# In the case of power residue being one, the relation between its index and modulus by an order of its base

By Junya SEBATA

(Received - -, -)
(Revised Dec. 18, 2018)

**Abstract.** Fermat found his little theorem by examining Mersenne prime. This thesis discloses the numerical structure of Fermat's observation on Mersenne prime and submits its expanded theorems, which differ from his little theorem. The structure is deduced from the more essential theorems which describe the relation between the index and the modulus of power residue being one.

## 1. Introduction

One ultimate instance often indicates multiple structures of mathmatics. Fermat found his little theorem by examining Mersenne prime [1: 26-27]. In this case, Fermat expanded the law as its base from 2 to the general numbers, and it led Euler's theorem. This thesis discloses the numerical structure of Fermat's observation on Mersenne prime and submits its other expanded theorems, which differ from his little theorem. The structure is deduced from the theme of this thesis, the more essential theorems, which describe the relation between the index and the modulus of power residue being one.

This thesis is consideration of the case of power residue being one, especially about the relation between its index and its modulus. On the section 2, an equality is displayed, which is the relation between a divisor of its index and a divisor of its modulus linked by the order of its base modulo the divisor of its modulus. Theorem2.2 claims about it. Additionally, Theorem2.3 suggests the method to exclude the obvious divisors of its index, especially one, and gives Theorem2.2 the fundamental significance. From Remark 2.5, the divisors structure in the relation between the index and the modulus is examined in more detail. At Example2.13 one method of primality test or prime factorization using the examined structure is showed, and the section 2 finishes.

In the discussion on the section 2, the usage of Theorem2.2 is not cleary referred to. But on the section 3, with discussing about the limited cases, it will be clear that the relation is the key ponint of the structure of a certain type of natural numbers, such as Mersenne number $2^p - 1$. Theorem3.2 confines a divisor of its modulus to a prime factor of its modulus, and finds the more simple relation with a divisor of its index than in Theorem2.2. Theorem3.3 confines its index to repeated multiplication of a prime number, and finds the general structure of Mersenne number $2^p - 1$, in other words Fermat's little theorem of the case of its base 2. Additionally, using the contrapositive

2010 Mathematics Subject Classification. Primary 11A07; Secondary 11A41.
*Key Words and Phrases.* power residue,primes,Mersenne prime,Fermat's little theorem.

of Theorem3.3, Theorem3.4 shows the numerical structure including the existence of Fermat's little theorem. Moreover, Theorem3.8 expands Theorem3.3 to more general numbers $a^x$, in other words, the general case of power residue being one.

On the section 4, Theorem4.2 gives the general and concrete instance of Theorem 3.3, including the instance previously pointed as Mersenne's and Fermat's one. The succeeding examples illustrate these theorems and considerations.

## 2. The fundamental theorems and their numerical structure

The proof of the next Lemma starts this consideration.

LEMMA 2.1. *When $a,\ n \geq 2,\ \ x \geq 1$ are natural numbers and*

$$a^x \equiv 1 \quad (mod\ n) \tag{1}$$

*is established, then $a$ and $n$ are coprime.*

PROOF. If $a$ and $n$ are not coprime, $a$ and $n$ have a common prime factor $q \geq 2$.
Now because of (1), with $k \geq 1$,

$$a^x = kn + 1$$

can be described.
Therefore,

$$a^x - kn = 1$$

however, the left side of this equality can be divided by $q$, and the right side of this equality can not be divided by $q$.
Therefore, $a$ and $n$ are coprime. □

The next theorem is the most central proposition of this thesis. It shows the equality which is the relation between a divisor $\gamma_x$ of the index $x$ and a divisor $\gamma_n$ of the modulus $n$ linked by the order $c$ of the base $a$ modulo $\gamma_n$.

THEOREM 2.2. *When $a,\ n \geq 2,\ \ x \geq 1$ are natural numbers and*

$$a^x \equiv 1 \quad (mod\ n) \tag{1}$$

*holds,*
*if there exists a divisor $\gamma_n \geq 2$ of $n$, which satisfies*

$$a^{f(\gamma_n)} \equiv 1 \quad (mod\ \gamma_n), \tag{2}$$

*then there exists a divisor $\gamma_x \geq 1$ of $x$ and*

$$f(\gamma_n) \ = \ k\gamma_x \quad (provided\ k \geq 1)$$

*is established.*

PROOF. Because of (1), for $l \geq 1$,

$$a^x \ = \ ln \ + \ 1$$

can be described.

$\gamma_n \geq 2$ is a divisor of $n$, therefore $\frac{n}{\gamma_n}$ is a natural number, and

$$a^x \ = \ (l \cdot \frac{n}{\gamma_n}) \cdot \gamma_n \ + \ 1 \ .$$

Consequently,

$$a^x \equiv 1 \quad (mod\ \gamma_n) \tag{3}$$

is established.
Because of Lemma2.1, $a$ and $\gamma_n$ are coprime, hence there exists a minimum $c \geq 1$ which satisfies

$$a^c \equiv 1 \quad (mod\ \gamma_n). \tag{4}$$

Incidentally, $c$ is the order or the cycle of $a$ modulo $\gamma_n$.
Because of (3), (4) and its minimality, $c$ is a divisor of $x$.
As well as it, because of (2), (4) and its minimality, $c$ is a divisor of $f(\gamma_n)$.
Consequently,

$$f(\gamma_n) \ = \ kc \quad (provided\ k \geq 1)$$

is established.
It is solved by taking $c$ as $\gamma_x$. □

In the previous theorem, all $x$ have the divisor 1, and when $\gamma_x$ takes 1, $f(\gamma_n)$ can take all natural numbers. Therefore the equality seems to give nothing, in other words, no limitation on either $\gamma_n$ or $\gamma_x$.

However the next theorem suggests the effective method to exclude the obvious divisors from the existence domain of $\gamma_x$, especially 1, and gives Theorem2.2 the fundamental significance, in other words, giving the concrete limitation between $\gamma_n$ and $\gamma_x$. Please note that it does not mean the excluded domain has no $\gamma_x$, but it is just not clear $\gamma_x$ exists in the excluded domain or does not exist in the excluded domain.

THEOREM 2.3. *In Theorem2.2, if*

$$n \text{ does not take any divisor more than or equal to } 2 \text{ in less than } a^\gamma, \tag{1}$$

*then*

$$\gamma_x > \gamma$$

*is established.*

PROOF. Because of (1), for any $\gamma_n \geq 2$,

$$\gamma_n \geq a^\gamma$$

is established.
Therefore, for any $\gamma \geq \gamma^{'} \geq 1$,

$$a^{\gamma^{'}} \not\equiv 1 \quad (mod\ \gamma_n)$$

is established.
$\gamma^{'}$ does not satisfy (4) of Theorem2.2, hence $\gamma^{'}$ can not be the order $c$ in the proof of Theorem2.2. Therefore,

$$c > \gamma$$

Consequently, there exists a divisor $\gamma_x$ which satisfies

$$\gamma_x > \gamma$$

and

$$f(\gamma_n) \ = \ k\gamma_x \quad (provided\ k \geq 1).$$

□

COROLLARY 2.4. *In Theorem2.3, if*

*n does not take any prime factor more than or equal to* 2 *in less than* $a^{\gamma}$, (1)

*then,*

$$\gamma_x > \gamma$$

*is established.*

PROOF. $n$ taking a divisor more than or equal to 2 in less than $a^{\gamma}$ is equivalent to $n$ taking a prime factor more than or equal to 2 in less than $a^{\gamma}$. □

REMARK 2.5. *The important point of Theorem2.3 is that to prove*

$$\gamma_x \neq \gamma$$

*need only giving*

$$a^{\gamma} \not\equiv 1 \quad (mod\ \gamma_n).$$

The next considerations are come from this remark.

LEMMA 2.6. *When* $\gamma_x$ *is a divisor of* $x$ *and* $\gamma_x^{'}$ *is a divisor of* $\gamma_x$,

*if*

$$a^{\gamma_x^{'}} \equiv 1 \quad (mod\ \gamma_n), \tag{1}$$

*is established, then*

$$a^{\gamma_x} \equiv 1 \quad (mod\ \gamma_n)$$

*is established.*

PROOF. Because of (1),

$$a^{\gamma_x^{'}} - 1 \equiv 0 \quad (mod\ \gamma_n)$$

and

$$a^{\gamma_x} - 1 = (a^{\gamma_x^{'}} - 1)(1 + a^{\gamma_x^{'}} + a^{\gamma_x^{'} \cdot 2} + \cdots + a^{\gamma_x^{'} \cdot (\frac{\gamma_x}{\gamma_x^{'}} - 1)}).$$

Therefore,

$$a^{\gamma_x} \equiv 1 \quad (mod\ \gamma_n)$$

is established. □

LEMMA 2.7. *When $\gamma_x$ is a divisor of $x$ and $\gamma_n$ is the maximum divisor of $n$ which satisfies*

$$a^{\gamma_x} \equiv 1 \quad (mod\ \gamma_n), \tag{1}$$

*then for any divisor $\gamma_x^{'}$ of $\gamma_x$, and for any divisor $\gamma_n^{'}$ of $n$, which is not a divisor of $\gamma_n$,*

$$a^{\gamma_x^{'}} \not\equiv 1 \quad (mod\ \gamma_n^{'})$$

*is established.*

PROOF. If

$$a^{\gamma_x^{'}} \equiv 1 \quad (mod\ \gamma_n^{'})$$

holds, because of Lemma2.6,

$$a^{\gamma_x} \equiv 1 \quad (mod\ \gamma_n^{'})$$

holds.
$\gamma_n^{'}$ is not a divisor of $\gamma_n$, hence there exists a prime factor $p$ of $\gamma_n^{'}$ of which the maximum index included in $\gamma_n^{'}$ is more than the maximum index included in $\gamma_n$.
In other words, the maximum index $r^{'}$ of $p$ included in $\gamma_n^{'}$ and the maximum index $r$ of

$p$ included in $\gamma_n$ satisfy

$$r^{'} > r \quad (provided\ r^{'}, r \geq 0)\ .$$

Therefore,

$$a^{\gamma_x} \equiv 1 \pmod{\gamma_n \cdot p},$$

however $\gamma_n$ is the maximum divisor satisfying (1). This is contradiction. □

REMARK 2.8. *When*

$$a^{\gamma_x} \equiv 1 \pmod{\gamma_n} \quad and \quad a^{\gamma_x^{'}} \equiv 1 \pmod{\gamma_n}$$

*hold,*

$$a^{gcd(\gamma_x, \gamma_x^{'})} \equiv 1 \pmod{\gamma_n}$$

*is established.*

*This proposition is not used in this thesis. However it seems important to understand the structure of the relation between the index $x$ and the modulus $n$, therefore picked up here. The simple proof is added below.*

PROOF. Describing $g = gcd(\gamma_x, \gamma_x^{'})$, and

$$a^{\gamma_x} - 1 = (a^g - 1)(1 + a^g + a^{g \cdot 2} + \cdots + a^{g \cdot (\frac{\gamma_x}{g} - 1)})$$
$$a^{\gamma_x^{'}} - 1 = (a^g - 1)(1 + a^g + a^{g \cdot 2} + \cdots + a^{g \cdot (\frac{\gamma_x^{'}}{g} - 1)})$$

hold.
$\frac{\gamma_x}{g}$ and $\frac{\gamma_x^{'}}{g}$ are coprime, therefore

$$(1 + a^g + a^{g \cdot 2} + \cdots + a^{g \cdot (\frac{\gamma_x}{g} - 1)})$$

and

$$(1 + a^g + a^{g \cdot 2} + \cdots + a^{g \cdot (\frac{\gamma_x^{'}}{g} - 1)})$$

are also coprime [1: 32]. Hence $\gamma_n \mid a^{gcd(\gamma_x, \gamma_x^{'})} - 1$. □

DEFINITION 2.9. *For simple description, the tree structure is introduced into divisors of the index $x$ and the modulus $n$.*

*Any different divisor of $x$ is described as any different point. The relation between a divisor $\gamma_x$ and a divisor $\gamma_x^{'}$ which is reduced from $\gamma_x$ with being devided by any one prime*

*factor more than or equal to* 2*, is denoted by the next symbol, an arrow:*

$$\gamma_x \ \leftarrow \ \gamma_x^{'} \quad .$$

$\gamma_x$ *is described as a high point of* $\gamma_x^{'}$*, and also* $\gamma_x^{'}$ *is described as a low point of* $\gamma_x$*.*

*By this definition, the tree structure of which the top is* $x$ *and the bottom is* 1 *is found in divisors of* $x$*. The same structure is defined in divisors of* $n$ *as well.*

THEOREM 2.10. *When Theorem2.2 (1) is established and* $\gamma_x$ *moves up from* 1 *to* $x$ *in the* $x$ *divisors tree,*
*the maximum* $\gamma_n$ *which satisfies*

$$a^{\gamma_x} \equiv 1 \quad (mod\ \gamma_n) \tag{1}$$

*moves up from* $gcd(a-1, n)$ *to* $n$ *in the* $n$ *divisors tree.*

PROOF. Because of Lemma2.6, and it is more clear from Lemma2.7. Additionally, the maximum $\gamma_n$ which satisfies (1) is equal to $gcd(a^{\gamma_x} - 1, n)$. □

COROLLARY 2.11. *For the conditions between* $\gamma_x$ *and* $\gamma_n$*:*

$$a^{\gamma_x} \equiv 1 \quad (mod\ \gamma_n) \tag{1}$$
$$a^{\gamma_x} \not\equiv 1 \quad (mod\ \gamma_n), \tag{2}$$

*when* $\gamma_x$ *moves up in the* $x$ *divisors tree, (1) is maintained and (2) is changeable.*
*As well as it, when* $\gamma_x$ *moves down in the* $x$ *divisors tree, (2) is maintained and (1) is changeable.*

PROOF. It is clear from Theorem2.10. □

LEMMA 2.12. *When* $a, b \geq 0$ *are integers,* $n \geq 2$ *is a natural number, and*

$$a \equiv b \quad (mod\ n) \tag{1}$$

*holds,*

$$gcd(a, n) \ = \ gcd(b, n) \quad (provided\ gcd(0, n) = n)$$

*is established.*

PROOF. Because of (1), there exists an integer $k$ which satisfies

$$a \ - \ b \ = kn$$

$$\begin{aligned} &\Leftrightarrow\ a\ -\ kn\ = b \\ &\Leftrightarrow\ b\ +\ kn\ = a\quad , \end{aligned}$$

therefore,

$$gcd(a,n)|b, \quad gcd(b,n)|a.$$

$a$ and $b$ can be described as

$$\begin{aligned} a &= l \cdot gcd(b,n) \qquad (provided\ l \geq 0) \\ b &= m \cdot gcd(a,n) \qquad (provided\ m \geq 0), \end{aligned}$$

therefore,

$$\begin{aligned} gcd(a,n) &= gcd(l \cdot gcd(b,n), n) = l^{'} \cdot gcd(b,n) \qquad (provided\ l^{'} \geq 1) \\ gcd(b,n) &= gcd(m \cdot gcd(a,n), n) = m^{'} \cdot gcd(a,n) \qquad (provided\ m^{'} \geq 1). \end{aligned}$$

Hence,

$$gcd(a,n) = l^{'} \cdot gcd(b,n) = l^{'} \cdot m^{'} \cdot gcd(a,n).$$

Because of $l^{'},\ m^{'} \geq 1$ and the equality above,

$$l^{'} = m^{'} = 1$$

is established. □

Example 2.13. *Not considering about efficiency, however, for a general natural number $n$, one example method of primality test or prime factorization using the propositions above is showed here.*

*For a general natural number $n$, there exists $x$ which satisfies*

$$a^x \equiv 1 \qquad (mod\ n),$$

*as the most simlply way, by repeatedly multiplying the base $a$ which is coprime with $n$. It means that $x$ is the order of the base $a$ modulo $n$.*

*Next, $x$ needs to be factorized. $x$ is smaller than $n$, therefore, it can be factorized easier than $n$, or changing $a$ to another base which is coprime with $n$ to find another $x$, or repeating this method on $x$ again.*

*Now, the difference between a prime and a composite can be confirmed only by using Euclidean algorithm on $a^{\gamma_x} - 1$ and $n$, taking $gcd(a^{\gamma_x} - 1, n)$, without one exception. The reasons are the statements below.*

*If $\gamma_x$ which is the one step lower than $x$ in the $x$ divisors tree satisfies*

$$a^{\gamma_x} \equiv 1 \quad (mod\ n),$$

*$\gamma_x < x$ should be the order of the base $a$ modulo $n$. This is contradiction, therefore, $\gamma_x$ always satisfies*

$$a^{\gamma_x} \not\equiv 1 \quad (mod\ n). \tag{1}$$

*When $n$ is a prime, $gcd(a^{\gamma_x} - 1, n)$ takes $1$ or $n$, however, because of (1), it can not be $n$. Therefore $gcd(a^{\gamma_x} - 1, n)$ takes only $1$.*

*In contrast, when $n$ is a composite, because of Theorem2.2 (4), there exist $c$ and $1 < \gamma_n < n$ which satisfy*

$$a^c \equiv 1 \quad (mod\ \gamma_n).$$

*In the case of $c < x$, because of Corollary2.11, this relation ascends the $x$ divisors tree, therefore if $c$ is a divisor of $\gamma_x$ which is the one step lower than $x$ in the $x$ divisors tree,*

$$a^{\gamma_x} \equiv 1 \quad (mod\ \gamma_n)$$

*is established. Therefore, $gcd(a^{\gamma_x} - 1, n)$ takes $1 < \gamma_n < n$ or an upper divisor of $\gamma_n$ in the $n$ divisors tree.*

*Consequently, when $n$ is a prime, the calculation result of $gcd(a^{\gamma_x} - 1, n)$ takes $1$. In contrast, when $n$ is a composite and there exists $c < x$, the calculation result of $gcd(a^{\gamma_x} - 1, n)$ takes $1 < \gamma_n < n$ or an upper divisor of $\gamma_n$. Therefore, it is enough to test the all $\gamma_x$ which are the one step lower than $x$ in the $x$ divisors tree.*

*However there exists the exception in the case of a composite number, namely for all $\gamma_n$, $c$ becomes equal to $x$. In this case, the calculation result becomes $1$ as well as a prime. One example method of primality test or prime factorization for this case is showed at Example3.7 on the next section.*

*Incidentally, to calculate $gcd(a^{\gamma_x} - 1, n)$ is not so difficult, because a natural number $n > t > 0$ which satisfies*

$$a^{\gamma_x} \equiv t \quad (mod\ n)$$

*can be calculated easier than $a^{\gamma_x}$, therefore, also $t - 1$ which satisfies*

$$a^{\gamma_x} - 1 \equiv t - 1 \quad (mod\ n).$$

*Additionally, because of Lemma2.12*

$$gcd(a^{\gamma_x} - 1, n) = gcd(t - 1, n),$$

*hence, it needs only to calculate $gcd(t - 1, n)$.*

In this section, the usage of Theorem2.2 is not cleary referred to. But on the next section, it will be clear that Theorem2.2 is the key point of the structure of a certain type of natural numbers, such as Mersenne number $2^p - 1$.

## 3. Elucidation of Mersenne number structure

COROLLARY 3.1. *When* $a,\ n \geq 2,\ \ x \geq 1$ *are natural numbers and*

$$a^x \equiv 1 \quad (mod\ n)$$

*holds,*
*for any divisor* $\gamma_n \geq 2$ *of* $n$

$$a^{\phi(\gamma_n)} \equiv 1 \quad (mod\ \gamma_n) \tag{1}$$

*holds.*
*Consequently, there exists a divisor* $\gamma_x \geq 1$ *of* $x$*, and*

$$\phi(\gamma_n) \ = \ k\gamma_x \quad (provided\ k \geq 1) \tag{2}$$

*is established.*

PROOF. Because of Lemma2.1, $a$ and $\gamma_n$ are coprime, therefore (1) is established by Euler's theorem. Because of Theorem2.2, (2) is established. □

Corollary3.1 is picked up here, because it seems interesting, however not being analyzed in this thesis in detail. This thesis goes an easier direction.

The next theorem confines a divisor $\gamma_n$ to a prime factor $p$ of the modulus $n$, and finds the more simple relation with a divisor $\gamma_x$ of the index $x$ than in Theorem2.2.

THEOREM 3.2. *When* $a,\ n \geq 2,\ \ x \geq 1$ *are natural numbers and*

$$a^x \equiv 1 \quad (mod\ n)$$

*holds,*
*for any prime factor* $p \geq 2$ *of* $n$

$$a^{p-1} \equiv 1 \quad (mod\ p) \tag{1}$$

*holds.*
*Consequently, there exists a divisor* $\gamma_x \geq 1$ *of* $x$*, and*

$$p \ = \ k\gamma_x \ + \ 1 \quad (provided\ k \geq 1) \tag{2}$$

*is established.*

PROOF. Because of Lemma2.1, $a$ and $p$ are coprime, therefore (1) is established by Fermat's little theorem.
Because of Theorem2.2,

$$p \ - \ 1 = \ k\gamma_x \quad (provided\ k \geq 1)$$

is established.
Consequently, (2) is established. □

The next theorem confines the index $x$ to repeated multiplication of a prime number $q^i$, and finds the general structure of Mersenne number $2^p - 1$.

THEOREM 3.3. *When $a$, $n \geq 2$ are natural numbers, $q \geq 2$ is a prime, $i \geq 1$ is a natural number, and*

$$a^{q^i} \equiv 1 \pmod{n}$$

*holds,*
*if*

$$n \text{ does not take any prime factor more than or equal to } 2 \text{ in less than } a, \tag{1}$$

*then*

$$n \equiv 1 \pmod{q}$$

*is established.*

PROOF. Because of Theorem3.2,
for any prime factor $p \geq 2$ of $n$, there exists a divisor $\gamma_x \geq 1$ of $x$, and

$$p = k\gamma_x + 1 \quad (\text{provided } k \geq 1) \tag{2}$$

is established.
Because of Theorem2.3 and (1),

$$\gamma_x > 1$$

is established.
Therefore $\gamma_x$ is either one of the numbers below:

$$\gamma_x = q^1,\ q^2,\ \cdots,\ q^{i-1},\ q^i \quad . \tag{3}$$

Because of (2) and (3),

$$n = k^{'}q + 1 \quad (\text{provided } k^{'} \geq 1)$$

can be described, hence

$$n \equiv 1 \pmod{q}$$

is established. □

THEOREM 3.4. *When $p, q \geq 2$ are prime numbers, $a \geq 2$ is a natural number, $p$ and $a$ are coprime, and*

$$p \not\equiv 1 \pmod{q} \tag{1}$$

*holds,*
*then for any $k \geq 1$, there exists the minimum $c \geq 1$ which satisfies*

$$x = kc \;\Rightarrow\; a^{q^x - 1} \equiv 1 \pmod{p}$$

*and*

$$x \neq kc \;\Rightarrow\; a^{q^x - 1} \not\equiv 1 \pmod{p}.$$

*Especially,*

$$a^{q^c - 1} \equiv 1 \pmod{p} \tag{2}$$

*is established.*
*Also in the case of $q = p$,*

$$c = 1 \tag{3}$$

*is established.*

PROOF. The next contrapositive of Theorem3.3 is used in this proof.
When

$$a,\ n \geq 2 \text{ are natural numbers},\ q \geq 2 \text{ is a prime},\ \text{and } i \geq 1 \text{ is a natural number}, \tag{4}$$

if

$$n \not\equiv 1 \pmod{q} \tag{5}$$

holds, then

$$n \text{ takes a prime factor more than or equal to } 2 \text{ in less than } a \tag{6}$$

is established, or for any $i$

$$a^{q^i} \not\equiv 1 \pmod{n} \tag{7}$$

is established.

At first, discussing the case of a natural number $n \geq 2$, provided that $n$ and $a$ are coprime and $n$ satisfies (1) as well as $p$; after that, $n$ is limited to a prime number $p$.

First, considering about an operation of taking the $q$th power residue of $a^{q^i}$,

$$(a^{q^i})^q = a^{q^{i+1}}$$

$$\Rightarrow \quad r^q \equiv (a^{q^i})^q = a^{q^{i+1}} \equiv r^{'} \quad (mod\ n)$$

, provided

$$a^{q^i} \equiv r \quad (mod\ n), \quad n > r \geq 0$$
$$a^{q^{i+1}} \equiv r^{'} \quad (mod\ n), \quad n > r^{'} \geq 0,$$

because of these equalities, when $i$ moves to $i+1$, an power residue $r$ moves to an power residue $r^{'}$, which satisfy

$$r^q \equiv r^{'} \quad (mod\ n).$$

Additionally, for any residue $n > r^{''} \geq 0$ modulo $n$, the result of the operation of taking the $q$th power residue of $r^{''}$ is decided uniquely to some residue $n > r^{'''} \geq 0$ modulo $n$. In other words, for any $n > r^{''} \geq 0$ modulo $n$, there exists $n > r^{'''} \geq 0$ modulo $n$, which satisfy

$$(r^{''})^q \equiv r^{'''} \quad (mod\ n).$$

Moreover, residues modulo $n$ are finit number, therefore, getting $i$ increased, the residue sequence necessarily takes again a residue which has already appeared in it. Hence the cycle exists in the residue sequence.

In other words, there exits $i^{'} \geq 1$ and the minimum $c \geq 1$ which satisfy

$$a^{q^{i^{'}}} \equiv a^{q^{i^{'}+kc}} \quad (mod\ n) \quad (provided\ for\ any\ k \geq 1). \tag{8}$$

Therefore,

$$\Leftrightarrow \ a^{q^{i^{'}}} \equiv a^{q^{i^{'}+kc}} \equiv a^{q^{i^{'}} \cdot q^{kc}} \equiv (a^{q^{i^{'}}})^{q^{kc}} \quad (mod\ n),$$

because of $a$ and $n$ are coprime, hence, $a^{q^{i^{'}}}$ and $n$ are coprime as well,

$$\Leftrightarrow \ 1 \equiv (a^{q^{i^{'}}})^{q^{kc}-1} \quad (mod\ n)$$
$$\Leftrightarrow \ 1 \equiv (a^{q^{i^{'}}})^{q^{kc}-1} \equiv a^{q^{i^{'}} \cdot (q^{kc}-1)} \equiv a^{(q^{kc}-1) \cdot q^{i^{'}}} \equiv (a^{q^{kc}-1})^{q^{i^{'}}} \quad (mod\ n)$$
$$\Leftrightarrow \ 1 \equiv (a^{q^{kc}-1})^{q^{i^{'}}} \quad (mod\ n). \tag{9}$$

Next, $r_c$ which satisfies

$$r_c \equiv a^{q^{kc}-1} \quad (mod\ n) \quad (provided\ n > r_c \geq 0)$$

is considered about.
Because of (9), $r_c$ satisfies

$$1 \equiv (r_c)^{q^{i^{'}}} \quad (mod\ n). \tag{10}$$

Because of $a$ and $n$ being coprime,

$$r_c \neq 0 \quad .$$

If $n > r_c \geq 2$, $r_c$ satisfies (4) and (5) of the contrapositive of Theorem3.3 as $a$ of it. However, because of (10), $r_c$ does not satisfy (7), therefore $r_c$ must satisfy (6).

Here, limiting $n$ to a prime number $p$, because of $p > r_c$, $p$ does not take any prime factor more than or equal to 2 in less than $r_c$. Therefore (6) is not established. This is contradiction.

Consequently,

$$r_c = 1 \quad .$$

Therefore,

$$a^{q^{kc}-1} \equiv 1 \pmod{p}.$$

When $x \neq kc$, if

$$a^{q^{x}-1} \equiv 1 \pmod{p}$$

holds, because of equivalence between (8) and (9), it contradicts the minimality of $c$.

When $q = p$, because of Fermat's little theorem, $c = 1$ is established. □

REMARK 3.5. *The starting point of consideration of Theorem3.4 is the interesting fact that the repeated operations of taking the qth power residue from a never take* 1*, because of the contrapositive of Theorem3.3, even though a and n are coprime. In short, the question of how the qth power residue sequence from a behaves like is the starting point.*

*Because of Theorem3.4(2),*

$$(2) \Leftrightarrow a \equiv a^{q^0} \equiv a^{q^c} \pmod{p}.$$

*Therefore, in the case of Theorem3.4, the qth power residue sequence from a returns to a again with making the cycle which has c times repetition and never takes* 1*. Also with their equivalence, the minimum cycle is c. In addition, because of Theorem3.4 (3), when* $q = p$*, the sequence is constant on a.*

*Also because of Theorem3.4 (3), this theorem includes the existence of Fermat's little theorem. Therefore, as well as Fermat's little theorem is used in Theorem3.2, Theorem 3.4 might use for extending the usage of Theorem2.2. Additionally, it might use for limiting or calculating an order of the base a modulo p by taking GCD between plural* $q^c - 1$*, especially* $p - 1$*.*

*To answer these possibility, several interesting questions are left in this theorem; for*

*example, how c is determined, does there exist any numerical structure around c, how about the case of*

$$p \equiv 1 \quad (mod\ q)$$

*and so on, however, these questions are not analyzed in this thesis. This thesis goes easier direction.*

COROLLARY 3.6. *For any divisor $\gamma \geq 2$ of n which satisfies Theorem3.3,*

$$\gamma \ \equiv \ 1 \quad (mod\ q) \tag{1}$$

*is established.*

PROOF. From the proof of Theorem3.3, for any prime factor $p$ of $n$ is described as

$$p \ = \ kq \ + \ 1 \quad (provided\ k \geq 1).$$

Additionally any divisor $\gamma$ is the product of $p$. □

EXAMPLE 3.7. *Continuing the discussion from Example2.13, namely in the case of a composite number, and for all $\gamma_n$, c becomes equal to x. Its one example method of primality test or prime factorization is showed here.*

*n can be described as*

$$n = \gamma_n \cdot \gamma_n^{'} \quad (provided\ \gamma_n, \gamma_n^{'} > 1).$$

*Because of Theorem3.3 and for all $\gamma_n$, c being equal to x; any prime factor p of n satisfies*

$$p = jx + 1 \quad (provided\ j \geq 1),$$

*therefore also $n, \gamma_n, \gamma_n^{'}$ satisfies*

$$\begin{aligned} n &= kx + 1 \quad (provided\ k \geq 1) \\ \gamma_n &= lx + 1 \quad (provided\ l \geq 1) \\ \gamma_n^{'} &= mx + 1 \quad (provided\ m \geq 1). \end{aligned}$$

*Hence*

$$\begin{aligned} & kx+1 = (lx+1)(mx+1) \\ \Leftrightarrow \quad & k = lmx + l + m \end{aligned} \tag{1}$$

*is established.*

*Consequently, when there exists $(l, m)$ which satisfies (1), $n$ is a composite number, or when there does not exist $(l, m)$ which satisfies (1), $n$ is a prime number. Incidentally, $x$ is a privided number, and $k$ can be calculated either $n$ is a prime or a composite.*

THEOREM 3.8. *When $a,\ n \geq 2$, $x \geq 1$ are natural numbers, $q \geq 2$ is a prime, $x$ has a prime factor $q$, $r \geq 1$ is the maximum index of $q$ included in $x$, and*

$$a^x \equiv 1 \pmod{n}$$

*holds,*
*if*

$$gcd(a^{\frac{x}{q^r}} - 1, n) = 1 \quad , \tag{1}$$

*then*

$$n \equiv 1 \pmod{q}$$

*is established.*

PROOF. Because of (1), for any divisor $\gamma_n \geq 2$ of $n$

$$a^{\frac{x}{q^r}} \not\equiv 1 \pmod{\gamma_n}$$

holds, and because of Corollary2.11, for any divisor $\gamma_x^{'}$ of $\frac{x}{q^r}$,

$$a^{\gamma_x^{'}} \not\equiv 1 \pmod{\gamma_n}$$

is established.
Therefore, for all $\gamma_n$, divisors of $\frac{x}{q^r}$ are the excluded domain, and any $\gamma_x$ of the existence domain is the outside of divisors of $\frac{x}{q^r}$.
Since any divisor of $x$, which is not a divisor of $\frac{x}{q^r}$, has a prime factor $q$, hence, any $\gamma_x$ of the existence domain has a prime factor $q$.
Therefore as well as the proof of Theorem3.3, because of Theorem3.2,

$$n \equiv 1 \pmod{q}$$

is established. □

REMARK 3.9. *The contrapositive of this theorem is interesting like the one of Theorem3.4. For any $x$, $a^x$ moves around*

$$a^x \not\equiv 1 \pmod{n},$$

*even though $a$ and $n$ are coprime. However, it is not analyzed in this thesis. This thesis goes an easier direction.*

On the next section, the numerical structure of Mersenne number $2^p - 1$ and its extension are considered concretely.

## 4. Concrete consideration of the expanded Mersenne number

For considering the numerical structure of Mersenne number $2^p - 1$ and its extension concretely, first, $n$ of Theorem3.3 is examined in detail.

REMARK 4.1. *Generally in the case of power residue being one, in other words, when*

$$a^x \equiv 1 \pmod{n}$$

*is established, the consideration of this remark starts from n in this equality.*

*When* $n \geq a^x$ *holds,* $a^x \not\equiv 1 \pmod{n}$, *therefore it is contradiction.*

*When* $n = a^x - 1$ *holds,* $a^x \equiv 1 \pmod{a^x - 1}$.

*When* $n < a^x - 1$ *holds,*

$$a^x = kn + 1 \quad (\textit{at least } k \geq 1),$$

*therefore*

$$a^x - 1 = kn$$

*is established.*
*Because of the cases above, n is a divisor of* $a^x - 1$.
*Consequently, to consider about n is equal to consider about divisors of* $a^x - 1$, *and*

$$n = \frac{a^x - 1}{k} \quad (\textit{provided } k \geq 1)$$

*can be described.*

*From the statements above, it is clear that Theorem3.3 mentions about the special character of the specific divisors of* $a^{q^i} - 1$.
*On the other hand, in the case of* $i = 1,\ a = 2$, *this is a Mersenne number* $2^q - 1$.
*Therefore it is also clear that the result of Theorem3.3,*

$$n \equiv 1 \pmod{q},$$

*accords to the Fermat's observation on divisors of a Mersenne number* $2^q - 1$. *In detail, the Fermat's observation is all divisors* $\gamma$ *of a Mersenne number* $2^q - 1$ *satisfy*

$$\gamma \equiv 1 \pmod{q}.$$

*In other words, Theorem3.3 and Corollary3.6 are an extension of the Fermat's observation.*

*By the way,*

$$a^x - 1 = (a-1)(1 + a + a^2 + \ \cdots\ + a^{x-2} + a^{x-1})\ ,$$

*and* $(a-1)$ *is the product only from prime factors of more than or equal to* 2 *and less than* $a$*. These observation above is the motivation of the next theorem.*

THEOREM 4.2. *When* $a \geq 2,\ i \geq 1$ *are natural numbers,* $q \geq 2$ *is a prime, and* $p_1,\ p_2,\ \cdots, p_{m-1},\ p_m$ *are all prime numbers more than or equal to* 2 *and less than* $a$*, and*

$$r_j \geq 0 \text{ is the maximum index of } p_j \text{ included in } \frac{a^{q^i}-1}{a-1} \quad (\text{provided } 1 \leq j \leq m), \tag{1}$$

*then*

$$\frac{a^{q^i}-1}{(a-1)p_1^{r_1} \cdot p_2^{r_2} \cdot \ \cdots \ \cdot p_{m-1}^{r_{m-1}} \cdot \ p_m^{r_m}} \ \equiv \ 1 \quad (mod\ q)$$

*is established.*

PROOF.

$$a^{q^i} \equiv 1 \quad (mod\ a^{q^i}-1)$$

is established.
For any divisor $\gamma \geq 2$ of $a^{q^i}-1$,

$$a^{q^i} = \frac{a^{q^i}-1}{\gamma} \cdot \gamma \ + \ 1 \quad ,$$

therefore

$$a^{q^i} \equiv 1 \quad (mod\ \gamma) \tag{2}$$

is established.
Because of (1) and

$$a^{q^i}-1 = (a-1)(1+a+a^2+\ \cdots \ + a^{q^i-2}+a^{q^i-1}),$$

$$\frac{a^{q^i}-1}{(a-1)p_1^{r_1} \cdot p_2^{r_2} \cdot \ \cdots \ \cdot p_{m-1}^{r_{m-1}} \cdot p_m^{r_m}} \tag{3}$$

is a divisor of $a^{q^i}-1$.
Therefore when (3) is more than or equal to 2, because of (2)

$$a^{q^i} \ \equiv \ 1 \quad (mod\ \frac{a^{q^i}-1}{(a-1)p_1^{r_1} \cdot p_2^{r_2} \cdot \ \cdots \ \cdot p_{m-1}^{r_{m-1}} \cdot p_m^{r_m}})$$

is established.
In Theorem3.3, if (3) is put into $n$, because of (1) $n$ does not have any prime factor more

than or equal to 2 in less than a, hence

$$\frac{a^{q^i}-1}{(a-1)p_1^{r_1}\cdot p_2^{r_2}\cdot\ \cdots\ \cdot p_{m-1}^{r_{m-1}}\cdot p_m^{r_m}}\ \equiv\ 1 \quad (mod\ q)$$

is established.
In the case of (3) being 1, it is obvious. □

COROLLARY 4.3. *n which satisfies Theorem3.3 is a divisor of (3) in Theorem4.2.*

PROOF. Because of Remark4.1, $n$ which satisfies

$$a^{q^i} \equiv 1 \quad (mod\ n)$$

is a divisor of $a^{q^i}-1$.
Additionally, $n$ satisfies (1) in Theorem3.3, hence all prime factors of $n$ are more than or equal to $a$.
Consequently, $n$ is a divisor of (3) in Theorem4.2. □

COROLLARY 4.4. *Any prime factor $p \geq a$ of $a^{q^i}-1$ satisfies*

$$p \equiv 1 \quad (mod\ q).$$

PROOF. $p$ is also a prime factor of (3) in Theorem4.2.
Because of the proof of Theorem3.3, a prime factor $p$ of (3) in Theorem4.2 satisfies

$$p \equiv 1 \quad (mod\ q).$$

□

REMARK 4.5. *By expanding the usual proof on Fermat's observation on Mersenne prime [1: 31-33], it is easy to prove Corollary4.4 and directly Theorem4.2. However the numerical structure described in this thesis would not be recognized from the usual proof.*

EXAMPLE 4.6. *In the case of $a=4,\ q=3,\ i=2$ of Theorem4.2,*

$$a^{q^i}-1 = 262143 \quad \frac{a^{q^i}-1}{a-1} = 87381 \quad .$$

*Prime numbers more than or equal to 2 and less than $a=4$ are $p_1=2,\ p_2=3$, therefore $r_1=0,\ r_2=2$.*

*Definitely,*

$$\frac{a^{q^i}-1}{(a-1)p_1^{r_1}p_2^{r_2}} = 9709 = 3\cdot 3236+1 \equiv 1 \quad (mod\ q=3).$$

*However by looking into* $r_2 = 0$*, because of* $87381 = 3 \cdot 29127$*, the residue is not always 1.*

EXAMPLE 4.7. *In the previous example,* $9709 = 7 \cdot 1387 = 7 \cdot 19 \cdot 73$.
*Definitely,*

$$7 = 3{\cdot}2{+}1 \equiv 1, \quad 1387 = 3{\cdot}462{+}1 \equiv 1, \quad 19 = 3{\cdot}6{+}1 \equiv 1, \quad 73 = 3{\cdot}24{+}1 \equiv 1 \quad (mod 3).$$

*The result fits to Corollary3.6.*

EXAMPLE 4.8. *In the case of* $a = 6,\ q = 5,\ i = 1$ *of Theorem4.2,*

$$a^{q^i}-1 = 7775 \qquad \frac{a^{q^i}-1}{a-1} = 1555 \quad .$$

*Prime numbers more than or equal to* 2 *and less than* $a = 6$ *are* $p_1 = 2,\ p_2 = 3,\ p_3 = 5$*, therefore* $r_1 = 0,\ r_2 = 0,\ r_3 = 1$.
*Definitely,*

$$\frac{a^{q^i}-1}{(a-1)p_1^{r_1}p_2^{r_2}} = 311 = 5\cdot 62+1 \equiv 1 \quad (mod\ q=5).$$

*By the way, it is easy to evaluate that* 311 *is a prime number.* $20 \cdot 20 = 400$*, hence looking into the numbers less than* 20 *is only needed. Additionally, the residue should be* 1 *modulo* 5 *and it should be an odd number. Therefore* 11 *is the only possible divisor, but* 311 *can not be devided by* 11.

COROLLARY 4.9. *When* $a = 3$*,* $i \geq 1$ *is a natural number,* $q \geq 2$ *is a prime, and* $r \geq 1$ *is the maximum index of* 2 *included in* $3^{q^i}-1$*, then*

$$\frac{3^{q^i}-1}{2^r} \ \equiv\ 1 \quad (mod\ q)$$

*is established.*

PROOF. In the case of $a = 3$ of Theorem4.2, 2 is only the prime number in more than or equal to 2 and less than $a = 3$. Additionally $a - 1 = 2$. □

EXAMPLE 4.10. *In the case of* $q = 23,\ i = 1$ *of Corollary4.9,*

$$a^{q^i} - 1 = 94143178826 \quad r = 1 \quad .$$

*Definitely,*

$$\frac{a^{q^i} - 1}{2} = 47071589413 = 23 \cdot 2046590844 + 1 \equiv 1 \quad (mod\ q = 23).$$

*By the way, for all* $q \leq 23$ *take* $r = 1$*, and there is no prime number which takes* $r \geq 2$*. The question about the existence of a prime number which takes* $r \geq 2$ *is considered in Remark4.14 a little bit more.*

EXAMPLE 4.11. *Checking the case of* $q = 8,\ i = 1$ *of Corollary4.9 for the example of* $q$ *not being a prime number,*

$$a^{q^i} - 1 = 6560 \quad r = 5$$

*and*

$$\frac{a^{q^i} - 1}{2^r} = 205 = 8 \cdot 25 + 5 \not\equiv 1 \quad (mod\ q = 8).$$

*Therefore in the case of* $q$ *not being a prime number, the residue is not always 1. From this result, it is clear that Theorem4.2 is also not always established in the case of* $q$ *not being a prime number.*

COROLLARY 4.12. *When* $a = 2,\ i \geq 1$ *is a natural number, and* $q \geq 3$ *is a prime, then*

$$2^{q^i - 1} \equiv 1 \quad (mod\ q)$$

*is established.*

PROOF. In the case of $a = 2$ of Theorem4.2, there is no number in more than or equal to 2 and less than $a = 2$, and $a - 1 = 1$.
Therefore,

$$2^{q^i} - 1 \equiv 1 \quad (mod\ q).$$

Since 2 and $q$ are coprime,

$$2^{q^i - 1} \equiv 1 \quad (mod\ q)$$

is established. □

PROOF. Corollary4.12 has an alternative proof not using Theorem4.2, but using Fermat's little theorem as below.

When $a$ and $q$ are coprime, because of Fermat's little theorem

$$a^{q-1} \equiv 1 \pmod{q}.$$

Since

$$q^i - 1 = (q-1)(1 + q + q^2 + \cdots + q^{i-2} + q^{i-1}),$$

$$\begin{aligned} a^{q^i-1} &= a^{(q-1)(1+q+q^2+\cdots+q^{i-2}+q^{i-1})} \\ &= (a^{(q-1)})^{(1+q+q^2+\cdots+q^{i-2}+q^{i-1})} \\ &\equiv (1)^{(1+q+q^2+\cdots+q^{i-2}+q^{i-1})} \pmod{q} \\ &\equiv 1 \pmod{q}. \end{aligned}$$

Take $a = 2,\ q \geq 3$ in the equality above. □

REMARK 4.13. *Because of the previous proof, Corollary4.12 and Fermat's little theorem of the case of its base 2 are equivalence. Therefore, it is clear that Theorem4.2 is the extension of Fermat's little theorem of the case of its base 2.*

REMARK 4.14. *At the last, in the general case but except $a = 2$, comparing Theorem 4.2 with Fermat's little theorem, it is clear that if there exists $r_j \neq 0$, the either proposition can not prove the other one in general. It is also the difference that Theorem4.2 can be established in the condition of $a$ and $q$ not being coprime.*

*The conditions; for all $r_j = 0$, $a$ and $q$ being coprime, and $a-1$ and $q$ being coprime, are needed for the both propositions becoming equivalence. Namely*

$$\begin{aligned} & \frac{a^{q^i} - 1}{a - 1} \equiv 1 \pmod{q} \\ \Leftrightarrow\ & a^{q^i} - 1 \equiv a - 1 \pmod{q} \\ \Leftrightarrow\ & a^{q^i} \equiv a \pmod{q} \\ \Leftrightarrow\ & a^{q^i-1} \equiv 1 \pmod{q} \\ \Leftrightarrow\ & a^{q-1} \equiv 1 \pmod{q} \end{aligned} \tag{1}$$

*By the way, from the statements above, the case of $q > 3,\ r = 1$ of Corollary4.9 is equivalent to Fermat's little theorem of the case of its base 3.*
*In contrast, when $q > 3,\ r \geq 2$,*

$$\frac{3^{q^i} - 1}{2 \cdot 2^{r-1}} \equiv 1 \pmod{q}$$

$$\Rightarrow \ \frac{3^{q^i}-1}{2} \equiv 2^{r-1} \quad (mod\ q)$$

*, and the left side of the equality is* $1$*, because of Fermat's little theorem and (1) of the direction from the bottom to the top.*
*Therefore,*

$$\Rightarrow \ 2^{r-1} \equiv 1 \quad (mod\ q). \tag{2}$$

*Consequently, the existence of* $r$ *which satisfies (2) is the necessary condition for the case of* $r \geq 2$ *of Corollary4.9 to be established. There exists at least one instance such as* $r = q$*, but it seems a little bit strict condition, because* $3^{q^i} - 1$ *should be divided by* $2^{q-1}$ *or something* $2^{r-1}$ *at least more than* $q$*.*

EXAMPLE 4.15. *In the case of* $a = 11,\ q = 3,\ i = 1$ *of Theorem4.2,*

$$a^{q^i} - 1 = 1330 \quad \frac{a^{q^i}-1}{a-1} = 133 \quad .$$

*Prime numbers more than or equal to* $2$ *and less than* $a = 11$ *are* $p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ p_4 = 7$*, therefore* $r_1 = 0,\ r_2 = 0,\ r_3 = 0,\ r_4 = 1$*.*
*Definitely,*

$$\frac{a^{q^i}-1}{(a-1)p_1^{r_1}p_2^{r_2}p_3^{r_3}p_4^{r_4}} = \frac{11^3-1}{10 \cdot 7} = 19 \equiv 1 \quad (mod\ q = 3). \tag{1}$$

*On the other hand, because of Fermat's little theorem,*

$$\begin{aligned} & 11^{3-1} \equiv 121 \equiv 1 \quad (mod\ q = 3) \\ \Leftrightarrow \ & \frac{11^3-1}{10} \equiv 19 \cdot 7 \equiv 1 \quad (mod\ q = 3) \end{aligned} \tag{2}$$

*However, in general, (2) can not prove (1), and (1) can not prove (2) as well.*

EXAMPLE 4.16. *In the case of* $a = 9,\ q = 3,\ i = 1$ *of Theorem4.2,*

$$a^{q^i} - 1 = 728 \quad \frac{a^{q^i}-1}{a-1} = 91 \quad .$$

*Prime numbers more than or equal to* $2$ *and less than* $a = 9$ *are* $p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ p_4 = 7$*, therefore* $r_1 = 0,\ r_2 = 0,\ r_3 = 0,\ r_4 = 1$*.*
*Even if* $a$ *and* $q$ *are not coprime,*

$$\frac{a^{q^i}-1}{(a-1)p_1^{r_1}p_2^{r_2}p_3^{r_3}p_4^{r_4}} = \frac{9^3-1}{8 \cdot 7} = 13 \equiv 1 \quad (mod\ q = 3).$$

*Definitely, Theorem4.2 is established.*

## References

[1] H. Tamai trans., Factorization and Primality Testing, By D.M. Bressoud, SIBaccess Co. Ltd., Tokyo, 2004; Springer-Verlag New York, Inc., New York, 1989.

Junya SEBATA
Sebata & CO.,LLC, 4-7-12 Momoi Suginami-ku Tokyo 167-0034 Japan
E-mail: n061470@jcom.home.ne.jp