ON A DISTRIBUTION PROPERTY OF THE RESIDUAL ORDER OF a (mod pq)

Leo Murata (Tokyo, Japan)

Koji Chinen (Higashi-Osaka, Japan)

Dedicated to Professors Zoltán Daróczy and Imre Kátai on their 75th anniversary

Communicated by Pavel Varbanets

(Received June 04, 2013; accepted June 24, 2013)

Abstract. In the authors' previous papers, for a positive integer a and a prime number p such that $(a, p) = 1$, the distribution of the residual orders $D_a(p)$ of a (mod p) was considered. Under the generalized Riemann hypothesis (GRH), the authors determined the natural density of the primes p satisfying $D_a(p) \equiv l \pmod{k}$ when k is a prime power, and proved the existence of an algorithm for computing the density when k is a composite integer other than prime powers. In this paper, we consider the distribution of the residual orders $D_a(pq)$ of a (mod pq) where p and q are distinct primes. Under GRH and some slight restriction to the base a, we determine the natural density of the prime pairs (p, q) satisfying $D_a(pq) \equiv l$ (mod 4) for $l = 0, 1, 2, 3$.

1. Introduction

Let p be an odd prime number and $\mathbf{Z}/p\mathbf{Z}^\times$ be the multiplicative group of all invertible residue classes modulo p. We define

$$D_a(p) := \left(\begin{array}{l} \text{the multiplicative order of the residue} \\ \text{class } a \pmod{p} \text{ in the group } \mathbf{Z}/p\mathbf{Z}^\times \end{array} \right).$$

Key words and phrases: Residual order, Artin's conjecture for primitive root.
2010 Mathematics Subject Classification: 11N05, 11N25, 11R18.
https://doi.org/10.71352/ac.41.187

In the papers [1] – [3] and [7], we are interested in a distribution property of $D_a(p)$ with p varies and introduced the set, for an arbitrary residue class $l \pmod{k}$,

$$Q_a(x;k,l) := \{p \leq x \ ; \ p: \text{ prime}, \ D_a(p) \equiv l \pmod{k}\}.$$

We studied about the existence of the natural density of $Q_a(x;k,l)$:

$$\Delta_a(k,l) = \lim_{x\to\infty} \frac{1}{\pi(x)} \sharp Q_a(x;k,l),$$

where $\pi(x)$ is the number of primes up to x. We proved that

1. We can prove the existence of the density $\Delta_a(k,l)$, for any residue class $l \pmod{k}$,

2. and in this proof, except for some special residue classes, we need Generalized Riemann Hypothesis.

3. We can calculate the exact value of the density $\Delta_a(k,l)$.

Our typical example is:

Theorem 1.1. *Let a be a natural number and we decompose a into $a = a_0^2 a_1$, a_1 is square-free. If a_1 is odd, then we have*

$$\Delta_a(4,0) = \Delta_a(4,2) = \frac{1}{3}, \tag{1.1}$$

$$\Delta_a(4,1) = \Delta_a(4,3) = \frac{1}{6}, \tag{1.2}$$

where we obtain (1.1) *unconditionally and* (1.2) *under GRH* (*see* [1] *and* [7] *for details*).

Here GRH means

Hypothesis 1.2. (Generalized Riemann Hypothesis) *For any positive integers k and m, we assume that the Riemann Hypothesis holds for the Dedekind zeta function $\zeta_K(s)$ for the field $K = \mathbf{Q}(\zeta_m, a^{1/k})$ where $\zeta_m = \exp(2\pi i/m)$.*

Now let p and q be two distinct prime numbers and let us consider the same distribution property of the residue class of a, but in the multiplicative group $\mathbf{Z}/pq\mathbf{Z}^\times$. The group $\mathbf{Z}/p\mathbf{Z}^\times$ is a simple cyclic group, but $\mathbf{Z}/pq\mathbf{Z}^\times$ is no more cyclic.

We are interested in the order of the residue class itself, namely we define

$$D_a(pq) := \left(\begin{array}{c} \text{the multiplicative order of the residue} \\ \text{class } a \pmod{pq} \text{ in the group } \mathbf{Z}/pq\mathbf{Z}^\times \end{array} \right) = \sharp\langle a \pmod{pq}\rangle.$$

and

$$R_a(x;k,l) := \{(p,q)\ ;\ p,q:\ \text{odd primes},\ p \le x,\ q \le x,\ D_a(pq) \equiv l \pmod{k}\}.$$

The purpose of the paper is

1. to prove the existence of the natural density $\varGamma_a(4,l)$ for $l = 0,1,2,3$,
2. and to calculate the explicit value of $\varGamma_a(4,l)$,

where the natural density means

$$\varGamma_a(k,l) := \lim_{x\to\infty} \pi(x)^{-2} \sharp R_a(x;k,l).$$

Our main theorem will be

Theorem 1.3. *Let a be a natural number and we decompose a into $a = a_0^2 a_1$, a_1 is square-free. If a_1 is odd, then we have*

(I) *the natural densities $\varGamma_a(4,l)$, $l = 0,1,2,3$ exist*

(II) *and the standard distribution is*

$$(\varGamma_a(4,0),\ \varGamma_a(4,1),\ \varGamma_a(4,2),\ \varGamma_a(4,3)) = \left(\frac{5}{9},\ \frac{1}{18},\ \frac{1}{3},\ \frac{1}{18}\right).$$

Moreover, for the existence of $\varGamma_a(4,1)$ and $\varGamma_a(4,3)$, we need GRH, whereas the existence of $\varGamma_a(4,0)$ and $\varGamma_a(4,2)$ is unconditional.

This theorem shows that, despite the change of group structure, as to the multiplicative order of a residue class, we can prove a similar result to Theorem 1.1. It is quite likely that there exists the density $\varGamma_a(k,l)$ for any residue class $l \pmod{k}$, but we cannot verify this so far.

As we describe in the next section, we can prove unconditionally from Theorem 1.1 that,

$$\varGamma_a(4,0) = \frac{5}{9}, \quad \varGamma_a(4,2) = \frac{1}{3}.$$

So the main interest of Theorem 1.3 is the equi-distribution property

$$\varGamma_a(4,1) = \varGamma_a(4,3) = \frac{1}{18},$$

and to prove this we need GRH and difficult considerations so far.

Throughout this paper, we use the following notations: $\pi(x;k,l)$ is the number of prime numbers up to x which are congruent to l mod k, $\varphi(n)$ means Euler's totient function, $\mu(n)$ is the Möbius function, $\omega(n)$ means the number of distinct prime factors of n, $\langle a_1, a_2, \cdots, a_i\rangle$ means the least common multiple of integers $a_1, a_2, \cdots, a_i$ and (a,b) is the largest common divisor of integers a and b.

2. $R_a(x;k,l)$ with $l=0$

In this section, we study the set

$$R_a(x;k,0)=\{(p,q)\ ;\ p,q:\ \text{odd primes},\ p\le x,\ q\le x,\ D_a(pq)\equiv 0 \pmod{k}\}.$$

The next lemma is useful in decomposing our problem about (mod pq) into problems about (mod p) and (mod q) (we omit the proof).

Lemma 2.1. *We have*

$$D_a(pq)=\langle D_a(p),D_a(q)\rangle. \tag{2.1}$$

If $D_a(pq)\equiv 0 \pmod 4$ then Lemma 2.1 shows that one of the $D_a(p)$ and $D_a(q)$ is congruent to 0 modulo 4. This means

$$\begin{aligned}\sharp R_a(x;4,0) &= 2\,\sharp\{p\le x; D_a(p)\equiv 0 \pmod 4\}-\\ &- \sharp\{p,q\le x; D_a(p)\equiv 0 \pmod 4,\ D_a(q)\equiv 0 \pmod 4\}.\end{aligned}$$

Then Theorem 1.1 gives $\mathit{\Gamma}_a(4,0)=5/9$ directly, similarly $\mathit{\Gamma}_a(2,0)=8/9$, and $\mathit{\Gamma}_a(4,2)=1/3$.

Remark. We can prove a little more general result. Here we take a "base" $a\in\mathbf{N}$. We put

$$a=a_0^2\cdot a_1,\quad a_1\text{: square free}$$

and let r be a prime number. When a_1 is odd,

$$\mathit{\Gamma}_a(r^h,0)=\begin{cases}\dfrac{1}{(r^2-1)^2}r(2r^2-r-2), & \text{if } h=1,\\[2ex] \dfrac{2r^h-2r^{h-2}-1}{r^{2(h-2)}(r^2-1)^2}, & \text{if } h\ge 2.\end{cases}$$

For example, for the same a, $\mathit{\Gamma}_a(2,0)=8/9$, $\mathit{\Gamma}_a(3,0)=39/64$.

3. $R_a(x;4,l)$, the case of $l=1,3$ (I)

As we described in the previous section, we can calculate $\sharp R_a(x;2,0)$, $\sharp R_a(x;4,0)$ and consequently $\sharp R_a(x;4,2)$. But the separation of $R_a(x;2,1)$ into $R_a(x;4,1)$ and $R_a(x;4,3)$ is rather difficult. We begin with reducing $\sharp R_a(x;4,1)$ to an infinite sum of $\sharp Q_a(x;k,l)$'s. The purpose of this section is the following formulas (3.1) and (3.2).

Proposition 3.1. *We have*

$$\begin{aligned}\sharp R_a(x;4,1) &= \sharp Q_a(x;4,1)^2 + \sharp Q_a(x;4,3)^2 + \\ &+ \sum_{\substack{D<x \\ D\equiv 1 \pmod 4 \\ D_0=1, D_1>1}} 2^{\omega(D_1)-1}\left(\sharp Q_a(x;4D,D) - \sharp Q_a(x;4D,3D)\right)^2 - \\ &- \sum_{\substack{D<x \\ D\equiv 3 \pmod 4 \\ D_0=1, D_1>1}} 2^{\omega(D_1)-1}\left(\sharp Q_a(x;4D,D) - \sharp Q_a(x;4D,3D)\right)^2, \end{aligned} \tag{3.1}$$

where $D = D_0D_1$*, all the prime factors of* D_0 *are congruent to* 1 mod 4 *and all the prime factors of* D_1 *are congruent to* 3 mod 4*. We have similarly*

$$\begin{aligned}\sharp R_a(x;4,3) &= 2\cdot\sharp Q_a(x;4,1)\sharp Q_a(x;4,3) - \\ &- \sum_{\substack{D<x \\ D\equiv 1 \pmod 4 \\ D_0=1, D_1>1}} 2^{\omega(D_1)-1}\left(\sharp Q_a(x;4D,D) - \sharp Q_a(x;4D,3D)\right)^2 + \\ &+ \sum_{\substack{D<x \\ D\equiv 3 \pmod 4 \\ D_0=1, D_1>1}} 2^{\omega(D_1)-1}\left(\sharp Q_a(x;4D,D) - \sharp Q_a(x;4D,3D)\right)^2. \end{aligned} \tag{3.2}$$

Proof. Here we prove only (3.1). By a simple equality

$$D_a(pq) = D_a(p)\frac{D_a(q)}{(D_a(p), D_a(q))},$$

we divide the condition

$$D_a(pq) \equiv 1 \pmod 4$$

into two cases:

(I) $D_a(p) \equiv 1 \pmod 4$ and $\dfrac{D_a(q)}{(D_a(p), D_a(q))} \equiv 1 \pmod 4$.

(II) $D_a(p) \equiv 3 \pmod 4$ and $\dfrac{D_a(q)}{(D_a(p), D_a(q))} \equiv 3 \pmod 4$.

First we consider (I).

$$\sum_{\substack{p,q\le x \\ D_a(pq)\equiv 1 \pmod 4 \\ D_a(p)\equiv 1 \pmod 4}} 1 = \sum_{\substack{p\le x \\ D_a(p)\equiv 1 \pmod 4}} \sum_{\substack{q\le x \\ \frac{D_a(q)}{(D_a(p),D_a(q))}\equiv 1 \pmod 4}} 1. \tag{3.3}$$

For a prime number p with $D_a(p) \equiv 1 \pmod 4$, we calculate the inner sum of (3.3). Let us introduce the number

$$Q = (D_a(p), D_a(q)).$$

Then

$$\begin{aligned}
\text{(the inner sum of (3.3))} &= \sum_{Q|D_a(p)} \sum_{\substack{q\le x \\ Q=(D_a(p),D_a(q)) \\ D_a(q)/Q\equiv 1 \pmod 4}} 1 = \\
&= \sum_{Q|D_a(p)} \sum_{Q'|\frac{D_a(p)}{Q}} \mu(Q') \sum_{\substack{q\le x \\ QQ'|D_a(q) \\ D_a(q)/Q\equiv 1 \pmod 4}} 1.
\end{aligned}$$

Since all the numbers $D_a(p)$, Q and Q' are odd,

$$D_a(q)/Q \equiv 1 \pmod 4 \Leftrightarrow D_a(q) \equiv Q \pmod{4Q}. \tag{3.4}$$

We introduce the number $\overline{Q'}$ by

$$\overline{Q'} = \begin{cases} 1, & \text{if } Q' \equiv 1, \pmod 4, \\ 3, & \text{if } Q' \equiv 3, \pmod 4. \end{cases} \tag{3.5}$$

Then

$$\begin{cases} D_a(q) \equiv Q \pmod{4Q} \\ D_a(q) \equiv 0 \pmod{QQ'} \end{cases} \Leftrightarrow D_a(q) \equiv \overline{Q'} \cdot QQ' \pmod{4QQ'}.$$

Consequently,

$$\text{(the inner sum of (3.3))} = \sum_{Q|D_a(p)} \sum_{Q'|\frac{D_a(p)}{Q}} \mu(Q') \sum_{\substack{q\le x \\ D_a(q)\equiv\overline{Q'}QQ' \pmod{4QQ'}}} 1.$$

Then (3.3) turns into:

$$\sum_{\substack{p,q\le x\\ D_a(pq)\equiv 1 \pmod 4\\ D_a(p)\equiv 1 \pmod 4}} 1 =$$

$$= \sum_{\substack{p\le x\\ D_a(p)\equiv 1 \pmod 4}} \sum_{Q|D_a(p)} \sum_{Q'|\frac{D_a(p)}{Q}} \mu(Q') \sum_{\substack{q\le x\\ D_a(q)\equiv \overline{Q'}QQ' \pmod{4QQ'}}} 1 =$$

$$= \sum_{\substack{Q<x\\ Q:\text{odd}}} \sum_{\substack{p\le x\\ D_a(p)\equiv 1 \pmod 4\\ Q|D_a(p)}} \sum_{Q'|\frac{D_a(p)}{Q}} \mu(Q') \sum_{\substack{q\le x\\ D_a(q)\equiv \overline{Q'}QQ' \pmod{4QQ'}}} 1 =$$

$$= \sum_{\substack{Q<x\\ Q:\text{odd}}} \sum_{\substack{Q'<x\\ Q':\text{odd}\\ QQ'<x}} \mu(Q') \sum_{\substack{p\le x\\ D_a(p)\equiv 1 \pmod 4\\ D_a(p)\equiv 0 \pmod Q\\ Q'|\frac{D_a(p)}{Q}}} \sum_{\substack{q\le x\\ D_a(q)\equiv \overline{Q'}QQ' \pmod{4QQ'}}} 1.$$

We put $QQ'=D$, then D is odd and consequently,

$$(3.3) = \sum_{\substack{D<x\\ D:\text{odd}}} \sum_{Q'|D} \mu(Q') \sum_{\substack{p\le x\\ D_a(p)\equiv 1 \pmod 4\\ D_a(p)\equiv 0 \pmod D}} \sum_{\substack{q\le x\\ D_a(q)\equiv \overline{Q'}D \pmod{4D}}} 1. \tag{3.6}$$

When $D\equiv 1 \pmod 4$, then

$$\begin{cases} D_a(p)\equiv 1 \pmod 4\\ D_a(p)\equiv 0 \pmod D\end{cases} \Leftrightarrow D_a(p)\equiv D \pmod{4D},$$

and when $D\equiv 3 \pmod 4$, then

$$\begin{cases} D_a(p)\equiv 1 \pmod 4\\ D_a(p)\equiv 0 \pmod D\end{cases} \Leftrightarrow D_a(p)\equiv 3D \pmod{4D}.$$

Therefore

$$\begin{aligned}(3.6) \quad &= \sum_{\substack{D<x\\ D\equiv 1 \pmod 4}} \sum_{Q'|D} \mu(Q')\sharp Q_a(x;4D,D)\cdot \sharp Q_a(x;4D,\overline{Q'}D) +\\ &+ \sum_{\substack{D<x\\ D\equiv 3 \pmod 4}} \sum_{Q'|D} \mu(Q')\sharp Q_a(x;4D,3D)\cdot \sharp Q_a(x;4D,\overline{Q'}D).\end{aligned}$$

We can obtain a similar formula for the case (II) on p.191, then we get an important formula:

$$
\begin{aligned}
\sum_{\substack{p,q\le x\\ D_a(pq)\equiv 1 \pmod 4}} 1 &= \sum_{\substack{D<x\\ D\equiv 1 \pmod 4}} \sum_{Q'|D} \mu(Q')\sharp Q_a(x;4D,D)\sharp Q_a(x;4D,\overline{Q'}D)\\
&+ \sum_{\substack{D<x\\ D\equiv 3 \pmod 4}} \sum_{Q'|D} \mu(Q')\sharp Q_a(x;4D,3D)\sharp Q_a(x;4D,\overline{Q'}D)\\
&+ \sum_{\substack{D<x\\ D\equiv 1 \pmod 4}} \sum_{Q'|D} \mu(Q')\sharp Q_a(x;4D,3D)\sharp Q_a(x;4D,\tilde{Q}'D)\\
&+ \sum_{\substack{D<x\\ D\equiv 3 \pmod 4}} \sum_{Q'|D} \mu(Q')\sharp Q_a(x;4D,D)\sharp Q_a(x;4D,\tilde{Q}'D), \qquad (3.7)
\end{aligned}
$$

where

$$
\overline{Q'} = \begin{cases} 1, & \text{if } Q'\equiv 1 \pmod 4,\\ 3, & \text{if } Q'\equiv 3 \pmod 4,\end{cases}
$$

$$
\tilde{Q}' = \begin{cases} 3, & \text{if } Q'\equiv 1 \pmod 4,\\ 1, & \text{if } Q'\equiv 3 \pmod 4.\end{cases}
$$

Here we need a lemma on arithmetical functions (we omit the proof):

Lemma 3.2. *Let D be an odd natural number and*

$$D = p_1^{e_1}p_2^{e_2}\cdots p_t^{e_t}q_1^{f_1}q_2^{f_2}\cdots q_s^{f_s},$$

where p_i's and q_j's are distinct primes with $p_i\equiv 1 \pmod 4$ and $q_j\equiv 3 \pmod 4$, be the primary decomposition of D ($e_i\ge 1$, $f_j\ge 1$). We define

$$
D_0 = \begin{cases} 1, & \textit{if } t=0,\\ p_1^{e_1}p_2^{e_2}\cdots p_t^{e_t}, & \textit{if } t\ge 1,\end{cases}
$$

$$
D_1 = \begin{cases} 1, & \textit{if } s=0,\\ q_1^{f_1}q_2^{f_2}\cdots q_s^{f_s}, & \textit{if } s\ge 1\end{cases}
$$

and $s=\omega(D_1)$. Then we have

$$
\sum_{\substack{Q'|D\\ Q'\equiv 1 \pmod 4}} \mu(Q') = \begin{cases} 1, & \textit{if } D_0=D_1=1,\\ 2^{s-1}, & \textit{if } D_0=1, D_1>1,\\ 0, & \textit{if } D_0>1,\end{cases}
$$

$$
\sum_{\substack{Q'|D\\ Q'\equiv 3 \pmod 4}} \mu(Q') = \begin{cases} -2^{s-1}, & \textit{if } D_0=1, D_1>1,\\ 0, & \textit{if } D_0>1.\end{cases}
$$

Taking Lemma 3.2 into account, we can derive Proposition 3.1 from (3.7) easily. ∎

4. $R_a(x;4,l)$, the case of $l=1,3$ (II) — evaluation of $\sharp Q_a(x;4D,D)$ and $\sharp Q_a(x;4D,3D)$

Proposition 3.1 shows that, in order to calculate the natural density $\Gamma_a(4,l)$ of $R_a(x;4,l)$, we need to study $\sharp Q_a(4D,lD)$, $l=1,3$. These two calculations proceed in parallel. Here we need some new notations (*cf.* [1] – [3] and [7], we make use of the same notations as those papers). For $\alpha \in \mathbf{N}$, let $\langle \alpha \pmod p\rangle$ denote the cyclic subgroup generated by $\alpha \pmod p$ in $\mathbf{Z}/p\mathbf{Z}^\times$ and $[\mathbf{Z}/p\mathbf{Z}^\times : \langle \alpha \pmod p\rangle]$ denote its index. Let

$$N_\alpha(x;n,s \pmod t) = \{p \le x;\, p:\ \text{prime},\ p \equiv s \pmod t,\ [\mathbf{Z}/p\mathbf{Z}^\times : \langle \alpha \pmod p\rangle] = n\}.$$

Our result is as follows and here we describe the proof only for $\sharp Q_a(x;4D,D)$.

Proposition 4.1. *We have*

$$Q_a(x;4D,D) = \bigcup_{f\ge 1}\bigcup_{k:\text{odd}} N_a(x;k\cdot 2^f, 1+kD\cdot 2^f \pmod{kD\cdot 2^{f+2}}), \tag{4.1}$$

$$Q_a(x;4D,3D) = \bigcup_{f\ge 1}\bigcup_{k:\text{odd}} N_a(x;k\cdot 2^f, 1+3kD\cdot 2^f \pmod{kD\cdot 2^{f+2}}) \tag{4.2}$$

and clearly these are disjoint unions.

Proof. We start from a simple facts:

$$\begin{aligned} Q_a(x;4D,D) &= Q_{a^D}(x;4,1) \cap Q_a(x;D,0),\\ Q_a(x;4D,3D) &= Q_{a^D}(x;4,3) \cap Q_a(x;D,0). \end{aligned} \tag{4.3}$$

Now we refer to Lemma 3.1 (iii) of [1]. This result gives

$$\begin{aligned} Q_{a^D}(x,4,1) &= \bigcup_{f\ge1}\bigcup_{l\ge0} N_{a^D}(x;(4l+1)\cdot 2^f, 1+2^f \pmod{2^{f+2}})\\ &\cup \bigcup_{f\ge1}\bigcup_{l\ge0} N_{a^D}(x;(4l+3)\cdot 2^f, 1+3\cdot 2^f \pmod{2^{f+2}}). \end{aligned}$$

Then, from (4.3), we have

$$\begin{aligned} Q_a(x,4D,D) &= \bigcup_{f\ge1}\bigcup_{l\ge0} N_{a^D}(x;(4l+1)\cdot 2^f, 1+2^f \pmod{2^{f+2}}) \cap Q_a(x;D,0)\\ &\cup \bigcup_{f\ge1}\bigcup_{l\ge0} N_{a^D}(x;(4l+3)\cdot 2^f, 1+3\cdot 2^f \pmod{2^{f+2}}) \cap Q_a(x;D,0). \end{aligned} \tag{4.4}$$

We remark here that, when $D | D_a(p)$, then

$$I_{a^D}(p) = D \cdot I_a(p), \tag{4.5}$$

where $I_\alpha(p)$ denote the index, i.e.

$$I_\alpha(p) = \frac{p-1}{D_\alpha(p)}.$$

Then we can prove

$$\begin{aligned} &N_{a^D}(x; (4l+1) \cdot 2^f, 1 + 2^f \pmod{2^{f+2}}) \cap Q_a(x; D, 0) = \\ &= N_a(x; k \cdot 2^f, 1 + 2^f \pmod{2^{f+2}}) \cap Q_a(x; D, 0), \end{aligned} \tag{4.6}$$

where k is the number defined by

$$k = \frac{4l+1}{D} \in \mathbf{N}$$

(we omit the proof).

We remark that by the fact (4.6), we succeed in unifying the sub-index into "a".

Now we are in a position to prove (4.1), and for this purpose it is sufficient to prove

$$\begin{aligned} &N_a(x; k \cdot 2^f, 1 + 2^f \pmod{2^{f+2}}) \cap Q_a(x; D, 0) = \\ &= N_a(x; k \cdot 2^f, 1 + kD \cdot 2^f \pmod{kD \cdot 2^{f+2}}). \end{aligned} \tag{4.7}$$

Proof of (4.7). Let

$$p \in N_a(x; k \cdot 2^f, 1 + 2^f \pmod{2^{f+2}}) \cap Q_a(x; D, 0).$$

Then

$$I_{a^D}(p) = 2^f Dk$$

and

$$p \equiv 1 \pmod{2^f \cdot Dk}.$$

With the condition $p \equiv 1 + 2^f \pmod{2^{f+2}}$, the Chinense remainder theorem shows

$$p \equiv 1 + kD \cdot 2^f \pmod{kD \cdot 2^{f+2}}.$$

This proves "$\subset$" in (4.7).

For the another inclusion, let

$$p \in N_a(x; k \cdot 2^f, 1 + kD \cdot 2^f \pmod{kD \cdot 2^{f+2}}),$$

then trivially $p \in N_a(x; k \cdot 2^f, 1 + 2^f \pmod{2^{f+2}})$. Now we put

$$p - 1 = kD \cdot 2^f + \beta\, kD \cdot 2^f$$

with $\beta \in \mathbf{N}$. Since $I_a(p) = k \cdot 2^f$, we have

$$D_a(p) = D(1 + 4\,\beta).$$

This shows $p \in Q_a(x; D, 0)$, and we proved (4.7) as well as Proposition 4.1. ■

5. Behavior of $\sharp Q_a(x; 4D, lD)$ (I) — existence of the natural density

In this section we present an asymptotic formula for $\sharp Q_a(x; 4D, lD)$. Our method is almost on the same line as [1, Section 4], so we omit the proof. First we prepare some notations. For any integer m, we define

$$m_0 = \prod_{\substack{q \mid m \\ q:\text{prime}}} q \quad (\text{i.e. the core of } m)$$

and introduce the number fields

$$\begin{aligned} K_m &= \mathbf{Q}(\zeta_{m_0}, a^{1/m}), \\ G_{k\cdot 2^f, n, d} &= K_{k\cdot 2^f}(\zeta_n, \zeta_{kd\cdot 2^f}, a^{1/k\cdot 2^f n}), \\ \tilde{G}_{k\cdot 2^f, n, d} &= G_{k\cdot 2^f, n, d}(\zeta_{kD\cdot 2^{f+2}}). \end{aligned}$$

We take automorphisms σ_1 and $\sigma_3 \in \mathrm{Aut}(\mathbf{Q}(\zeta_{kD\cdot 2^{f+2}})/\mathbf{Q})$ defined by

$$\text{(5.1)} \qquad \begin{aligned} \sigma_1 &: \zeta_{kD\cdot 2^{f+2}} \mapsto {\zeta_{kD\cdot 2^{f+2}}}^{1+kD\cdot 2^f} \\ \sigma_3 &: \zeta_{kD\cdot 2^{f+2}} \mapsto {\zeta_{kD\cdot 2^{f+2}}}^{1+3kD\cdot 2^f} \end{aligned}$$

and consider σ_1^* and $\sigma_3^* \in \mathrm{Aut}(\tilde{G}_{k\cdot 2^f, n, d}/K_{k\cdot 2^f})$ satisfying

$$\text{(5.2)} \qquad \begin{cases} \sigma_j^*|_{G_{k\cdot 2^f, n, d}} = \text{id.} \\ \sigma_j^*|_{\mathbf{Q}(\zeta_{kD\cdot 2^{f+2}})} = \sigma_j \end{cases} \qquad (j = 1, 3)$$

(we use σ_1 for estimating $\sharp Q_a(x; 4D, D)$ and σ_3 for $\sharp Q_a(x; 4D, 3D)$).

We define the number $c_j(n) = c_j(k, n, d)$ by

$$c_j(n) = \begin{cases} 1, & \text{if } \sigma_j^* \text{ exists,} \\ 0, & \text{if not.} \end{cases}$$

$$
\begin{tikzcd}[arrows=dash]
 & \tilde{G}_{k\cdot 2^f,n,d} \arrow[dd] \\
G_{k\cdot 2^f,n,d} \arrow[ur] \arrow[d] & \\
K_{k\cdot 2^f} \arrow[d] & \mathbf{Q}(\zeta_{kD\cdot 2^{f+2}}) \\
\mathbf{Q} \arrow[ur] &
\end{tikzcd}
$$

Now our result is the following:

Theorem 5.1. *Let a be a natural number and we decompose a into $a = a_0^2 a_1$, a_1 is square-free. We assume GRH.*

(i) *For any odd natural number D and $l = 1, 3$, we have*

$$\sharp Q_a(x; 4D, lD) = \Delta_a(4D, lD) \operatorname{li} x + O\left(\frac{x}{\log x \log\log x} \cdot D^2 \log D \right),$$

where the constant implied by O-symbol is absolute.

(ii) *The densities $\Delta_a(4D, lD)$ $(l = 1, 3)$ are given by the following:*

$$\Delta_a(4D, D) = \sum_{\substack{f\geq 1\\ k:\mathrm{odd}}} \frac{2k_0}{\varphi(k_0)} \sum_{d|2k_0} \frac{\mu(d)}{d} \sum_{n=1}^{\infty} \frac{\mu(n)c_1(n)}{[\tilde{G}_{k\cdot 2^f,n,d} : \mathbf{Q}]}, \tag{5.3}$$

$$\Delta_a(4D, 3D) = \sum_{\substack{f\geq 1\\ k:\mathrm{odd}}} \frac{2k_0}{\varphi(k_0)} \sum_{d|2k_0} \frac{\mu(d)}{d} \sum_{n=1}^{\infty} \frac{\mu(n)c_3(n)}{[\tilde{G}_{k\cdot 2^f,n,d} : \mathbf{Q}]}. \tag{5.4}$$

6. Behavior of $\sharp Q_a(x; 4D, lD)$ (II) — the case a_1 is odd

We can prove the following Theorem 6.1 and it is effectively used in determining the densities $\Gamma_a(4, l)$ $(l = 1, 3)$:

Theorem 6.1. *Let $a = a_0^2 a_1$, a_1 is square free and a_1 is odd. Then we have for any odd natural number D,*

$$\Delta_a(4D, D) = \Delta_a(4D, 3D).$$

This section is allotted to the proof of Theorem 6.1.

We prove Theorem 6.1 by showing that the series expressing $\Delta_a(4D, D)$ and $\Delta_a(4D, 3D)$ (see (5.3) and (5.4)) coincide each other, more precisely, the coefficients $c_1(n)$ and $c_3(n)$ always the same. The methods are similar to those of our previous papers [1] and [2] (see [1, Proposition 4.8] and [2, Section 3]).

The coefficient $c_j(n)$ actually depends on five parameters d, f, k, n and D. The cases where $f \geq 2$ or $f = 1$ and d is even are rather simple and are treated like [1, Proposition 4.8] (see Proposition 6.2). For the case $f = 1$ and d is odd, we must investigate closely the behavior of σ_j (see (5.1)) on certain number fields. It needs a little complicated calculation and will be dealt with in several steps (see Propositions 6.7, 6.9 and 6.10).

Here we review the notation (see also (5.1) and (5.2)):

$$\begin{aligned} &f, n \in \mathbf{N};\ \ k \in \mathbf{N}, k : \text{odd};\\ &d \in \mathbf{N}, d | k_0;\ \ D \in \mathbf{N}, D : \text{odd}, D > 1. \end{aligned}$$

From now on, we assume $a = a_0^2 a_1$, a_1 is square free and a_1 is odd. The following proposition can be proved similarly to [1, Proposition 4.8], so we omit the proof:

Proposition 6.2. (i) *When $f \geq 2$, we have*

$$c_1(n) = c_3(n).$$

(ii) *When $f = 1$ and d is even, we have*

$$c_1(n) = c_3(n) = 0.$$

Now we proceed to the case $f = 1$ and d is odd. Here we follow the lines of [2, Section 3]. Let

$$L = \mathbf{Q}(\zeta_{8kD}), \quad M = G_{4k,n,d} = \mathbf{Q}(\zeta_n, \zeta_{2kd}, a^{1/2kn}).$$

Then we have $LM = \tilde{G}_{4k,n,d}$. We put $K = L \cap M$. In this case, $\sigma_j \in \mathrm{Aut}(L/\mathbf{Q})$ is defined by

$$\begin{aligned} \sigma_1 &: \zeta_{8kD} \mapsto {\zeta_{8kD}}^{1+2kD} \\ \sigma_3 &: \zeta_{8kD} \mapsto {\zeta_{8kD}}^{1+6kD}. \end{aligned} \tag{6.1}$$

We know that

$$\sigma_j|_K = \mathrm{id} \Leftrightarrow c_j(n) = 1$$

for $K = M \cap L$ (see [2, p.700]). So the procedure will be as follows:

1° We calculate the degree $[K : \mathbf{Q}]$.

2° We determine the intersection field K and investigate the behavior of σ_j on K.

$$\begin{tikzcd}
 & LM = \tilde{G}_{4k,n,d} = G_{4k,n,d}(\zeta_{8kD}) \arrow[dl, dash] \arrow[dd, dash] \\
M = G_{4k,n,d} = \mathbf{Q}(\zeta_n, \zeta_{2kd}, a^{1/2kn}) \arrow[dd, dash] & \\
 & L = \mathbf{Q}(\zeta_{8kD}) \arrow[dl, dash] \\
K = G_{4k,n,d} \cap \mathbf{Q}(\zeta_{8kD}) \arrow[d, dash] & \\
\mathbf{Q} &
\end{tikzcd}$$

1° Calculation of $[K : \mathbf{Q}]$

First we need the following (the proof is elementary and we omit it):

Lemma 6.3. *Let $D, k, n \in \mathbf{N}$, D, k be odd, $d|k$, d, n be square free and we denote the odd part of n by $\underline{n}$. Then we have*

$$\frac{\varphi(\langle \underline{n}, kd \rangle)\varphi(kD)}{\varphi(\langle \underline{n}, kd, kD \rangle)} = \varphi(kD'),$$

where $d' = (d, D)$, $n' = \prod_{p:\mathrm{prime},\ p|\underline{n},\ p|D,\ p\nmid k} p$ and $D' = d'n'$.

Remark. Note that $(n', d') = (n', kd') = 1$ and $D'|D$.

We know $\mathrm{Gal}(LM/M) \cong \mathrm{Gal}(L/K)$ for $K = M \cap L$ (see [2, Lemma 3.1]) and so $[L : K] = [\tilde{G}_{4k,n,d} : G_{4k,n,d}]$. From this, we can calculate $[K : \mathbf{Q}]$ by

$$[K : \mathbf{Q}] = \frac{[L : \mathbf{Q}]}{[L : K]} = \frac{[\mathbf{Q}(\zeta_{8kD}) : \mathbf{Q}]}{[\tilde{G}_{4k,n,d} : G_{4k,n,d}]} = \frac{[\mathbf{Q}(\zeta_{8kD}) : \mathbf{Q}][G_{4k,n,d} : \mathbf{Q}]}{[\tilde{G}_{4k,n,d} : \mathbf{Q}]}.$$

Note that

$$\begin{aligned}
G_{4k,n,d} &= \mathbf{Q}(\zeta_{\langle n, 2kd \rangle}, a^{1/2kn}), \\
\tilde{G}_{4k,n,d} &= \mathbf{Q}(\zeta_{\langle n, 2kd, 8kD \rangle}, a^{1/2kn}).
\end{aligned}$$

Using [7, Proposition 3.1], we can calculate the degrees $[G_{4k,n,d} : \mathbf{Q}]$ and $[\tilde{G}_{4k,n,d} : \mathbf{Q}]$:

Proposition 6.4. *The degrees* $[G_{4k,n,d} : \mathbf{Q}]$ *and* $[\tilde{G}_{4k,n,d} : \mathbf{Q}]$ *are given as follows:*

Cases		$[G_{4k,n,d} : \mathbf{Q}]$
$a_1 \equiv 1 \pmod 4$	$a_1 \nmid \langle \underline{n}, kd \rangle$	$2kn\varphi(\langle \underline{n}, kd \rangle)$
	$a_1 \mid \langle \underline{n}, kd \rangle$	$kn\varphi(\langle \underline{n}, kd \rangle)$
$a_1 \equiv 3 \pmod 4$		$2kn\varphi(\langle \underline{n}, kd \rangle)$

Cases		$[\tilde{G}_{4k,n,d} : \mathbf{Q}]$
$a_1 \equiv 1 \pmod 4$	$a_1 \nmid \langle \underline{n}, kd, kD \rangle$	$8kn\varphi(\langle \underline{n}, kd, kD \rangle)$
	$a_1 \mid \langle \underline{n}, kd, kD \rangle$	$4kn\varphi(\langle \underline{n}, kd, kD \rangle)$
$a_1 \equiv 3 \pmod 4$	$a_1 \nmid \langle \underline{n}, kd, kD \rangle$	$8kn\varphi(\langle \underline{n}, kd, kD \rangle)$
	$a_1 \mid \langle \underline{n}, kd, kD \rangle$	$4kn\varphi(\langle \underline{n}, kd, kD \rangle)$

Proof. It is easy from [7, Proposition 3.1]. ■

Remark. Read the table like "$[G_{4k,n,d} : \mathbf{Q}] = kn\varphi(\langle \underline{n}, kd \rangle)$ if and only if $a_1 \equiv 1 \pmod 4$ and $a_1 \mid \langle \underline{n}, kd \rangle$", etc.

Next, since kD is odd, we have

$$[\mathbf{Q}(\zeta_{8kD}) : \mathbf{Q}] = 4\varphi(kD). \tag{6.2}$$

Now we can determine the degree $[K : \mathbf{Q}]$ as follows:

Proposition 6.5. *The degrees* $[K : \mathbf{Q}]$ *are given as follows:*

Cases		$[K : \mathbf{Q}]$
(I) $a_1 \equiv 1 \pmod 4$	(i) $a_1 \mid \langle \underline{n}, kd \rangle$, $a_1 \mid \langle \underline{n}, kd, kD \rangle$	$\varphi(kD')$
	(ii) $a_1 \nmid \langle \underline{n}, kd \rangle$, $a_1 \nmid \langle \underline{n}, kd, kD \rangle$	$\varphi(kD')$
	(iii) $a_1 \nmid \langle \underline{n}, kd \rangle$, $a_1 \mid \langle \underline{n}, kd, kD \rangle$	$2\varphi(kD')$
(II) $a_1 \equiv 3 \pmod 4$	(i) $a_1 \mid \langle \underline{n}, kd, kD \rangle$	$2\varphi(kD')$
	(ii) $a_1 \nmid \langle \underline{n}, kd, kD \rangle$	$\varphi(kD')$

Proof. The proof is easy from Proposition 6.4 and (6.2). ■

Remark. Read the table like "When $a_1 \equiv 1 \pmod 4$, $[K : \mathbf{Q}] = \varphi(kD')$ if and only if $a_1 \nmid \langle \underline{n}, kd \rangle$ and $a_1 \nmid \langle \underline{n}, kd, kD \rangle$", etc.

2° Determination of K and $c_j(n)$

Recall

$$\begin{aligned} L &= \mathbf{Q}(\zeta_{8kD}), \\ M &= G_{4k,n,d} = \mathbf{Q}(\zeta_n, \zeta_{2kd}, a^{1/2kn}). \end{aligned}$$

We determine the intersection field $K = L \cap M$ with the help of the fact that K is a subfield of the cyclotomic field L. Recall $D' = d'n'$, $d' = (d, D)$ and $n' = \prod_{p|\underline{n},\ p|D,\ p\nmid k} p$.

Lemma 6.6.

$$\mathbf{Q}(\zeta_{kD'}) \subset L \cap M.$$

Proof can be carried out in an elementary manner and we omit it.

First we deal with the cases (I-i), (I-ii) and (II-ii) in Proposition 6.5 (where $[K : \mathbf{Q}] = \varphi(kD')$):

Proposition 6.7. *If $[K : \mathbf{Q}] = \varphi(kD')$, then $K = \mathbf{Q}(\zeta_{kD'})$ and $c_1(n) = = c_3(n) = 1$.*

Proof. The fact $[K : \mathbf{Q}] = \varphi(kD')$ and Lemma 6.6 implies $K = \mathbf{Q}(\zeta_{kD'})$. We look into the actions of σ_1 and σ_3. Putting $D = D'D''$, we have $\zeta_{kD'} = {\zeta_{8kD}}^{8D''}$ and

$$\sigma_1(\zeta_{kD'}) = ({\zeta_{8kD}}^{8D''})^{1+2kD} = {\zeta_{8kD}}^{8D''} {\zeta_{8kD}}^{16kDD''} = \zeta_{kD'}.$$

This shows $\sigma_1|_K = \mathrm{id}$ and $c_1(n) = 1$. Similarly we can easily see $\sigma_3|_K = \mathrm{id}$ and $c_3(n) = 1$. ■

For the cases (I-iii) and (II-i) in Proposition 6.5 (where $[K : \mathbf{Q}] = 2\varphi(kD')$), we know $\mathbf{Q}(\zeta_{kD'}) \subset K = L \cap M$ and $[K : \mathbf{Q}(\zeta_{kD'})] = 2$ from Proposition 6.5 and Lemma 6.6. So, to determine the field K, we must find a quadratic algebraic number α such that $\alpha \in L \cap M$ and $\alpha \notin \mathbf{Q}(\zeta_{kD'})$. Then we have

$$K = \mathbf{Q}(\zeta_{kD'}, \alpha).$$

$$\begin{tikzcd}[column sep=small]
L = \mathbf{Q}(\zeta_{8kD}) \arrow[dr, dash] & & M = \mathbf{Q}(\zeta_n, \zeta_{2kd}, a^{1/2kn}) \arrow[dl, dash] \\
& K = L \cap M \arrow[d, dash, "2"] & \\
& \mathbf{Q}(\zeta_{kD'}) \arrow[d, dash, "\varphi(kD')"] & \\
& \mathbf{Q} &
\end{tikzcd}$$

The following lemma is required:

Lemma 6.8. *Let $m \in \mathbf{Z}$, D_m be the discriminant of $\mathbf{Q}(\sqrt{m})$ and $d = |D_m|$. Then we have*

$$\mathbf{Q}(\sqrt{m}) \subset \mathbf{Q}(\zeta_d).$$

Conversely, if $\mathbf{Q}(\sqrt{m}) \subset \mathbf{Q}(\zeta_n)$, then $d|n$.

Proof. See a suitable textbook in algebraic number theory (see also [2, Lemma 3.2]). ■

First we consider the case (I-iii) of Proposition 6.5 (recall the conditions $a_1 \nmid \langle \underline{n}, kd \rangle$ and $a_1 | \langle \underline{n}, kd, kD \rangle$). We decompose a_1 as $a_1 = b_1 b_2$, where b_1 is the product of all the primes which divide $\langle \underline{n}, kd \rangle$. The following conditions are frequently used in the subsequent discussion:

$$\begin{gathered} b_1 | \langle \underline{n}, kd \rangle, \quad b_2 \nmid \langle \underline{n}, kd \rangle, \quad b_2 | kD, \\ (b_2, \langle \underline{n}, kd \rangle) = 1, \quad (b_2, kD') = 1. \end{gathered}$$

Proposition 6.9. *When $a_1 \equiv 1 \pmod 4$, $a_1 \nmid \langle \underline{n}, kd \rangle$ and $a_1 | \langle \underline{n}, kd, kD \rangle$, we have*

$$K = \mathbf{Q}\left(\zeta_{kD'}, \sqrt{(-1)^{\frac{b_2 - 1}{2}} b_2} \right)$$

and

$$c_1(n) = c_3(n) = 1.$$

Proof. First we consider the case $b_1 \equiv 1 \pmod 4$. Then $b_2 \equiv 1 \pmod 4$ since $a_1 \equiv 1 \pmod 4$. We can see $\sqrt{b_1} \in M = G_{4k,n,d} = \mathbf{Q}(\zeta_{2\langle \underline{n}, kd \rangle}, a^{1/2kn})$ because

$\mathbf{Q}(\sqrt{b_1}) \subset \mathbf{Q}(\zeta_{b_1})$ (see Lemma 6.8) and $\zeta_{b_1} = \zeta_{2\langle \underline{n}, kd\rangle}{}^{2\langle \underline{n}, kd\rangle / b_1} \in M$ (note that $b_1 | \langle \underline{n}, kd\rangle$). On the other hand, we see

$$\sqrt{b_2} = \frac{\sqrt{a_1}}{\sqrt{b_1}} \in M$$

since $\sqrt{a_1} \in M$. Moreover we know $\sqrt{b_2} \in L$ because $\mathbf{Q}(\sqrt{b_2}) \subset \mathbf{Q}(\zeta_{b_2})$ (see Lemma 6.8) and $\zeta_{b_1} = \zeta_{8kD}{}^{8kD/b_2} \in L$ (note that $b_2 | kD$). Thus we have $\sqrt{b_2} \in L \cap M$. We also notice that $\sqrt{b_2} \notin \mathbf{Q}(\zeta_{kD'})$ since $(b_2, kD') = 1$. Hence we obtain

$$K = \mathbf{Q}(\zeta_{kD'}, \sqrt{b_2}).$$

Next we consider the action of σ_1 on K. We already know $\sigma_1(\zeta_{kD'}) = \zeta_{kD'}$ (see the proof of Proposition 6.7). As to $\sqrt{b_2}$, we have

$$\sigma_1(\zeta_{b_2}) = \sigma_1(\zeta_{8kD}{}^{8 \cdot kD/b_2}) = (\zeta_{8kD}{}^{1+2kD})^{8 \cdot kD/b_2} = \zeta_{b_2},$$

for $b_2 | kD$. So, $\mathbf{Q}(\zeta_{b_2})$ is fixed by σ_1. Since $\sqrt{b_2} \in \mathbf{Q}(\zeta_{b_2})$, $\sqrt{b_2}^{\sigma_2} = \sqrt{b_2}$. Thus we have proved $\sigma_1|_K = \mathrm{id}$ and $c_1(n) = 1$. The case $b_1 \equiv 3 \pmod 4$ is similar: we have $K = \mathbf{Q}(\zeta_{kD'}, \sqrt{-b_2})$ and can verify $\sigma_3|_K = \mathrm{id}$, thus $c_3(n) = 1$. ■

The case (II-i) in Proposition6.5 can be dealt with similarly to the previous proposition, so we state the result without proof:

Proposition 6.10. *Let* $a_1 \equiv 3 \pmod 4$ *and* $a_1 | \langle \underline{n}, kd, kD\rangle$. *Then we have the following:*

(a) *If* $a_1 \nmid \langle \underline{n}, kd\rangle$, *then*

$$K = \mathbf{Q}\left(\zeta_{kD'}, \sqrt{(-1)^{\frac{b_2-3}{2}} b_2}\right).$$

(b) *If* $a_1 | \langle \underline{n}, kd\rangle$, *then*

$$K = \mathbf{Q}\left(\zeta_{kD'}, \sqrt{-1}\right).$$

In both cases, $c_1(n) = c_3(n)$.

The results which are obtained in this section are summarized in the following theorem:

Theorem 6.11. *If* a_1 *is odd, then the coefficients* $c_j(n)$ *in* (5.3) *and* (5.4) *always satisfy*

$$c_1(n) = c_3(n).$$

More precisely,

if $f \geq 2$, *then* $c_1(n) = c_3(n)$;

if $f = 1$ *and* d *is even, then* $c_1(n) = c_3(n) = 0$;

if $f = 1$ *and* d *is odd,*

(I) *if* $a_1 \equiv 1 \pmod 4$ *and*

(i) $a_1 | \langle \underline{n}, kd \rangle$, $a_1 | \langle \underline{n}, kd, kD \rangle$,

(ii) $a_1 \nmid \langle \underline{n}, kd \rangle$, $a_1 \nmid \langle \underline{n}, kd, kD \rangle$,
then $K = \mathbf{Q}(\zeta_{kD'})$, $c_1(n) = c_3(n) = 1$;

(iii) $a_1 \nmid \langle \underline{n}, kd \rangle$, $a_1 | \langle \underline{n}, kd, kD \rangle$,
then $K = \mathbf{Q}\left(\zeta_{kD'}, \sqrt{(-1)^{\frac{b_2-1}{2}} b_2}\right)$, $c_1(n) = c_3(n) = 1$;

(II) *if* $a_1 \equiv 3 \pmod 4$ *and*

(i-a) $a_1 \nmid \langle \underline{n}, kd \rangle$, $a_1 | \langle \underline{n}, kd, kD \rangle$,
then $K = \mathbf{Q}\left(\zeta_{kD'}, \sqrt{(-1)^{\frac{b_2-3}{2}} b_2}\right)$, $c_1(n) = c_3(n)$;

(i-b) $a_1 | \langle \underline{n}, kd \rangle$, $a_1 | \langle \underline{n}, kd, kD \rangle$,
then $K = \mathbf{Q}(\zeta_{kD'}, \sqrt{-1})$, $c_1(n) = c_3(n)$;

(ii) $a_1 \nmid \langle \underline{n}, kd, kD \rangle$,
then $K = \mathbf{Q}(\zeta_{kD'})$, $c_1(n) = c_3(n) = 1$.

We know from Theorem 6.11 that the series (5.3) and (5.4) are the same, and this completes the proof of Theorem 6.1.

7. The existence of the density $\Gamma_a(4, l)$

We prove the main result Theorem 1.3. Let us start from the formula (3.1). Our proof bases upon the following facts:

1° We assume GRH. When a_1 is odd, then for $l = 1, 3$,

$$\sharp Q_a(x; 4, l) = \frac{1}{6} \operatorname{li} x + O\left(\frac{x}{\log x \log\log x}\right) \tag{7.1}$$

([7, Theorem 1.2]).

2° We assume GRH. In Section 5, we proved, for any $D < x$,

$$\sharp Q_a(x;4D,lD) = \Delta_a(4D,lD)\,\mathrm{li}\,x + O\left(\frac{x}{\log x \log\log x}\cdot D^2 \log D\right), \tag{7.2}$$

where $\Delta_a(4D,lD)$ is a positive constant, the natural density of $Q_a(x;4D,lD)$ $(l=1,3)$. And if a_1 is odd, then

$$\Delta_a(4D,D) = \Delta_a(4D,3D). \tag{7.3}$$

3° Furthermore here we remark that

$$\sharp Q_a(x;4D,lD) \le \pi(x;D,1), \tag{7.4}$$

in fact, if $p \in Q_a(x;4D,lD)$, then $p-1$ is divisible by $D_a(p)$, which is divisible by D. Similarly we have

$$\sharp Q_a(x;4D,lD) \le \frac{x}{D}. \tag{7.5}$$

Proof of Theorem 1.3. We take

$$\begin{aligned} y &= (\log\log x)^{1/3}, \\ z &= (\log x)^{20/3}. \end{aligned}$$

$$\sum_{\substack{D<x \\ D\equiv 1 \pmod 4 \\ D_0=1, D_1>1}} 2^{s-1}\left(\sharp Q_a(x;4D,D) - \sharp Q_a(x;4D,3D)\right)^2 =$$

$$= \left(\sum_{\substack{1<D<y \\ D\equiv 1 \pmod 4 \\ D_0=1, D_1>1}} + \sum_{\substack{y\le D<z \\ D\equiv 1 \pmod 4 \\ D_0=1, D_1>1}} + \sum_{\substack{z\le D<x \\ D\equiv 1 \pmod 4 \\ D_0=1, D_1>1}}\right)\times$$

$$\times 2^{s-1}\left(\sharp Q_a(x;4D,D) - \sharp Q_a(x;4D,3D)\right)^2 =$$

$$= E_1 + E_2 + E_3, \quad \text{say.}$$

Estimate of E_1. By making use of (7.2) and (7.3), we have

$$\begin{aligned}
E_1 = & \sum_{\substack{D<y \\ D\equiv 1 \pmod 4 \\ D_0=1, D_1>1}} 2^{s-1}\{(\Delta_a(4D,D)-\Delta_a(4D,3D))\mathrm{li}\, x + \\
& +O\left(\frac{x}{\log x \log\log x} D^2 \log D\right)\Big\}^2 = \\
= & \sum_{\substack{D<y \\ D\equiv 1 \pmod 4 \\ D_0=1, D_1>1}} 2^{s-1} O\left(\frac{x^2}{(\log x)^2(\log\log x)^2} D^4 \log^2 D\right) \ll \\
\ll & \sum_{D<y} D^{\log 2}\cdot D^4 \log^2 D \frac{x^2}{(\log x)^2(\log\log x)^2} = \\
= & \, o\left(\frac{x^2}{\log^2 x}\right),
\end{aligned} \tag{7.6}$$

since $y = (\log\log x)^{1/3}$.

Estimate of E_3. Here we use the estimate (7.5):

$$\begin{aligned}
E_3 & < \sum_{\substack{z\le D<x \\ D\equiv 1 \pmod 4 \\ D_0=1, D_1>1}} 2^{s-1}\left(\frac{x}{D}\right)^2 < \\
& < \sum_{z<D} D^{\log 2}\frac{x^2}{D^2} = \\
& = x^2 O\left(z^{\log 2 -1}\right).
\end{aligned}$$

Since $z = (\log x)^{20/3}$, we have

$$E_3 = o\left(\frac{1}{\log^2 x}\right). \tag{7.7}$$

Estimate of E_2. Here we use the estimate (7.4):

$$\sharp Q_a(x; 4D, lD) \le \pi(x; D, 1),$$

and in our case, D satisfies

$$D < z = (\log x)^{20/3},$$

then we have

$$\pi(x; D, 1) \ll \frac{1}{\varphi(D)}\pi(x).$$

Then,

$$E_2 < \sum_{y<D<z} D^{\log 2} \left\{ \frac{1}{\varphi(D)} \pi(x) \right\}^2 \ll$$

$$\ll \pi(x)^2 \sum_{y<D} \frac{D^{\log 2}}{D^2} (\log\log D)^2 \ll \tag{7.8}$$

$$\ll \pi(x)^2 y^{-0.3} =$$

$$= o(\pi(x)^2).$$

Now, combining (3.1), (7.1), (7.6) – (7.8), we proved

$$\sharp R_a(x;4,1) = \frac{1}{18} (\mathrm{li}\, x)^2 + o((\mathrm{li}\,(x))^2),$$

and this gives the natural density of $R_a(x;4,1)$, i.e. $\mathit{\Gamma}_a(4,1) = 1/18$. Similarly, $\mathit{\Gamma}_a(4,3) = 1/18$.

8. Numerical examples

In this section, we show some results of numerical experiment on the density $\mathit{\Gamma}_a(4,l)$. For the computer calculation, we use the relation (2.1), that is, we first calculate the residual orders $D_a(p)$ in $0 < p \le x$ for some x, and next we use the GCD algorithm to get $D_a(pq)$. We use the data of $D_a(p)$ which are already obtained in our previous papers [2] and [3]. Here we take x up to 10^7 and show the values $\pi(x)^{-2} \sharp R_a(x;4,l)$ for several a's. The program is written in the C language, compiled by GCC. If $x = 10^7$, then we have about $2.2 \cdot 10^{11}$ pairs (p,q) satisfying $0 < q < p \le x$. We did numerical experiments to calculate $D_a(pq)$ from the data $(D_a(p), D_a(q))$ by the GCD algorithm in the range above. Calculation time depends on a, but it takes approximately 20 hours for each a at 2.66GHz CPU.

(i) The case $a_1 \equiv 1 \pmod 4$

We show two examples $a = 13$ and 20 (Tables 8.1 and 8.2). The theoretical densities are

$$\mathit{\Gamma}_a(4,0) = \frac{5}{9} = 0.555555..., \qquad \mathit{\Gamma}_a(4,1) = \frac{1}{18} = 0.05555...,$$

$$\mathit{\Gamma}_a(4,2) = \frac{1}{3} = 0.333333..., \qquad \mathit{\Gamma}_a(4,3) = \frac{1}{18} = 0.05555....$$

x	$l=0$	$l=1$	$l=2$	$l=3$
10^2	0.507246	0.036232	0.416667	0.039855
10^3	0.583147	0.055768	0.305750	0.055335
10^4	0.547737	0.055817	0.340427	0.056020
10^5	0.556690	0.055162	0.332985	0.055163
10^6	0.554714	0.055844	0.333596	0.055846
10^7	0.555568	0.055465	0.333504	0.055464

Table 8.1. The case $a = 13$

x	$l=0$	$l=1$	$l=2$	$l=3$
10^2	0.584980	0.039526	0.304348	0.071146
10^3	0.546112	0.054399	0.345455	0.054034
10^4	0.546999	0.058023	0.337129	0.057849
10^5	0.553677	0.056013	0.334307	0.056004
10^6	0.555689	0.055712	0.332883	0.055716
10^7	0.555655	0.055542	0.333261	0.055542

Table 8.2. The case $a = 20$

(ii) The case $a_1 \equiv 3 \pmod 4$

We show two examples $a = 11$ and 12 (Tables 8.3 and 8.4). The theoretical densities are

$$\varGamma_a(4,0) = \frac{5}{9} = 0.555555..., \qquad \varGamma_a(4,1) = \frac{1}{18} = 0.05555...,$$
$$\varGamma_a(4,2) = \frac{1}{3} = 0.333333..., \qquad \varGamma_a(4,3) = \frac{1}{18} = 0.05555....$$

x	$l=0$	$l=1$	$l=2$	$l=3$
10^2	0.525692	0.019763	0.415020	0.039526
10^3	0.585907	0.043008	0.328222	0.042862
10^4	0.548096	0.059315	0.333240	0.059348
10^5	0.555764	0.055373	0.333472	0.055391
10^6	0.555451	0.055442	0.333664	0.055443
10^7	0.555532	0.055543	0.333380	0.055544

Table 8.3. The case $a = 11$

x	$l=0$	$l=1$	$l=2$	$l=3$
10^2	0.584980	0.051383	0.304348	0.059289
10^3	0.554217	0.052647	0.341292	0.051844
10^4	0.557908	0.055952	0.330073	0.056067
10^5	0.555208	0.055452	0.333889	0.055450
10^6	0.554873	0.055455	0.334217	0.055455
10^7	0.555667	0.055590	0.333154	0.055590

Table 8.4. The case $a = 12$

(iii) The case $a_1 \equiv 2 \pmod 4$

We show two examples $a = 2$ and 10 (Tables 8.5 and 8.6). At present, we know the theoretical densities $\Gamma_a(4,0)$ and $\Gamma_a(4,2)$ only:

$$\Gamma_2(4,0) = \frac{95}{144} = 0.659722..., \qquad \Gamma_2(4,2) = \frac{147}{576} = 0.255208...,$$
$$\Gamma_{10}(4,0) = \frac{5}{9} = 0.555555..., \qquad \Gamma_{10}(4,2) = \frac{1}{3} = 0.333333....$$

The calculation of the exact theoretical density of $\Gamma_2(4,1)$ needs much deeper considerations of the algebraic quantities which appear in our Section 5.

x	$l=0$	$l=1$	$l=2$	$l=3$
10^2	0.619565	0.057971	0.278986	0.043478
10^3	0.671019	0.053026	0.240603	0.035351
10^4	0.662134	0.047510	0.256798	0.033558
10^5	0.660447	0.050167	0.254528	0.034858
10^6	0.659085	0.050778	0.255461	0.034676
10^7	0.659746	0.050637	0.255088	0.034528

Table 8.5. The case $a = 2$

x	$l=0$	$l=1$	$l=2$	$l=3$
10^2	0.462451	0.106719	0.359684	0.071146
10^3	0.546112	0.057977	0.337349	0.058562
10^4	0.550286	0.055265	0.339327	0.055122
10^5	0.556737	0.055526	0.332222	0.055515
10^6	0.554601	0.055575	0.334251	0.055573
10^7	0.555573	0.055500	0.333428	0.055500

Table 8.6. The case $a = 10$

References

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

[2] **Chinen, K. and L. Murata,** On a distribution property of the residual order of a (mod p) — III, *J. Math. Soc. Japan*, **58-3** (2006), 693–720.

[3] **Chinen, K. and L. Murata,** On a distribution property of the residual order of a (mod p) — IV, in *Number Theory: Tradition and Modernization*, W. Zhang and Y. Tanigawa, eds., Developments in Math. **15**, 11–22, Springer Verlag, 2006.

[4] **Hasse, H.,** 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. unteibarer Ordnung mod p ist, *Math. Ann.*, **162** (1965), 74–76.

[5] **Hooley, C.,** On Artin's conjecture, *J. Reine Angew. Math.*, **225** (1967), 209–220.

[6] **Lagarias, J.C. and A.M. Odlyzko,** Effective versions of the Chebotarev density theorem, in *Algebraic Number Fields (Durham, 1975)*, 409–464, Academic Press, London, 1977.

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

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

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

K. Chinen
Department of Mathematics
School of Science and Engineering
Kinki University
3-4-1, Kowakae
Higashi-Osaka, 577-8502
Japan
chinen@math.kindai.ac.jp