<table>
<thead>
<tr>
<th>Title</th>
<th>On the number of the lattice points in the area $0 &lt; x &lt; n, 0 &lt; y \leq ax^k/n$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Miyawaki, Isao</td>
</tr>
<tr>
<td>Citation</td>
<td>Osaka Journal of Mathematics. 12(3) P.647-P.671</td>
</tr>
<tr>
<td>Issue Date</td>
<td>1975</td>
</tr>
<tr>
<td>Text Version</td>
<td>publisher</td>
</tr>
<tr>
<td>URL</td>
<td><a href="https://doi.org/10.18910/12189">https://doi.org/10.18910/12189</a></td>
</tr>
<tr>
<td>DOI</td>
<td>10.18910/12189</td>
</tr>
<tr>
<td>rights</td>
<td></td>
</tr>
</tbody>
</table>
ON THE NUMBER OF THE LATTICE POINTS IN THE AREA 
0 < x < n, 0 < y ≤ axk/n.

ISAO MIYAWAKI

(Received October 18, 1974)

1. Introduction

Let \( S_{a}^{(k)}(n) \) be the number of the lattice points in the area \( 0 < x < n, 0 < y \leq ax^{k}/n \), where \( k \) and \( n \) are positive integers and \( a \) is a positive integer which is prime to \( n \). Then we have

\[
S_{a}^{(k)}(n) = \sum_{r=1}^{\frac{n}{a}} \lfloor ax^{k}/n \rfloor,
\]

where \( \lfloor \rfloor \) denotes the Gauss symbol. Let

\[
ax^{k}/n = \lfloor ax^{k}/n \rfloor + \{ ax^{k}/n \},
\]

where \( \{ ax^{k}/n \} \) denotes the fractional part of \( ax^{k}/n \). Then we have

\[
\sum_{r=1}^{\frac{n}{a}} ax^{k}/n = S_{a}^{(k)}(n) + \frac{1}{2} \sum_{r=1}^{\frac{n}{a}} \{ ax^{k}/n \}
\]
or

\[
S_{a}^{(k)}(n) = \sum_{r=1}^{\frac{n}{a}} ax^{k}/n - \frac{1}{2} \sum_{r=1}^{\frac{n}{a}} \{ ax^{k}/n \}.
\]

We put

\[
S_{a}^{(k)}(n) = \sum_{r=1}^{\frac{n}{a}} ax^{k}/n - \frac{n-1}{2} + c_{a}^{(k)}(n),
\]

\[
c_{a}^{(k)}(n) = \frac{n-1}{2} - \sum_{r=1}^{\frac{n}{a}} \{ ax^{k}/n \}.
\]

If we suppose that \( S_{a}^{(k)}(n) \) behaves approximately as \( \sum_{r=1}^{\frac{n}{a}} ax^{k}/n - \frac{n-1}{2} \) then \( c_{a}^{(k)}(n) \) can be regarded as error term. T. Honda has conjectured the followings.

**Conjecture 1.** For a fixed \( k \) and any positive real number \( \varepsilon \) we have

\[
c_{a}^{(k)}(n) = O(n^{(ck^{-1})/k+\varepsilon}),
\]

for \( a=1 \).
Conjecture 2. \( c_1^{(2)}(n) \geq 0 \) and \( c_1^{(3)}(n) = 0 \) if and only if \( n \) is an integer of the following type

\[ n = p_1 \cdots p_j, \]

where \( p_1, \ldots, p_j \) are distinct primes and each \( p_i \) is equal to 2 or congruent to 1 modulo 4.

In this paper we shall give the complete proof of the above conjectures. Conjecture 1 is true not only in the case \( a = 1 \) but also in the case \( a \) is any positive integer which is prime to \( n \). In the case \( k \) is odd, \( c_1^{(k)}(n) \) is a very simple quantity. On the other hand in the case \( k \) is even, \( c_1^{(k)}(n) \) is an interesting quantity which is rather difficult to handle. For example, \( c_1^{(2)}(n) \) can be expressed in terms of the class numbers of imaginary quadratic fields whose discriminants are divisors of \( n \). For the even \( k > 2 \), \( c_1^{(2)}(n) \) is also related to some class numbers of some subfields of the cyclotomic field \( \mathbb{Q}(\zeta) \) where \( \zeta \) is a primitive \( n \)-th root of unity.

I would like to express my deep gratitude to Professor T. Honda for his presenting this problem to me.

2. Preliminaries

For positive integers \( k, n \) and an integer \( x \), we denote by \( N^{(k)}(x, n) \) the number of the elements of the set

\[ \{ y \in \mathbb{Z} | y^k \equiv x \mod n, \ 0 \leq y < n \}. \]

Lemma 1. Let \( n = \prod_{i=1}^{j} p_i^{e_i} \) be the prime decomposition of \( n \). Then we have

\[ N^{(k)}(x, n) = \prod_{i=1}^{j} N^{(k)}(x, p_i^{e_i}). \]

Proof. Consider the following map

\[ f; \mathbb{Z}/n\mathbb{Z} \to \prod_{i=1}^{j} \mathbb{Z}/p_i^{e_i}\mathbb{Z}, \quad (f(a \mod n) = \prod_{i=1}^{j} a \mod p_i^{e_i}). \]

We can easily see that this \( f \) is a ring isomorphism. From this we can immediately obtain the lemma.

Let \( n \) be a positive integer which is not equal to 1. We denote by \((\mathbb{Z}/n\mathbb{Z})^\times\) the unit group of the residue ring \( \mathbb{Z}/n\mathbb{Z} \). We put

\[ \Gamma(n) = \{ \chi | \chi; (\mathbb{Z}/n\mathbb{Z})^\times \to U, \text{ homomorphism} \}, \]

where \( U = \{ z \in C | |z| = 1 \} \). Then \( \Gamma(n) \) is an abelian group isomorphic to \((\mathbb{Z}/n\mathbb{Z})^\times\). An element \( \chi \) of \( \Gamma(n) \) is extended on \( \mathbb{Z} \) by setting
This function is denoted by $\chi$, and is called a character modulo $n$. If $\chi$ has always the value 1 for any $a$ such that $(a, n) = 1$, then $\chi$ is called the trivial character modulo $n$, and denoted by 1. If $\chi$ is a non-trivial character modulo $n$ and there is no character $\chi'$ of $(\mathbb{Z}/n\mathbb{Z})^*$ with a proper divisor $n'$ of $n$ satisfying $\chi'(a) = \chi(a)$ for any $(a, n) = 1$, then $\chi$ is called a primitive character modulo $n$. Any non-trivial character $\chi$ modulo $n$ can be uniquely decomposed to the following form

$$\chi = \chi_0 \chi',$$

where $\chi_0$ is the trivial character modulo $n$ and $\chi'$ is a primitive character modulo $n'$ with some divisor $n'$ of $n$. We call this $n'$ the conductor of $\chi$ and denote it by $f_\chi$. If $\chi$ is a primitive character modulo some $n$, then we call $\chi$ simply primitive.

In this case the conductor $f_\chi$ is equal to $n$. Let $n = \prod_{i=1}^{f_\chi} p_i^{e_i}$ be the prime decomposition of $n$. Then we have $(\mathbb{Z}/n\mathbb{Z})^* = \prod_{i=1}^{f_\chi} (\mathbb{Z}/p_i^{e_i}\mathbb{Z})^*$. Therefore if $\chi$ is a character modulo $n$, then $\chi$ has the following unique decomposition

$$\chi = \prod_{i=1}^{f_\chi} \chi_i,$$

where each $\chi_i$ is a character modulo $p_i^{e_i}$. It is clear that $\chi$ is primitive, if and only if each $\chi_i$ is primitive. Let $\chi$ be a character modulo $n$. Then we put $H_\chi = -\frac{1}{n} \sum_{a=1}^{n} \chi(a)a$.

**Lemma 2.** Let $\chi$ be a non-trivial character modulo $n$. If $\chi(-1) = 1$ then we have $H_\chi = 0$.

**Proof.** First we should note $\chi(n) = 0$. Then we have

$$H_\chi = -\frac{1}{2n} \left( \sum_{a=1}^{n-1} \chi(a)a + \sum_{a=1}^{n-1} \chi(-a+n)(-a+n) \right)$$

$$= -\frac{1}{2n} \left( \sum_{a=1}^{n-1} \chi(a)a + \sum_{a=1}^{n-1} \chi(-a)(-a+n) \right)$$

$$= -\frac{1}{2n} \sum_{a=1}^{n-1} \chi(a)(a+(-a+n))$$

$$= -\frac{1}{2} \sum_{a=1}^{n-1} \chi(a) = 0.$$

We put

$$\Gamma^{(w)}(n) = \{ \chi \in \Gamma(n) | \chi^k = 1 \}.$$
Lemma 3. Let $p$ be a prime number. Then we have

(i) $N^{(k)}(b, \rho^e) = \sum_{\chi \in \Gamma^{(k)}(\rho^e)} \chi(b) = 1 + \sum_{\chi : \text{primitive}} \chi(b)$

if $(b, p) = 1$,

(ii) $N^{(k)}(b, \rho) = 1 + \sum_{f_x = b, x^k = 1} \chi(b)$.

Proof. If we note that $\Gamma^{(k)}(\rho^e)$ is the character group of the factor group $(\mathbb{Z}/\rho^e \mathbb{Z})^\times / (\mathbb{Z}/\rho^e \mathbb{Z})^{\times k}$ and $\chi(b)$ is zero for any $(b, \rho^e) \neq 1$, then we can easily obtain the lemma.

Lemma 4. We denote by $\#\Gamma^{(k)}(n)$ the number of the elements of the set $\Gamma^{(k)}(n)$. Let $p$ be a prime. Then we have

(i) $\#\Gamma^{(k)}(p^e) = (p - 1, k)$ if $(p, k) = 1$,

(ii) $\#\Gamma^{(k)}(p^e) = \left\{ \begin{array}{ll} p^{e-1}(p - 1, k) & \text{if } e_0 + 1 \geq e, \\
(p + 2) & \text{if } e_0 + 1 < e,
\end{array} \right.$

where we define $e_o$ by

$p^o || k, \quad e_o > 0$.

(iii) $\#\Gamma^{(k)}(2^e) = \left\{ \begin{array}{ll} 2^{e-1} & \text{if } e \leq e_0 + 2, \\
2^{e+1} & \text{if } e \geq e_0 + 3,
\end{array} \right.$

where we define $e_o$ by

$2^o || k, \quad e_o > 0$.

Especially for a fixed $k$, there is a constant $c_0$ such that

$\#\Gamma^{(k)}(p^e) \leq c_0$

for any $p$ and $e$.

Proof. If we note the following facts

$(\mathbb{Z}/p^e \mathbb{Z})^\times \approx \mathbb{Z}/(p - 1)p^{e-1} \mathbb{Z}$ if $p \neq 2$,

$(\mathbb{Z}/2^e \mathbb{Z})^\times \approx \mathbb{Z}/2 \mathbb{Z} + \mathbb{Z}/2^{e-2} \mathbb{Z}$ if $e \geq 2$,

$(\mathbb{Z}/p^e \mathbb{Z})^\times / (\mathbb{Z}/p^e \mathbb{Z})^{\times k} \approx \Gamma^{(k)}(p^e),$

then we have immediately the lemma 4.

3. Main theorem and its proof

Let $n \geq 2$ be a positive integer and $n = \prod_{i=1}^{j} p_i^{e_i}$ be the prime decomposition of $n$. We define index sets $A(n)$ and $B(n)$ as follows
For a subset $\alpha = \{\alpha_1, \ldots, \alpha_i\}$ of the set $A(n)$ we denote by $d_{\alpha}$ the integer
\[
d_{\alpha} = \prod_{i=1}^{\alpha} p_{\alpha_i} , \quad \text{if } \alpha \neq \phi
\]
\[
d_{\phi} = 1 .
\]

For a fixed positive integer $k$, we put
\[
e_i = ks_i + r_i , \quad s_i \geq 0 , \quad 1 \leq r_i \leq k ,
\]
and
\[
n_0 = n_0^{(k)} = \prod_{i=1}^{k} p^{\lfloor k \tau_i + r_i - 1 \rfloor}.
\]

Let $d$ be a positive divisor of $n$. Then we put
\[
n(d) = n^{(k)}(d) = n/(d^k, n)
\]
\[
d^{(k)}(n) = d^{(k)}(d^{(k)}) = d^{(k)}/(d^k, n).
\]

Under the above notation we have the following proposition.

**Proposition 1.**

\[
c_{a}^{(k)}(n) = \sum_{\chi : \text{primitive}} \chi(a)H_x - \sum_{d \mid n , \; x^k = 1} \mu(d_a) \left[ \frac{(d_a, n)/d_a - 1}{2} + \frac{(d_a, n)}{d_a} \right] \],
\]

where we denote by $\mu(\cdot)$ the M"obius function.

**Proof.** By the definition of $c_{a}^{(k)}(n)$ we have
\[
c_{a}^{(k)}(n) = \frac{n-1}{2} - \sum_{i=1}^{\infty} N^{(k)}(a^{-1}x, n),
\]
where we consider $a^{-1}x$ in $(Z/nZ)^\times$. If $(x, d_{a}(\alpha))=1$ then by Lemma 1 and Lemma 2 we have
\[
N^{(k)}(a^{-1}x, n) = \prod_{i=1}^{j} \left( 1 + \sum_{\chi : \text{primitive}} \chi(a^{-1}x) \right).
\]

Therefore we get
\[ c^{(k)}_a(n) = \frac{n-1}{2} \left[ \frac{1}{n} \sum_{\chi: \text{primitive}} \chi(a^{-1}) \chi \left( \sum_{\mu(d_{\alpha}) \neq 0} \frac{1}{n} \sum_{i=1}^{\chi(d_{\alpha})} \prod_{i=1}^{\chi(d_{\alpha})} (1 + \sum_{x^k = 1} \chi(x)) x \right) \right. \\
+ \sum_{d_{\alpha} \in \mathbb{N}^+} \mu(d_{\alpha}) \left\{ \frac{1}{n} \sum_{x^k = 1} \prod_{x^k = 1} \chi(x) d_{\alpha} x \right\} \\
- \sum_{F_{x}} \left\{ a(d_{\alpha}) x \right\} \right] \\
= \frac{n-1}{2} \frac{n(n-1)-1}{2n} \sum_{\chi: \text{primitive}} \sum_{x^k = 1}^{n-1} \chi(a^{-1}) x - \sum_{\mu(d_{\alpha}) \neq 0} \mu(d_{\alpha}) \\
\cdot \left[ \frac{d_{\alpha}}{n} \left( \frac{n}{d_{\alpha}} - 1 \right) \right] \\
- \sum_{F_{x}} \left\{ a(d_{\alpha}) x \right\} , \\
\right. \\
\\text{where we should note that} \\
\frac{1}{n} \sum_{x^k = 1}^{n-1} \chi(x) x = \frac{1}{n} \sum_{x = 1}^{\chi(n)} \sum_{i=1}^{\chi(n)} \chi(x)(x + i f_{x}) = \frac{1}{n} \sum_{x = 1}^{f_{x}} \sum_{i=1}^{\chi(n)} \chi(x) x = -H_{x}. \\
\] \\
Then we have \\
\[ c^{(k)}_a(n) = \sum_{\chi: \text{primitive}} \overline{\chi}(a) H_{x} - \left[ \sum_{\mu(d_{\alpha}) \neq 0} \mu(d_{\alpha}) \left\{ \frac{n}{d_{\alpha}} - 1 \right\} \sum_{\chi: \text{primitive}} \overline{\chi}(a) \chi(d_{\alpha}) H_{x} \\
\frac{n}{d_{\alpha}} \sum_{F_{x}}^{n(d_{\alpha})} \left\{ a(d_{\alpha}) x \right\} \right] . \\
\] \\
On the other hand we see that \\
\[ - \sum_{x^k = 1}^{n(d_{\alpha})} \left\{ a(d_{\alpha}) x \right\} = c^{(k)}_{\beta}(n(d_{\alpha})) - \frac{n(d_{\alpha})-1}{2} . \\
\] \\
Therefore we have \\
\[ c^{(k)}_a(n) = \sum_{\chi: \text{primitive}} \overline{\chi}(a) H_{x} - \sum_{\mu(d_{\alpha}) \neq 0} \mu(d_{\alpha}) \left\{ \frac{n}{d_{\alpha}} - 1 \right\} \frac{n}{d_{\alpha}} n(d_{\alpha}) - \frac{n(d_{\alpha})-1}{2} \\
\frac{n}{d_{\alpha}} n(d_{\alpha}) \sum_{F_{x}}^{n(d_{\alpha})} c^{(k)}_{\beta}(n(d_{\alpha})) \]
\[
\sum_{\chi \text{ primitive}} \frac{1}{n(d_a)} \chi(a) H_x - \sum_{a \equiv 1 \mod d} \mu(d_a) \left[ \frac{(n/d_a, n(d_a)) - 1}{2} \right] + \frac{n}{d_a(n(d_a))} \sum_{\chi \text{ primitive}} \frac{\chi(a) \chi(d_a) H_x}{(f_x, d_a) = 1}.
\]

But by the definition of \( n(d) \) we have
\[
\frac{n}{n(d_a)} = \frac{n}{(d_a, n)} = (d_a, n).
\]

Therefore we get
\[
c_i(n) = \sum_{\chi \text{ primitive}} \frac{1}{n(d_a)} \chi(a) H_x - \sum_{a \equiv 1 \mod d} \mu(d) \left[ \frac{(d_a, n)}{2} \right] + \frac{(d_a, n)}{d_a} \sum_{\chi \text{ primitive}} \frac{\chi(a) \chi(d_a) H_x}{(f_x, d_a) = 1}.
\]

Thus Proposition 1 is proved.

Let \( \chi \) be a non-trivial character modulo \( n \) such that \( \chi^k = 1 \). Then we define the integer \( n(\chi) = n^k(\chi) \) as follows,
\[
n(\chi) = \prod_{p \text{ prime}} p^{[\nu_p(n/d_a)] + \lambda^1 + \lambda^2},
\]
\[
\epsilon(\chi, n) = \epsilon_{(\chi, n)} = \begin{cases} 0 & \text{if } p \mid f_x \lor \nu_p \left( \frac{n}{f_x} \right) - k \left[ \nu_p \left( \frac{n}{f_x} \right) \right] \leq 1, \\ 1 & \text{otherwise}, \end{cases}
\]
where we denote by \( \nu_p(\cdot) \) the normalized \( p \)-adic exponential valuation of the field of the rational numbers \( \mathbb{Q} \). Then we can easily obtain the following two remarks.

**Remark 1.** For a prime \( p \) if \( p \) divides \( n(\chi) \), then \( p^2 \) divides \( n/f_x \).

**Remark 2.** If \( n(\chi) \) is divisible by \( d \), then \( n/d_a = 0 \mod f_x \).

**Lemma 5.** Let \( n \) be a positive integer. For distinct primes \( p_1, \ldots, p_j \) such that \( p_i \mid n \) \((i = 1, \ldots, j)\), we put \( d_0 = p_1 \cdots p_j \) and \( n(d_0) = n/(d_0, n) \). Let \( \chi \) be a character modulo \( n(d_0) \). Then \( \chi \) induces the character modulo \( n \) through the homomorphism \((\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/n(d_0)\mathbb{Z})^\times \). Denoting this also \( \chi \) we have that if \( d \) divides \( n(d_0)(\chi) \) then \( dd_a \) divides \( n(\chi) \).

Proof. We shall show that \( \nu_p(\chi) \leq \nu_p(n(\chi)) \) for every prime \( p \). We consider the two cases.
The case I. \( p \neq p_i \ (i = 1, \ldots, j) \).

By the definition of \( n(d_0) \) we have
\[
\nu_p(n) = \nu_p(n(d_0))
\]
and
\[
\nu_p(n/f_x) = \nu_p(n(d_0)/f_x).
\]

It follows from this
\[
\varepsilon_{p,n} = \varepsilon_{p,w(d_0)}.
\]

From this and by the definition of \( d \) we have
\[
\nu_p(dd_0) = \nu_p(d) = [\nu_p(n(d_0)/f_x)/k] + \varepsilon_{p,w(d_0)}
\]
\[= [\nu_p(n(f_x))/k] + \varepsilon_{p,n}
\]
\[= \nu_p(n(f_x)).
\]

Thus Lemma 5 is proved in our case.

The case II. \( p = p_i \) (for some \( i \))

By the definition of \( n(d_0) \) we have
\[
\nu_p(n(d_0)/f_x) = \begin{cases} \nu_p(n/f_x) - k & \text{if } p^k | n, \\ 0 & \text{if } p^k \nmid n. \end{cases}
\]

Therefore we shall consider the two cases.

(i) The case \( \nu_p(n(d_0)/f_x) = \nu_p(n/f_x) - k \).

In this case we have
\[
\nu_p(n/f_x) - k \left[ \nu_p(n/f_x) \frac{1}{k} \right] = \nu_p(n(d_0)/f_x) + k - k[\nu_p(n(d_0)/f_x)/k + 1]
\]
\[= \nu_p(n(d_0)/f_x) - k[\nu_p(n(d_0)/f_x)/k].
\]

This shows that \( \varepsilon_{p,n} = \varepsilon_{p,w(d_0)} \). Noting this we have
\[
\nu_p(dd_0) = 1 + \nu_p(d) \leq 1 + [\nu_p(n(d_0)/f_x)/k] + \varepsilon_{p,w(d_0)}
\]
\[= 1 + [\nu_p(n/f_x)/k - 1] + \varepsilon_{p,n}
\]
\[= [\nu_p(n/f_x)/k] + \varepsilon_{p,n}
\]
\[= \nu_p(n(f_x)).
\]

This also completes the proof of Lemma 5 in our case.

(ii) The case \( \nu_p(n(d_0)/f_x) = 0 \)

In this case we should note that \( \nu_p(f_x) = 0 \). Then we have
\[
\nu_p(n(d_0)/f_x) - k[\nu_p(n(d_0)/f_x)/k] = 0.
\]

It follows
This shows \( v_p(d) = 0 \). On the other hand we have
\[
  v_p(n) \geq 2 + v_p(n(d_0))
\]
This shows that
\[
  v_p(n/f_X) = 0
\]
or
\[
  v_p(n/f_X) = \frac{1}{k} > 1, \quad (i.e., \epsilon_{p,n} = 1)
\]
Therefore \( v_p(n/f_X)[k] > 0 \)

Thus Lemma 5 is completely proved.

The following lemma is a converse of Lemma 5 in a sense.

**Lemma 6.** Let \( \chi \) be a character modulo \( n \) and \( d \) be a positive divisor of \( n(\chi) \). Let \( p_1, \ldots, p_j \) be distinct primes each of which is a divisor of \( d \). If we put \( d_0 = p_1 \cdots p_j \) and \( d = d_0 d' \) with a positive integer \( d' \), then \( \chi \) is a character modulo \( n(d_0) \) and \( d' \) is a divisor of \( n(d_0)(\chi) \).

**Proof.** The former assertion is obvious by Remark 2. So we shall show the latter half in the same manner as in Lemma 5. Let \( p \) be a prime.

(I) The case \( p \neq p_i \) (\( i = 1, \ldots, j \))
In this case we can show that \( v_p(n(\chi)) = v_p(n(d_0)(\chi)) \) by the same method as in the case (I) of Lemma 5. Then we have
\[
  v_p(d') = v_p(d) \leq v_p(n(\chi)) = v_p(n(d_0)(\chi))
\]

(II) The case \( p = p_i \) (for some \( i \)).
In this case we have
\[
  v_p(d) \leq v_p(n(\chi))
\]
This shows that
\[
  [v_p(n/f_X)[k] > 0
\]
or
\[
  [v_p(n/f_X)[k] = 0 \quad \text{and} \quad \epsilon_{p,n} = 1
\]
Therefore we shall consider the two cases.
(i) The case \( [v_p(n/f_X)[k] > 0 \).
In this case we can easily see that
\[ v_p(n/f_\chi)/k = v_p\left(\frac{1}{f_\chi (p^k, n)}\right)^{1/k} + 1 \]
\[ = v_p\left(\frac{1}{f_\chi (d_\chi, n)}\right)^{1/k} + 1. \]

Therefore we have
\[ v_p(d') = v_p(d) - 1 \leq [v_p(n/f_\chi)/k] + \varepsilon_{p; n} - 1 \]
\[ = [v_p(n(d_\chi)/f_\chi)/k] + 1 + \varepsilon_{p; n} - 1. \]

But we can show by the same method as in the case (II)-(i) of Lemma 5 that \( \varepsilon_{p; n} = \varepsilon_{p; n(d_\chi)}. \) Therefore it follows
\[ v_p(d') \leq v_p(n(d_\chi)(\chi)). \]

(ii) The case \([v_p(n/f_\chi)/k] = 0 \) and \( \varepsilon_{p; n} = 1. \)

In this case we have
\[ v_p(d') = v_p(d) - 1 \leq \varepsilon_{p; n} - 1 = 0. \]

This shows that
\[ v_p(d') = 0. \]

Therefore we have
\[ v_p(d') \leq v_p(n(d_\chi)(\chi)). \]

These complete the proof of Lemma 6.

Now we are in a position to state our main Theorem.

**Theorem 1.** Notation being as above. Then

\[ c^\nu_p(n) = \frac{n_{\phi} - 1}{2} + \sum_{\chi: \text{primitive}} \chi^{-1}(a) H_x \left\{ \sum_{d | n(\chi)} \frac{(d^k, n)}{d} \chi^{-1}(d^k, n) \right\} \cdot \left( \sum_{\alpha \in B(n)} \mu(d_\alpha) \chi(d_\alpha) \right). \]

**Proof.** Let \( n = \prod_{i=1}^j p_i^e_i \) be the prime decomposition of \( n. \) Then we put \( s(n) = \sum_{i=1}^j (e_i - 1). \) We shall prove our theorem by the induction with respect to \( s(n). \) If \( s(n) = 0, \) i.e., \( n \) is a square-free integer, then by taking \( B(n) = \phi \) in Proposition 1 we get
\[ c^{(\chi)}_a(n) = \sum_{\chi: \text{primitive}} \chi^{-1}(a)H_\chi. \]

On the other hand, in this case we have \( n_0 = 1, n(\chi) = 1 \) and \( B(n) = \phi \). This shows that our theorem is true in our case. If \( s(n) > 0 \), then we assume that the theorem is valid for any \( m \) such that \( s(m) < s(n) \). Now we can easily see that \( s(n(d_\alpha)) < s(n) \) with respect to \( n(d_\alpha) \) of Proposition 1. Therefore by the assumption we have

\[ (2) \quad c^{(\chi)}_{a_\alpha, n(d_\alpha)}(n(d_\alpha)) = \frac{n(d_\alpha) - 1}{2} + \sum_{\chi: \text{primitive}} \chi^{-1}(d^{*}_a(n) a) H_\chi \]

\[ \cdot \left\{ \sum_{d \mid n(d_\alpha)} \frac{(d^k, n(d_\alpha))}{d} \chi^{-1} \left( \frac{d^k}{(d^k, n(d_\alpha))} \right) \right\}. \]

Hereafter we shall only consider primitive characters which take values \( k \)-th roots of unity or zero, though we shall not mention it explicitly. From (2) and Proposition 1 we get

\[ c^{(\chi)}_a(n) = \sum_{\chi: \text{primitive}} \chi^{-1}(a)H_\chi - \sum_{\alpha \in B(n)} \mu(d_\alpha) \left[ \left( \frac{d^k, n}{2} \right) - 1 + \frac{(d^k, n(d_\alpha))}{d} \chi^{-1} \left( \frac{d^k}{(d^k, n(d_\alpha))} \right) \right] \]

\[ \cdot \left\{ \sum_{\beta \subset B(n(d_\alpha))} \mu(d_\beta) \chi(d_\beta) \right\} - \sum_{\alpha \in B(n)} \chi(d_\alpha) \chi^{-1}(a)H_\chi. \]

Therefore if we prove the following two facts (I) and (II), then the proof of Theorem 1 is completed.

\[ (I) \quad \sum_{\alpha \in B(n)} \mu(d_\alpha) \left[ \frac{(d^k, n)}{2} \left( \frac{d^k, n}{2d_\alpha} - 1 \right) \right] = \frac{n_0 - 1}{2}. \]
First we shall prove (I). By the definition of $n(d_a)$ we get

$$n(d_a)_0 = \left( \frac{n}{(d_a^*, n)} \right)_0$$

and

$$n(d_a)_0 \frac{(d_a^*, n)}{d_a} = \left( \frac{n}{(d_a^*, n)} \right)_0 \frac{(d_a^*, n)}{d_a}.$$  

By examining $p$-adic valuation of $(n/(d_a^*, n))_0 \cdot ((d_a^*, n)/d_a)$ for each $p$ such that $p | n$, we can easily see that

$$n(d_a)_0 \frac{(d_a^*, n)}{d_a} = n_0.$$  

On the other hand we have

$$- \sum_{\alpha \in B(n)} \mu(d_a) = - \sum_{d | d_{B(n)}} \mu(d) = - \left( \sum_{d | d_{B(n)}} \mu(d) \right) - 1 = 1.$$  

It follows (I).

Next we shall prove (II). We can rewrite the left hand side of (II) to the following formula

$$(3) \quad \sum_{f_x \mid n} \chi^{-1}(a) H_x \left[ \sum_{\alpha \in B(n)} \mu(d_a) \chi(d_a) \right]$$

$$- \left\{ \sum_{\alpha \in B(n)} \frac{\mu(d_a) \cdot (d_a^*, n) \cdot (d_a^*, n)}{d} \frac{(d_k^*, n) d_k}{(d_k, n(d_a))} \right\} \chi^{-1}(d_a) \chi(d_a).$$

Here we note that
\[
\frac{(d^k_d, n)}{d^k_d} \cdot \frac{(d^k_d, n(d_d))}{d^k_d} = \frac{(d^k_d, n)}{d^k_d} \cdot \frac{n}{d^k_d} = \frac{(d^k_d)^k}{d^k_d}
\]
and
\[
\frac{d^k_d(n) d^k_d}{(d^k_d, n(d_d))} = \frac{d^k_d}{(d^k_d, n)} \cdot \frac{d^k_d}{(d^k_d, n)} = \frac{(d^k_d)^k}{(d^k_d)^k}.
\]

And by Lemma 5 we note that
\[
d^k_d | n(\chi).
\]

By the definition of \( n(d) \) we can easily see that
\[
(n(d_d))(d) = n(dd_d).
\]

Then we can rewrite the inside of the bracket of (3) as follows
\[
(4) = \left\{ \sum_{\beta \subset B(n)} \mu(d_a) \chi(d_a) \right\} - \left\{ \sum_{d \mid n(\chi)} \frac{(d^k_d, n)}{d} \chi^{-1} \left( \frac{d^k_d}{n}, n \right) \right\}
\]
\[
\cdot \left\{ \sum_{d = d_d} \mu(d_a) \right\},
\]
\[
\sum_{\beta \subset B(n)} \mu(d_a) \chi(d_a) \sum_{d = d_d} \mu(d_a) \}
\]
\[
\sum_{\alpha \subset B(n)} \mu(d_a) \chi(d_a) \sum_{d = d_d} \mu(d_a) \}
\]
\[
\sum_{d \mid n(\chi)} \frac{(d^k_d, n)}{d} \chi^{-1} \left( \frac{d^k_d}{n}, n \right) \sum_{\beta \subset B(n)} \mu(d_a) \chi(d_a) \}
\]
\[
\sum_{\alpha \subset B(n)} \mu(d_a) \chi(d_a) \sum_{d = d_d} \mu(d_a) \}
\]
\[
\sum_{d \mid n(\chi)} \frac{(d^k_d, n)}{d} \chi^{-1} \left( \frac{d^k_d}{n}, n \right) \sum_{\alpha \subset B(n)} \mu(d_a) \chi(d_a) \}
\]
\[
\sum_{d \mid n(\chi)} \frac{(d^k_d, n)}{d} \chi^{-1} \left( \frac{d^k_d}{n}, n \right) \sum_{\alpha \subset B(n)} \mu(d_a) \chi(d_a) \}
\]

Here we can easily see that if \( \beta \subset B(n) \) and \( d_{\beta} | n(d(\chi)) \) then \( \beta \subset B(n(d_a)) \). This shows that we may change \( B(n(d_a)) \) of the last term of (4) for \( B(n) \). Moreover by Lemma 6 we see that \( d_{\beta} \mid n(d_a) \) implies that \( f_{\chi} \mid n(d_a) \) and \( d'_{\beta} \mid n(d_a)(\chi) \). Therefore we may exclude these conditions of (4). Then we have
\[
(4) = \left\{ \sum_{\alpha \subset B(n)} \mu(d_a) \chi(d_a) \right\} - \left\{ \sum_{d \mid n(\chi)} \frac{(d^k_d, n)}{d} \chi^{-1} \left( \frac{d^k_d}{n}, n \right) \right\}
\]
\[
\cdot \left\{ \sum_{\beta \subset B(n)} \mu(d_a) \right\},
\]
\[
\sum_{\beta \subset B(n)} \mu(d_a) \chi(d_a) \sum_{d = d_d} \mu(d_a) \}
\]
\[
\sum_{\alpha \subset B(n)} \mu(d_a) \chi(d_a) \sum_{d = d_d} \mu(d_a) \}
\]
\[
\sum_{d \mid n(\chi)} \frac{(d^k_d, n)}{d} \chi^{-1} \left( \frac{d^k_d}{n}, n \right) \sum_{\beta \subset B(n)} \mu(d_a) \chi(d_a) \}
\]
\[
\sum_{\alpha \subset B(n)} \mu(d_a) \chi(d_a) \sum_{d = d_d} \mu(d_a) \}
\]
\[
\sum_{d \mid n(\chi)} \frac{(d^k_d, n)}{d} \chi^{-1} \left( \frac{d^k_d}{n}, n \right) \sum_{\alpha \subset B(n)} \mu(d_a) \chi(d_a) \}
\]
\[
\sum_{d \mid n(\chi)} \frac{(d^k_d, n)}{d} \chi^{-1} \left( \frac{d^k_d}{n}, n \right) \sum_{\alpha \subset B(n)} \mu(d_a) \chi(d_a) \}
\]
which implies (II). Thus the proof of Theorem 1 is completed.

Let \( Q(\sqrt{D}) = K \) be a quadratic extension field of \( Q \) with discriminant \( D \). We denote by \( \left( \frac{D}{n} \right) \) or \( \chi_{n}(D) \) the Kronecker's symbol of \( K \). Then \( \left( \frac{D}{n} \right) \) is a primitive character modulo \( |D| \).

REMARK 3. Conversely it is well-known that every primitive character of degree 2 is of such type.

Let \( h(D) \) be the class number of \( K = Q(\sqrt{D}) \) and \( 2\omega_{D} \) be the number of the roots of unity in \( K \). Then the following Lemma 7 is well-known.

**Lemma 7.** Notation being as above. Then we have

\[
H_{\omega_{D}} = \begin{cases} 
0 & \text{if } D > 0, \\
\frac{h(D)}{\omega_{D}} & \text{if } D > 0.
\end{cases}
\]

REMARK 4. It is also well-known that if \( \left( \frac{D}{-1} \right) = 1 \) then \( D > 0 \) and if \( \left( \frac{D}{-1} \right) = -1 \) then \( D < 0 \).

**Corollary 1.** In the case \( k = 2 \) we have

\[
c_{a}^{2}(n) = \frac{n_a - 1}{2} + \sum_{\substack{D < 0 \\mid D \mid n}} \left( \frac{D}{a} \right)^{-1} \frac{h(D)}{\omega_{D}} \sum_{d \mid n(\chi_{D})} d \prod_{\substack{p \mid d(\chi_{D}) \\ (p, D) = 1}} \left[ 1 - \left( \frac{D}{p} \right) \right],
\]

where \( D \) runs over all the discriminants of the imaginary quadratic fields dividing \( n \).

Proof. By the definition of \( n(\chi_{D}) \) we can easily see that if \( d \) divides \( n(\chi_{D}) \) then \( d^2 \) divides \( n \). It follows

\[
\left( \frac{d^2, n}{d} \right) = d \quad \text{and} \quad \left( \frac{d^2, n}{d^2} \right) = 1.
\]

Therefore by Remark 3, Remark 4, Lemma 2, Lemma 7 and the above facts, Theorem 1 implies our Corollary.

Our Corollary in the case \( a = 1 \) and \( n \) = prime is obtained by T. Honda in [2]

**Corollary 2.** If \( k = 2 \) then \( c_{a}^{2}(n) \geq 0 \). Moreover \( c_{a}^{2}(n) = 0 \), if and only if \( n \) is of the following type

\[
n = p_1 \cdots p_j \quad \text{or} \quad 2p_1 \cdots p_j,
\]

where \( p_1, \ldots, p_j \) are distinct primes each of which is congruent to 1 modulo 4.
Proof. The first assertion is obvious from Corollary 1. We shall prove the second assertion. If \( c^{(2)}_1(n) = 0 \) then \( n \) must be square-free, because if \( n \) is not square-free then \( n > 1 \), which implies \( c^{(2)}_1(n) > 0 \). Consequently we have by Corollary 1

\[
c^{(2)}_1(n) = \sum_{\substack{|D| \equiv n}} \frac{h(D)}{w_D}.
\]

If there exists some \( p \) such that \( p \mid n \) and \( p \equiv 3 \mod 4 \), then \(-p\) is the discriminant of \( \mathbb{Q}(\sqrt{-p}) \). This shows

\[
c^{(2)}_1(n) \geq \frac{h(-p)}{w_p} > 0.
\]

Thus \( n \) must be an integer of such type as in our Corollary. The converse is clear.

**Corollary 3.** If \( k \) is an odd integer, then we have

\[
c^{(k)}_a(n) = \frac{n_0-1}{2},
\]

therefore \( |c^{(k)}_a(n)| < n^{(k-1)/2} \).

Proof. Let \( \chi \) be any character modulo \( n \) of degree \( k \). Then we have

\[
\chi(-1)^a = \chi((-1)^a) = 1
\]

and

\[
\chi(-1)^k = 1.
\]

This shows \( \chi(-1)=1 \). Therefore by Lemma 2 we have \( H_x=0 \). This shows the first assertion of our Corollary by Theorem 1. We can immediately obtain the second assertion by a simple calculation.

**Remark 5.** \( c^{(k)}_a(n) \) is not always non-negative for even \( k > 2 \). For example \( c^{(4)}_a(29) = -2 \). (See the table of at the end of the section 5.)

4. **Proof of Conjecture 1**

Let \( \chi \) be a primitive character modulo \( f_x \). Then we define the Dirichlet’s \( L \)-function by

\[
L(s, \chi) = \sum_{n=1}^{\infty} \chi(n)n^{-s}.
\]

We denote by \( G(\chi) \) the Gauss’s sum with respect to \( \chi \), i.e.,

\[
G(\chi) = \sum_{a=1}^{f_x} \chi(a)\zeta^a,
\]
where \( \zeta = \exp(2\pi i/f_x) \). Then the following two lemmas are well-known. (See Hasse \[1\] and Prachar \[3\]).

**Lemma 8.**

\[ |L(1, \chi)| < 3 \log f_x . \]

**Lemma 9.**

\[ L(1, \chi) = \frac{\pi i G(\chi)}{f_x^2} \sum_{a=1}^{f_x} \chi(a)a . \]

Moreover

\[ G(\chi)G(\overline{\chi}) = \chi(-1)f_x , \]

in particular

\[ |G(\chi)| = \sqrt{f_x} . \]

**Lemma 10.**

\[ |H_x| < \sqrt{f_x} \log f_x . \]

**Proof.** By Lemma 8 and Lemma 9 we have

\[ |H_x| = \left| \frac{1}{f_x} L(1, \chi) f_x^2 \right| \]

\[ < \frac{f_x}{|G(\chi)|} \log f_x = \sqrt{f_x} \log f_x . \]

It is obvious that \( f_x \) is equal to \( f_x \). This completes the proof.

We denote by \( \delta(n) \) the number of prime divisors of \( n \).

**Lemma 11.** For any positive number \( \varepsilon \) and a given positive constant \( A \) we have

\[ A^{\varepsilon(n)} = O(n^\varepsilon) , \]

where \( O \) denotes the Landau’s large \( O \)-symbol.

**Proof.** We may suppose \( A > 1 \). Let \( p_0 \) be a sufficiently large prime number such that

\[ \frac{\log A}{\log p_0} < \varepsilon . \]

We denote by \( \delta_0 \) the number of primes which are less than \( p_0 \) and by \( \delta'(n) \) the number of prime divisors of \( n \) each of which is not smaller than \( p_0 \). Then we can easily see that

\[ \delta(n) \leq \delta'(n) + \delta_0 . \]
By the definition of $\delta'(n)$ we have
\[ p_{\delta'(n)}^*(n) \leq n. \]
Therefore we have
\[ \delta'(n) \leq \frac{\log n}{\log p_0}. \]
From this we get
\[ A_{\delta'(n)}^* \leq A_{\delta'(n)+\delta_0}^* = A_{\delta_0}^* A_{\delta'(n)}^* \]
\[ = A_{\delta_0}^* n^{\log A_{\delta'(n)}^*} = A_{\delta_0}^* n^{\log A_{\delta'(n)}^* \log A/\log n} \leq A_{\delta_0}^* n^{(\log n^* \log p_0)^* \log A/\log n} \leq A_{\delta_0}^* n^* . \]
This completes the proof.

**Lemma 12.** For any positive number $\varepsilon$ we have
\[ \sum_{d|n} 1 = O(n^\varepsilon) . \]

**Proof.** See Prachar [3]-I-Satz 5.2.

Now we shall prove Conjecture 1.

**Theorem 2.** For any positive number $\varepsilon$ and a fixed positive integer $k$ we have
\[ c_a^{(k)}(n) = O(n^{(k-1)/k + \varepsilon}) . \]

**Proof.** By Theorem 1 we have
\[ \sum_{d|n} |H_x| \sum_{d|n(x)} \left( \frac{d^*, n}{d} \right) \Pi_{p|n(d)(x)} \left( \frac{1 - \chi(p)}{p} \right) . \]
We have already known that
\[ n_0 \leq n^{(k-1)/k} . \]
Therefore we shall show that
\[ \sum_{d|n} |H_x| \sum_{d|n(x)} \left( \frac{d^*, n}{d} \right) \Pi_{p|n(d)(x)} \left( \frac{1 - \chi(p)}{p} \right) = O(n^{(k-1)/k} + \varepsilon) . \]
First we get by Lemma 11
\[ \Pi_{p|n(d)(x)} \left( \frac{1 - \chi(p)}{p} \right) \leq \Pi_{p|n} 2 = 2^{\delta(n)} = O(n^\varepsilon) . \]
Next we get
\[ \sum_{d|n} 1 < \Pi_{p|n} \left( \sum_{x \in \mathbb{R}} 1 \right) . \]
But by Lemma 3 we know that

\[ \sum_{f \chi \equiv p^m} \chi(f) \leq A, \quad \text{for some positive constant } A. \]

Hence by Lemma 11 we also get

\[ \sum_{f \chi \equiv p^m} \chi(f) = O(n^a). \]

Lastly we shall show that

\[ \left( \left| H_x \right| \sum_{d \mid n(x)} \frac{(d^k, n)}{d} \right) n^{(k-1)/k} = O(n^a) \]

We transform this into

\[ \left( \left| H_x \right| \sum_{d \mid n(x)} \frac{(d^k, n)}{d} \right) n^{(k-1)/k} = \frac{H_x}{f_x^{(k-1)/k}} \sum_{d \mid n(x)} \left( \frac{(d^k, n)}{f_x} \left( \frac{n^{(k-1)/k}}{f_x} \right) \right). \]

Then we have by Lemma 10

\[ \left| H_x \right| f_x^{(k-1)/k} \leq \left( f_x^{(k-1)/k} / f_x \right) \log f_x \leq \log f_x. \]

Moreover by Remark 2 we can easily see that

\[ \frac{(d^k, n)}{d} \left( \frac{n^{(k-1)/k}}{f_x} \right) < 1. \]

From these and by Lemma 12 we have

\[ \left( \left| H_x \right| \sum_{d \mid n(x)} \frac{(d^k, n)}{d} \right) n^{(k-1)/k} \leq \sum_{d \mid n(x)} \log n \]

\[ \leq \log n \sum_{d \mid n} 1 \]

\[ = O(n^a). \]

This completes the proof of our Theorem.

5. Number theoretic properties of some \( c^{(n)}(x) \).

**Lemma 13.** Let \( k \) be a positive integer and \( p \) be a prime number which is prime to \( k \). We denote by \( k_0 \) the greatest common divisor of \( k \) and \( p-1 \). Then we have

\[ N^{(k)}(x, p) = N^{(k_0)}(x, p). \]

Proof. If \( x \equiv 0 \mod p \) then the lemma is trivial. Hence we assume \( x \not\equiv 0 \mod p \). Consider the following sequence of groups and homomorphisms
\{1\} \longrightarrow (\mathbb{Z}/p\mathbb{Z})^{\times (p-1)/k_0} \longrightarrow (\mathbb{Z}/p\mathbb{Z})^{\times k_0} \longrightarrow (\mathbb{Z}/p\mathbb{Z})^{\times k_0} \longrightarrow \{1\},

where we define the homomorphisms \(g_1, g_2\) and \(g_3\) as follows

\[
\begin{align*}
g_1(a) &= a \cdot a \in (\mathbb{Z}/p\mathbb{Z})^{\times (p-1)/k_0}, \\
g_2(a) &= a^{k_0} \cdot a \in (\mathbb{Z}/p\mathbb{Z})^{\times k_0}, \\
g_3(a) &= a^{k/k_0} \cdot a \in (\mathbb{Z}/p\mathbb{Z})^{\times k_0}.
\end{align*}
\]

By the definition of \(k_0\), we see that \(k/k_0\) is prime to \((p-1)/k_0\). This shows that \(g_3\) is an isomorphism and the above sequence is exact. By the definition of \(N^{(h_0)}(x, p)\) and \(N^{(k)}(x, p)\) we see that \(N^{(h_0)}(x, p)\) is not zero if and only if \(x \in \text{Im}(g_1) = (\mathbb{Z}/p\mathbb{Z})^{\times k_0}\) and \(N^{(k)}(x, p)\) is not zero if and only if \(x \in \text{Im}(g_3 \circ g_2) = (\mathbb{Z}/p\mathbb{Z})^{\times k_0}\). Therefore \(N^{(h_0)}(x, p)\) is not zero if and only if so is \(N^{(k)}(x, p)\). If \(x \in (\mathbb{Z}/p\mathbb{Z})^{\times k_0}\) then \(N^{(h_0)}(x, p) = \#\ker(g_2) = \#\ker(g_3 \circ g_2) = N^{(k)}(x, p)\). Thus Lemma 13 is proved.

**Proposition 2.** Let \(p_1, \ldots, p_j\) be distinct primes each of which is prime to \(p\) and \(k_i\) be the greatest common divisor of \(k\) and \(p_i-1\). If we denote by \(k_0\) the least common multiple of \(k_1, \ldots, k_j\), then

\[
c_{a^{(k)}}^{(k)}(p_1, \ldots, p_j) = c_{a^{(k_0)}}^{(k_0)}(p_1, \ldots, p_j).
\]

**Proof.** By Lemma 13 it is obvious that

\[
N^{(k)}(x, p) = N^{(k_0)}(x, p) = N^{(k_0)}(x, p).
\]

Then by Lemma 1 we have

\[
N^{(k)}(x, p_1, \ldots, p_j) = N^{(k)}(x, p_1, \ldots, p_j).
\]

On the other hand we have already shown in the proof of Proposition 1 that

\[
c_{a^{(k)}}^{(k)}(n) = \frac{n-1}{2} \left( - \frac{1}{n} \sum_{a=1}^{n-1} N^{(k)}(a^{-1}x, n),
\right.
\]

where we consider \(a^{-1}x\) in \((\mathbb{Z}/n\mathbb{Z})^{\times}\). Therefore we can immediately obtain the lemma.

**Lemma 14.** Let \(p\) be a prime such that

\[
p-1 \equiv 0 \text{ mod } 2k
\]

and \(\chi\) be a character of modulo \(p\) of degree \(k\), then

\[
\chi(-1) = 1.
\]

**Proof.** If we put \(p-1=2mk\) with a positive integer \(m\), then the order of \(-1\) in \((\mathbb{Z}/p\mathbb{Z})^{\times}\) is \(mk\). Therefore there exists some \(x_o \in (\mathbb{Z}/p\mathbb{Z})\) such that
which implies $\chi(-1) = \chi(x_0^k)^k = 1$.

**Proposition 3.** Let $p_1, \ldots, p_j$ be distinct primes each of which is prime to $k$ and congruent to 1 modulo $2k$ then

$$c_\chi^{(k)}(p_1 \cdots p_j) = 0.$$ 

Proof. We put $n = p_1 \cdots p_j$. Let $\chi$ be any character of conductor $f_\chi | n$, then by the decomposition (1) in §2 of $\chi$ and Lemma 14 we see that $\chi(-1) = 1$. Therefore by Lemma 2 and Theorem 1 we can immediately obtain our Proposition.

In the case $k=2$, we have obtained the very beautiful formula for $c_\chi^{(2)}(n)$ in corollary 2. But when $k$ is an even integer $> 2$, $c_\chi^{(k)}(n)$ is more complicated. From now on till the end of this section we shall only consider the case $k=4$ and $n = p$, where $p$ is a prime. If $p \equiv 2 \pmod{4}$, then $c_\chi^{(4)}(2) = 0$ and there is nothing to say. If $p \equiv 3 \pmod{4}$, then $c_\chi^{(4)}(p) = c_\chi^{(2)}(p)$ by Proposition 2. Further if $p \equiv 1 \pmod{8}$, then $c_\chi^{(4)}(p) = 0$ by Proposition 3. Therefore we may confine ourselves to the cases $p \equiv 5 \pmod{8}$.

Let $p$ be a prime which is congruent to 5 modulo 8. Then the unit group $(\mathbb{Z}/p\mathbb{Z})^\times$ of the residue ring $\mathbb{Z}/p\mathbb{Z}$ is a cyclic group of order $p-1$ which is divisible by 4. We denote by $H$ (respectively $H_0$) the unique subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$ of index 4 (respectively 2). Let $K$ be the $p$-th cyclotomic field i.e., $K = \mathbb{Q}(\zeta)$, where $\zeta = \exp\left(\frac{2\pi i}{p}\right)$. Then there exists the subfield $L$ (respectively $L_0$) corresponding to the group $H$ (respectively $H_0$). As the order of $-1$ is 2, $H$ does not contain $-1$ but $H_0$ contains it. This shows that $L$ is a totally imaginary field and $L_0$ is the maximal totally real subfield of $L$. Hence we obtain the following diagram

$$\begin{array}{ccc}
K = \mathbb{Q}(\zeta) & \longrightarrow & \{1\} \\
\downarrow & & \downarrow \\
L & \longrightarrow & H(\mp -1) \\
\downarrow & & \downarrow \\
L_0 & \longrightarrow & H_0(\mp -1) \\
\downarrow & & \downarrow \\
\mathbb{Q} & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^\times.
\end{array}$$

Hereafter till the end of this section we shall use the following notations.

$$\zeta = \exp\left(\frac{2\pi i}{p}\right),$$

$h = \text{the class number of } L$

$h_0 = \text{the class number of } L_0$
\( h^* = h/h_0 \)
\( E = \) the unit group of \( L \)
\( E_0 = \) the unit group of \( L_0 \)
\( w = \) the number of the roots of unity of \( L \)

By the condition on \( p \) we can easily see that the element 2 is not a quadratic residue of modulo \( p \). This shows that the group \((\mathbb{Z}/p\mathbb{Z})^*/H\) is generated by the class represented by 2. We shall denote by \( \chi^{(j)} (j=0, 1, 2, 3) \) the character of \((\mathbb{Z}/p\mathbb{Z})^*/H\) which takes value \( \sqrt{-1}^j \) at the class 2 mod \( H \). From these characters we obtain the characters modulo \( p \) in the sense of section 2 and we also denote them by \( \chi^{(j)} (j=0, 1, 2, 3) \). We can easily see that these characters except \( \chi^{(0)} \) have the conductor \( p \). Then the group of characters \( \{\chi^{(j)} | j=0, 1, 2, 3\} \) corresponds to \( L \) and \( \{\chi^{(0)}, \chi^{(2)}\} \) corresponds to \( L_0 \). Now we quote the following formula for \( h^* \) from Hasse [1].

**Lemma 15.** Let \( E' \) be the group generated by \( E_0 \) and the roots of unity contained in \( L \). Then we have

\[
h^* = Qw \prod_{j=1, 2} \frac{1}{2p} \left( \sum_{x=1}^{p-1} \chi^{(j)}(x)x \right) ,
\]

where \( Q \) is defined by \( Q = [E; E'] \). In our case we can easily see \( Q = 1 \).

**Proof.** See Hasse [1] III-(*).

**Theorem 3.** If we use the above notation, then we have

\[
h^* = \frac{w}{4} \left\{ \left( \frac{c^{(4)}(p)}{2} \right)^2 + \left( \frac{c^{(4)}(p)}{2} \right)^2 \right\} .
\]

**Proof.** We put

\[
\frac{1}{p} \sum_{x=1}^{p-1} \chi^{(1)}(x)x = a+bi \quad a, b \in \mathbb{Q} .
\]

Then we have

\[
\frac{1}{p} \sum_{x=1}^{p-1} \chi^{(3)}(x)x = a-bi .
\]

We shall prove that

\[
(7) \quad a = -\frac{c^{(4)}(p)}{2} ,
\]

\[
(8) \quad b = -\frac{c^{(4)}(p)}{2} .
\]

By the definition of \( a \) we get
As \( p \equiv 1 \mod 4 \), if \( x \equiv y^2 \mod p \) then \( -x \equiv y'^2 \mod p \) for some \( y' \in \mathbb{Z}/p\mathbb{Z} \). From this we get

\[
(9) \quad \frac{\sum_{x \equiv y \mod p}^p x}{p} \equiv \frac{p(p-1)}{4}.
\]

On the other hand we have by the definition of \( c_1^{(q)}(p) \)

\[
(10) \quad c_1^{(q)}(p) = \frac{p-1}{2} - \frac{4}{p} \sum_{x \equiv y \mod p}^p x.
\]

By (9) and (10) we have

\[
a = \left( \frac{p-1}{4} c_1^{(q)}(p) \right) - \frac{p-1}{4} = -\frac{c_1^{(q)}(p)}{2}.
\]

Thus we obtain the formula (7). Next we shall prove (8). By the definition of \( b \) we have

\[
b = \left\{ \frac{1}{p} \sum_{x \equiv y \mod p}^p x \right\} - \frac{\sum_{x \equiv y \mod p}^p x}{p} = \frac{1}{p} \left\{ 2 \sum_{x \equiv y \mod p}^p x \right\}
\]

On the other hand by the definition of \( c_2^{(q)}(p) \) we have also

\[
c_2^{(q)}(p) = \frac{p-1}{2} - \frac{4}{p} \sum_{x \equiv y \mod p}^p x.
\]

Therefore we obtain
Thus we have completed the proof of our Theorem.

Remark 6. We can easily see that

\[ w = 10 \quad \text{if } p = 5, \]
\[ w = 2 \quad \text{otherwise.} \]

For the even \( k > 2 \) it can be considered that \( \psi(p) \)’s have similar relations to some relative class numbers. But for the composite \( n \)'s such relations are more complicated. We shall give the table of \( \Lambda^*, \psi(p) \) and \( \psi_2(p) \).

<table>
<thead>
<tr>
<th>( p )</th>
<th>( \psi(p) )</th>
<th>( \psi_2(p) )</th>
<th>( \Lambda^* )</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>6/5</td>
<td>2/5</td>
<td>1</td>
</tr>
<tr>
<td>13</td>
<td>2</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>29</td>
<td>-2</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>37</td>
<td>2</td>
<td>-2</td>
<td>1</td>
</tr>
<tr>
<td>53</td>
<td>-2</td>
<td>-2</td>
<td>1</td>
</tr>
<tr>
<td>61</td>
<td>2</td>
<td>-2</td>
<td>1</td>
</tr>
<tr>
<td>101</td>
<td>-6</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>109</td>
<td>10</td>
<td>6</td>
<td>17</td>
</tr>
<tr>
<td>149</td>
<td>6</td>
<td>6</td>
<td>9</td>
</tr>
<tr>
<td>157</td>
<td>2</td>
<td>6</td>
<td>5</td>
</tr>
<tr>
<td>173</td>
<td>-6</td>
<td>-2</td>
<td>5</td>
</tr>
<tr>
<td>181</td>
<td>14</td>
<td>2</td>
<td>25</td>
</tr>
<tr>
<td>197</td>
<td>-2</td>
<td>-6</td>
<td>5</td>
</tr>
<tr>
<td>229</td>
<td>6</td>
<td>10</td>
<td>17</td>
</tr>
<tr>
<td>269</td>
<td>10</td>
<td>-2</td>
<td>13</td>
</tr>
<tr>
<td>277</td>
<td>-6</td>
<td>10</td>
<td>17</td>
</tr>
<tr>
<td>293</td>
<td>6</td>
<td>-6</td>
<td>9</td>
</tr>
<tr>
<td>317</td>
<td>2</td>
<td>10</td>
<td>13</td>
</tr>
<tr>
<td>349</td>
<td>-6</td>
<td>-2</td>
<td>5</td>
</tr>
<tr>
<td>389</td>
<td>18</td>
<td>2</td>
<td>41</td>
</tr>
<tr>
<td>397</td>
<td>2</td>
<td>-10</td>
<td>13</td>
</tr>
<tr>
<td>421</td>
<td>2</td>
<td>14</td>
<td>25</td>
</tr>
<tr>
<td>461</td>
<td>-2</td>
<td>-14</td>
<td>25</td>
</tr>
</tbody>
</table>
6. An afterthought

We shall give another elementary proof of Corollary 3.

**Proposition 4.** If the following congruence equation has a solution

\[(10) \quad x^k \equiv -1 \pmod{n},\]

then

\[c_a^{(k)}(n) = \frac{n_0^{(k)} - 1}{2}.\]

**Proof.** If (10) has a solution, then it is clear that

\[N^{(k)}(x, n) = N^{(k)}(-x, n) = N^{(k)}(n-x, n).\]

Hence by the definition of \(c_a^{(k)}(n)\) we have

\[c_a^{(k)}(n) = \frac{n-1}{2} \cdot \frac{1}{n} \sum_{x=1}^{n-1} N^{(k)}(a^{-1}x, n)x \]

\[= \frac{n-1}{2} \cdot \frac{1}{2n} \sum_{x=1}^{n-1} \{N^{(k)}(a^{-1}x, n)x + N^{(k)}(a^{-1}(n-x), n)(n-x)\} \]

\[= \frac{n-1}{2} \cdot \frac{1}{2n} \sum_{x=1}^{n-1} nN^{(k)}(a^{-1}x, n),\]

where we consider \(a^{-1}x\) in \(\mathbb{Z}/n\mathbb{Z}\). But we can easily see that

\[\sum_{x=1}^{n-1} N^{(k)}(a^{-1}x, n) = n.\]

From this it follows that

\[c_a^{(k)}(n) = \frac{n-1}{2} \cdot \frac{1}{2} (n - N^{(k)}(0, n)) \]

\[= \frac{N^{(k)}(0, n) - 1}{2}.\]

But by a simple computation we get

\[N^{(k)}(0, n) = n_0^{(k)}.\]

Thus we obtain Proposition 4.

Considering the definition of \(c_a^{(k)}(n)\), if \(ax^k \equiv 0 \pmod{n}\) then \(\left\lfloor \frac{ax^k}{n} \right\rfloor = \frac{ax^k}{n}\), but we suppose that \(\left\lfloor \frac{ax^k}{n} \right\rfloor\) is approximately \(\frac{ax^k}{n} - \frac{1}{2}\). Therefore \(\frac{n_0^{(k)} - 1}{2}\) can be considered the known error term. From this point of view we had better to
consider that \( d_a^{(k)}(n) = c_a^{(k)}(n) - \frac{n^{(k)} - 1}{2} \) is the essential error term. The proof of

Theorem 2 shows that the order of \( d_a^{(k)}(n) \) is less than \( n^{(k-1)/k} \) for any \( \varepsilon > 0 \). The Corollary 2 is true with slight modification of \( d_a^{(k)}(n) \).

OSAKA UNIVERSITY

References


