とし，$n-1 = 2^s m$, $(m, 2) = 1$ と表わす．さらに，各 i に対して $p_i - 1 = 2^{s_i} m_i$, $(m_i, 2) = 1$ と表わし，$\nu = \min\limits_{1 \leq i \leq r} s_i$ とおく．

系 3.2 から，$|B_{spsp}| \leq |B_{epsp}| \leq \varphi(n)/2$.

(a) $|B_{epsp}| = \varphi(n)/2$ の場合．命題 3.5 から，n は Carmichael 数で各 i に対して $s_i < s$．ここで，$\tilde{C}$ を B_{spsp} によって生成される $(\mathbb{Z}/n\mathbb{Z})^\times$ の部分群とすれば，補註 2.10 から，$|\tilde{C}|$ と $|B_{epsp}|$ は 2 巾を除いて等しく，

$$\mathrm{ord}_2|B_{epsp}| - \mathrm{ord}_2|\tilde{C}| = \Big(-1 + \sum_{i=1}^{r} s_i\Big) - \{1 + r(\nu - 1)\} = -2 + \sum_{i=1}^{r}(s_i - \nu + 1).$$

さらに，

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

実際, n が Carmichael 数なので, $r \geq 3$．したがって, 各 i に対して $s_i - \nu + 1 \geq 1$ なので, $-2 + \sum\limits_{i=1}^{r}(s_i - \nu + 1) \geq 1$．ここで，$-2 + \sum\limits_{i=1}^{r}(s_i - \nu + 1) = 1$ と仮定すれば，$r = 3$ で $s_1 = s_2 = s_3 = 1$．したがって，補題 2.3 から $s = 1$．これは $s > \nu$ に反する．

以上のことから，$|B_{spsp}| \le |\tilde{C}| \le |B_{epsp}|/4 = \varphi(n)/8$.

(b) $|B_{epsp}| = \varphi(n)/3$ の場合．$n = 9$ で $|B_{spsp}| = \varphi(n)/3$.

(c) $|B_{epsp}| = \varphi(n)/4$ の場合．命題 3.5 から，$r = 2$, $p_2 = 2p_1 - 1$，または，n は Carmichael 数で $r = 3$, $s_1 = s_2 = s_3$，または，n は Carmichael 数で一つの i に対して $s_i = s$ で $j \ne i$ なら $s_j < s$．ここで，命題 3.4 から

$$B_{spsp} = B_{epsp} \Leftrightarrow s = 1, \text{ または, } r = 1, \text{ または, } r = 2,\ s_1 = s_2 = 1,\ e_1 \equiv e_2 \equiv 1 \mod 2.$$

以上のことから

$$|B_{spsp}| = \varphi(n)/4 \Leftrightarrow$$
$$r = 2,\ s = 1,\ p_2 = 2p_1 - 1, \text{ または，} n \text{ は Carmichael 数で } r = 3,\ s_1 = s_2 = s_3 = 1.$$

を得る．ここで，$p_2 = 2p_1 - 1$ の場合，$s = s_1$.

例 3.8. $|B_{spsp}| = \varphi(n)/4$ となる $n < 10^5$.

第 1 の型

$15 = 3 \times 5$
$91 = 7 \times 13$
$703 = 19 \times 37$
$1891 = 31 \times 61$
$12403 = 79 \times 157$
$38503 = 139 \times 277$
$79003 = 199 \times 397$
$88831 = 211 \times 421$

第 2 の型

$8911 = 7 \times 19 \times 67$

補註 3.9. n を奇数 > 1 とし，$n - 1 = 2^s m$, $(m, 2) = 1$ と表わす．また，$\nu = \min_{p|n} \mathrm{ord}_2(p-1)$ とおく．このとき，

(1) $B_{epsp} = \{\pm 1\} \Leftrightarrow n$ が 3 の巾，または，$n \equiv 3 \mod 4$ で n の各素因数 p に対して $(m, p-1) = 1$，または，$n = p^\alpha q^\beta$ (p, q は相異なる素数で $p \equiv q \equiv 3 \mod 4$, $(m, p-1) = (m, q-1) = 1$, $\alpha \equiv \beta \equiv 1 \mod 2$).

(2) $B_{spsp} = \{\pm 1\} \Leftrightarrow \nu = 1$ で n の各素因数 p に対して $(m, p-1) = 1$.

覚書 3.10. 系 3.2 は Solovay, Strassen [14] に，系 3.7(1) は Monier と Rabin による ([9, Prop.1], [11, Th.1]).

また，Monier [9] は Prop.3 の証明の中で命題 3.5(1) に相当することを，Prop.1 の証明の中で系 3.7(2) に相当することを述べている．一方，Rabin [11] は Th.1 の証明の中で n が $p_1p_2p_3$ (p_1, p_2, p_3 は相異なる素数で $p_1 \equiv p_2 \equiv p_3 \equiv 3 \mod 4$) の形の Carmaichael 数なら $|B_{spsp}| = \varphi(n)/4$ が成立することに言及している．

また，Monier [9] は Th.9 の証明の中で命題 3.4 に相当することを述べている．$n \equiv 3 \mod 4$ なら $B_{epsp} = B_{spsp}$ となることは Malm [8] による．

[4] の第 3 章 2 節, [5] の第 5 章 1 節, [12] の第 2 章 8 節, 9 節に擬素数, Euler 擬素数, 強擬素数, Carmichael 数に関する話題が収集されている．また，擬素数，Euler 擬素数，強擬素数に関する多くの数値データを [13] に見出すことができる．

参考文献

[1] W. R. Alford, A. Granville, C. Pomerance, There are infinitely many Carmichael numbers. Ann. of Math. 140 (1994) 703–722

[2] R. Baillie, S. S. Wagstaff Jr., Lucas pseudo-primes. Math. Comp. 35 (1980) 1391–1417

[3] R. D. Carmichael, On composite numbers P which satisfy the Fermat congruence $a^{P-1} \equiv 1 \pmod{P}$. Amer. Math. Monthly 19 (1912) 22–27

[4] 木田祐司，牧野潔夫，UBASIC によるコンピュータ整数論．日本評論社 (1994)

[5] N. Koblitz, A course in number theory and cryptography, 2nd ed. Springer-Verlag (1994)/邦訳：桜井幸一 (訳)，数論アルゴリズムと楕円暗号理論入門．シュプリンガー・フェアラーク東京 (1996)

[6] A. Korselt, Problème chinois. L'Intermédiaire des Mathématiciens 6 (1899) 142–143

[7] G. L. Miller, Riemann's hypothesis and a test for primality. J. Comput. and System Sci. 13 (1976) 300–317

[8] D. E. G. Malm, On Monte-Carlo primality tests. Notices Amer. Math. Soc. 24 (1977) 529

[9] L. Monier, Evaluation and comparison of two efficient probabilistic primality testing algorithm. Theoret. Comput. Sci. 12 (1980) 97–108

[10] C. Pomerance, J. L. Selfridge, S. S. Wagstaff Jr., The pseudoprimes to $2.5 \cdot 10^9$. Math. Comp. 35 (1980) 1003–1026

[11] M. O. Rabin, Probabilistic algorithm for testing primality. J. Number Theory 12 (1980) 128–138

[12] P. Ribenboim, The little book of big primes, Springer-Verlag (1991)/邦訳：吾郷孝視 (訳)，素数の世界，第 2 版．共立出版 (2001)

[13] 新宮領貞治, 素数判定と素因数分解について．2002 年度修士論文，中央大学理工学研究科

[14] R. Solovay, V. Strassen, A fast Monte-Carlo test for primality. SIAM J. Comput. 6 (1977) 84–85

[15] H. C. Williams, Primality testing on a computer. Ars Comb. 5 (1978) 127–185