



Title	On the number of the lattice points in the area $0 < x < n, 0 < y \leq ax^k / n$.
Author(s)	Miyawaki, Isao
Citation	Osaka Journal of Mathematics. 1975, 12(3), p. 647-671
Version Type	VoR
URL	https://doi.org/10.18910/12189
rights	
Note	

The University of Osaka Institutional Knowledge Archive : OUKA

<https://ir.library.osaka-u.ac.jp/>

The University of Osaka

ON THE NUMBER OF THE LATTICE POINTS IN THE AREA

$$0 < x < n, \quad 0 < y \leq ax^k/n.$$

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

$$S_a^{(k)}(n) = \sum_{x=1}^{n-1} [ax^k/n],$$

where $[]$ denotes the Gauss symbol. Let

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

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

$$\sum_{x=1}^{n-1} ax^k/n = S_a^{(k)}(n) + \sum_{x=1}^{n-1} \{ax^k/n\}$$

or

$$S_a^{(k)}(n) = \sum_{x=1}^{n-1} ax^k/n - \sum_{x=1}^{n-1} \{ax^k/n\}.$$

We put

$$S_a^{(k)}(n) = \sum_{x=1}^{n-1} ax^k/n - \frac{n-1}{2} + c_a^{(k)}(n),$$

$$c_a^{(k)}(n) = \frac{n-1}{2} - \sum_{x=1}^{n-1} \{ax^k/n\}.$$

If we suppose that $S_a^{(k)}(n)$ behaves approximately as $\sum_{x=1}^{n-1} ax^k/n - \frac{n-1}{2}$ 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 ε we have

$$c_a^{(k)}(n) = O(n^{((k-1)/k)+\varepsilon}),$$

for $a=1$.

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

$$n = p_1 \cdots p_j,$$

where p_1, \dots, 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, $c_a^{(k)}(n)$ is a very simple quantity. On the other hand in the case k is even, $c_a^{(k)}(n)$ 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 $k > 2$, $c_a^{(k)}(n)$ is also related to some class numbers of some subfields of the cyclotomic field $\mathbb{Q}(\zeta)$ where ζ 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

$$\{y \in \mathbb{Z} \mid y^k \equiv x \pmod{n}, \quad 0 \leq y < n\}.$$

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

$$f; \mathbb{Z}/n\mathbb{Z} \rightarrow \prod_{i=1}^j \mathbb{Z}/p_i^{e_i}\mathbb{Z}, \quad (f(a \bmod n) = \prod_{i=1}^j a \bmod p_i^{e_i}).$$

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

$$\Gamma(n) = \{\chi \mid \chi; (\mathbb{Z}/n\mathbb{Z})^\times \rightarrow U, \text{ homomorphism} \},$$

where $U = \{z \in \mathbb{C} \mid |z| = 1\}$. Then $\Gamma(n)$ is an abelian group isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$. An element χ of $\Gamma(n)$ is extended on \mathbb{Z} by setting

$$\chi(a) = \begin{cases} 0 & \text{if } (a, n) \neq 1 \\ \chi(a \bmod n) & \text{otherwise.} \end{cases}$$

This function is denoted by χ , and is called a character modulo n . If χ has always the value 1 for any a such that $(a, n)=1$, then χ is called the trivial character modulo n , and denoted by 1. If χ is a non-trivial character modulo n and there is no character χ' of $(\mathbb{Z}/n'\mathbb{Z})^\times$ with a proper divisor n' of n satisfying $\chi'(a)=\chi(a)$ for any $(a, n)=1$, then χ is called a primitive character modulo n . Any non-trivial character χ modulo n can be uniquely decomposed to the following form

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

where χ_0 is the trivial character modulo n and χ' is a primitive character modulo n' with some divisor n' of n . We call this n' the conductor of χ and denote it by f_χ . If χ is a primitive character modulo some n , then we call χ simply primitive.

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

$$(1) \quad \chi = \prod_{i=1}^j \chi_i,$$

where each χ_i is a character modulo $p_i^{e_i}$. It is clear that χ is primitive, if and only if each χ_i is primitive. Let χ be a character modulo n . Then we put

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

Lemma 2. *Let χ 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

$$\begin{aligned} H_\chi &= -\frac{1}{2n} \left(\sum_{a=1}^{n-1} \chi(a)a + \sum_{a=1}^{n-1} \chi(-a+n)(-a+n) \right) \\ &= -\frac{1}{2n} \left(\sum_{a=1}^{n-1} \chi(a)a + \sum_{a=1}^{n-1} \chi(-a)(-a+n) \right) \\ &= -\frac{1}{2n} \sum_{a=1}^{n-1} \chi(a)(a+(-a+n)) \\ &= -\frac{1}{2} \sum_{a=1}^{n-1} \chi(a) = 0. \end{aligned}$$

We put

$$\Gamma^{(k)}(n) = \{ \chi \in \Gamma(n) \mid \chi^k = 1 \}.$$

Lemma 3. *Let p be a prime number. Then we have*

$$(i) \quad N^{(k)}(b, p^e) = \sum_{\chi \in \Gamma^{(k)}(p^e)} \chi(b) = 1 + \sum_{\substack{\chi: \text{primitive} \\ f_{\chi} | p^e \\ \chi^k = 1}} \chi(b)$$

if $(b, p) = 1$,

$$(ii) \quad N^{(k)}(b, p) = 1 + \sum_{\substack{f_{\chi} = p \\ \chi^k = 1}} \chi(b).$$

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

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

$$(ii) \quad \#\Gamma^{(k)}(p^e) = \begin{cases} p^{e-1}(p-1, k) & \text{if } e_0 + 1 \geq e, \\ (p \neq 2) \quad p^{e_0}(p-1, k) & \text{if } e_0 + 1 < e, \end{cases}$$

where we define e_0 by

$$p^{e_0} || k, \quad e_0 > 0,$$

$$(iii) \quad \#\Gamma^{(k)}(2^e) = \begin{cases} 2^{e-1} & \text{if } e \leq e_0 + 2 \\ 2^{e_0+1} & \text{if } e \geq e_0 + 3, \end{cases}$$

where we define e_0 by

$$2^{e_0} || k, \quad e_0 > 0.$$

Epecially 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

$$\begin{aligned} (\mathbb{Z}/p^e\mathbb{Z})^\times &\cong \mathbb{Z}/(p-1)p^{e-1}\mathbb{Z} && \text{if } p \neq 2, \\ (\mathbb{Z}/2^e\mathbb{Z})^\times &\cong \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2^{e-2}\mathbb{Z} && \text{if } e \geq 2, \\ (\mathbb{Z}/p^e\mathbb{Z})^\times / (\mathbb{Z}/p^e\mathbb{Z})^{\times k} &\cong \Gamma^{(k)}(p^e), \end{aligned}$$

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

$$A(n) = \{1, 2, \dots, j\}$$

$$B(n) = \{i \in A(n) \mid e_i \geq 2\}.$$

For a subset $\alpha = \{\alpha_1, \dots, \alpha_i\}$ of the set $A(n)$ we denote by d_α the integer

$$d_\alpha = \prod_{i=1}^l p_{\alpha_i}, \quad \text{if } \alpha \neq \phi$$

$$d_\phi = 1.$$

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

$$n_0 = n_0^{(k)} = \prod_{i=1}^j p_i^{(k-1)s_i + r_i - 1}.$$

Let d be a positive divisor of n . Then we put

$$n(d) = n^{(k)}(d) = n / (d^k, n),$$

$$d^*(n) = d^*(d)^{(k)} = d^k / (d^k, n).$$

Under the above notation we have the following proposition.

Proposition 1.

$$c_\alpha^{(k)}(n) = \sum_{\substack{\chi: \text{primitive} \\ f_\chi | n, \chi^k = 1}} \overline{\chi(a)} H_\chi - \left[\sum_{\substack{\alpha \subset B(n) \\ \alpha \neq \phi}} \mu(d_\alpha) \left\{ \frac{(d_\alpha^k, n)/d_\alpha - 1}{2} + \frac{(d_\alpha^k, n)}{d_\alpha} \right. \right. \\ \left. \left. \cdot c_{\alpha d_\alpha^{(k)}(n)}^{(k)}(n(d_\alpha)) - \sum_{\substack{\chi: \text{primitive} \\ f_\chi | n, \chi^k = 1 \\ (f_\chi, d_\alpha) = 1}} \chi(d_\alpha) \overline{\chi(a)} H_\chi \right\} \right],$$

where we denote by $\mu(\cdot)$ the Möbius function.

Proof. By the definition of $c_\alpha^{(k)}(n)$ we have

$$c_\alpha^{(k)}(n) = \frac{n-1}{2} - \frac{1}{2} \sum_{x=1}^{n-1} N^{(k)}(a^{-1}x, n),$$

where we consider $a^{-1}x$ in $(\mathbb{Z}/n\mathbb{Z})^\times$. If $(x, d_{B(n)}) = 1$ then by Lemma 1 and Lemma 2 we have

$$N^{(k)}(a^{-1}x, n) = \prod_{i=1}^j (1 + \sum_{\substack{\chi: \text{primitive} \\ f_\chi | p_i^{\alpha_i}, \chi^k = 1}} \chi(a^{-1}x)).$$

Therefore we get

$$\begin{aligned}
c_a^{(k)}(n) &= \frac{n-1}{2} - \left[\frac{1}{n} \sum_{x=1}^{n-1} \prod_{i=1}^j (1 + \sum_{\substack{\chi: \text{primitive} \\ f_x | p_i^e, \chi^k=1}} \chi(a^{-1}x)) x \right. \\
&\quad + \sum_{\substack{\alpha \in B(n) \\ \alpha \neq \phi}} \mu(d_\alpha) \left\{ \frac{1}{n} \sum_{x=1}^{(n/d_\alpha)^{-1}} \prod_{i \in \alpha} (1 + \sum_{\substack{\chi: \text{primitive} \\ f_x | p_i^e, \chi^k=1}} \chi(a^{-1}d_\alpha x)) d_\alpha x \right. \\
&\quad \left. \left. - \sum_{x=1}^{(n/d_\alpha)^{-1}} \left\{ \frac{a(d_\alpha x)^k}{n} \right\} \right\} \right] \\
&= \frac{n-1}{2} - \frac{n(n-1)}{2n} - \frac{1}{n} \sum_{\substack{\chi: \text{primitive} \\ f_x | n, \chi^k=1}} \sum_{x=1}^{n-1} \chi(a^{-1}x)x - \sum_{\substack{\alpha \in B(n) \\ \alpha \neq \phi}} \mu(d_\alpha) \\
&\quad \cdot \left[\frac{d_\alpha}{n} \cdot \frac{(n/d_\alpha)((n/d_\alpha)-1)}{2} - \frac{d_\alpha}{n} \sum_{\substack{\chi: \text{primitive} \\ f_x | n, \chi^k=1 \\ (f_x, d_\alpha)=1}} \sum_{x=1}^{(n/d_\alpha)^{-1}} \chi(a^{-1}d_\alpha x)x \right. \\
&\quad \left. - \sum_{x=1}^{(n/d_\alpha)^{-1}} \left\{ \frac{ad_\alpha^*(n)x^k}{n(d_\alpha)} \right\} \right],
\end{aligned}$$

where we should note that

$$\frac{1}{n} \sum_{x=1}^{n-1} \chi(x)x = \frac{1}{n} \sum_{x=1}^{f_x-1} \sum_{i=0}^{(n/f_x)^{-1}} \chi(x)(x+if_x) = \frac{1}{n} \frac{n}{f_x} \sum_{x=1}^{f_x-1} \chi(x)x = -H_x.$$

Then we have

$$\begin{aligned}
c_a^{(k)}(n) &= \sum_{\substack{\chi: \text{primitive} \\ f_x | n, \chi^k=1}} \overline{\chi(a)} H_x - \left[\sum_{\substack{\alpha \in B(n) \\ \alpha \neq \phi}} \mu(d_\alpha) \left\{ \frac{(n/d_\alpha)-1}{2} - \sum_{\substack{\chi: \text{primitive} \\ f_x | n, \chi^k=1 \\ (f_x, d_\alpha)=1}} \overline{\chi(a)} \chi(d_\alpha) H_x \right. \right. \\
&\quad \left. \left. - \frac{n}{d_\alpha n(d_\alpha)} \sum_{x=1}^{(n/d_\alpha)^{-1}} \left\{ \frac{ad_\alpha^*(n)x^k}{n(d_\alpha)} \right\} \right\} \right].
\end{aligned}$$

On the other hand we see that

$$- \sum_{x=1}^{(n/d_\alpha)^{-1}} \left\{ \frac{ad_\alpha^*(n)x^k}{n(d_\alpha)} \right\} = c_{ad_\alpha^*(n)}^{(k)}(n(d_\alpha)) - \frac{n(d_\alpha)-1}{2}.$$

Therefore we have

$$\begin{aligned}
c_a^{(k)}(n) &= \sum_{\substack{\chi: \text{primitive} \\ f_x | n, \chi^k=1}} \overline{\chi(a)} H_x - \sum_{\substack{\alpha \in B(n) \\ \alpha \neq \phi}} \mu(d_\alpha) \left[\frac{(n/d_\alpha)-1}{2} - \frac{n}{d_\alpha n(d_\alpha)} \cdot \frac{n(d_\alpha)-1}{2} \right. \\
&\quad \left. - \sum_{\substack{\chi: \text{primitive} \\ f_x | n, \chi^k=1 \\ (f_x, d_\alpha)=1}} \overline{\chi(a)} \chi(d_\alpha) H_x + \frac{n}{d_\alpha n(d_\alpha)} c_{ad_\alpha^*(n)}^{(k)}(n(d_\alpha)) \right]
\end{aligned}$$

$$= \sum_{\substack{\chi: \text{primitive} \\ f_x | n, \chi^k = 1}} \overline{\chi(a)} H_x - \sum_{\substack{a \in B(n) \\ a \neq \phi}} \mu(d_a) \left[\frac{(n/d_a n(d_a)) - 1}{2} \right. \\ \left. + \frac{n}{d_a(n(d_a))} c_{aa^*(n)}^{(k)}(n(d_a)) - \sum_{\substack{\chi: \text{primitive} \\ f_x | n, \chi^k = 1 \\ (f_x, d_a) = 1}} \overline{\chi(a)} \chi(d_a) H_x \right].$$

But by the definition of $n(d)$ we have

$$\frac{n}{n(d_a)} = \frac{n}{\frac{n}{(d_a^k, n)}} = (d_a^k, n).$$

Therefore we get

$$c_a^{(k)}(n) = \sum_{\substack{\chi: \text{primitive} \\ f_x | n, \chi^k = 1}} \overline{\chi(a)} H_x - \sum_{\substack{a \in B(n) \\ a \neq \phi}} \mu(d) \left[\frac{((d_a^k, n)/d_a) - 1}{2} \right. \\ \left. + \frac{(d_a^k, n)}{d_a} c_{aa^*(n)}^{(k)}(n(d_a)) - \sum_{\substack{\chi: \text{primitive} \\ f_x | n, \chi^k = 1 \\ (f_x, d_a) = 1}} \overline{\chi(a)} \chi(d_a) H_x \right].$$

Thus Proposition 1 is proved

Let χ be a non-trivial character modulo n such that $\chi^k = 1$. Then we define the integer $n(\chi) = n^{(k)}(\chi)$ as follows,

$$n(\chi) = \prod_{p: \text{prime}} p^{[v_p(n/f_x)/k] + \varepsilon_{p,n}},$$

$$\varepsilon_{p,n} = \varepsilon_{p,n}^{(k)} = \begin{cases} 0 & \text{if } p | f_x \text{ or } v_p\left(\frac{n}{f_x}\right) - k \left[v_p\left(\frac{n}{f_x}\right) \frac{1}{k} \right] \leq 1, \\ 1 & \text{otherwise,} \end{cases}$$

where we denote by $v_p(\cdot)$ 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 $n/(d^k, n) \equiv 0 \pmod{f_x}$.

Lemma 5. Let n be a positive integer. For distinct primes p_1, \dots, p_j such that $p_i^2 | n$ ($i=1, \dots, j$), we put $d_0 = p_1 \cdots p_j$ and $n(d_0) = n/(d_0^k, n)$. Let χ be a character modulo $n(d_0)$. Then χ induces the character modulo n through the homomorphism $(\mathbb{Z}/n\mathbb{Z})^\times \rightarrow (\mathbb{Z}/n(d_0)\mathbb{Z})^\times$. Denoting this also χ we have that if d divides $n(d_0)(\chi)$ then dd_0 divides $n(\chi)$.

Proof. We shall show that $v_p(dd_0) \leq v_p(n(\chi))$ for every prime p . We consider the two cases.

The case I. $p \neq p_i$ ($i=1, \dots, j$).

By the definition of $n(d_0)$ we have

$$v_p(n) = v_p(n(d_0))$$

and

$$v_p(n/f_x) = v_p(n(d_0)/f_x).$$

It follows from this

$$\varepsilon_{p,n} = \varepsilon_{p,n(d_0)}.$$

From this and by the definition of d we have

$$\begin{aligned} v_p(dd_0) &= v_p(d) \leq [v_p(n(d_0)/f_x)/k] + \varepsilon_{p,n(d_0)} \\ &= [v_p(n/f_x)/k] + \varepsilon_{p,n} \\ &= v_p(n(X)). \end{aligned}$$

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

$$v_p(n(d_0)/f_x) = \begin{cases} v_p(n/f_x) - k & \text{if } p^k | n, \\ 0 & \text{if } p^k \nmid n. \end{cases}$$

Therefore we shall consider the two cases.

(i) The case $v_p(n(d_0)/f_x) = v_p(n/f_x) - k$.

In this case we have

$$\begin{aligned} v_p(n/f_x) - k \left[\frac{v_p(n/f_x)}{k} \right] &= v_p(n(d_0)/f_x) + k - k[v_p(n(d_0)/f_x)/k + 1] \\ &= v_p(n(d_0)/f_x) - k[v_p(n(d_0)/f_x)/k]. \end{aligned}$$

This shows that $\varepsilon_{p,n} = \varepsilon_{p,n(d_0)}$. Noting this we have

$$\begin{aligned} v_p(dd_0) &= 1 + v_p(d) \leq 1 + [v_p(n(d_0)/f_x)/k] + \varepsilon_{p,n(d_0)} \\ &= 1 + [v_p(n/f_x)/k - 1] + \varepsilon_{p,n} \\ &= [v_p(n/f_x)/k] + \varepsilon_{p,n} \\ &= v_p(n(X)). \end{aligned}$$

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

(ii) The case $v_p(n(d_0)/f_x) = 0$

In this case we should note that $v_p(f_x) = 0$. Then we have

$$v_p(n(d_0)/f_x) - k[v_p(n(d_0)/f_x)/k] = 0.$$

It follows

$$\varepsilon_{p, n(d_0)} = 0.$$

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

$$[v_p(n/f_x)/k] > 0.$$

or

$$v_p(n/f_x) - k \left[v_p(n/f_x) \frac{1}{k} \right] > 1, \quad (\text{i.e., } \varepsilon_{p, n} = 1).$$

Therefore $[v_p(n/f_x)/k] + \varepsilon_{p, n}$ is positive in both cases. Then we have

$$\begin{aligned} v_p(dd_0) &= v_p(d_0) = 1 \leq [v_p(n/f_x)/k] + \varepsilon_{p, n} \\ &= v_p(n(X)). \end{aligned}$$

Thus Lemma 5 is completely proved.

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

Lemma 6. *Let χ be a character modulo n and d be a positive divisor of $n(\chi)$. Let p_1, \dots, 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 χ 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 $p \nmid p_i$ ($i=1, \dots, j$)

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

$$[v_p(n/f_x)/k] = 0 \quad \text{and} \quad \varepsilon_{p, n} = 1.$$

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

$$\begin{aligned} v_p(n/f_x)/k &= v_p\left(\frac{1}{f_x} \frac{n}{(p^k, n)}\right) \frac{1}{k} + 1 \\ &= v_p\left(\frac{1}{f_x} \frac{n}{(d_0^k, n)}\right) \frac{1}{k} + 1. \end{aligned}$$

Therefore we have

$$\begin{aligned} v_p(d') &= v_p(d) - 1 \leq [v_p(n/f_x)/k] + \varepsilon_{p,n} - 1 \\ &= [v_p(n(d_0)/f_x)/k] + 1 + \varepsilon_{p,n} - 1. \end{aligned}$$

But we can show by the same method as in the case (II)-(i) of Lemma 5 that $\varepsilon_{p,n} = \varepsilon_{p,n(d_0)}$. Therefore it follows

$$v_p(d') \leq v_p(n(d_0)(\chi)).$$

(ii) The case $[v_p(n/f_x)/k] = 0$ 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

$$v_p(d') \leq v_p(n(d_0)(\chi)).$$

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*

$$\begin{aligned} c_a^{(k)}(n) &= \frac{n_0 - 1}{2} + \sum_{\substack{\chi; \text{ primitive} \\ \chi^k = 1 \\ f_x | n}} \chi^{-1}(a) H_x \left\{ \sum_{d | n(\chi)} \frac{(d^k, n)}{d} \chi^{-1} \left(\frac{d^k}{(d^k, n)} \right) \right. \\ &\quad \left. \cdot \left(\sum_{\substack{d_a | n(d)(\chi) \\ (d_a, f_x) = 1 \\ \alpha \in B(n)}} \mu(d_a) \chi(d_a) \right) \right\}. \end{aligned}$$

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

$$c_a^{(k)}(n) = \sum_{\substack{\chi; \text{ primitive} \\ \chi^k=1 \\ f_x|n}} \chi^{-1}(a)H_x.$$

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 $s(n(d_a))<s(n)$ with respect to $n(d_a)$ of Proposition 1. Therefore by the assumption we have

$$(2) \quad c_{\alpha_a^*(n)a}^{(k)}(n(d_a)) = \frac{n(d_a)_0-1}{2} + \sum_{\substack{\chi; \text{ primitive} \\ \chi^k=1 \\ f_x|n(d_a)}} \chi^{-1}(d_a^*(n)a)H_x \\ \cdot \left\{ \sum_{d|n(d_a)(\chi)} \frac{(d^k, n(d_a))}{d} \chi^{-1}\left(\frac{d^k}{(d^k, n(d_a))}\right) \right. \\ \left. \cdot \left(\sum_{\substack{d_\beta|(n(d_a))(d)(\chi) \\ (d_\beta, f_x)=1 \\ \beta \subset B(n(d_a))}} \mu(d_\beta)\chi(d_\beta) \right) \right\}.$$

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

$$c_a^{(k)}(n) = \sum_{f_x|n} \chi^{-1}(a)H_x - \sum_{\substack{\alpha \subset B(n) \\ \alpha \neq \phi}} \mu(d_\alpha) \left[\left(\frac{(d^k, n)-1}{2} \right) + \frac{(d^k, n)}{d} \right. \\ \cdot \left\{ \frac{n(d_a)_0-1}{2} + \sum_{f_x|n(d_a)} \chi^{-1}(d_a^*(n)a)H_x \sum_{d|n(d_a)(\chi)} \frac{(d^k, n(d_a))}{d} \chi^{-1}\left(\frac{d^k}{(d^k, n(d_a))}\right) \right. \\ \left. \cdot \sum_{\substack{\beta \subset B(n(d_a)) \\ d_\beta|(n(d_a))(d)(\chi) \\ (d_\beta, f_x)=1}} \mu(d_\beta)\chi(d_\beta) \right\} - \sum_{\substack{f_x|n \\ (f_x, d_a)=1}} \chi(d_a)\chi^{-1}(a)H_x \Big].$$

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

$$(I) \quad - \sum_{\substack{\alpha \subset B(n) \\ \alpha \neq \phi}} \mu(d_\alpha) \left\{ \frac{(d^k, n)-1}{2} + \frac{(d^k, n)(n(d_a)_0-1)}{2d_a} \right\} = \frac{n_0-1}{2}.$$

$$\begin{aligned}
(II) \quad & \sum_{f_x|n} \chi^{-1}(a) H_x - \sum_{\substack{\alpha \in B(n) \\ \alpha \neq \phi}} \mu(d_\alpha) \left[\left\{ \frac{(d_\alpha^k, n)}{d_\alpha} \sum_{f_x|n(d_\alpha)} \chi^{-1}(d_\alpha^*(n)a) H_x \right. \right. \\
& \quad \left. \sum_{d|n(d_\alpha)(\chi)} \frac{(d^k, n(d_\alpha))}{d} \chi^{-1} \left(\frac{d^k}{(d^k, n(d_\alpha))} \right) \sum_{\substack{\beta \in B(n(d_\alpha)) \\ d_\beta|n(d_\alpha)(d)(\chi) \\ (d_\beta, f_x)=1}} \mu(d_\beta) \chi(d_\beta) \right\} \\
& \quad \left. - \sum_{\substack{f_x|n \\ (f_x, d_\alpha)=1}} \chi(d_\alpha) \chi^{-1}(a) H_x \right] \\
& = \sum_{f_x|n} \chi^{-1}(a) H_x \sum_{d|n(\chi)} \frac{(d^k, n)}{d} \chi^{-1} \left(\frac{d^k}{(d^k, n)} \right) \sum_{\substack{\alpha \in B(n) \\ d_\alpha|n(d)(\chi) \\ (d_\alpha, f_x)=1}} \mu(d_\alpha) \chi(d_\alpha).
\end{aligned}$$

First we shall prove (I). By the definition of $n(d_\alpha)$ we get

$$n(d_\alpha)_0 = \left(\frac{n}{(d_\alpha^k, n)} \right)_0$$

and

$$n(d_\alpha)_0 \frac{(d_\alpha^k, n)}{d_\alpha} = \left(\frac{n}{(d_\alpha^k, n)} \right)_0 \frac{(d_\alpha^k, n)}{d_\alpha}.$$

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

$$n(d_\alpha)_0 \frac{(d_\alpha^k, n)}{d_\alpha} = n_0.$$

On the other hand we have

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

It follows (I).

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

$$\begin{aligned}
(3) \quad & \sum_{f_x|n} \chi^{-1}(a) H_x \left[\left\{ \sum_{\substack{\alpha \in B(n) \\ (d_\alpha, f_x)=1}} \mu(d_\alpha) \chi(d_\alpha) \right\} \right. \\
& \quad \left. - \left\{ \sum_{\substack{\alpha \in B(n) \\ \alpha \neq \phi \\ f_x|n(d_\alpha)}} \sum_{d|n(d_\alpha)(\chi)} \sum_{\substack{\beta \in B(n(d_\alpha)) \\ d_\beta|n(d_\alpha)(d)(\chi) \\ (d_\beta, f_x)=1}} \mu(d_\alpha) \cdot \frac{(d_\alpha^k, n)}{d_\alpha} \cdot \frac{(d^k, n(d_\alpha))}{d} \right. \right. \\
& \quad \left. \left. \cdot \chi^{-1} \left(\frac{d_\alpha^*(n) d^k}{(d^k, n(d_\alpha))} \right) \mu(d_\beta) \chi(d_\beta) \right\} \right].
\end{aligned}$$

Here we note that

$$\frac{(d_\alpha^k, n)}{d_\alpha} \cdot \frac{(d^k, n(d_\alpha))}{d} = \frac{(d_\alpha^k, n) \left(d^k, \frac{n}{(d_\alpha^k, n)} \right)}{dd_\alpha} = \frac{((dd_\alpha)^k, n)}{dd_\alpha}$$

and

$$\frac{d_\alpha^*(n)d^k}{(d^k, n(d_\alpha))} = \frac{d_\alpha^k}{(d_\alpha^k, n)} \cdot \frac{d^k}{\left(d^k, \frac{n}{(d_\alpha^k, n)} \right)} = \frac{(dd_\alpha)^k}{((dd_\alpha)^k, n)}.$$

And by Lemma 5 we note that

$$dd_\alpha | n(\chi).$$

By the definition of $n(d)$ we can easily see that

$$(n(d_\alpha))(d) = n(dd_\alpha).$$

Then we can rewrite the inside of the bracket of (3) as follows

$$(4) \quad \left\{ \sum_{\substack{\alpha \subset B(n) \\ (d_\alpha, f_\chi)=1}} \mu(d_\alpha) \chi(d_\alpha) \right\} - \left\{ \sum_{\substack{d | n(\chi) \\ d \neq 1}} \frac{(d^k, n)}{d} \chi^{-1} \left(\frac{d^k}{(d^k, n)} \right) \right. \\ \cdot \sum_{\substack{d=d'd_\alpha \\ d' | n(d_\alpha)(\chi) \\ \alpha \subset B(n) \\ \alpha \neq \phi \\ f_\chi | n(d_\alpha)}} \mu(d_\alpha) \sum_{\substack{\beta \subset B(n(d_\alpha)) \\ d_\beta | n(d)(\chi) \\ (d_\beta, f_\chi)=1}} \mu(d_\beta) \chi(d_\beta) \left. \right\}.$$

Here we can easily see that if $\beta \subset B(n)$ and $d_\beta | n(d)(\chi)$ then $\beta \subset B(n(d_\alpha))$. This shows that we may change $B(n(d_\alpha))$ of the last term of (4) for $B(n)$. Moreover by Lemma 6 we see that $d_\alpha | d$ implies that $f_\chi | n(d_\alpha)$ and $d' | n(d_\alpha)(\chi)$. Therefore we may exclude these conditions of (4). Then we have

$$(4) = \left\{ \sum_{\substack{\alpha \subset B(n) \\ (d_\alpha, f_\chi)=1}} \mu(d_\alpha) \chi(d_\alpha) \right\} - \left\{ \sum_{\substack{d | n(\chi) \\ d \neq 1}} \frac{(d^k, n)}{d} \chi^{-1} \left(\frac{d^k}{(d^k, n)} \right) \right. \\ \cdot \sum_{\substack{\beta \subset B(n) \\ d_\beta | n(d)(\chi) \\ (d_\beta, f_\chi)=1}} \mu(d_\beta) \chi(d_\beta) \sum_{\substack{d=d'd_\alpha \\ \alpha \subset B(n) \\ \alpha \neq \phi}} \mu(d_\alpha) \left. \right\} \\ = \left\{ \sum_{\substack{\alpha \subset B(n) \\ (d_\alpha, f_\chi)=1}} \mu(d_\alpha) \chi(d_\alpha) \right\} + \left\{ \sum_{\substack{d | n(\chi) \\ d \neq 1}} \frac{(d^k, n)}{d} \chi^{-1} \left(\frac{d^k}{(d^k, n)} \right) \sum_{\substack{\beta \subset B(n) \\ d_\beta | n(d)(\chi) \\ (d_\beta, f_\chi)=1}} \mu(d_\beta) \chi(d_\beta) \right\} \\ = \sum_{\substack{d | n(\chi) \\ (d_\alpha, f_\chi)=1 \\ d_\alpha | n(d)(\chi)}} \frac{(d^k, n)}{d} \chi^{-1} \left(\frac{d^k}{(d^k, n)} \right) \sum_{\substack{\alpha \subset B(n) \\ (d_\alpha, f_\chi)=1 \\ d_\alpha | n(d)(\chi)}} \mu(d_\alpha) \chi(d_\alpha).$$

which implies (II). Thus the proof of Theorem 1 is completed.

Let $\mathbf{Q}(\sqrt{D})=K$ be a quadratic extension field of \mathbf{Q} with discriminant D . We denote by $\left(\frac{D}{n}\right)$ or $\chi_D(n)$ the Kronecker's symbol of K . Then $\left(\frac{D}{\cdot}\right)$ 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 $K=\mathbf{Q}(\sqrt{D})$ and $2w_D$ 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*

$$H_{\chi_D} = \begin{cases} 0 & \text{if } D > 0, \\ \frac{h(D)}{w_D} & \text{if } D < 0. \end{cases}$$

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*

$$c_a^{(2)}(n) = \frac{n_0-1}{2} + \sum_{\substack{|D| \mid n \\ D < 0}} \left(\frac{D}{a}\right)^{-1} \frac{h(D)}{w_D} \sum_{d \mid n(\chi_D)} d \prod_{\substack{p \mid n(d)(\chi_D) \\ (p, D)=1}} \left\{1 - \left(\frac{D}{p}\right)\right\},$$

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

$$\frac{(d^2, n)}{d} = d \quad \text{and} \quad \frac{(d^2, n)}{d^2} = 1.$$

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 $n=\text{prime}$ is obtained by T. Honda in [2]

Corollary 2. *If $k=2$ then $c_1^{(2)}(n) \geq 0$. Moreover $c_1^{(2)}(n)=0$, 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, \dots, 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 $c_1^{(2)}(n)=0$ then n must be square-free, because if n is not square-free then $n_0>1$, which implies $c_1^{(2)}(n)>0$. Consequently we have by Corollary 1

$$c_1^{(2)}(n) = \sum_{|D||n} \frac{h(D)}{w_D}.$$

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

$$c_1^{(2)}(n) \geq \frac{h(-p)}{w_{-p}} > 0.$$

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*

$$c_a^{(k)}(n) = \frac{n_0 - 1}{2},$$

therefore $|c_a^{(k)}(n)| < n^{(k-1)/k}$.

Proof. Let χ be any character modulo n of degree k . Then we have

$$\chi(-1)^2 = \chi((-1)^2) = 1$$

and

$$\chi(-1)^k = 1.$$

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

REMARK 5. $c_1^{(k)}(n)$ is not always non-negative for even $k>2$. For example $c_1^{(4)}(29)=-2$. (See the table of at the end of the section 5.)

4. Proof of Conjecture 1

Let χ be a primitive character modulo f_χ . 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 χ , i.e.,

$$G(\chi) = \sum_{a=1}^{f_\chi} \chi(a)\zeta^a,$$

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

$$G(\chi)G(\bar{\chi}) = \chi(-1)f_x,$$

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

$$\begin{aligned} |H_x| &= \left| \frac{1}{f_x} \cdot \frac{L(1, \bar{\chi})f_x^2}{\pi i G(\bar{\chi})} \right| \\ &< \frac{f_x}{|G(\bar{\chi})|} \log f_x = \sqrt{f_x} \log f_x. \end{aligned}$$

It is obvious that $f_{\bar{x}}$ 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 ε and a given positive constant A we have

$$A^{\delta(n)} = O(n^\varepsilon),$$

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 δ_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

$$p_0^{\delta'(n)} \leq n.$$

Therefore we have

$$\delta'(n) \leq \frac{\log n}{\log p_0}.$$

From this we get

$$\begin{aligned} A^{\delta(n)} &\leq A^{\delta'(n)+\delta_0} = A^{\delta_0} A^{\delta'(n)} \\ &= A^{\delta_0} n^{\log_n A^{\delta'(n)}} = A^{\delta_0} n^{\delta'(n) \log A / \log n} \\ &\leq A^{\delta_0} n^{(\log n / \log p_0) \cdot (\log A / \log n)} \leq A^{\delta_0} n^{\varepsilon}. \end{aligned}$$

This completes the proof.

Lemma 12. *For any positive number ε 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 ε and a fixed positive integer k we have*

$$c_a^{(k)}(n) = O(n^{((k-1)/k)+\varepsilon}).$$

Proof. By Theorem 1 we have

$$|c_a^{(k)}(n)| \leq \frac{n_0-1}{2} + \sum_{f_x|n} |H_x| \sum_{d|n(\chi)} \frac{(d^k, n)}{d} \prod_{\substack{p|n(d)(\chi) \\ (p, f_x)=1}} |1-\chi(p)|.$$

We have already known that

$$n_0 \leq n^{(k-1)/k}.$$

Therefore we shall show that

$$\sum_{f_x|n} |H_x| \sum_{d|n(\chi)} \frac{(d^k, n)}{d} \prod_{\substack{p|n(d)(\chi) \\ (p, f_x)=1}} |1-\chi(p)| = O(n^{((k-1)/k)+\varepsilon}).$$

First we get by Lemma 11

$$\prod_{\substack{p|n(d)(\chi) \\ (p, f_x)=1}} |1-\chi(p)| \leq \prod_{p|n} 2 = 2^{\delta(n)} = O(n^{\varepsilon}).$$

Next we get

$$\sum_{\substack{\chi \\ f_x|n}} 1 < \prod_{p|n} \left(\sum_{\substack{\chi \\ f_x=p^{\alpha}}} 1 \right).$$

But by Lemma 3 we know that

$$\sum_{\substack{\chi \\ f_{\chi} = p^{\alpha}}} 1 < A, \quad \text{for some positive constant } A.$$

Hence by Lemma 11 we also get

$$\sum_{\substack{\chi \\ f_{\chi} | n}} 1 < A^{\delta(n)} = O(n^{\epsilon}).$$

Lastly we shall show that

$$\left(|H_{\chi}| \sum_{d|n(\chi)} \frac{(d^k, n)}{d} \right) / n^{(k-1)/k} = O(n^{\epsilon})$$

We transform this into

$$\left(|H_{\chi}| \sum_{d|n(\chi)} \frac{(d^k, n)}{d} \right) / n^{(k-1)/k} = \frac{|H_{\chi}|}{f_{\chi}^{(k-1)/k}} \cdot \sum_{d|n(\chi)} \left(\frac{(d^k, n)}{d} / \left(\frac{n}{f_{\chi}} \right)^{(k-1)/k} \right).$$

Then we have by Lemma 10

$$|H_{\chi}| / f_{\chi}^{(k-1)/k} \leq (f_{\chi}^{1/2} / f_{\chi}^{(k-1)/k}) \log f_{\chi} \leq \log f_{\chi}.$$

Moreover by Remark 2 we can easily see that

$$\frac{(d^k, n)}{d} / \left(\frac{n}{f_{\chi}} \right)^{(k-1)/k} < 1.$$

From these and by Lemma 12 we have

$$\begin{aligned} \left(|H_{\chi}| \sum_{d|n(\chi)} \frac{(d^k, n)}{d} \right) / n^{(k-1)/k} &\leq \sum_{d|n(\chi)} \log n \\ &< \log n \sum_{d|n} 1 \\ &= O(n^{\epsilon}). \end{aligned}$$

This completes the proof of our Theorem.

5. Number theoretic properties of some $c_a^{(k)}(n)$.

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 $x \equiv 0 \pmod{p}$ then the lemma is trivial. Hence we assume $x \not\equiv 0 \pmod{p}$. Consider the following sequence of groups and homomorphisms

$$\{1\} \longrightarrow (\mathbb{Z}/p\mathbb{Z})^{\times(p-1)/k_0} \xrightarrow{g_1} (\mathbb{Z}/p\mathbb{Z})^\times \xrightarrow{g_2} (\mathbb{Z}/p\mathbb{Z})^{\times k_0} \xrightarrow{g_3} (\mathbb{Z}/p\mathbb{Z})^{\times k_0} \longrightarrow \{1\},$$

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

$$\begin{aligned} g_1(a) &= a \quad \forall a \in (\mathbb{Z}/p\mathbb{Z})^{\times(p-1)/k_0}, \\ g_2(a) &= a^{k_0} \quad \forall a \in (\mathbb{Z}/p\mathbb{Z})^{\times k_0}, \\ g_3(a) &= a^{k/k_0} \quad \forall a \in (\mathbb{Z}/p\mathbb{Z})^{\times k_0}. \end{aligned}$$

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 $N^{(k_0)}(x, p)$ and $N^{(k)}(x, p)$ we see that $N^{(k_0)}(x, p)$ is not zero if and only if $x \in \text{Im}(g_2) = (\mathbb{Z}/p\mathbb{Z})^{\times k_0}$ 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 $N^{(k_0)}(x, p)$ 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 $N^{(k_0)}(x, p) = \# \text{Ker}(g_2) = \# \text{Ker}(g_3 \circ g_2) = N^{(k)}(x, p)$. Thus Lemma 13 is proved.

Proposition 2. *Let p_1, \dots, p_j be distinct primes each of which is prime to k 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, \dots, k_j , then*

$$c_a^{(k)}(p_1 \cdots p_j) = c_a^{(k_0)}(p_1 \cdots p_j).$$

Proof. By Lemma 13 it is obvious that

$$N^{(k)}(x, p) = N^{(k_i)}(x, p) = N^{(k_0)}(x, p).$$

Then by Lemma 1 we have

$$N^{(k)}(x, p_1 \cdots p_j) = N^{(k_0)}(x, p_1 \cdots p_j).$$

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

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

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*

$$p-1 \equiv 0 \pmod{2k}$$

and χ 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 $x_0 \in (\mathbb{Z}/p\mathbb{Z})^\times$ such that

$$x_0^{mk} \equiv -1 \pmod{p},$$

which implies $\chi(-1) = \chi(x_0^m)^k = 1$.

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

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

Proof. We put $n = p_1 \cdots p_j$. Let χ be any character of conductor $f_\chi | n$, then by the decomposition (1) in §2 of χ 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 $c_a^{(2)}(n)$ in corollary 2. But when k is an even integer > 2 , $c_a^{(k)}(n)$ is more complicated. From now on till the end of the this section we shall only consider the case $k=4$ and $n=p$, where p is a prime. If $p=2$, then $c_a^{(4)}(2)=0$ and there is nothing to say. If $p \equiv 3 \pmod{4}$, then $c_a^{(4)}(p) = c_a^{(2)}(p)$ by Proposition 2. Further if $p \equiv 1 \pmod{8}$, then $c_a^{(4)}(p) = 0$ 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 $(\mathbf{Z}/p\mathbf{Z})^\times$ of the residue ring $\mathbf{Z}/p\mathbf{Z}$ is a cyclic group of order $p-1$ which is divisible by 4. We denote by H (respectively H_0) the unique subgroup of $(\mathbf{Z}/p\mathbf{Z})^\times$ of index 4 (respectively 2). Let K be the p -th cyclotomic field i.e., $K = \mathbf{Q}(\zeta)$, 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

$$\begin{array}{ccc} K = \mathbf{Q}(\zeta) & \text{---} & \{1\} \\ | & & | \\ L & \text{---} & H(\nexists -1) \\ | & & | \\ L_0 & \text{---} & H_0(\ni -1) \\ | & & | \\ \mathbf{Q} & \text{---} & (\mathbf{Z}/p\mathbf{Z})^\times. \end{array}$$

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

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

h = the class number of L

h_0 = 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 $(\mathbb{Z}/p\mathbb{Z})^\times/H$ is generated by the class represented by 2. We shall denote by $\chi^{(j)}$ ($j=0, 1, 2, 3$) the character of $(\mathbb{Z}/p\mathbb{Z})^\times/H$ 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*

$$h^* = Qw \prod_{j=1,3} \frac{1}{2p} \left(\sum_{x=1}^{p-1} -\chi^{(j)}(x)x \right),$$

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*

$$h^* = \frac{w}{4} \left\{ \left(\frac{c_1^{(4)}(p)}{2} \right)^2 + \left(\frac{c_2^{(4)}(p)}{2} \right)^2 \right\}.$$

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

$$(7) \quad a = -\frac{c_1^{(4)}(p)}{2},$$

$$(8) \quad b = -\frac{c_2^{(4)}(p)}{2}.$$

By the definition of a we get

$$\begin{aligned}
 a &= \frac{1}{p} \left\{ \sum_{\substack{x=1 \\ x \equiv y^4 \pmod{p}}}^{p-1} x - \sum_{\substack{x=1 \\ x \equiv y_1^2 \pmod{p} \\ x \not\equiv y_2^4 \pmod{p}}}^{p-1} x \right\} \\
 &= \frac{1}{p} \left\{ 2 \sum_{\substack{x=1 \\ x \equiv y^4 \pmod{p}}}^{p-1} x - \sum_{\substack{x=1 \\ x \equiv y^2 \pmod{p}}}^{p-1} x \right\}.
 \end{aligned}$$

As $p \equiv 1 \pmod{4}$, if $x \equiv y^2 \pmod{p}$ then $-x \equiv y'^2 \pmod{p}$ for some $y' \in \mathbb{Z}/p\mathbb{Z}$. From this we get

$$(9) \quad \sum_{\substack{x=1 \\ x \equiv y^2 \pmod{p}}}^{p-1} x = \frac{p(p-1)}{4}.$$

On the other hand we have by the definition of $c_1^{(4)}(p)$

$$(10) \quad c_1^{(4)}(p) = \frac{p-1}{2} - \frac{4}{p} \sum_{\substack{x=1 \\ x \equiv y^4 \pmod{p}}}^{p-1} x.$$

By (9) and (10) we have

$$\begin{aligned}
 a &= \left(\frac{p-1}{4} - \frac{c_1^{(4)}(p)}{2} \right) - \frac{p-1}{4} \\
 &= -\frac{c_1^{(4)}(p)}{2}.
 \end{aligned}$$

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

$$\begin{aligned}
 b &= \left\{ \frac{1}{p} \sum_{\substack{x=1 \\ x \equiv 2y^4 \pmod{p}}}^{p-1} x - \sum_{\substack{x=1 \\ x \equiv 2y_1^2 \pmod{p} \\ x \not\equiv 2y_2^4 \pmod{p}}}^{p-1} x \right\} \\
 &= \frac{1}{p} \left\{ 2 \sum_{\substack{x=1 \\ x \equiv 2y^4 \pmod{p}}}^{p-1} x - \sum_{\substack{x=1 \\ y \equiv y^2 \pmod{p}}}^{p-1} x \right\} \\
 &= \frac{1}{p} \left\{ 2 \sum_{\substack{x=1 \\ x \equiv 2y^4 \pmod{p}}}^{p-1} x - \frac{p(p-1)}{4} \right\}.
 \end{aligned}$$

On the other hand by the definition of $c_2^{(4)}(p)$ we have also

$$c_2^{(4)}(p) = \frac{p-1}{2} - \frac{4}{p} \sum_{\substack{x=1 \\ x \equiv 2y^4 \pmod{p}}}^{p-1} x.$$

Therefore we obtain

$$b = \left(\frac{p-1}{4} - \frac{c_2^{(4)}(p)}{2} \right) - \frac{p-1}{4} \\ = -\frac{c_2^{(2)}(p)}{2}.$$

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 $c_a^{(k)}(p)$'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 h^* , $c_1^{(4)}(p)$ and $c_2^{(4)}(p)$.

Table ($p \equiv 5(8)$, $p < 500$)

p	$c_1^{(4)}(p)$	$c_2^{(4)}(p)$	h^*
5	6/5	2/5	1
13	2	2	1
29	-2	2	1
37	2	-2	1
53	-2	-2	1
61	2	-2	1
101	-6	2	5
109	10	6	17
149	6	6	9
157	2	6	5
173	-6	-2	5
181	14	2	25
197	-2	-6	5
229	6	10	17
269	10	-2	13
277	-6	10	17
293	6	-6	9
317	2	10	13
349	-6	-2	5
389	18	2	41
397	2	-10	13
421	2	14	25
461	-2	-14	25

6. An afterthought

We shall give an 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

$$\begin{aligned} c_a^{(k)}(n) &= \frac{n-1}{2} - \frac{1}{n} \sum_{x=1}^{n-1} N^{(k)}(a^{-1}x, n)x \\ &= \frac{n-1}{2} - \frac{1}{2n} \sum_{x=1}^{n-1} \{N^{(k)}(a^{-1}x, n)x + N^{(k)}(a^{-1}(n-x), n)(n-x)\} \\ &= \frac{n-1}{2} - \frac{1}{2n} \sum_{x=1}^{n-1} nN^{(k)}(a^{-1}x, n), \end{aligned}$$

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

$$\sum_{x=0}^{n-1} N^{(k)}(a^{-1}x, n) = n.$$

From this it follows that

$$\begin{aligned} c_a^{(k)}(n) &= \frac{n-1}{2} - \frac{1}{2}(n - N^{(k)}(0, n)) \\ &= \frac{N^{(k)}(0, n) - 1}{2}. \end{aligned}$$

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 $\left[\frac{ax^k}{n}\right] = \frac{ax^k}{n}$, but we suppose that $\left[\frac{ax^k}{n}\right]$ 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 $d_a^{(k)}(n) = c_a^{(k)}(n) - \frac{n_0^{(k)} - 1}{2}$ is the essential error term. The proof of Theorem 2 shows that the order of $d_a^{(k)}(n)$ is less than $n^{((k-1)/k)+\varepsilon}$ for any $\varepsilon > 0$. The Corollary 2 is true with slight modification of $d_a^{(k)}(n)$.

OSAKA UNIVERSITY

References

- [1] H. Hasse: Über die Klassenzahl Abelscher Zahlkörper, Akademie-Verlag, Berlin, 1952.
- [2] T. Honda: *A few remarks on class numbers of imaginary quadratic number fields*, Osaka J. Math. 12 (1975), 19–21.
- [3] K. Prachar: Primzahlverteilung, Springer-Verlag, Berlin-Göttingen-Heidelberg, 1957.

