Miyawaki, I.
Osaka J. Math.
12 (1975), 647–671

ON THE NUMBER OF THE LATTICE POINTS IN THE AREA $0<x<n$, $0<y\leqslant ax^k/n$.

ISAO MIYAWAKI

(Received October 18, 1974)

1. Introduction

Let $S_a^{(k)}(n)$ be the number of the lattice points in the area $0<x<n$, $0<y\leqslant ax^k/n$, 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

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

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

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

or

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

We put

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

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

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

$$n = p_1 \cdot \cdots \cdot p_j ,$$

where $p_1, \cdots, p_j$ 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 $\boldsymbol{Q}(\zeta)$ 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

$$\{y \in \boldsymbol{Z} \mid y^k \equiv x \bmod n, \quad 0 \leqslant y < n\} .$$

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

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

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 $(\boldsymbol{Z}/n\boldsymbol{Z})^\times$ the unit group of the residue ring $\boldsymbol{Z}/n\boldsymbol{Z}$. We put

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

where $U=\{z \in \boldsymbol{C} \mid |z|=1\}$. Then $\Gamma(n)$ is an abelian group isomorphic to $(\boldsymbol{Z}/n\boldsymbol{Z})^\times$. An element χ of $\Gamma(n)$ is extended on $\boldsymbol{Z}$ 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 $(\boldsymbol{Z}/n'\boldsymbol{Z})^\times$ 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 $(\boldsymbol{Z}/n\boldsymbol{Z})^\times=\prod_{i=1}^{j}(\boldsymbol{Z}/p_i^{e_i}\boldsymbol{Z})^\times$. Therefore if χ is a character modulo n, then χ has the following unique decomposition

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

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

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

We put

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

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

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

if $(b, p)=1$,

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

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

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

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

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

where we define e_0 by

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

(iii) $\sharp\Gamma^{(k)}(2^e)=\begin{cases} 2^{e-1} & \text{if } e\leqslant e_0+2\\ 2^{e_0+1} & \text{if } e\geqslant e_0+3,\end{cases}$

where we define e_0 by

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

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

$$\sharp\Gamma^{(k)}(p^e)\leqslant c_0$$

for any p and e.

Proof. If we note the following facts

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

then we have immediately the lemma 4.

3. Main theorem and its proof

Let $n\geqslant 2$ 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

$$A(n)=\{1, 2, \cdots, j\}$$
$$B(n)=\{i \in A(n) \mid e_i \geqslant 2\} .$$

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

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

For a fixed positive integer k, we put

$$e_i=k s_i+r_i,\ s_i \geqslant 0,\ 1 \leqslant r_i \leqslant k ,$$

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.

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

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

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

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

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

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

Therefore we get

$$c_a^{(k)}(n)=\frac{n-1}{2}-\Bigg[\frac{1}{n}\sum_{x=1}^{n-1}\prod_{i=1}^{j}\Big(1+\sum_{\substack{\chi:\text{ primitive}\\ f_\chi|p_i^{e_i},\ \chi^k=1}}\chi(a^{-1}x)\Big)x$$

$$+\sum_{\substack{\alpha\subset B(n)\\ \alpha\neq\phi}}\mu(d_\alpha)\Bigg\{\frac{1}{n}\sum_{x=1}^{(n/d_\alpha)-1}\prod_{i\notin\alpha}\Big(1+\sum_{\substack{\chi:\text{ primitive}\\ f_\chi|p_i^{e_i},\ \chi^k=1}}\chi(a^{-1}d_\alpha x)\Big)d_\alpha x$$

$$-\sum_{x=1}^{(n/d_\alpha)-1}\overline{\left\{\frac{a(d_\alpha x)^k}{n}\right\}}\Bigg\}\Bigg]$$

$$=\frac{n-1}{2}-\frac{n(n-1)}{2n}-\frac{1}{n}\sum_{\substack{\chi:\text{ primitive}\\ f_\chi|n,\ \chi^k=1}}\sum_{x=1}^{n-1}\chi(a^{-1}x)x-\sum_{\substack{\alpha\subset B(n)\\ \alpha\neq\phi}}\mu(d_\alpha)$$

$$\cdot\Bigg[\frac{d_\alpha}{n}\cdot\frac{(n/d_\alpha)((n/d_\alpha)-1)}{2}-\frac{d_\alpha}{n}\sum_{\substack{\chi:\text{ primitive}\\ f_\chi|n,\ \chi^k=1\\ (f_\chi,d_\alpha)=1}}\sum_{x=1}^{(n/d_\alpha)-1}\chi(a^{-1}d_\alpha x)x$$

$$-\sum_{x=1}^{(n/d_\alpha)-1}\overline{\left\{\frac{ad_\alpha^*(n)x^k}{n(d_\alpha)}\right\}}\Bigg],$$

where we should note that

$$\frac{1}{n}\sum_{x=1}^{n-1}\chi(x)x=\frac{1}{n}\sum_{x=1}^{f_\chi-1}\sum_{i=0}^{(n/f_\chi)-1}\chi(x)(x+if_\chi)=\frac{1}{n}\frac{n}{f_\chi}\sum_{x=1}^{f_\chi-1}\chi(x)x=-H_\chi\,.$$

Then we have

$$c_a^{(k)}(n)=\sum_{\substack{\chi:\text{ primitive}\\ f_\chi|n,\ \chi^k=1}}\overline{\chi(a)}H_\chi-\Bigg[\sum_{\substack{\alpha\subset B(n)\\ \alpha\neq\phi}}\mu(d_\alpha)\Bigg\{\frac{(n/d_\alpha)-1}{2}-\sum_{\substack{\chi:\text{ primitive}\\ f_\chi|n,\ \chi^k=1\\ (f_\chi,d_\alpha)=1}}\overline{\chi(a)}\chi(d_\alpha)H_\chi$$

$$-\frac{n}{d_\alpha n(d_\alpha)}\sum_{x=1}^{n(d_\alpha)-1}\overline{\left\{\frac{ad_\alpha^*(n)x^k}{n(d)_\alpha}\right\}}\Bigg\}\Bigg].$$

On the other hand we see that

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

Therefore we have

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

$$-\sum_{\substack{\chi:\text{ primitive}\\ f_\chi|n,\ \chi^k=1\\ (f_\chi,d_\alpha)=1}}\overline{\chi(a)}\chi(d_\alpha)H_\chi+\frac{n}{d_\alpha n(d_\alpha)}c_{ad_\alpha^*(n)}^{(k)}(n(d_\alpha))\Bigg]$$

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

$$+\frac{n}{d_\alpha(n(d_\alpha))} c^{(k)}_{ad^*_\alpha(n)}(n(d_\alpha)) - \sum_{\substack{\chi:\text{ primitive}\\ f_\chi|n,\ \chi^k=1\\ (f_\chi, d_\alpha)=1}} \overline{\chi(a)}\chi(d_\alpha)H_\chi\Bigg].$$

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

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

Therefore we get

$$c_a^{(k)}(n) = \sum_{\substack{\chi:\text{ primitive}\\ f_\chi|n,\ \chi^k=1}} \overline{\chi(a)}H_\chi - \sum_{\substack{\alpha\subset B(n)\\ \alpha\neq\phi}} \mu(d)\Bigg[\frac{((d_\alpha^k, n)/d_\alpha)-1}{2}$$

$$+\frac{(d_\alpha^k, n)}{d_\alpha} c^{(k)}_{ad^*_\alpha(n)}(n(d_\alpha)) - \sum_{\substack{\chi:\text{ primitive}\\ f_\chi|n,\ \chi^k=1\\ (f_\chi, d_\alpha)=1}} \overline{\chi(a)}\chi(d_\alpha)H_\chi\Bigg].$$

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,

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

$$\varepsilon_{p,n} = \varepsilon^{(k)}_{p,n} = \begin{cases} 0 & \text{if } p|f_\chi \text{ or } v_p\left(\dfrac{n}{f_\chi}\right)-k\left[v_p\left(\dfrac{n}{f_\chi}\right)\dfrac{1}{k}\right]\leqslant 1, \\ 1 & \text{otherwise,}\end{cases}$$

where we denote by $v_p(\cdot)$ the normalized p-adic exponential valuation of the field of the rational numbers $\boldsymbol{Q}$. 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_χ.

REMARK 2. If $n(\chi)$ is divisible by d, then $n/(d^k, n)\equiv 0 \bmod f_\chi$.

Lemma 5. *Let n be a positive integer. For distinct primes $p_1, \cdots, p_j$ such that $p_i^2|n$ $(i=1, \cdots, j)$, we put $d_0=p_1\cdot\cdots\cdot p_j$ 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 $(\boldsymbol{Z}/n\boldsymbol{Z})^\times \to (\boldsymbol{Z}/n(d_0)\boldsymbol{Z})^\times$. 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 $v_p(dd_0)\leqslant v_p(n(\chi))$ for every prime p. We consider the two cases.

The case I. $p \neq p_i$ $(i=1, \cdots, j)$.
By the definition of $n(d_0)$ we have

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

and

$$v_p(n/f_\chi) = v_p(n(d_0)/f_\chi).$$

It follows from this

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

From this and by the definition of d we have

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

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

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

Therefore we shall consider the two cases.
(i) The case $v_p(n(d_0)/f_\chi) = v_p(n/f_\chi) - k$.
In this case we have

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

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

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

This also completes the proof of Lemma 5 in our case.
(ii) The case $v_p(n(d_0)/f_\chi) = 0$
In this case we should note that $v_p(f_\chi) = 0$. Then we have

$$v_p(n(d_0)/f_\chi) - k[v_p(n(d_0)/f_\chi)/k] = 0.$$

It follows

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

This shows $v_p(d)=0$. On the other hand we have

$$v_p(n) \geqslant 2+v_p(n(d_0)) .$$

This shows that

$$[v_p(n/f_\chi)/k] > 0 .$$

or

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

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

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

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 $p_1, \cdots, p_j$ be distinct primes each of which is a divisor of d. If we put $d_0=p_1\cdot\cdots\cdot p_j$ and $d=d_0d'$ 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 $p \neq p_i$ $(i=1, \cdots, j)$

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

$$v_p(d') = v_p(d) \leqslant v_p(n)(\chi)) = v_p(n(d_0)(\chi))$$

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

In this case we have

$$v_p(d) \leqslant v_p(n(\chi)) .$$

This shows that

$$[v_p(n/f_\chi)/k] > 0$$

or

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

Therefore we shall consider the two cases.

(i) The case $[v_p(n/f_\chi)/k] > 0$.

In this case we can easily see that

$$v_p(n/f_\chi)/k = v_p\Big(\frac{1}{f_\chi}\frac{n}{(p^k, n)}\Big)\frac{1}{k}+1$$
$$= v_p\Big(\frac{1}{f_\chi}\frac{n}{(d_0^k, n)}\Big)\frac{1}{k}+1 .$$

Therefore we have

$$v_p(d') = v_p(d)-1 \leqslant [v_p(n/f_\chi)/k])+\varepsilon_{p,n}-1$$
$$=[v_p(n(d_0)/f_\chi)/k]+1+\varepsilon_{p,n}-1 .$$

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

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

(ii) The case $[v_p(n/f_\chi)/k]=0$ and $\varepsilon_{p,n}=1$.
In this case we have

$$v_p(d') = v_p(d)-1 \leqslant \varepsilon_{p,n}-1 = 0 .$$

This shows that

$$v_p(d') = 0 .$$

Therefore we have

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

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*

$$c_\alpha^{(k)}(n) = \frac{n_0-1}{2} + \sum_{\substack{\chi\,;\,\text{primitive}\\ \chi^k=1\\ f_\chi \mid n}} \chi^{-1}(a) H_\chi\Big\{\sum_{d\mid n(\chi)} \frac{(d^k, n)}{d}\chi^{-1}\Big(\frac{d^k}{(d^k, n)}\Big)$$
$$\cdot\Big(\sum_{\substack{d_\alpha \mid n(d)(\chi)\\ (d_\alpha, f_\chi)=1\\ \alpha\subset B(n)}} \mu(d_\alpha)\chi(d_\alpha)\Big)\Big\} .$$

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 respectt 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

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

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

$$(2)\qquad c^{(k)}_{d_\alpha^*(n)a}(n(d_\alpha)) = \frac{n(d_\alpha)_0-1}{2} + \sum_{\substack{\chi\,;\,\text{primitive}\\ \chi^k=1\\ f_\chi | n(d_\alpha)}} \chi^{-1}(d_\alpha^*(n)a)H_\chi$$
$$\cdot\left\{\sum_{d|n(d_\alpha)(\chi)} \frac{(d^k, n(d_\alpha))}{d}\chi^{-1}\left(\frac{d^k}{(d^k, n(d_\alpha))}\right)\right.$$
$$\left.\cdot\Big(\sum_{\substack{d_\beta|(n(d_\alpha))(d)(\chi)\\ (d_\beta, f_\chi)=1\\ \beta\subset B(n(d_\alpha))}} \mu(d_\beta)\chi(d_\beta)\Big)\right\}.$$

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

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

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

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

(II)
$$\sum_{f_\chi|n}\chi^{-1}(a)H_\chi-\sum_{\substack{\alpha\subset B(n)\\ \alpha\neq\phi}}\mu(d_\alpha)\Bigg[\Bigg\{\frac{(d_\alpha^k, n)}{d_\alpha}\sum_{f_\chi|n(d_\alpha)}\chi^{-1}(d_\alpha^*(n)a)H_\chi$$
$$\sum_{d|n(d_\alpha)(\chi)}\frac{(d^k, n(d_\alpha))}{d}\chi^{-1}\Big(\frac{d^k}{(d^k, n(d_\alpha))}\Big)\sum_{\substack{\beta\subset B(n(d_\alpha))\\ d_\beta|n(d_\alpha)(d)(\chi)\\ (d_\beta, f_\chi)=1}}\mu(d_\beta)\chi(d_\beta)\Bigg\}$$
$$-\sum_{\substack{f_\chi|n\\ (f_\chi, d_\alpha)=1}}\chi(d_\alpha)\chi^{-1}(a)H_\chi\Bigg]$$
$$=\sum_{f_\chi|n}\chi^{-1}(a)H_\chi\sum_{d|n(\chi)}\frac{(d^k, n)}{d}\chi^{-1}\Big(\frac{d^k}{(d^k, n)}\Big)\sum_{\substack{\alpha\subset B(n)\\ d_\alpha|n(d)(\chi)\\ (d_\alpha, f_\chi)=1}}\mu(d_\alpha)\chi(d_\alpha)\,.$$

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

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

and

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

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

$$-\sum_{\substack{\alpha\subset B(n)\\ \alpha\neq\phi}}\mu(d_\alpha)=-\sum_{\substack{d|d_{B(n)}\\ d\neq1}}\mu(d)=-((\sum_{d|d_{B(n)}}\mu(d))-1)=1\,.$$

It follows (I).

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

(3)
$$\sum_{f_\chi|n}\chi^{-1}(a)H_\chi\Bigg[\Bigg\{\sum_{\substack{\alpha\subset B(n)\\ (d_\alpha, f_\chi)=1}}\mu(d_\alpha)\chi(d_\alpha)\Bigg\}$$
$$-\Bigg\{\sum_{\substack{\alpha\subset B(n)\\ \alpha\neq\phi\\ f_\chi|n(d_\alpha)}}\sum_{d|n(d_\alpha)(\chi)}\sum_{\substack{\beta\subset B(n(d_\alpha))\\ d_\beta|n(d_\alpha)(d)(\chi)\\ (d_\beta, f_\chi)=1}}\mu(d_\alpha)\cdot\frac{(d_\alpha^k, n)}{d_\alpha}\cdot\frac{(d^k, n(d_\alpha))}{d}$$
$$\cdot\chi^{-1}\Big(\frac{d_\alpha^*(n)d^k}{(d^k, n(d_\alpha))}\Big)\mu(d_\beta)\chi(d_\beta)\Bigg\}\Bigg]\,.$$

Here we note that

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

and

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

And by Lemma 5 we note that

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

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

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

Here we can easily see that if $\beta\subset B(n)$ and $d_\beta\mid n(d)(\chi)$ 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 $d_\alpha\mid d$ implies that $f_\chi\mid n(d_\alpha)$ and $d'\mid n(d_\alpha)(\chi)$. Therefore we may exclude these conditions of (4). Then we have

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

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

Let $\boldsymbol{Q}(\sqrt{D})=K$ be a quadratic extension field of $\boldsymbol{Q}$ 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 $K=\boldsymbol{Q}(\sqrt{D})$ 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*

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

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*

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

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 $n=$prime is obtained by T. Honda in [2]

Corollary 2. *If $k=2$ then $c_1^{(2)}(n)\geqslant 0$. Moreover $c_1^{(2)}(n)=0$, if and only if n is of the following type*

$$n=p_1\cdot\cdots\cdot p_j \quad \text{or} \quad 2p_1\cdot\cdots\cdot p_j\,,$$

where $p_1,\cdots,p_j$ 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 $c_1^{(2)}(n)>0$. Consequentely 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 $p\equiv 3 \bmod 4$, then $-p$ is the discriminant of $\boldsymbol{Q}(\sqrt{-p})$. This shows

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

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 $\zeta=\exp(2\pi i/f_\chi)$. Then the following two lemmas are well-known. (See Hasse [1] and Prachar [3]).

Lemma 8.

$$|L(1, \chi)|<3 \log f_\chi .$$

Lemma 9.

$$L(1, \chi)=\frac{\pi i G(\chi)}{f_\chi^2} \sum_{a=1}^{f_\chi} \bar{\chi}(a) a .$$

Moreover

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

in particular

$$|G(\chi)|=\sqrt{f_\chi} .$$

Lemma 10.

$$|H_\chi|<\sqrt{f_\chi} \log f_\chi .$$

Proof. By Lemma 8 and Lemma 9 we have

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

It is obvious that $f_{\bar{\chi}}$ is equal to f_χ. 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

$$\delta(n) \leqslant \delta'(n)+\delta_0 .$$

By the definition of $\delta'(n)$ we have

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

Therefore we have

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

From this we get

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

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

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

We have already known that

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

Therefore we shall show that

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

First we get by Lemma 11

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

Next we get

$$\sum_{\substack{\chi \\ f_\chi|n}} 1 < \prod_{p|n} \Big(\sum_{\substack{\chi \\ f_\chi = p^\alpha}} 1 \Big) .$$

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

$$\sum_{\substack{\chi \\ f_\chi \mid n}} 1 < A^{\delta(n)} = O(n^\varepsilon)\,.$$

Lastly we shall show that

$$\Big(|H_\chi| \sum_{d \mid n(\chi)} \frac{(d^k, n)}{d}\Big) \Big/ n^{(k-1)/k} = O(n^\varepsilon)$$

We transform this into

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

Then we have by Lemma 10

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

Moreover by Remark 2 we can easily see that

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

From these and by Lemma 12 we have

$$\begin{aligned} \Big(|H_\chi| \sum_{d \mid n(\chi)} \frac{(d^k, n)}{d}\Big) \Big/ n^{(k-1)/k} &\leqslant \sum_{d \mid n(\chi)} \log n \\ &< \log n \sum_{d \mid n} 1 \\ &= O(n^\varepsilon)\,. \end{aligned}$$

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

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

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

$$g_1(a) = a \ {}^{\forall} a \in (\boldsymbol{Z}/p\boldsymbol{Z})^{\times(p-1)/k_0},$$
$$g_2(a) = a^{k_0} \ {}^{\forall} a \in (\boldsymbol{Z}/p\boldsymbol{Z})^{\times k_0},$$
$$g_3(a) = a^{k/k_0} \ {}^{\forall} a \in (\boldsymbol{Z}/p\boldsymbol{Z})^{\times k_0}.$$

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 $x \in \mathrm{Im}(g_2) = (\boldsymbol{Z}/p\boldsymbol{Z})^{\times k_0}$ and $N^{(k)}(x, p)$ is not zero if and only if $x \in \mathrm{Im}(g_3 \circ g_2) = (\boldsymbol{Z}/p\boldsymbol{Z})^{\times k_0}$. Therefore $N^{(k_0)}(x, p)$ is not zero if and only if so is $N^{(k)}(x, p)$. If $x \in (\boldsymbol{Z}/p\boldsymbol{Z})^{\times k_0}$ then $N^{(k_0)}(x, p) = \#\mathrm{Ker}(g_2) = \#\mathrm{Ker}(g_3 \circ g_2) = N^{(k)}(x, p)$. Thus Lemma 13 is proved.

Proposition 2. *Let $p_1, \cdots, p_j$ 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 $k_1, \cdots, k_j$, then*

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

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

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

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 $(\boldsymbol{Z}/n\boldsymbol{Z})^{\times}$. Therefore we can immediately obtain the lemma.

Lemma 14. *Let p be a prime such that*

$$p - 1 \equiv 0 \bmod 2k$$

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 $(\boldsymbol{Z}/p\boldsymbol{Z})^{\times}$ is mk. Therefore there exists some $x_0 \in (\boldsymbol{Z}/p\boldsymbol{Z})$ such that

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

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

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

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

Proof. We put $n=p_1 \cdot \cdots \cdot p_j$. 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 $p\equiv 3 \mod 4$, then $c_a^{(4)}(p)=c_a^{(2)}(p)$ by Proposition 2. Further if $p\equiv 1 \mod 8$, then $c_a^{(4)}(p)=0$ by Proposition 3. Therefore we may confine ourselves to the cases $p\equiv 5 \mod 8$.

Let p be a prime which is congruent to 5 modulo 8. Then the unit group $(\boldsymbol{Z}/p\boldsymbol{Z})^\times$ of the residue ring $\boldsymbol{Z}/p\boldsymbol{Z}$ is a cyclic group of order $p-1$ which is divisible by 4. We denote by H (respectively H_0) the unique subgroup of $(\boldsymbol{Z}/p\boldsymbol{Z})^\times$ of index 4 (respectively 2). Let K be the p-th cyclotomic field i.e., $K=\boldsymbol{Q}(\zeta)$, 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

$$\begin{array}{ccc}
K=\boldsymbol{Q}(\zeta) & \text{———} & \{1\} \\
| & & | \\
L & \text{———} & H(\not\ni -1) \\
| & & | \\
L_0 & \text{———} & H_0(\ni -1) \\
| & & | \\
\boldsymbol{Q} & \text{———} & (\boldsymbol{Z}/p\boldsymbol{Z})^\times.
\end{array}$$

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

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

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

$$h_0 = \text{the class number of } L_0$$

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

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

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

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

$$\frac{1}{p}\sum_{x=1}^{p-1} \chi^{(1)}(x)x = a+bi \qquad a, b \in \boldsymbol{Q}.$$

Then we have

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

We shall prove that

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

$$b = -\frac{c_1^{(4)}(p)}{2}. \tag{8}$$

By the definition of a we get

$$a=\frac{1}{p}\{\sum_{\substack{x=1\\x\equiv y^4 \bmod p}}^{p-1} x-\sum_{\substack{x=1\\x\equiv y_1{}^2 \bmod p\\x\not\equiv y_2{}^4 \bmod p}}^{p-1} x\}$$

$$=\frac{1}{p}\{2\sum_{\substack{x=1\\x\equiv y^4 \bmod p}}^{p-1} x-\sum_{\substack{x=1\\x\equiv y^2 \bmod p}}^{p-1} x\}.$$

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

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

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

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

By (9) and (10) we have

$$a=\left(\frac{p-1}{4}-\frac{c_1^{(4)}(p)}{2}\right)-\frac{p-1}{4}$$

$$=-\frac{c_1^{(4)}(p)}{2}.$$

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

$$b=\left\{\frac{1}{p}\sum_{\substack{x=1\\x\equiv 2y^4 \bmod p}}^{p-1} x-\sum_{\substack{x=1\\x\equiv 2y_1{}^2\\x\not\equiv 2y_2{}^4 \bmod p}}^{p-1} x\right\}$$

$$=\frac{1}{p}\{2\sum_{\substack{x=1\\x\equiv 2y^4 \bmod p}}^{p-1} x-\sum_{\substack{x=1\\y\equiv 2y^2 \bmod p}}^{p-1} x\}$$

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

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

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

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

$$w=10 \qquad \text{if } p=5\,,$$
$$w=2 \qquad \text{otherwise}\,.$$

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*

$$x^k \equiv -1 \mod n, \tag{10}$$

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 defintion 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 $\boldsymbol{Z}/n\boldsymbol{Z}$. 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 $ax^k \equiv 0 \mod n$ 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.