J. Math. Soc. Japan
Vol. 58, No. 3, 2006

On a distribution property of the residual order of $a \pmod p$ — III

By Koji CHINEN and Leo MURATA*

(Received May 19, 2004)
(Revised Jul. 19, 2005)

Abstract. Let a be a positive integer which is not a perfect b-th power with $b \geq 2$, q be a prime number and $Q_a(x; q^i, j)$ be the set of primes $p \leq x$ such that the residual order of $a \pmod p$ in $(\boldsymbol{Z}/p\boldsymbol{Z})^\times$ is congruent to j modulo q^i. In this paper, which is a sequel of our previous papers [**1**] and [**6**], under the assumption of the Generalized Riemann Hypothesis, we determine the natural densities of $Q_a(x; q^i, j)$ for $i \geq 3$ if $q = 2$, $i \geq 1$ if q is an odd prime, and for an arbitrary nonzero integer j (the main results of this paper are announced without proof in [**3**], [**7**] and [**2**]).

1. Introduction.

This paper is a sequel of our previous papers [**1**] and [**6**], and here we present full proofs of the results announced in [**3**], [**7**] and [**2**].

Let a (≥ 2) be a natural number which is not a perfect b-th power with $b \geq 2$, j and k be integers with $0 \leq j < k$. For a prime p with $p \nmid a$, we define the number

$$D_a(p) = \sharp\langle a \pmod p\rangle$$
$$\text{(the order of the class } a \pmod p \text{ in } (\boldsymbol{Z}/p\boldsymbol{Z})^\times)$$

and consider the set

$$Q_a(x; k, j) = \{p \leq x \ ; \ p \nmid a,\ D_a(p) \equiv j \pmod k\}.$$

The set $Q_a(x; k, 0)$ attracted attention of many mathematicians and its natural density is completely determined (see Hasse [**4**], [**5**], Odoni [**8**], Wiertelak [**12**]). But when $j \neq 0$, determining the density of $Q_a(x; k, j)$ requires much more exacting analysis. In [**1**] and [**6**], we considered the set $Q_a(x; 4, j)$ with $j = 1$ and 3 (when $j = 2$, we can get the density easily).

All primes $\leq x$ are divided into the two sets, $Q_a(x; 2, 0)$ and $Q_a(x; 2, 1)$, and our motivation of studying $Q_a(x; 4, j)$ came from the observation that, for an *usual* a,

$$\sharp Q_a(x; 2, 0) \sim \frac{2}{3}\pi(x), \qquad \sharp Q_a(x; 2, 1) \sim \frac{1}{3}\pi(x),$$

2000 *Mathematics Subject Classification.* Primary 11A07; Secondary 11N05, 11N25.

Key Words and Phrases. residual order, residual index, Artin's conjecture for primitive roots.

*This research was supported by Grant-in-Aid for Scientific Research (No. 14540048) from the Ministry of Education, Culture, Sports, Science and Technology in Japan.

where $\pi(x)$ denotes the number of primes up to x. This means that, when p varies, the parity of $D_a(p)$ – even or odd – is *not* equi-distribution.

In order to study this phenomenon more closely, we investigated the density of $Q_a(x;4,j)$ and observed how the two sets $Q_a(x;2,0)$ and $Q_a(x;2,1)$ are divided into $Q_a(x;4,j)$'s. Then we found out that the densities mod 4 had even more intricate structures. In fact, in [**1**] and [**6**], we proved the existence of the density of $Q_a(x;4,j)$ on the assumption of Generalized Riemann Hypothesis (= GRH) for a certain family of algebraic number fields, and determined these values exactly:

Theorem 1.1 ([**6**]). *Let $\nu_p(a)$ denote the non-negative integer such that $p^{\nu_p(a)} \parallel a$. We assume GRH, then the natural densities $\delta_a(j)$ of $Q_a(x;4,j)$ $(j=1,3)$ exist and both equal to $1/6$ if $\nu_2(a)$ is even, while if $\nu_2(a)$ is odd, then*

$$\delta_a(3)-\delta_a(1)=C\prod_{p:\nu_p(a)\text{ is odd}}\frac{(1-(\frac{-1}{p}))p}{p^3-p^2-p-1}$$

where

$$C:=\frac{1}{8}\prod_{p\equiv 3 \pmod 4}\left(1-\frac{2p}{(p^2+1)(p-1)}\right)\approx 0.080456$$

and $(\frac{-1}{p})$ is the Legendre symbol.

In particular, $\delta_a(3)$ is equal to $\delta_a(1)$ if the square-free part of a is odd or divisible by any $p\equiv 1 \pmod 4$, and $\delta_a(3)$ is strictly greater in all other cases.

In the present paper, we extend this result to the case of an arbitrary prime power modulus, i.e. we consider the density of $Q_a(x;q^i,j)$ ($i\geq 3$ if $q=2$, $i\geq 1$ if q is an odd prime). In this study, we are interested in the relation between $Q_a(x;q^{i-1},j)$ and $Q_a(x;q^i,j)$. Of course $Q_a(x;q^{i-1},j)$ is decomposed into

$$Q_a(x;q^i,j+tq^{i-1}),\qquad (t=0,1,\cdots,q-1)$$

so we investigate whether $\sharp Q_a(x;q^i,j+tq^{i-1})\sim\frac{1}{q}\sharp Q_a(x;q^{i-1},j)$ for any t — a local equi-distribution property — or not.

Roughly speaking, our results show that, when $q\geq 3$ (i.e. an odd prime), we have the above "equi-distribution property" for $i\geq 2$ (q: odd prime), and for $i\geq 4$ ($q=2$), but *do not have* for the other cases.

Let $\Delta_a(q^i,j)$ be the natural density of the set $Q_a(x;q^i,j)$. We prove the existence of the density in Section 2 (Theorem 2.1). The basic mechanism is the same as that of [**1**, Section 4, Part I], so we give only the outline.

In Section 3, in order to calculate the density explicitly, we start from the formula (2.2) of Theorem 2.1, and consider the most difficult quantity — the coefficient $c_r(k,n,d)$, which is determined according to the existence or nonexistence of a certain automorphism over an algebraic number field of the Kummer type.

The computation of $\Delta_a(q,j)$ (q: an odd prime) needs somewhat hard calculation, and is outlined in Section 4 (the reader is also referred to [**6**, Section 5]). The precise statement is given in Theorem 1.2.

On the contrary, the case of higher power moduli (Theorem 1.3) is treated with less complexity (with two exceptions $\Delta_a(8,2)$ and $\Delta_a(8,6)$). In this case, we can employ two different methods according to the values (q^i, j). For some cases, we prove the recurrence relation between $\Delta_a(q^i, j)$ and $\Delta_a(q^{i-1}, j)$ directly. For other cases, we observe that all $\Delta_a(q^i, j)$ $(1 \le j \le q^{i-1}$, $q^e \parallel j$ for a fixed $e)$ have the same infinite series expression and therefore the same value. Then we obtain the exact values of them from the unconditional result for $\Delta_a(q^e, 0) - \Delta_a(q^{e+1}, 0)$ (see (5.1)). See also Wiertelak [**11**].

Let a_1 be the square free part of a. For an odd prime q, let $G = (\boldsymbol{Z}/q\boldsymbol{Z})^\times$, $\hat{G}$ be the character group of G, $(\frac{\cdot}{q})$ the Legendre symbol, and we define for each $\chi \in \hat{G}$, an absolute constant C_χ by

$$C_\chi = \prod_{\substack{p:\text{prime} \\ p \neq q}} \frac{p^3 - p^2 - p + \chi(p)}{(p-1)(p^2 - \chi(p))}. \tag{1.1}$$

Moreover we define

$$\eta_{\chi,a} = \begin{cases} 1, & \text{if } a_1 \equiv 1 \pmod 4, \\ \dfrac{\chi(2)^2}{16}, & \text{if } a_1 \equiv 2 \pmod 4, \\ \dfrac{\chi(2)}{4}, & \text{if } a_1 \equiv 3 \pmod 4. \end{cases}$$

Here are our main results:

Theorem 1.2. *Let q be an odd prime, $1 \le h \le q-1$, and we assume GRH.*

(I) *If $q \nmid a_1$, then*

$$\Delta_a(q,h) = \frac{q^2}{(q-1)(q^2-1)} - \frac{1}{(q-1)^2} \sum_{\chi \in \hat{G}} C_\chi \chi(-h) \left(1 + \eta_{\chi,a} \prod_{p \mid 2a_1} \frac{p(\chi(p)-1)}{p^3 - p^2 - p + \chi(p)}\right).$$

(II) *If $q \mid a_1$, then*

$$\Delta_a(q,h) = \frac{q^2}{(q-1)(q^2-1)} - \frac{1}{(q-1)^2} \left[\sum_{\chi \in \hat{G}} C_\chi \left\{\chi(-h) - \left(\chi(-h) + 2\sum_r \chi(r)^{-1}\right)\eta_{\chi,a} \cdot \prod_{p \mid 2\underline{a_1}} \frac{p(\chi(p)-1)}{p^3 - p^2 - p + \chi(p)}\right\}\right],$$

where $\sum_r$ means a sum over all r $(1 \le r \le q-1)$ such that $(\frac{hr+1}{q}) = 1$ and $\underline{a_1}$ is the q-free part of a_1 (i.e. $\underline{a_1} = a_1/q$).

Theorem 1.3. *We assume GRH.*

(I) *We have* $\Delta_a(8,2) = \Delta_a(4,3)$, $\Delta_a(8,6) = \Delta_a(4,1)$, *and* $\Delta_a(8,j) = \frac{1}{2}\Delta_a(4,j)$ *unless* $j = 2, 6$.

(II) (*Local equi-distribution property*) *We suppose* $i \geq 2$ *when* q *is an odd prime, and* $i \geq 4$ *when* $q = 2$. *Then for an arbitrary* j, *we have the relation*

$$\Delta_a(q^i, j) = \frac{1}{q}\Delta_a(q^{i-1}, j).$$

In general, the constants C_χ are not real numbers, and we are interested in the fact that the real number $\Delta_a(q^i, j)$ is expressed as a combination of these complex constants.

We take $q = 5$, — the smallest modulus where non-real C_χ appears — and $\hat{G} = \{\chi_0, \chi_1, \chi_2, \chi_3\}$, where χ_0 is principal and $\chi_1^2 = \chi_0$. From Theorem 1.2,

$$\begin{aligned} C_{\chi_0} &= 1, \quad C_{\chi_1} = \prod_{p \equiv 2,3 \pmod 5} \left(1 - \frac{2p}{(p-1)(p^2+1)}\right) \approx 0.1293079, \\ C_{\chi_2} &= \prod_{p \equiv 2 \pmod 5} \left(1 + \frac{(p(\sqrt{-1}-1))}{(p-1)(p^2-\sqrt{-1})}\right) \prod_{p \equiv 3 \pmod 5} \left(1 - \frac{(p(\sqrt{-1}+1))}{(p-1)(p^2+\sqrt{-1})}\right) \\ &\quad \cdot \prod_{p \equiv 4 \pmod 5} \left(1 - \frac{2p}{(p-1)(p^2+1)}\right) \approx 0.3640896 + 0.2240411\sqrt{-1} \end{aligned} \tag{1.2}$$

and $C_{\chi_3} = \overline{C_{\chi_2}}$. Then for $a = 13$, we have

$$\begin{aligned} \Delta_{13}(5,1) &= \frac{25}{96} - \frac{1}{16}\left\{1 + \frac{1059}{1007}C_{\chi_1} - 2\mathrm{Re}\left(\frac{10255371 - 52338\sqrt{-1}}{10150565}C_{\chi_2}\right)\right\} \\ &\approx 0.235543, \\ \Delta_{13}(5,2) &= \frac{25}{96} - \frac{1}{16}\left\{1 - \frac{1059}{1007}C_{\chi_1} + 2\mathrm{Re}\left(\frac{10255371 - 52338\sqrt{-1}}{10150565}C_{\chi_2}\right)\right\} \\ &\approx 0.178356, \\ \Delta_{13}(5,3) &= \frac{25}{96} - \frac{1}{16}\left\{1 - \frac{1059}{1007}C_{\chi_1} - 2\mathrm{Re}\left(\frac{10255371 - 52338\sqrt{-1}}{10150565}C_{\chi_2}\right)\right\} \\ &\approx 0.234475, \\ \Delta_{13}(5,4) &= \frac{25}{96} - \frac{1}{16}\left\{1 + \frac{1059}{1007}C_{\chi_1} + 2\mathrm{Re}\left(\frac{10255371 - 52338\sqrt{-1}}{10150565}C_{\chi_2}\right)\right\} \\ &\approx 0.143292. \end{aligned} \tag{1.3}$$

These "theoretical densities" are well-matched with experimental densities. For more examples, *cf.* Section 6.

We give the explicit values of $\Delta_a(q^i, j)$, but it seems very difficult to prove $\Delta_a(q^i, j) >$

0, because we have only little knowledge about number theoretical properties of C_χ's from its Euler product expression.

We start from the observations $\Delta_a(2,1) = 1/3$ and $\Delta_a(4,3) = 1/6$ for a usual a, but now we know that (q^i, j) for which "$\Delta_a(q^i, j) \in \boldsymbol{Q}$" are rather exceptional. For example, when q is an odd prime, $\Delta_a(q^i, j) \in \boldsymbol{Q}$ seems to happen only when $q|j$ (see also Theorem 1.1).

2. Existence of the Density.

First we introduce some more notations. For $k \in \boldsymbol{Z}$, let $\zeta_k = \exp(2\pi i/k)$. We denote Euler's totient and the Möbius function by $\varphi(k)$ and $\mu(k)$, respectively. For a prime power q^t, $q^t \parallel m$ means that $q^t|m$ and $q^{t+1} \nmid m$. Note that $q^0 \parallel m$ means $q \nmid m$. For integers $m_1, m_2, \cdots, m_n$, $\langle m_1, m_2, \cdots, m_n\rangle$ denotes the least common multiple of $m_1, m_2, \cdots, m_n$.

We assume $a \in \boldsymbol{N}$ is not a perfect b-th power with $b \geq 2$. We are interested in the set $Q_a(x; q^i, j)$ with $1 \leq j \leq q^i - 1$, so we put $j = hq^e$ with $q \nmid h$ and $0 \leq e \leq i-1$. For $1 \leq r < q^i$ $(q \nmid r)$, $f \geq e$ and $l \geq 0$, let

$$k = \{(\overline{h}r) \pmod{q^{i-e}} + lq^{i-e}\}q^{f-e} \tag{2.1}$$

where $h\overline{h} \equiv 1 \pmod{q^{i-e}}$, and $(\overline{h}r) \pmod{q^{i-e}}$ means the least natural number which is congruent to $\overline{h}r$ modulo q^{i-e}. And let

$$k_0 = \prod_{\substack{p|k \\ p:\text{prime}}} p \quad (\text{the core of } k).$$

For above f, i, k and $n \geq 1, d \geq 1, d|k_0$, we define the following two types of number fields:

$$G_{k,n,d} = \boldsymbol{Q}\big(a^{1/kn}, \zeta_{kd}, \zeta_n\big),$$
$$\tilde{G}_{k,n,d} = G_{k,n,d}(\zeta_{q^{f+i}})$$

(note that k and d depend on f and i). We take an automorphism $\sigma_r \in \mathrm{Gal}(\boldsymbol{Q}(\zeta_{q^{f+i}})/\boldsymbol{Q})$ determined uniquely by the condition $\sigma_r : \zeta_{q^{f+i}} \mapsto \zeta_{q^{f+i}}^{1+rq^f}$ $(1 \leq r < q^i,\ q \nmid r)$, and we consider an automorphism $\sigma_r^* \in \mathrm{Gal}(\tilde{G}_{k,n,d}/G_{k,n,d})$ which satisfies $\sigma_r^*|_{\boldsymbol{Q}(\zeta_{q^{f+i}})} = \sigma_r$. Clearly, such a σ_r^* is unique if it exists (see [**1**, Lemma 4.3]).

The main result of this section is the following:

THEOREM 2.1. *Under GRH, we have*

$$\sharp Q_a(x; q^i, hq^e) = \Delta_a(q^i, hq^e)\,\mathrm{li}\ x + O\bigg(\frac{x}{\log x \log\log x}\bigg)$$

as $x \to \infty$, *where*

$$\Delta_a(q^i, hq^e) = \sum_{\substack{1 \le r < q^i \\ q \nmid r}} \sum_{f \ge e} \sum_{l \ge 0} \frac{k_0}{\varphi(k_0)} \sum_{d | k_0} \frac{\mu(d)}{d} \sum_{n=1}^{\infty} \frac{\mu(n) c_r(k, n, d)}{[\tilde{G}_{k,n,d} : \boldsymbol{Q}]} \tag{2.2}$$

and

$$c_r(k, n, d) = \begin{cases} 1, & \text{if } \sigma_r^* \text{ exists,} \\ 0, & \text{otherwise.} \end{cases}$$

The series in the right hand side of (2.2) *always converge.*

Remark. We can find $\Delta_a(2^i, 2^{i-1})$ $(i \ge 3)$ unconditionally because $\Delta_a(2^i, 2^{i-1}) = \Delta_a(2^{i-1}, 0) - \Delta_a(2^i, 0)$ (see Lemma 5.1 (ii)).

The following lemma is the starting point of the proof of Theorem 2.1. It is a generalization of [**1**, Lemma 3.1 (iii), (iv)]. We give the proof here because it was omitted in [**1**].

Lemma 2.2. *Let $I_a(p) = |(\boldsymbol{Z}/p\boldsymbol{Z})^\times : \langle a \pmod p \rangle|$, the residual index mod p of a. Then,*

$$\sharp Q_a(x; q^i, hq^e) = \sum_{\substack{1 \le r < q^i \\ q \nmid r}} \sum_{f \ge e} \sum_{l \ge 0} \sharp\{p \le x \ ; \ I_a(p) = k, \ p \equiv 1 + rq^f \pmod{q^{f+i}}\}. \tag{2.3}$$

Proof. We take $p \in Q_a(x; q^i, hq^e)$ and define f by $q^f \parallel p - 1$. We have $f \ge e$ because $q^e | D_a(p)$. We can write $p - 1 = q^f(r + mq^i)$ and $D_a(p) = hq^e + nq^i$ $(m, n, r \in \boldsymbol{N} \cup \{0\},\ q \nmid r)$. Then by the relation $D_a(p) I_a(p) = p - 1$, we have

$$(h + nq^{i-e}) I_a(p) = q^{f-e}(r + mq^i).$$

We can see $q^{f-e} \parallel I_a(p)$ and

$$h \cdot \frac{I_a(p)}{q^{f-e}} \equiv r \pmod{q^{i-e}}.$$

This yields

$$I_a(p) \equiv \{(\bar{h} r) \pmod{q^{i-e}}\} \cdot q^{f-e} \pmod{q^{f+i-2e}}. \tag{2.4}$$

Conversely, $p \equiv 1 + rq^f \pmod{q^{f+i}}$ and (2.4) similarly lead to $D_a(p) \equiv hq^e \pmod{q^i}$ if we note $f \ge e$. Writing (2.4) in a form

$$I_a(p) = \{(\bar{h} r) \pmod{q^{i-e}} + lq^{i-e}\} q^{f-e} \quad (l \ge 0),$$

we obtain the desired result. □

We can now prove Theorem 2.1. The estimation of (2.3) can be carried out by a similar manner to [**1**, Section 4]. In fact, the prime set in (2.3) is $N_a(x;k;1+rq^f \pmod{q^{f+i}})$ in the notation of [**1**, (3.1)]. Here we sketch the proof (it can be done along the same line as Part I of [**1**, Section 4], so we leave the details to the reader).

First we decompose $N_a(x;k;1+rq^f \pmod{q^{f+i}})$ as follows:

$$\begin{aligned}&\sharp N_a\big(x;k;1+rq^f \pmod{q^{f+i}}\big)\\&\quad=\frac{1}{[K_k:\boldsymbol{Q}]}\frac{k_0}{\varphi(k_0)}\sum_{d|k_0}\frac{\mu(d)}{d}\sharp B\big(x;K_k;a^{1/k};kd;1+rq^f \pmod{q^{f+i}}\big),\end{aligned}$$

where $K_k=\boldsymbol{Q}(\zeta_{k_0},a^{1/k})$,

$$B(x;K_k;a^{1/k};N;s \pmod t)=\left\{\begin{array}{l}\mathfrak{p}: \text{ a prime ideal in } K_k,\ N\mathfrak{p}=p^1\le x,\\ p\equiv 1 \pmod N,\ p\equiv s \pmod t,\\ a^{1/k} \text{ is a primitive root mod } \mathfrak{p}\end{array}\right\}$$

and $N\mathfrak{p}$ is the (absolute) norm of $\mathfrak{p}$ (note that p is a rational prime). Moreover we introduce the set

$$P(x;K_k;a^{1/k};kd;s \pmod t;n)=\left\{\begin{array}{l}\mathfrak{p}: \text{ a prime ideal in } K_k,\ N\mathfrak{p}=p^1\le x,\\ p\equiv 1 \pmod{kd},\ p\equiv s \pmod t,\\ \text{the equation } X^q\equiv a^{1/k} \pmod{\mathfrak{p}}\\ \text{is solvable in } O_{K_k} \text{ for any } q|n\end{array}\right\}.$$

Then we have

$$\begin{aligned}&\sharp B\big(x;K_k;a^{1/k};kd;1+rq^f \pmod{q^{f+i}}\big)\\&\quad=\sum_n{}'\,\mu(n)\sharp P\big(x;K_k;a^{1/k};kd;1+rq^f \pmod{q^{f+i}};n\big)+O\bigg(\frac{x(\log\log x)^3}{\log^2 x}\bigg),\end{aligned}$$

where $\sum'_n$ means the sum over such an $n\le x$ which is either 1 or a positive square free integer composed entirely of prime factors not exceeding $(1/8)\log x$, and the constant implied by the O-symbol depends only on a, q, i and e (see Propositions 1 and 2 of [**1**]).

By the uniqueness of σ_r^*, we can prove similarly to [**1**, Proposition 4.4]

$$\sharp P\big(x;K_k;a^{1/k};kd;1+rq^f \pmod{q^{f+i}};n\big)=\pi\big(x;\tilde{G}_{k,n,d}/K_k,\{\sigma_r^*\}\big)+O(k^2\sqrt{x}),$$

where

$$\pi(x;L/K,C)=\sharp\{\mathfrak{p}: \text{ a prime ideal in } K, \text{ unramified in } L,\ (\mathfrak{p},L/K)=C,\ N\mathfrak{p}\le x\}$$

for a finite Galois extension L/K and a conjugacy class C in $\mathrm{Gal}(L/K)$ and $(\mathfrak{p},L/K)$ is the Frobenius symbol. The constant implied by the O-symbol depends only on a, q, i and e.

For the value of $[\tilde{G}_{k,n,d} : K_k]$ and the discriminant $d_{\tilde{G}_{k,n,d}}$ of $\tilde{G}_{k,n,d}$, we have the estimates

$$[\tilde{G}_{k,n,d} : K_k] = \delta \frac{d}{k_0\varphi((n,k_0))} \cdot kn\varphi(n)$$

where δ is an absolute constant, and

$$\log \left| d_{\tilde{G}_{k,n,d}} \right| \ll (nkd)^3 \log(nkd),$$

where the constant implied by $\ll$ depend only on a, q, i and e (for the proof, see, for example [**10**]).

All these results allow us to estimate the remainder terms, and we obtain the theorem.

3. Determination of $c_r(k,n,d)$.

Theorem 2.1 shows that the set $Q_a(x; q^i, hq^e)$ has a natural density. For explicit computation of the natural density $\Delta_a(q^i, hq^e)$, we need to determine the values of coefficients $c_r(k,n,d)$. To this end, we consider the number fields $\boldsymbol{Q}(\zeta_{q^{f+i}})$, $G_{k,n,d}$, $\tilde{G}_{k,n,d}$ and their automorphisms. First we introduce a preliminary lemma:

Lemma 3.1. *Let K be a number field, M be a finite extension of K, and L be a finite Galois extension of K. Then we have the following*:

(I) *LM is a Galois extension of M. For $\sigma \in \mathrm{Gal}(LM/M)$, $\sigma \mapsto \sigma|_L$ gives an injective homomorphism from $\mathrm{Gal}(LM/M)$ to $\mathrm{Gal}(L/K)$, and $[LM : M] \mid [L : K]$.*

(II) *The following three conditions are equivalent*:
- (i) $\mathrm{Gal}(LM/M) \cong \mathrm{Gal}(L/K)$,
- (ii) $[LM : M] = [L : K]$,
- (iii) $K = L \cap M$.

Proof. The proof is elementary and we omit it. □

Now we proceed to the determination of $c_r(k,n,d)$.

The strategy. We apply Lemma 3.1 to the case where $L = \boldsymbol{Q}(\zeta_{q^{f+i}})$ and $M = G_{k,n,d}$. Then $LM = \tilde{G}_{k,n,d}$. We consider the automorphism σ_r on the intersection field $K = L \cap M$.

(i) *The case $\sigma_r|_K = \mathrm{id}$.*

We have $\sigma_r \in \mathrm{Gal}(\boldsymbol{Q}(\zeta_{q^{f+i}})/K)$, so from Lemma 3.1, we can take $\tau \in \mathrm{Gal}(\tilde{G}_{k,n,d}/G_{k,n,d}) \cong \mathrm{Gal}(\boldsymbol{Q}(\zeta_{q^{f+i}})/K)$ such that $\tau|_{\boldsymbol{Q}(\zeta_{q^{f+i}})} = \sigma_r$. Thus $\tau = \sigma_r^*$, and we have $c_r(k,n,d) = 1$.

(ii) *The case $\sigma_r|_K \neq \mathrm{id}$.*

Similarly, we can easily verify that there is no $\tau \in \mathrm{Gal}(\tilde{G}_{k,n,d}/G_{k,n,d})$ with the property $\tau|_{\boldsymbol{Q}(\zeta_{q^{f+i}})} = \sigma_r$, and we have $c_r(k,n,d) = 0$.

So, what we have to do is to determine the intersection K and to verify if $\sigma_r|_K = \mathrm{id}$ or not. For this purpose, we need two lemmas:

LEMMA 3.2. *Let m be positive and square free, $m \neq 1, 0$, and let d_m be the discriminant of $\boldsymbol{Q}(\sqrt{m})$. Then the least cyclotomic field which contains $\boldsymbol{Q}(\sqrt{m})$ is $\boldsymbol{Q}(\zeta_{|d_m|})$. Especially,*

$$\begin{aligned} &\boldsymbol{Q}(\sqrt{m}) \subset \boldsymbol{Q}(\zeta_m) \text{ and } \boldsymbol{Q}(\sqrt{-m}) \subset \boldsymbol{Q}(\zeta_{4m}), && \text{if } m \equiv 1 \pmod 4, \\ &\boldsymbol{Q}(\sqrt{\pm m}) \subset \boldsymbol{Q}(\zeta_{4m}), && \text{if } m \equiv 2 \pmod 4, \\ &\boldsymbol{Q}(\sqrt{m}) \subset \boldsymbol{Q}(\zeta_{4m}) \text{ and } \boldsymbol{Q}(\sqrt{-m}) \subset \boldsymbol{Q}(\zeta_m), && \text{if } m \equiv 3 \pmod 4. \end{aligned}$$

PROOF. See a suitable textbook of algebraic number theory. □

LEMMA 3.3. (I) *If kn is odd,*

$$\begin{aligned} \left[G_{k,n,d} : \boldsymbol{Q}\right] &= kn\,\varphi(\langle kd, n\rangle), \\ \left[\tilde{G}_{k,n,d} : \boldsymbol{Q}\right] &= kn\,\varphi(\langle kd, n, q^{f+i}\rangle). \end{aligned}$$

(II) *If kn is even,*

$$\left[G_{k,n,d} : \boldsymbol{Q}\right] = \begin{cases} kn\,\varphi(\langle kd, n\rangle), \\ \frac{1}{2}kn\,\varphi(\langle kd, n\rangle), \end{cases}$$

where the latter case happens when one of the following conditions is satisfied:

(a) $a_1 \equiv 1 \pmod 4$ *and* $a_1 | \langle kd, n\rangle$,

(b) $a_1 \equiv 2 \pmod 4$ *and* $4a_1 | \langle kd, n\rangle$,

(c) $a_1 \equiv 3 \pmod 4$ *and* $4a_1 | \langle kd, n\rangle$,

and

$$\left[\tilde{G}_{k,n,d} : \boldsymbol{Q}\right] = \begin{cases} kn\varphi(\langle kd, n, q^{f+i}\rangle), \\ \frac{1}{2}kn\varphi(\langle kd, n, q^{f+i}\rangle), \end{cases}$$

where the latter case happens when one of the following conditions is satisfied:

(a') $a_1 \equiv 1 \pmod 4$ *and* $a_1 | \langle kd, n, q^{f+i}\rangle$,

(b') $a_1 \equiv 2 \pmod 4$ *and* $4a_1 | \langle kd, n, q^{f+i}\rangle$,

(c') $a_1 \equiv 3 \pmod 4$ *and* $4a_1 | \langle kd, n, q^{f+i}\rangle$.

PROOF. This is a direct consequence of [**6**, Proposition 3.1]. □

Lemma 3.3 allows us to calculate $[\tilde{G}_{k,n,d} : G_{k,n,d}]$. If we find a field K' such that $K' \subset G_{k,n,d}$, $K' \subset \boldsymbol{Q}(\zeta_{q^{f+i}})$ and $[\boldsymbol{Q}(\zeta_{q^{f+i}}) : K'] = [\tilde{G}_{k,n,d} : G_{k,n,d}]$, then by Lemma 3.1, we can conclude $K = K'$.

We have to consider the two cases, q is an odd prime and $q = 2$, separately. We state the results for odd q first:

Theorem 3.4 (The values of $c_r(k,n,d)$ — q: odd prime). *We assume q is an odd prime. Then the intersection field $K = G_{k,n,d} \cap \boldsymbol{Q}(\zeta_{q^{f+i}})$ and the number $c_r(k,n,d)$ are given in Table* 1. *In this table, G_q is the Gauss sum defined by*

$$G_q = \sum_{x \in \boldsymbol{Z}/q\boldsymbol{Z}^\times} \left(\frac{x}{q}\right) {\zeta_q}^x.$$

Table 1. The number $c_r(k,n,d)$ for odd q.

<table>
<tr><th>$f-e$</th><th>d</th><th>n</th><th>kn</th><th colspan="2">a_1</th><th>K</th><th colspan="2">$c_r(k,n,d)$</th></tr>
<tr><td rowspan="2">$f-e \geq 1$</td><td>$q \mid d$</td><td>all</td><td>all</td><td colspan="2">all</td><td>$\boldsymbol{Q}(\zeta_{q^{f-e+1}})$</td><td>1, if $e \geq 1$
0, if $e = 0$</td><td>(A)</td></tr>
<tr><td>$q \nmid d$</td><td>all</td><td>all</td><td colspan="2">all</td><td>$\boldsymbol{Q}(\zeta_{q^{f-e}})$</td><td>1</td><td>(B)</td></tr>
<tr><td rowspan="5">$f-e=0$</td><td rowspan="5">all</td><td>$q \mid n$</td><td>all</td><td colspan="2">all</td><td>$\boldsymbol{Q}(\zeta_q)$</td><td>1, if $e \geq 1$
0, if $e = 0$</td><td>(C)</td></tr>
<tr><td rowspan="4">$q \nmid n$</td><td>odd</td><td colspan="2">all</td><td rowspan="3">$\boldsymbol{Q}$</td><td rowspan="3">1, if $e \geq 1$
or $e = 0$ and
$r \not\equiv -1 \pmod{q}$
0, otherwise</td><td rowspan="3">(D)</td></tr>
<tr><td rowspan="3">even</td><td colspan="2">$q \nmid a_1$</td></tr>
<tr><td rowspan="2">$q \mid a_1$</td><td>none of (a'), (b'), (c')</td></tr>
<tr><td>(a') or (b') or (c')</td><td>$\boldsymbol{Q}(G_q)$</td><td>1, if $e \geq 1$
or $e = 0$,
$r \not\equiv -1 \pmod{q}$,
$(\frac{r+1}{q}) = 1$,
0, otherwise</td><td>(E)</td></tr>
</table>

Proof. We give proofs for only a few typical cases.

The case (A). From Lemma 3.3, we can easily see that

$$\begin{aligned}[\tilde{G}_{k,n,d} : G_{k,n,d}] &= \frac{[\tilde{G}_{k,n,d} : \boldsymbol{Q}]}{[G_{k,n,d} : \boldsymbol{Q}]} = \frac{kn\,\varphi(q^{f+i})\varphi(\langle \underline{kd}, \underline{n}\rangle)}{kn\,\varphi(q^{f-e+1})\varphi(\langle \underline{kd}, \underline{n}\rangle)} \\ &= q^{e+i-1},\end{aligned}$$

where $\underline{m}$ denotes the q free part of an integer m, i.e. $\underline{m} = m/q^e$ for $q^e \parallel m$. So, the intersection K must satisfy

$$[\boldsymbol{Q}(\zeta_{q^{f+i}}) : K] = q^{e+i-1}.$$

Since $\boldsymbol{Q}(\zeta_{q^{f+i}})/\boldsymbol{Q}(\zeta_q)$ is cyclic (note that q is odd), the subgroup of $\mathrm{Gal}(\boldsymbol{Q}(\zeta_{q^{f+i}})/\boldsymbol{Q})$ is uniquely determined by its order, and so is K. Thus we have

$$K = \boldsymbol{Q}(\zeta_{q^{f-e+1}}).$$

Note that $\zeta_{q^{f-e+1}} = \zeta_{q^{f+i}}^{q^{e+i-1}}$ and

$$\zeta_{q^{f-e+1}}^{\sigma_r} = \zeta_{q^{f-e+1}} \cdot \zeta_{q^{f+i}}^{rq^{e+f+i-1}}.$$

Then we can see $\zeta_{q^{f-e+1}}^{\sigma_r} = \zeta_{q^{f-e+1}}$ and $\sigma_r|_K = \mathrm{id}$ if $e \geq 1$. On the other hand, if $e = 0$, $rq^{f+i-1} \not\equiv 0 \pmod{q^{f+i}}$ because $(r, q) = 1$. Hence $\zeta_{q^{f-e+1}}^{\sigma_r} \neq \zeta_{q^{f-e+1}}$ and $\sigma_r|_K \neq \mathrm{id}$. Therefore,

$$c_r(k, n, d) = \begin{cases} 1, & \text{if } e \geq 1, \\ 0, & \text{if } e = 0. \end{cases}$$

(We can prove (B), (C) and (D) similarly.)

The case (E). From Lemma 3.3, we can see

$$\left[\tilde{G}_{k,n,d} : G_{k,n,d}\right] = \frac{1}{2} q^{e+i-1}(q-1).$$

Noting that $f - e = 0$, we have $[\boldsymbol{Q}(\zeta_{q^{f+i}}) : K] = \frac{1}{2} q^{e+i-1}(q-1)$ and therefore $[K : \boldsymbol{Q}] = 2$.

Similarly to the case (A), K is determined uniquely by these conditions: since $K \subset \boldsymbol{Q}(\zeta_q) \subset \boldsymbol{Q}(\zeta_{q^{f+i}})$ and K is quadratic, we conclude that $K = \boldsymbol{Q}(G_q)$.

Now we proceed to the observation of σ_r. Note that σ_r does not exist when $e = 0$ and $r \equiv -1 \pmod{q}$, because $q | (1 + rq^f)$ (recall $f = e = 0$), and so $c_r(k, n, d) = 0$. In the cases where $e \geq 1$ or $e = 0$ and $r \not\equiv -1 \pmod{q}$, σ_r always exists, so we check whether $\sigma_r|_K = \mathrm{id}$ or not (recall the discussion before Lemma 3.2). Since $f = e$, we have

$$\zeta_q^{\sigma_r} = \left(\zeta_{q^{e+i}}^{q^{e+i-1}}\right)^{1+rq^e} = \zeta_q \cdot \zeta_{q^{e+i}}^{rq^{2e+i-1}}.$$

When $e \geq 1$, we have $\zeta_{q^{e+i}}^{rq^{2e+i-1}} = 1$, so $\zeta_q^{\sigma_r} = \zeta_q$. Thus $\sigma_r|_K = \mathrm{id}$ and σ_r^* exists.

When $e = 0$ and $r \not\equiv -1 \pmod{q}$, we have

$$\zeta_q^{\sigma_r} = \zeta_q \cdot \zeta_{q^i}^{rq^{i-1}} = \zeta_q^{r+1}.$$

Note that $\mathrm{Gal}(\boldsymbol{Q}(\zeta_q)/\boldsymbol{Q}) \cong (\boldsymbol{Z}/q\boldsymbol{Z})^\times$. Since q is odd, the quadratic residues mod q form a subgroup of index 2 in $(\boldsymbol{Z}/q\boldsymbol{Z})^\times$. Hence we can conclude

$$\sigma_r|_K = \mathrm{id}, \quad \text{if } \left(\frac{r+1}{q}\right) = 1$$

and

$$\sigma_r|_K \neq \mathrm{id}, \quad \text{if } \left(\frac{r+1}{q}\right) = -1,$$

which proves Table 1 (E). The cases (b') and (c') can be dealt with similarly. □

We can easily see the following:

Corollary 3.5. *Let q be an odd prime. When $e \geq 1$, we have*

$$c_r(k,n,d) = 1$$

for all r,k,n,d.

Note that $c_r(k,n,d)$ does not depend on r when $e \geq 1$, above all.

Now we proceed to the case $q = 2$.

Theorem 3.6 (The values of $c_r(k,n,d)$ — $q = 2$). *We assume $q = 2$. Then the intersection field $K = G_{k,n,d} \cap \boldsymbol{Q}(\zeta_{q^{f+i}})$ and the number $c_r(k,n,d)$ are given in Tables 2 and 3 (in next pages), where $\underline{m}$ denotes the odd part of an integer m (i.e., $\underline{m} = m/2^e$ with $2^e \parallel m$) and $a_1' = \underline{a_1}$ when $a_1 \equiv 2 \pmod 4$.*

Proof. We can prove this theorem similarly to Theorem 3.4. In Table 3, note that we have only to consider the case $e \geq 1$, and therefore k and d are always odd. The reader is also referred to [**6**, Section 4]. □

We can easily see the following:

Corollary 3.7. *Let $q = 2$. When $e \geq 3$, we have*

$$c_r(k,n,d) = 1$$

for all r,k,n,d.

4. Proof of Theorem 1.2.

In this section we prove Theorem 1.2. Let q be an odd prime. Then for $1 \leq h \leq q-1$, we have from (2.2) that

$$\Delta_a(q,h) = \sum_{1\leq r<q} \sum_{f\geq 0} \sum_{l\geq 0} \frac{k_0}{\varphi(k_0)} \sum_{d|k_0} \frac{\mu(d)}{d} \sum_{n=1}^{\infty} \frac{\mu(n)c_r(k,n,d)}{[\tilde{G}_{k,n,d} : \boldsymbol{Q}]}, \tag{4.1}$$

where $k = \{(\overline{h}r) \pmod q) + lq\}q^f$. This number k is a little hard to deal with, so first we remove the dependence on h from k. When r runs through the range $1 \leq r < q$, $(\overline{h}r) \pmod q$ also runs through the same range, so we change the variables $(\overline{h}r) \pmod q \mapsto r$. Then $k = (r+lq)q^f$, $c_r(k,n,d)$ is transformed to $c_{hr}(k,n,d)$ (the suffix hr is understood modulo q) and

Table 2. The number $c_r(k,n,d)$ for $q=2$ (I) (the case $f-e\geq 1$).

d	a_1		K	$c_r(k,n,d)$	
even	$a_1\equiv 1,3 \pmod 4$		$\boldsymbol{Q}(\zeta_{2^{f-e+1}})$	$1,\ \text{if } e\geq 1$ $0,\ \text{if } e=0$	(A)
even	$a_1\equiv 2 \pmod 4$	$a_1'\nmid\langle \underline{kd},\underline{n}\rangle$	$\boldsymbol{Q}(\zeta_{2^{f-e+1}})$	$1,\ \text{if } e\geq 1$ $0,\ \text{if } e=0$	(A)
even	$a_1\equiv 2 \pmod 4$	$a_1'\mid\langle \underline{kd},\underline{n}\rangle$, $f-e\geq 2$	$\boldsymbol{Q}(\zeta_{2^{f-e+1}})$	$1,\ \text{if } e\geq 1$ $0,\ \text{if } e=0$	(A)
even	$a_1\equiv 2 \pmod 4$	$a_1'\mid\langle \underline{kd},\underline{n}\rangle$, $f-e=1$	$\boldsymbol{Q}(\zeta_8)$	$1,\ \text{if } e\geq 2$ $0,\ \text{if } e=0,1$	(B)
odd	$a_1\equiv 1 \pmod 4$		$\boldsymbol{Q}(\zeta_{2^{f-e}})$	1	(C)
odd	$a_2\equiv 2 \pmod 4$	$a_1'\nmid\langle \underline{kd},\underline{n}\rangle$	$\boldsymbol{Q}(\zeta_{2^{f-e}})$	1	(C)
odd	$a_2\equiv 2 \pmod 4$	$a_1'\mid\langle \underline{kd},\underline{n}\rangle$, $f-e\geq 3$	$\boldsymbol{Q}(\zeta_{2^{f-e}})$	1	(C)
odd	$a_2\equiv 2 \pmod 4$	$a_1'\mid\langle \underline{kd},\underline{n}\rangle$, $f-e=1,2$	$\boldsymbol{Q}(\sqrt{2})$ if $a_1'\equiv 1 \pmod 4$, $f-e=1$	$1,\ \text{if } e\geq 2$ or $e=0, r\equiv 3 \pmod 4$, $0,\ \text{if } e=1$ or $e=0, r\equiv 1 \pmod 4$	(D)
odd	$a_2\equiv 2 \pmod 4$	$a_1'\mid\langle \underline{kd},\underline{n}\rangle$, $f-e=1,2$	$\boldsymbol{Q}(\sqrt{-2})$ if $a_1'\equiv 3 \pmod 4$, $f-e=1$	$1,\ \text{if } e\geq 2$ or $e=0, r\equiv 1 \pmod 4$, $0,\ \text{if } e=1$ or $e=0, r\equiv 3 \pmod 4$	(E)
odd	$a_2\equiv 2 \pmod 4$	$a_1'\mid\langle \underline{kd},\underline{n}\rangle$, $f-e=1,2$	$\boldsymbol{Q}(\zeta_8)$	$1,\ \text{if } e\geq 1$ $0,\ \text{if } e=0$	(F)
odd	$a_1\equiv 3 \pmod 4$	$a_1\nmid\langle \underline{kd},\underline{n}\rangle$ or $a_1\mid\langle \underline{kd},\underline{n}\rangle$, $f-e\geq 2$	$\boldsymbol{Q}(\zeta_{2^{f-e}})$	1	(G)
odd	$a_1\equiv 3 \pmod 4$	$a_1\mid\langle \underline{kd},\underline{n}\rangle$, $f-e=1$	$\boldsymbol{Q}(\zeta_4)$	$1,\ \text{if } e\geq 1$ $0,\ \text{if } e=0$	(H)

$$\varDelta_a(q,h)=\sum_{1\leq r<q}\sum_{f\geq 0}\sum_{l\geq 0}\frac{k_0}{\varphi(k_0)}\sum_{d\mid k_0}\frac{\mu(d)}{d}\sum_{n=1}^{\infty}\frac{\mu(n)c_{hr}(k,n,d)}{[\tilde{G}_{k,n,d}:\boldsymbol{Q}]}. \tag{4.2}$$

We should also note that we have to consider only square free n because of $\mu(n)$. Theorem 3.4 tells us that, when $f-e=f\geq 1$,

$$c_r(k,n,d)=\begin{cases}1, & \text{if } q\nmid d,\\ 0, & \text{if } q\mid d.\end{cases}$$

So it is convenient to divide (4.2) into two parts, $f\geq 1$ and $f=0$:

Table 3. The number $c_r(k,n,d)$ for $q=2$ (II) (the case $f-e\geq 0$).

<table>
<tr><th>n</th><th colspan="2">a_1</th><th>K</th><th colspan="2">$c_r(k,n,d)$</th></tr>
<tr><td rowspan="6">even</td><td colspan="2">$a_1\equiv 1 \pmod 4$</td><td rowspan="2">$\boldsymbol{Q}$</td><td rowspan="2">1</td><td rowspan="2">(I)</td></tr>
<tr><td rowspan="3">$a_1\equiv 2 \pmod 4$</td><td>$a_1'\nmid\langle kd,\underline{n}\rangle$</td></tr>
<tr><td rowspan="2">$a_1'\mid\langle kd,\underline{n}\rangle$</td><td>$\boldsymbol{Q}(\sqrt{2})$ if
$a_1'\equiv 1 \pmod 4$</td><td>1, if $e\geq 3$ or
$e=1, r\equiv 3 \pmod 4$,
0, if $e=2$ or
$e=1, r\equiv 1 \pmod 4$</td><td>(J)</td></tr>
<tr><td>$\boldsymbol{Q}(\sqrt{-2})$ if
$a_1'\equiv 3 \pmod 4$</td><td>1, if $e\geq 3$ or
$e=1, r\equiv 1 \pmod 4$,
0, if $e=2$ or
$e=1, r\equiv 3 \pmod 4$</td><td>(K)</td></tr>
<tr><td rowspan="2">$a_1\equiv 3 \pmod 4$</td><td>$a_1\nmid\langle kd,\underline{n}\rangle$</td><td>$\boldsymbol{Q}$</td><td>1</td><td>(L)</td></tr>
<tr><td>$a_1\mid\langle kd,\underline{n}\rangle$</td><td>$\boldsymbol{Q}(\zeta_4)$</td><td>1, if $e\geq 2$
0, if $e=1$</td><td>(M)</td></tr>
<tr><td>odd</td><td colspan="2">all</td><td>$\boldsymbol{Q}$</td><td>1</td><td>(N)</td></tr>
</table>

$$\Delta^{(1)}=\Delta_a^{(1)}(q,h)=\sum_{1\leq r<q}\sum_{f\geq 1}\sum_{l\geq 0}\frac{k_0}{\varphi(k_0)}\sum_{d\mid k_0}\frac{\mu(d)}{d}\sum_{n=1}^{\infty}\frac{\mu(n)c_{hr}(k,n,d)}{[\tilde{G}_{k,n,d}:\boldsymbol{Q}]},$$

$$\Delta^{(0)}=\Delta_a^{(0)}(q,h)=\sum_{\substack{1\leq r<q\\ f=0}}\sum_{l\geq 0}\frac{k_0}{\varphi(k_0)}\sum_{d\mid k_0}\frac{\mu(d)}{d}\sum_{n=1}^{\infty}\frac{\mu(n)c_{hr}(k,n,d)}{[\tilde{G}_{k,n,d}:\boldsymbol{Q}]},$$

and we estimate $\Delta^{(1)}$ first. It turns out that $\Delta^{(1)}$ is independent of the choice of a and h:

Theorem 4.1. *We assume GRH. For any a and h, we have*

$$\Delta_a^{(1)}(q,h)=\frac{1}{(q-1)(q^2-1)}.$$

Proof. Recall that $\underline{m}$ means the q free part of an integer m. We write $k=\underline{k}q^f$ and the sum over r and l in the form $\sum_{\underline{k}\geq 1, q\nmid\underline{k}}$. We need explicit descriptions of the degree $[\tilde{G}_{k,n,d}:\boldsymbol{Q}]$. In the present case, the second conditions of (a'), (b') and (c') in Lemma 3.3 become

$$s\mid\langle\underline{k}d,\underline{n}\rangle,$$

where $s=\underline{a_1}$ or $4\underline{a_1}$ according to whether $a_1\equiv 1 \pmod 4$ or $a_1\equiv 2,3 \pmod 4$. Noting that

$$kn\varphi(\langle kd,n,q^{f+1}\rangle)=\underline{k}q^f n\cdot\varphi(q^{f+1})\varphi(\langle\underline{k}d,\underline{n}\rangle)$$

(we can assume n is square free), we have

$$\frac{k_0}{\varphi(k_0)}\frac{\mu(d)}{d}\frac{\mu(n)}{kn\varphi(\langle kd,n,q^{f+1}\rangle)}=\frac{1}{q^{2f}(q-1)}\frac{k_0}{\varphi(k_0)}\frac{\mu(d)}{d}\frac{\mu(n)}{\underline{k}n\varphi(\langle \underline{k}d,\underline{n}\rangle)}.$$

We put

$$A(\underline{k},d,n)=\frac{k_0}{\varphi(k_0)}\frac{\mu(d)}{d}\frac{\mu(n)}{\underline{k}n\varphi(\langle \underline{k}d,\underline{n}\rangle)}.$$

For simplicity, we abbreviate the summation $\sum_{\underline{k}\geq 1, q\nmid \underline{k}}\sum_{d|k_0, q\nmid d}\sum_{n=1}^{\infty}$ into $\sum_{\underline{k}}\sum_d\sum_n$. Here we remark that we can prove

$$\sum_{\underline{k}}\sum_d\sum_n A(\underline{k},d,n)=1 \tag{4.3}$$

(see Appendix for proof). Then, since

$$kn: \text{ odd} \Leftrightarrow \underline{k}\text{: odd and } n\text{: odd}$$

and $\sum_{f\geq 1} 1/q^{2f}(q-1)=1/(q-1)(q^2-1)$, we have by Lemma 3.3 that

$$\begin{aligned}
(q-1)(q^2-1)\Delta^{(1)} &= \Bigg[\sum_{\substack{\underline{k}\\ \underline{k}:\text{odd}}}\sum_d\sum_{\substack{n\\ n:\text{odd}}} + \sum_{\substack{\underline{k}\\ \underline{k}:\text{odd}}}\sum_d\Bigg\{\sum_{\substack{n\\ n:\text{even}\\ s\nmid\langle \underline{k}d,\underline{n}\rangle}} +2\sum_{\substack{n\\ n:\text{even}\\ s|\langle \underline{k}d,\underline{n}\rangle}}\Bigg\}\\
&\quad + \sum_{\substack{\underline{k}\\ \underline{k}:\text{even}}}\sum_d\Bigg\{\sum_{\substack{n\\ s\nmid\langle \underline{k}d,\underline{n}\rangle}} +2\sum_{\substack{n\\ s|\langle \underline{k}d,\underline{n}\rangle}}\Bigg\}\Bigg]A(\underline{k},d,n)\\
&= \Bigg\{\sum_{\substack{\underline{k}\\ \underline{k}:\text{odd}}}\sum_d\sum_{\substack{n\\ n:\text{odd}}} + \Bigg(\sum_{\substack{\underline{k}\\ \underline{k}:\text{odd}}}\sum_d\sum_{\substack{n\\ n:\text{even}}} - \sum_{\substack{\underline{k}\\ \underline{k}:\text{odd}}}\sum_d\sum_{\substack{n\\ n:\text{even}\\ s|\langle \underline{k}d,\underline{n}\rangle}}\Bigg)\\
&\quad + 2\sum_{\substack{\underline{k}\\ \underline{k}:\text{odd}}}\sum_d\sum_{\substack{n\\ n:\text{even}\\ s|\langle \underline{k}d,\underline{n}\rangle}} + \Bigg(\sum_{\substack{\underline{k}\\ \underline{k}:\text{even}}}\sum_d\sum_n - \sum_{\substack{\underline{k}\\ \underline{k}:\text{even}}}\sum_d\sum_{\substack{n\\ s|\langle \underline{k}d,\underline{n}\rangle}}\Bigg)\\
&\quad + 2\sum_{\substack{\underline{k}\\ \underline{k}:\text{even}}}\sum_d\sum_{\substack{n\\ s|\langle \underline{k}d,\underline{n}\rangle}}\Bigg\}A(\underline{k},d,n)\\
&= \Bigg(\sum_{\underline{k}}\sum_d\sum_n + \sum_{\substack{\underline{k}\\ \underline{k}:\text{odd}}}\sum_d\sum_{\substack{n\\ n:\text{even}\\ s|\langle \underline{k}d,\underline{n}\rangle}} + \sum_{\substack{\underline{k}\\ \underline{k}:\text{even}}}\sum_d\sum_{\substack{n\\ s|\langle \underline{k}d,\underline{n}\rangle}}\Bigg)A(\underline{k},d,n).
\end{aligned}$$

The first threefold sum is equal to 1 by (4.3). The second threefold sum is equal to

$$-\frac{1}{2}\sum_{\substack{\underline{k}\\ \underline{k}:\text{odd}}}\sum_{d}\sum_{\substack{n\\ n:\text{odd}\\ s|2\langle \underline{k}d,\underline{n}\rangle}} A(\underline{k},d,n) = -\frac{1}{2}E, \text{ say,}$$

and similarly, the third threefold sum is equal to

$$\frac{1}{2}\sum_{\substack{\underline{k}\\ \underline{k}:\text{even}}}\sum_{d}\sum_{\substack{n\\ n:\text{odd}\\ s|\langle \underline{k}d,\underline{n}\rangle}} A(\underline{k},d,n) = \frac{1}{2}E', \text{ say.}$$

Note that $k_0/\varphi(k_0) = k/\varphi(k)$. If we put $k = 2^j k'$ $(j \geq 1)$, we have $\underline{k} = 2^j \underline{k'}$. Then we can verify that the sum E' is equal to

$$\sum_{j\geq 1}\sum_{\substack{\underline{k'}\geq 1\\ q\nmid \underline{k'}\\ \underline{k'}:\text{odd}}} \frac{2^j k'}{\varphi(2^j k')}\sum_{\substack{d|2^j k'\\ q\nmid d}}\frac{\mu(d)}{d}\sum_{\substack{n=1\\ n:\text{odd}\\ s|\langle 2^j \underline{k'}d,\underline{n}\rangle}}^{\infty}\frac{\mu(n)}{2^j \underline{k'}n\varphi(\langle 2^j \underline{k'}d,\underline{n}\rangle)}$$

$$= \sum_{j\geq 1}\sum_{\substack{\underline{k'}\geq 1\\ q\nmid \underline{k'}\\ \underline{k'}:\text{odd}}}\sum_{\substack{d|k'\\ q\nmid d}}\left(\frac{\mu(d)}{d}\sum_{\substack{n=1\\ n:\text{odd}\\ s|\langle 2^j \underline{k'}d,\underline{n}\rangle}}^{\infty}\frac{\mu(n)}{2^j \underline{k'}n\varphi(\langle 2^j \underline{k'}d,\underline{n}\rangle)} + \frac{\mu(2d)}{2d}\sum_{\substack{n=1\\ n:\text{odd}\\ s|\langle 2^j \underline{k'}\cdot 2d,\underline{n}\rangle}}^{\infty}\frac{\mu(n)}{2^j \underline{k'}n\varphi(\langle 2^j \underline{k'}\cdot 2d,\underline{n}\rangle)}\right)$$

$$= \sum_{j\geq 1}\frac{1}{2^{2j-1}}\sum_{\substack{\underline{k'}\geq 1\\ q\nmid \underline{k'}\\ \underline{k'}:\text{odd}}}\frac{k'}{\varphi(k')}\sum_{\substack{d|k'\\ q\nmid d}}\left(\frac{\mu(d)}{d}\sum_{\substack{n=1\\ n:\text{odd}\\ s|2^j\langle \underline{k'}d,\underline{n}\rangle}}^{\infty}\frac{\mu(n)}{\underline{k'}n\varphi(\langle \underline{k'}d,\underline{n}\rangle)} - \frac{1}{4}\frac{\mu(d)}{d}\sum_{\substack{n=1\\ n:\text{odd}\\ s|2^{j+1}\langle \underline{k'}d,\underline{n}\rangle}}^{\infty}\frac{\mu(n)}{\underline{k'}n\varphi(\langle \underline{k'}d,\underline{n}\rangle)}\right).$$

(a') When $a_1 \equiv 1 \pmod 4$, $s = \underline{a_1}$ is odd, so we have

$$s|2^j\langle \underline{k'}d,\underline{n}\rangle \Leftrightarrow s|\langle \underline{k'}d,\underline{n}\rangle,$$
$$s|2^{j+1}\langle \underline{k'}d,\underline{n}\rangle \Leftrightarrow s|\langle \underline{k'}d,\underline{n}\rangle.$$

Therefore

$$E' = \sum_{\substack{\underline{k'}\\ \underline{k'}:\text{odd}}}\sum_{d}\sum_{\substack{n\\ n:\text{odd}\\ s|\langle \underline{k'}d,\underline{n}\rangle}} A(\underline{k'},d,n) = E.$$

Consequently we have

$$(q-1)(q^2-1)\Delta^{(1)} = 1. \tag{4.4}$$

(b') When $a_1 \equiv 2 \pmod 4$, $s = 4\underline{a_1}$ and $8 \parallel s$, so putting $s = 8s'$, we have

$$s|2^j\langle \underline{k}'d, \underline{n}\rangle \Leftrightarrow \begin{cases} j \geq 3, \\ s'|\langle \underline{k}'d, \underline{n}\rangle, \end{cases}$$

$$s|2^{j+1}\langle \underline{k}'d, \underline{n}\rangle \Leftrightarrow \begin{cases} j \geq 2, \\ s'|\langle \underline{k}'d, \underline{n}\rangle. \end{cases}$$

Therefore

$$E' = \left(\sum_{j\geq 3}\frac{1}{2^{2j-2}} - \frac{1}{4}\sum_{j\geq 2}\frac{1}{2^{2j-2}}\right)\sum_{\underline{k}}\sum_{d}\sum_{\substack{n \\ n:\text{odd} \\ s'|\langle \underline{k}'d,\underline{n}\rangle}} A(\underline{k}, d, n) = 0.$$

Moreover, we have $E = 0$ since $s|\langle \underline{k}d, \underline{n}\rangle$ does not hold in this case. Hence we get the same formula as (4.4).

(c') When $a_1 \equiv 3 \pmod 4$, $s = 4\underline{a_1}$ and $4 \parallel s$, so putting $s = 4s'$, we have

$$s|2^j\langle \underline{k}'d, \underline{n}\rangle \Leftrightarrow \begin{cases} j \geq 2, \\ s'|\langle \underline{k}'d, \underline{n}\rangle, \end{cases}$$

$$s|2^{j+1}\langle \underline{k}'d, \underline{n}\rangle \Leftrightarrow s'|\langle \underline{k}'d, \underline{n}\rangle.$$

Therefore

$$E' = \left(\sum_{j\geq 2}\frac{1}{2^{2j-2}} - \frac{1}{4}\sum_{j\geq 1}\frac{1}{2^{2j-2}}\right)\sum_{\underline{k}}\sum_{d}\sum_{\substack{n \\ n:\text{odd} \\ s'|\langle \underline{k}'d,\underline{n}\rangle}} A(\underline{k}, d, n) = 0$$

and $E = 0$. Hence we get the same formula as (4.4). □

We proceed to the calculation of $\Delta^{(0)}$. In the calculation of $\Delta_a^{(0)}(q,h)$, we encounter the sums over a specific residue class modulo q. To deal with such sums, we need the following lemma:

Lemma 4.2. *Let $G = (\boldsymbol{Z}/q\boldsymbol{Z})^\times$ and $\hat{G}$ be the character group of G. For any $r \in G$ and $m \in \boldsymbol{Z}$, we define*

$$f_r(m) = \frac{1}{q-1}\sum_{\chi\in\hat{G}}\chi(r)^{-1}\chi(m).$$

Then

$$f_r(m) = \begin{cases} 1, & \textit{if } m \equiv r \pmod q, \\ 0, & \textit{otherwise.} \end{cases}$$

Now we have:

Theorem 4.3. (I) *If $q \nmid a_1$, then we have under GRH that*

$$\Delta_a^{(0)}(q,h) = \frac{1}{q-1} - \frac{1}{(q-1)^2} \sum_{\chi \in \hat{G}} C_\chi \chi(-h) \biggl(1 + \eta_{\chi,a} \prod_{p|2a_1} \frac{p(\chi(p)-1)}{p^3 - p^2 - p + \chi(p)}\biggr).$$

(II) *If $q|a_1$, then we have under GRH that*

$$\Delta_a^{(0)}(q,h) = \frac{1}{q-1} - \frac{1}{(q-1)^2} \biggl[\sum_{\chi \in \hat{G}} C_\chi \biggl\{ \chi(-h) - \biggl(\chi(-h) + 2 \sum_r \chi(r)^{-1} \biggr) \eta_{\chi,a} \cdot \prod_{p|2\underline{a_1}} \frac{p(\chi(p)-1)}{p^3-p^2-p+\chi(p)} \biggr\} \biggr],$$

where $\sum_r$ means a sum over all r $(1 \le r \le q-1)$ such that $(\frac{hr+1}{q}) = 1$ and $\underline{a_1}$ is the q-free part of a_1 (i.e. $\underline{a_1} = a_1/q$).

Proof. We give a proof of (I) only, because we can prove (II) in a similar way. In this proof we abbreviate the sum $\sum_{k \ge 1,\, q\nmid k} \sum_{d|k_0} \sum_{n \ge 1,\, q \nmid n}$ into $\sum_k \sum_d \sum_n$ and let

$$A(k,d,n) = \frac{k_0}{\varphi(k_0)} \frac{\mu(d)}{d} \frac{\mu(n)}{kn\varphi(\langle kd, \underline{n} \rangle)}.$$

We define $s = a_1$ or $s = 4a_1$ according to $a_1 \equiv 1 \pmod 4$ or $a_1 \equiv 2, 3 \pmod 4$.

By Lemma 3.3, Theorem 3.4 and a method similar to Theorem 4.1, we obtain

$$(q-1)\Delta_a^{(0)}(q,h) = \biggl\{ \sum_k \sum_d \sum_n - \frac{1}{2} \sum_{\substack{k \\ k:\mathrm{odd}}} \sum_d \sum_{\substack{n \\ n:\mathrm{odd} \\ s|\langle kd,\underline{n}\rangle}} + \frac{1}{2} \sum_{\substack{k \\ k:\mathrm{even}}} \sum_d \sum_{\substack{n \\ n:\mathrm{odd} \\ s|\langle kd,\underline{n}\rangle}} - \biggl(\sum_{\substack{k \\ hr\equiv -1 \ (\mathrm{mod}\ q)}} \sum_d \sum_n - \frac{1}{2} \sum_{\substack{k \\ k:\mathrm{odd} \\ hr \equiv -1 \ (\mathrm{mod}\ q)}} \sum_d \sum_{\substack{n \\ n:\mathrm{odd} \\ s|\langle kd,\underline{n}\rangle}} + \frac{1}{2} \sum_{\substack{k \\ k:\mathrm{even} \\ hr\equiv -1 \ (\mathrm{mod}\ q)}} \sum_d \sum_{\substack{n \\ n:\mathrm{odd} \\ s|\langle kd,\underline{n}\rangle}} \biggr) \biggr\} A(k,d,n).$$

From Lemma 4.2, we have the following:

(a') When $a_1 \equiv 1 \pmod 4$,

$$(q-1)\Delta_a^{(0)}(q,h) = \sum_k \sum_d \sum_n A(k,d,n) - \frac{1}{q-1} \sum_{\chi \in \hat{G}} \chi(-h) \cdot \left\{ \sum_k \sum_d \sum_n + \left(\frac{3}{2} \sum_{j \geq 1} \left(\frac{\chi(2)}{4} \right)^j - \frac{1}{2} \right) \sum_{\substack{k \\ k:\text{odd}}} \sum_d \sum_{\substack{n \\ n:\text{odd} \\ s \mid \langle kd, \underline{n} \rangle}} \right\} \cdot \chi(k) A(k,d,n).$$

(b') When $a_1 \equiv 2 \pmod 4$,

$$(q-1)\Delta_a^{(0)}(q,h) = \sum_k \sum_d \sum_n A(k,d,n) - \frac{1}{q-1} \sum_{\chi \in \hat{G}} \chi(-h) \cdot \left\{ \sum_k \sum_d \sum_n + \frac{1}{2}(\chi(2)-1) \sum_{j \geq 3} \left(\frac{\chi(2)}{4} \right)^{j-1} \sum_{\substack{k \\ k:\text{odd}}} \sum_d \sum_{\substack{n \\ n:\text{odd} \\ s' \mid \langle kd, \underline{n} \rangle}} \right\} \cdot \chi(k) A(k,d,n),$$

where s' is the odd part of s.

(c') When $a_1 \equiv 3 \pmod 4$,

$$(q-1)\Delta_a^{(0)}(q,h) = \sum_k \sum_d \sum_n A(k,d,n) - \frac{1}{q-1} \sum_{\chi \in \hat{G}} \chi(-h) \cdot \left\{ \sum_k \sum_d \sum_n + \frac{1}{2}(\chi(2)-1) \sum_{j \geq 2} \left(\frac{\chi(2)}{4} \right)^{j-1} \sum_{\substack{k \\ k:\text{odd}}} \sum_d \sum_{\substack{n \\ n:\text{odd} \\ s' \mid \langle kd, \underline{n} \rangle}} \right\} \cdot \chi(k) A(k,d,n),$$

where s' is the odd part of s.

Now we can prove

$$\sum_k \sum_d \sum_n \chi(k) A(k,d,n) = C_\chi \tag{4.5}$$

(see Appendix for proof). Then

$$\sum_{\substack{k \\ k:\text{odd}}} \sum_d \sum_{\substack{n \\ n:\text{odd} \\ s \mid \langle kd, \underline{n} \rangle}} \chi(k) A(k,d,n) = \frac{4-\chi(2)}{2+\chi(2)} C_\chi \prod_{p \mid s} \frac{p(\chi(p)-1)}{p^3 - p^2 - p + \chi(p)}$$

(in the last formula, s should be replaced by s' when $a_1 \equiv 2, 3 \pmod 4$).

Combining these results we obtain the conclusion. □

5. Proof of Theorem 1.3.

In this section we sketch the proof of Theorem 1.3. First we state a lemma which is needed for the proof of (II).

Lemma 5.1. (i) *Let q be an odd prime. Then for all $e \geq 1$, we have*

$$\Delta_a(q^e, 0) = \frac{1}{q^{e-2}(q^2-1)}.$$

(ii) *If $a_1 \neq 2$, then for all $i \geq 1$, we have*

$$\Delta_a(2^i, 0) = \frac{1}{3 \cdot 2^{i-2}}.$$

If $a_1 = 2$, we have

$$\Delta_a(2, 0) = \frac{17}{24}, \quad \Delta_a(4, 0) = \frac{5}{12}$$

and for all $i \geq 3$,

$$\Delta_a(2^i, 0) = \frac{1}{3 \cdot 2^{i-1}}.$$

Proof. See Wiertelak [**12**]. A little weaker but simpler formulation can be found in [**1**, Theorem 1.1]. □

Proof of (I). When $q^i = 2^3$, we obtain $\Delta_a(8, 2) = \Delta_a(4, 3)$ and $\Delta_a(8, 6) = \Delta_a(4, 1)$ under GRH by direct calculation of the series (2.2). For other j, we can prove the recurrence relation by Method II of (II) below (see also the remark after Theorem 2.1).

Proof of (II). We employ two different methods.

Method I. Here we consider the case where q is an odd prime, $i \geq 2$ and $q|j$. In this case the value $\Delta_a(q^i, j)$ can be found directly, not via the recurrence relation stated in the theorem. Assume $q^e \parallel j$ ($e \geq 1$). First we note the following identity:

$$\Delta_a(q^e, 0) - \Delta_a(q^{e+1}, 0) = \sum_{\substack{1 \leq j \leq q^i - 1 \\ q^e \| j}} \Delta_a(q^i, j) \tag{5.1}$$

for $i \geq e + 1$. We have

$$\Delta_a(q^e, 0) - \Delta_a(q^{e+1}, 0) = \frac{1}{q^{e-1}(q+1)}$$

from Lemma 5.1 (i).

On the other hand, we can verify from Corollary 3.5 that all the summands in the right hand side of (5.1) have the same value. Indeed, the series in (2.2) becomes

$$\Delta_a(q^i, j) = \Delta_a(q^i, hq^e) = \sum_{\substack{1\le r<q^i \\ q\nmid r}} \sum_{f\ge e}\sum_{l\ge 0} \frac{k_0}{\varphi(k_0)} \sum_{d|k_0} \frac{\mu(d)}{d} \sum_{n=1}^{\infty} \frac{\mu(n)}{[\tilde{G}_{k,n,d} : \boldsymbol{Q}]} \tag{5.2}$$

where $k = \{(\overline{h}r) \pmod{q^{i-e}} + lq^{i-e}\}q^{f-e}$. If r runs through $1 \le r < q^i$, $(q, r) = 1$, then $(\overline{h}r) \pmod{q^{i-e}}$ takes each value in $\{y\ ;\ 1 \le y < q^{i-e}, (y, q) = 1\}$ exactly $q^e - 1$ times. This shows that (5.2) does not depend on h.

It follows that the quantity $\Delta_a(q^e, 0) - \Delta_a(q^{e+1}, 0)$ is divided equally among $\varphi(q^{i-e})$ summands in (5.1). Thus we have under GRH

$$\Delta_a(q^i, j) = \frac{1}{\varphi(q^{i-e})} \cdot \frac{1}{q^{e-1}(q+1)} = \frac{1}{q^{i-2}(q^2-1)}$$

for all j $(q|j)$.

The same method can be applied to the case $(q^i, j) = (2^i, j)$ where $i \ge 4$ and $8|j$ if we use Lemma 5.1 (ii) and Corollary 3.7:

Theorem 5.2. *We assume GRH. Let $i \ge 4$. If $a_1 \ne 2$, for all j with $8|j$, we have*

$$\Delta_a(2^i, j) = \frac{1}{3 \cdot 2^{i-2}}.$$

If $a_1 = 2$, for all j with $8|j$, we have

$$\Delta_a(2^i, j) = \frac{1}{3 \cdot 2^{i-1}}$$

(the case $(2^i, j) = (16, 8)$ is unconditional, cf. the remark after Theorem 2.1).

When $i \ge 4$ and $4 \parallel j$, a slightly more delicate but similar argument yields the following result:

Theorem 5.3. *We assume GRH. Let $i \ge 4$ and $4 \parallel j$. Then we have*

$$\Delta_a(2^i, j) = \begin{cases} \dfrac{1}{3 \cdot 2^{i-3}}, & \text{if } a_1 = 2, \\[2ex] \dfrac{1}{3 \cdot 2^{i-2}}, & \text{otherwise.} \end{cases}$$

Method II. Next we consider the case $j = h$ where q is an odd prime, $i \ge 2$ and $q \nmid h$. We assume $q \nmid a_1$ (the case $q|a_1$ is similar).

From (2.2), the partial sums for $f \ge 1$ becomes

$$\Delta_a^{(1)}(q^i,h)=\sum_{\substack{1\le r<q^i\\ q\nmid r}}\sum_{l\ge 0}\sum_{f\ge 1}\frac{k_0}{\varphi(k_0)}\sum_{d|k_0}\frac{\mu(d)}{d}\sum_{n=1}^{\infty}\frac{\mu(n)c_r(k,n,d)}{[\tilde{G}_{k,n,d}:\boldsymbol{Q}]}, \tag{5.3}$$

$$\Delta_a^{(1)}(q^{i-1},h')=\sum_{\substack{1\le r<q^{i-1}\\ q\nmid r}}\sum_{l\ge 0}\sum_{f\ge 1}\frac{k_0'}{\varphi(k_0')}\sum_{d|k_0'}\frac{\mu(d)}{d}\sum_{n=1}^{\infty}\frac{\mu(n)c_r(k',n,d)}{[\tilde{G}_{k',n,d}:\boldsymbol{Q}]}, \tag{5.4}$$

where $h'\equiv h \pmod{q^{i-1}}$, $k=\{(\overline{h}r) \pmod{q^i}+lq^i\}q^f$ and $k'=\{(\overline{h'}r) \pmod{q^{i-1}}+lq^{i-1}\}q^f$.

The degree $[\tilde{G}_{k,n,d}:\boldsymbol{Q}]$ in (5.3) equals

$$\varepsilon kn\varphi(\langle kd,n,q^{f+i}\rangle)=q\cdot\varepsilon kn\varphi(\langle kd,n,q^{f+i-1}\rangle), \quad (\varepsilon=1 \text{ or } 1/2)$$

which always coincides with q times $[\tilde{G}_{k',n,d}:\boldsymbol{Q}]$ in (5.4), since the parity of kn and the divisibility condition (*cf.* Lemma 3.3) remain unchanged:

$$s|\langle kd,n,q^{f+i}\rangle \Leftrightarrow s|\langle kd,n,q^{f+i-1}\rangle. \quad (s=a_1 \text{ or } 4a_1).$$

Next we can easily verify that the numbers $\underline{k}=k/q^f$ and $\underline{k'}=k'/q^f$ run through the same range, then the sums with respect to r and l in (5.3) and (5.4) both turn out to be $\sum_{\underline{k}\ge 1,\, q\nmid \underline{k}}$.

Hence we have $\Delta_a^{(1)}(q^i,h)=\Delta_a^{(1)}(q^{i-1},h')/q$.

We can prove the same formula for $\Delta_a^{(0)}(q^i,h)=\Delta_a(q^i,h)-\Delta_a^{(1)}(q^i,h)$ similarly, then obtain the conclusion.

A similar machinery works for the following cases:

$$\Delta_a(2^i,h) \qquad (i\ge 3,\ h:\text{odd}),$$
$$\Delta_a(2^i,j) \qquad (i\ge 4,\ 2\parallel j).$$

6. Numerical Examples.

In this section we show some numerical examples (both theoretical and experimental) of the densities $\Delta_a(q^i,j)$.

6.1. Odd Prime Moduli.

We take $q=5$. For the values of C_χ, see (1.2).

Example 6.1. We take $a=13$. Let us compare the "theoretical densities" (table 4) and "experimental densities" (table 5). As the experimental densities, we use the value $\sharp Q_a(x;5,j)/\pi(x)$ with $x=179424673$ (the first 10^7 primes).

Example 6.2. We take $a=5$, $\underline{a_1}=1$. Then, under GRH, we have theoretically,

Table 4. Theoretical values of $\varDelta_a(5,j)$.

a	$j=0$	$j=1$	$j=2$	$j=3$	$j=4$
13	0.208333	0.235543	0.178356	0.234475	0.143292
21	0.208333	0.235494	0.176925	0.233715	0.145532
2	0.208333	0.240605	0.178686	0.229270	0.143106
14	0.208333	0.235235	0.177947	0.234248	0.144237
3	0.208333	0.238076	0.169818	0.235252	0.148521
7	0.208333	0.236323	0.177549	0.233657	0.144139

Table 5. Experimental values of $\varDelta_a(5,j)$.

a	$j=0$	$j=1$	$j=2$	$j=3$	$j=4$
13	0.208290	0.235644	0.178338	0.234455	0.143274
21	0.208355	0.235556	0.176819	0.233788	0.145483
2	0.208334	0.240509	0.178770	0.229434	0.142952
14	0.208359	0.235345	0.177819	0.234200	0.144276
3	0.208339	0.238149	0.169796	0.235340	0.148377
7	0.208388	0.236100	0.177606	0.233777	0.144128

$$\begin{aligned}\varDelta_5(5,1) &= \frac{25}{96} - \frac{1}{16}\{1 - 3C_{\chi_1} + (1+2\sqrt{-1})C_{\chi_2} + (1-2\sqrt{-1})C_{\chi_3}\}\\ &\approx 0.232661,\end{aligned}$$

$$\begin{aligned}\varDelta_5(5,2) &= \frac{25}{96} - \frac{1}{16}\{1 + 3C_{\chi_1} - (2-\sqrt{-1})C_{\chi_2} - (2+\sqrt{-1})C_{\chi_3}\}\\ &\approx 0.292699,\end{aligned}$$

$$\begin{aligned}\varDelta_5(5,3) &= \frac{25}{96} - \frac{1}{16}\{1 + 3C_{\chi_1} + (2-\sqrt{-1})C_{\chi_2} + (2+\sqrt{-1})C_{\chi_3}\}\\ &\approx 0.054644,\end{aligned}$$

$$\begin{aligned}\varDelta_5(5,4) &= \frac{25}{96} - \frac{1}{16}\{1 - 3C_{\chi_1} - (1+2\sqrt{-1})C_{\chi_2} - (1-2\sqrt{-1})C_{\chi_3}\}\\ &\approx 0.211663.\end{aligned}$$

The following Tables 6 and 7 show the comparison of theoretical values of $\varDelta_a(5,j)$ with their experimental values.

6.2. Higher Power Moduli.

Here we show some results of computer experiments on $\varDelta_a(q^i,j)$ $(i \geq 2)$ to observe the phenomenon $\varDelta_a(q^i,j) = \frac{1}{q}\varDelta_a(q^{i-1},j)$.

The following tables show the experimental densities $\sharp Q_a(x;5^2,j)/\pi(x)$ with $x = 179424673$. We know all their theoretical densities from Tables 4, 6 and Theorem 1.3 (II). Examining the following tables, we verify the above relation numerically.

Table 6. Theoretical values of $\Delta_a(5, j)$.

a	$j=0$	$j=1$	$j=2$	$j=3$	$j=4$
5	0.208333	0.232661	0.292699	0.054644	0.211663
10	0.208333	0.239555	0.166783	0.241173	0.144156
30	0.208333	0.236025	0.181032	0.232697	0.141913
15	0.208333	0.230120	0.180710	0.224360	0.156478

Table 7. Experimental values of $\Delta_a(5, j)$ with $x = 179424673$.

a	$j=0$	$j=1$	$j=2$	$j=3$	$j=4$
5	0.208356	0.232685	0.292800	0.054449	0.211710
10	0.208358	0.239664	0.166742	0.241154	0.144082
30	0.208296	0.236104	0.181086	0.232714	0.141800
15	0.208341	0.230307	0.180646	0.224381	0.156325

$a = 2$

$j=0$	$j=1$	$j=2$	$j=3$	$j=4$	$j=5$	$j=6$	$j=7$	$j=8$	$j=9$
0.041681	0.048136	0.035808	0.045871	0.028601	0.041675	0.048085	0.035785	0.045928	0.028616
$j=10$	$j=11$	$j=12$	$j=13$	$j=14$	$j=15$	$j=16$	$j=17$	$j=18$	$j=19$
0.041641	0.048126	0.035732	0.045811	0.028565	0.041690	0.048125	0.035697	0.045834	0.028591
$j=20$	$j=21$	$j=22$	$j=23$	$j=24$					
0.041648	0.048038	0.035749	0.045991	0.028579					

$a = 3$

$j=0$	$j=1$	$j=2$	$j=3$	$j=4$	$j=5$	$j=6$	$j=7$	$j=8$	$j=9$
0.041641	0.047685	0.033986	0.047026	0.029693	0.041696	0.047582	0.033967	0.047093	0.029713
$j=10$	$j=11$	$j=12$	$j=13$	$j=14$	$j=15$	$j=16$	$j=17$	$j=18$	$j=19$
0.041647	0.047604	0.033958	0.047095	0.029695	0.041733	0.047666	0.033949	0.047060	0.029600
$j=20$	$j=21$	$j=22$	$j=23$	$j=24$					
0.041621	0.047612	0.033936	0.047066	0.029676					

$a = 5$

$j=0$	$j=1$	$j=2$	$j=3$	$j=4$	$j=5$	$j=6$	$j=7$	$j=8$	$j=9$
0.041645	0.046523	0.058576	0.010876	0.042363	0.041712	0.046593	0.058550	0.010871	0.042389
$j=10$	$j=11$	$j=12$	$j=13$	$j=14$	$j=15$	$j=16$	$j=17$	$j=18$	$j=19$
0.041678	0.046492	0.058554	0.010918	0.042290	0.041632	0.046549	0.058538	0.010899	0.042301
$j=20$	$j=21$	$j=22$	$j=23$	$j=24$					
0.041690	0.046528	0.058582	0.010886	0.042367					

$a = 10$

$j=0$	$j=1$	$j=2$	$j=3$	$j=4$	$j=5$	$j=6$	$j=7$	$j=8$	$j=9$
0.041657	0.048004	0.033357	0.048235	0.028830	0.041650	0.047946	0.033342	0.048316	0.028824
$j=10$	$j=11$	$j=12$	$j=13$	$j=14$	$j=15$	$j=16$	$j=17$	$j=18$	$j=19$
0.041741	0.047961	0.033369	0.048190	0.028822	0.041652	0.047869	0.033325	0.048194	0.028812
$j=20$	$j=21$	$j=22$	$j=23$	$j=24$					
0.041659	0.047883	0.033350	0.048219	0.028792					

Next we see the case $\Delta_a(2^i, j)$ for $i = 2, 3, 4$. When $i = 3$, we find the *break* of the local equi-distribution (written in bold face), on the contrary, when $i = 4$, we confirm the local equi-distribution property as in the case $q^i = 5^2$. For the theoretical densities $\Delta_a(4, j)$, the reader is referred to Sections 1 and 2 of [**6**].

$a = 2, i = 2$

$j = 0$	$j = 1$	$j = 2$	$j = 3$
0.416669	0.065372	0.291650	0.226309

$a = 2, i = 3$

$j = 0$	$j = 1$	$j = 2$	$j = 3$	$j = 4$	$j = 5$	$j = 6$	$j = 7$
0.083335	0.032733	**0.226335**	0.113143	**0.333334**	0.032640	**0.065315**	0.113166

$a = 2, i = 4$

$j = 0$	$j = 1$	$j = 2$	$j = 3$	$j = 4$	$j = 5$	$j = 6$	$j = 7$
0.041643	0.016356	0.113147	0.056497	0.166697	0.016317	0.032617	0.056562
$j = 8$	$j = 9$	$j = 10$	$j = 11$	$j = 12$	$j = 13$	$j = 14$	$j = 15$
0.041691	0.016377	0.113188	0.056645	0.166638	0.016322	0.032698	0.056604

$a = 5, i = 2$

$j = 0$	$j = 1$	$j = 2$	$j = 3$
0.333346	0.166743	0.333298	0.166613

$a = 5, i = 3$

$j = 0$	$j = 1$	$j = 2$	$j = 3$	$j = 4$	$j = 5$	$j = 6$	$j = 7$
0.166730	0.083405	0.166543	0.083284	0.166616	0.083338	0.166754	0.083329

$a = 5, i = 4$

$j = 0$	$j = 1$	$j = 2$	$j = 3$	$j = 4$	$j = 5$	$j = 6$	$j = 7$
0.083341	0.041719	0.083250	0.041605	0.083335	0.041677	0.083369	0.041584
$j = 8$	$j = 9$	$j = 10$	$j = 11$	$j = 12$	$j = 13$	$j = 14$	$j = 15$
0.083389	0.041687	0.083293	0.041679	0.083282	0.041661	0.083386	0.041745

$a = 10, i = 2$

$j = 0$	$j = 1$	$j = 2$	$j = 3$
0.333378	0.166623	0.333356	0.166644

$a = 10, i = 3$

$j=0$	$j=1$	$j=2$	$j=3$	$j=4$	$j=5$	$j=6$	$j=7$
0.166707	0.083309	0.166710	0.083324	0.166671	0.083314	0.166646	0.083320

$a = 10, i = 4$

$j=0$	$j=1$	$j=2$	$j=3$	$j=4$	$j=5$	$j=6$	$j=7$
0.083345	0.041666	0.083309	0.041629	0.083319	0.041675	0.083354	0.041672
$j=8$	$j=9$	$j=10$	$j=11$	$j=12$	$j=13$	$j=14$	$j=15$
0.083362	0.041643	0.083401	0.041694	0.083352	0.041639	0.083292	0.041648

Appendix. Proofs of (4.3) and (4.5).

Here we give a proof of (4.5). In Section 4, there are many other triple sums with respect to k, d and n. All these are variants of (4.5) and are estimated similarly (the reader is also referred to [**1**, Section 5]).

Let

$$S_\chi = \sum_{\substack{k\ge1\\ q\nmid k}} \sum_{d\mid k_0} \sum_{\substack{n\ge1\\ q\nmid n}} \chi(k)A(k,d,n).$$

Note that $\underline{n} = n$. The series

$$\sum_{d\mid k_0} \frac{\mu(d)}{d} \sum_{\substack{n\ge1\\ q\nmid n}} \frac{\mu(n)}{n\varphi(\langle kd, n\rangle)}$$

are absolutely convergent since $\sum_{n\ge1} 1/n\varphi(n)$ converges (see Prachar [**9**, Satz 5.1]). So we have

$$S_\chi = \sum_{\substack{k\ge1\\ q\nmid k}} \frac{\chi(k)k_0}{\varphi(k_0)k} \sum_{\substack{n\ge1\\ q\nmid n}} \frac{\mu(n)}{n} \sum_{d\mid k_0} \frac{\mu(d)}{d\varphi(\langle kd, n\rangle)}.$$

Putting $k = \prod_{i=1}^t q_i^{e_i}$ (q_i: prime, $q_i \ne q$) and $d = \prod_{i=1}^t q_i^{\varepsilon_i}$ ($\varepsilon_i = 0, 1$), we have

$$S_\chi = \sum_{\substack{k\ge1\\ q\nmid k}} \frac{\chi(k)k_0}{\varphi(k_0)k} \sum_{\substack{n\ge1\\ q\nmid n}} \frac{\mu(n)}{n} \prod_{\substack{p\mid \underline{n}\\ p\ne q_i}} \frac{1}{p-1} \sum_{d\mid k_0} \frac{\mu(d)}{d\varphi(kd)}.$$

Since the function $h_1(d) := \varphi(kd)/\varphi(k)$ is multiplicative, we have

$$S_\chi = \sum_{\substack{k\ge 1\\ q\nmid k}} \frac{\chi(k)k_0}{\varphi(k_0)k} \sum_{\substack{n\ge 1\\ q\nmid n}} \frac{\mu(n)}{n} \prod_{\substack{p|\underline{n}\\ p\ne q_i}} \frac{1}{p-1}\frac{1}{\varphi(k)} \prod_{i=1}^{t}\left(1-\frac{1}{q_i h_1(q_i)}\right)$$

$$= \sum_{\substack{k\ge 1\\ q\nmid k}} \frac{\chi(k)k_0}{\varphi(k_0)k} \prod_{i=1}^{t} \frac{q_i+1}{q_i^{e_i+1}} \sum_{\substack{n\ge 1\\ q\nmid n}} \frac{\mu(n)}{n} \prod_{\substack{p|\underline{n}\\ p\ne q_i}} \frac{1}{p-1}.$$

Let $h_2(n) = \prod_{p|n,\, p\ne q_i}(p-1)$. Then it is multiplicative and for a prime p,

$$h_2(p) = \begin{cases} 1, & \text{if } p = q_i, \\ p-1, & \text{otherwise.} \end{cases}$$

So we have

$$S_\chi = \sum_{\substack{k\ge 1\\ q\nmid k}} \frac{\chi(k)k_0}{\varphi(k_0)k} \prod_{i=1}^{t} \frac{q_i+1}{q_i^{e_i+1}} \prod_{p\ne q, q_i}\left(1-\frac{1}{p(p-1)}\right) \prod_{i=1}^{t}\left(1-\frac{1}{q_i}\right)$$

$$= \prod_{p\ne q}\left(1-\frac{1}{p(p-1)}\right) \sum_{\substack{k\ge 1\\ q\nmid k}} \chi(k) \prod_{i=1}^{t} \frac{(q_i+1)(q_i-1)}{q_i^{2e_i}(q_i^2-q_i-1)}.$$

Since the function

$$h_3(k) = \left\{\prod_{i=1}^{t} \frac{(q_i+1)(q_i-1)}{q_i^{2e_i}(q_i^2-q_i-1)}\right\}^{-1}$$

is multiplicative, we have

$$S_\chi = \prod_{p\ne q}\left(1-\frac{1}{p(p-1)}\right)\left(1+\frac{\chi(p)}{h_3(p)}+\frac{\chi(p^2)}{h_3(p^2)}+\cdots\right)$$

$$= \prod_{p\ne q}\left(1-\frac{1}{p(p-1)}\right)\left\{1+\frac{(p+1)(p-1)}{p^2-p-1}\sum_{j=1}^{\infty}\left(\frac{\chi(p)}{p^2}\right)\right\}$$

$$= \prod_{p\ne q}\left(1-\frac{1}{p(p-1)}\right)\left(1+\frac{(p+1)(p-1)}{p^2-p-1}\frac{\chi(p)}{p^2-\chi(p)}\right).$$

We get (4.5) from this formula and (4.3) for $\chi = 1$.

References

[1] K. Chinen and L. Murata, On a distribution property of the residual order of a (mod p), J. Number Theory, **105** (2004), 60–81.

[2] K. Chinen and L. Murata, On a distribution property of the residual order of a (mod p), II, In: Proceedings of the Conference "New Aspects of Analytic Number Theory", held at Kyoto University, November 26–30, 2001, RIMS Kokyuroku, **1274** (2002), 62–69.

[3] K. Chinen and L. Murata, On a distribution property of the residual order of a (mod p) — IV, In: Proceedings of the Conference "Analytic Number Theory and Surrounding Areas" held at Kyoto University, September 29–October 3, 2003, RIMS Kokyuroku, **1384** (2004), 169–174.

[4] H. Hasse, Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von durch eine vorgegebene Primzahl $l \neq 2$ teilbarer bzw. unteilbarer Ordnung mod p ist, Math. Ann., **162** (1965), 74–76.

[5] H. Hasse, Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von gerader bzw. ungerader Ordnung mod p ist, Math. Ann., **166** (1966), 19–23.

[6] L. Murata, and K. Chinen, On a distribution property of the residual order of a (mod p) — II, J. Number Theory, **105** (2004), 82–100.

[7] L. Murata, and K. Chinen, On a distribution property of the residual order of a (mod p), III, In: Proceedings of the Conference "Diophantine Problems and Analytic Number Theory", held at Kyoto University, October 21–25, 2002, RIMS Kokyuroku, **1319** (2003), 139–147.

[8] R. W. K. Odoni, A conjecture of Krishnamurthy on decimal periods and some allied problems, J. Number Theory, **13** (1981), 303–319.

[9] K. Prachar, Primzahlverteilung, Springer, 1957.

[10] J.-P. Serre, Quelques applications du théorème de densité de Chebotarev, Publ. Math. Inst. Hautes Études Sci., **54** (1981), 323–401.

[11] K. Wiertelak, On the density of some sets of primes, I, Acta Arith., **34** (1978), 183–196.

[12] K. Wiertelak, On the density of some sets of primes, IV, Acta Arith., **43** (1984), 177–190.

Koji Chinen
Department of Mathematics, Faculty of Engineering
Osaka Institute of Technology
Omiya, Asahi-ku, Osaka 535-8585
Japan
E-mail: YHK03302@nifty.ne.jp

Leo Murata
Department of Mathematics, Faculty of Economics
Meiji Gakuin University
1-2-37 Shirokanedai
Minato-ku, Tokyo 108-8636
Japan
E-mail: leo@eco.meijigakuin.ac.jp