

# ON A DISTRIBUTION PROPERTY OF THE RESIDUAL ORDER OF $a \pmod{p}$ — IV

Koji Chinen<sup>1</sup> and Leo Murata<sup>2</sup>

<sup>1</sup>*Department of Mathematics, Faculty of Engineering, Osaka Institute of Technology,  
Omiya, Asahi-ku, Osaka 535-8585, Japan*

YHK03302@nifty.ne.jp

<sup>2</sup>*Department of Mathematics, Faculty of Economics, Meiji Gakuin University, 1-2-37  
Shirokanedai, Minato-ku, Tokyo 108-8636, Japan*

leo@eco.meijigakuin.ac.jp

**Abstract** Let  $a$  be a positive integer and  $Q_a(x; k, l)$  be the set of primes  $p \leq x$  such that the residual order of  $a \pmod{p}$  in  $\mathbf{Z}/p\mathbf{Z}$  is congruent to  $l$  modulo  $k$ . In this paper, under the assumption of the Generalized Riemann Hypothesis, we prove that for any residue class  $l \pmod{k}$  the set  $Q_a(x; k, l)$  has the natural density  $\Delta_a(k, l)$  and the values of  $\Delta_a(k, l)$  are effectively computable. We also consider some number theoretical properties of  $\Delta_a(k, l)$  as a number theoretical function of  $k$  and  $l$ .

**Keywords:** Residual order, Artin's conjecture for primitive roots

**2000 Mathematics Subject Classification:** 11N05, 11N25, 11R18

## 1. Introduction

Let  $a$  be a positive integer which we assume is not a perfect  $b$ -th power with  $b \geq 2$  and  $p$  a prime number not dividing  $a$ . We define  $D_a(p) = \# \langle a \pmod{p} \rangle$  — the multiplicative order of  $a \pmod{p}$  in  $(\mathbf{Z}/p\mathbf{Z})^\times$ , and for an arbitrary residue class  $l \pmod{k}$  with  $k \geq 2$ , we consider the set

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

and denote its natural density by  $\Delta_a(k, l)$ , to be precise,

$$\Delta_a(k, l) = \lim_{x \rightarrow \infty} \frac{\#Q_a(x; k, l)}{\pi(x)},$$

where  $\pi(x) = \sum_{p \leq x} 1$ .

In [1] and [7], we studied the case  $k = 4$ . There assuming the Generalized Riemann Hypothesis (GRH), we proved that any  $Q_a(x; 4, l)$  has the natural density  $\Delta_a(4, l)$ , and determined its explicit value. In [2], we extended our previous result to the case  $k = q^r$ , a prime power. On the basis of these results, we succeeded in revealing the relation between the natural density of  $Q_a(x; q^{r-1}, l)$  and that of  $Q_a(x; q^r, l)$ . It is clear that, for any  $r \geq 1$ ,

$$\Delta_a(q^{r-1}, l) = \sum_{t=0}^{q-1} \Delta_a(q^r, l + tq^{r-1})$$

and we were able to verify that, when  $r$  is not “very small”, we have

$$\Delta_a(q^r, j + tq^{r-1}) = \frac{1}{q} \Delta_a(q^{r-1}, j),$$

for any  $t$ , — “equi-distribution property” — for details, see [2].

In this paper we study the most general case —  $k$  being composite.

Our main result is :

**Theorem 1.1.** *We assume GRH, and assume  $a$  is not a perfect  $b$ -th power with  $b \geq 2$ . Then, for any residue class  $l \pmod{k}$ , the set  $Q_a(x; k, l)$  has the natural density  $\Delta_a(k, l)$ , and the values of  $\Delta_a(k, l)$  are effectively computable.*

From this result, we find some interesting relationships between  $\Delta_a(k, l)$  and  $\Delta_a(k', l')$  with  $k'|k$  and  $l' \equiv l \pmod{k'}$ .

In order to prove Theorem 1.1, we make use of two combined methods.

Let  $I_a(p)$  be the **residual index** of  $a \pmod{p}$ , i.e.  $I_a(p) = |(\mathbf{Z}/p\mathbf{Z})^\times : \langle a \pmod{p} \rangle|$ . The first method is the one we already used in [1] and [7], and consists of the following: in order to calculate the density  $\Delta_a(4, 1)$ , first we decompose the set  $Q_a(x; 4, 1)$ , which reads in terms of cardinality:

$$\begin{aligned} & \#Q_a(x; 4, 1) \\ &= \sum_{f \geq 1} \sum_{l \geq 0} \#\{p \leq x : I_a(p) = 2^f + l \cdot 2^{f+2}, p \equiv 1 + 2^f \pmod{2^{f+2}}\} \\ &+ \sum_{f \geq 1} \sum_{l \geq 0} \#\{p \leq x : I_a(p) = 3 \cdot 2^f + l \cdot 2^{f+2}, p \equiv 1 + 3 \cdot 2^f \pmod{2^{f+2}}\} \end{aligned} \tag{1.1}$$

(cf. [1] formula (3.4)). We calculate all cardinal numbers on the right hand side. In the process the calculations of the extension degree  $[\tilde{G}_{k,n,d} : \mathbf{Q}]$  and the coefficients  $c_r(k, n, d)$  ( $r = 1, 3$ ) play crucial roles (for details,

see [1]). The technique used here is a generalization of that of Hooley [5], in which under GRH he obtained a quantitative result on Artin’s conjecture for primitive roots. This method is feasible again in this paper (Section 2).

Let

$$k = p_1^{e_1} \dots p_r^{e_r}$$

be the prime power decomposition of  $k$ , where  $p_i$ ’s are distinct primes and  $e_i \geq 1$ . If  $l$  satisfies the condition  $p_i^{e_i} \nmid l$  for any  $i$ ,  $1 \leq i \leq r$ , we can apply the above method to such  $Q_a(x; k, l)$ ’s. Then we can prove the existence of its natural density and can calculate it directly (Theorem 2.2).

Our second method is more elementary. For  $Q_a(x; k, l)$  such that  $p_i^{e_i} \mid l$  for some  $i$ , we can prove in Theorem 3.1 that the natural density of such  $Q_a(x; k, l)$  is written as a linear combination of the densities of

$$Q_a(x; k, l') \quad \text{with } p_i^{e_i} \nmid l' \quad \text{for any } i, 1 \leq i \leq r,$$

and those of

$$Q_a(x; k', l'') \quad \text{with } k' \mid k.$$

Then, by Theorem 2.2, we can prove inductively the existence of the natural density of  $Q_a(x; k, l)$  and determine simultaneously its explicit value.

Here we remark that, if  $p_i^{e_i} \mid l$  for all  $i$ , then  $l = 0$  and we already have a similar result in Hasse [3], [4] and Odoni [8].

## 2. Existence of the Density — $l$ not divisible by any $p_i^{e_i}$

Let  $k = \prod_{i=1}^r p_i^{e_i}$  as above and put  $l = h \prod_{i=1}^r p_i^{f_i}$  ( $(h, k) = 1$ ). In this section, we assume  $0 \leq f_i \leq e_i - 1$  for all  $i$ . For  $g_i \geq f_i$ , let

$$k' = k'(g_1, \dots, g_r) = \prod_{i=1}^r p_i^{g_i} \quad \text{and} \quad k'' = k''(g_1, \dots, g_r) = \prod_{i=1}^r p_i^{e_i + g_i}.$$

Then under GRH, we can prove the existence of the density  $\Delta_a(k, l)$  in a similar manner to that of [2, Section 2]. In fact, we can decompose the set  $Q_a(x; k, l)$  which reads, in terms of cardinality,

**Lemma 2.1.** *Under the above notations, we have*

$$\#Q_a(x; k, l) = \sum_{g_1 \geq f_1} \dots \sum_{g_r \geq f_r} \sum_{\substack{0 < v < k \\ (v, k) = 1}} \sum_{t \geq 0} \#N_a(x; m; 1 + vk' \pmod{k''}), \tag{2.1}$$

where

$$N_a(x; m; 1 + vk' \pmod{k''}) = \left\{ p \leq x : I_a(p) = m, p \equiv 1 + vk' \pmod{k''} \right\},$$

$$m = \left\{ \bar{h}v \pmod{\prod_{i=1}^r p_i^{e_i - f_i}} + t \prod_{i=1}^r p_i^{e_i - f_i} \right\} \cdot \prod_{i=1}^r p_i^{g_i - f_i} \quad (2.2)$$

and where  $\bar{h}h \equiv 1 \pmod{\prod_{i=1}^r p_i^{e_i - f_i}}$ .

*Proof.* The proof goes on the same lines as in [2, Lemma 2.2] and is omitted.  $\square$

This decomposition turns out to yield the existence of the density  $\Delta_a(k, l)$ . Before stating the main theorem of this section, we introduce some notations. For  $k \in \mathbf{N}$ , let  $\zeta_k = \exp(2\pi i/k)$ . We denote Euler's totient by  $\varphi(k)$ . We define the following two types of number fields:

$$G_{m,n,d} = \mathbf{Q}(a^{1/mn}, \zeta_{md}, \zeta_n),$$

$$\tilde{G}_{m,n,d} = G_{m,n,d}(\zeta_{kk'}).$$

$$\begin{array}{ccc} & & \tilde{G}_{m,n,d} \\ & \nearrow & \downarrow \\ G_{m,n,d} = \mathbf{Q}(\zeta_n, \zeta_{md}, a^{1/mn}) & & \mathbf{Q}(\zeta_{kk'}) \\ \downarrow & \nearrow & \\ \mathbf{Q} & & \end{array}$$

We take an automorphism  $\sigma_v \in \text{Gal}(\mathbf{Q}(\zeta_{kk'})/\mathbf{Q})$  determined uniquely by the condition  $\sigma_v : \zeta_{kk'} \mapsto \zeta_{kk'}^{1+vk'}$  ( $0 < v < k$ ,  $(v, k) = 1$ ), and we consider the automorphism  $\sigma_v^* \in \text{Gal}(\tilde{G}_{m,n,d}/G_{m,n,d})$  which satisfies  $\sigma_v^*|_{\mathbf{Q}(\zeta_{kk'})} = \sigma_v$ . We can verify that such a  $\sigma_v^*$  is unique if it exists (see [1, Lemma 4.3]).

**Theorem 2.2.** *Let  $k$  and  $l$  be as above. Then under GRH, we have*

$$\sharp Q_a(x; k, l) = \Delta_a(k, l) \text{li } x + O\left(\frac{x}{\log x \log \log x}\right)$$

as  $x \rightarrow \infty$ , where

$$\Delta_a(k, l) = \sum_{g_1 \geq f_1} \cdots \sum_{g_r \geq f_r} \sum_{\substack{0 < v < k \\ (v, k) = 1}} \sum_{t \geq 0} \frac{m}{\varphi(m)} \sum_{d|m} \frac{\mu(d)}{d} \sum_{n=1}^{\infty} \frac{\mu(n) c_v(m, n, d)}{[\tilde{G}_{m, n, d} : \mathbf{Q}]}. \quad (2.3)$$

The series on the right hand side always converges, the number  $m$  is defined by (2.2) and

$$c_v(m, n, d) = \begin{cases} 1, & \text{if } \sigma_v^* \text{ exists,} \\ 0, & \text{otherwise.} \end{cases}$$

**Remark 1.** When  $(1 + vk', k) > 1$ , we define  $c_v(m, n, d) = 0$  (in this case  $\sigma_v$  does not exist).

*Proof.* We can prove this theorem similarly to [1, Section 4], and so we state the outline only (see also [2, Section 2]). From (2.1) we have

$$\begin{aligned} & \#N_a(x; m; 1 + vk' \pmod{k''}) \\ &= \frac{1}{[K_m : \mathbf{Q}]} \frac{m_0}{\varphi(m_0)} \sum_{d|m_0} \frac{\mu(d)}{d} \#B(x; K_m; a^{1/m}; md; 1 + vk' \pmod{k''}), \end{aligned}$$

where  $K_m = \mathbf{Q}(\zeta_{m_0}, a^{1/m})$ ,  $m_0 = \prod_{p|m, p:\text{prime}} p$ ,

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

and  $N\mathfrak{p}$  is the (absolute) norm of  $\mathfrak{p}$ . Next we define

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

Then we have

$$\begin{aligned} & \#B(x; K_m; a^{1/m}; md; 1 + vk' \pmod{k''}) \\ &= \sum_n' \mu(n) \#P(x; K_m; a^{1/m}; md; 1 + vk' \pmod{k''}; n) \\ &+ O\left(\frac{x(\log \log x)^3}{\log^2 x}\right), \end{aligned}$$

where  $\sum'_n$  means the sum over such  $n \leq x$  which are either 1 or a square free positive integer composed entirely of prime factors not exceeding  $(1/8)\log x$ , and the constant implied by the  $O$ -symbol depends only on  $a$ ,  $k$  and  $l$  (see Propositions 4.1 and 4.2 of [1]).

By the uniqueness of  $\sigma^*$ , we can prove similarly as in [1, Proposition 4.4],

$$\begin{aligned} \sharp P(x; K_m; a^{1/m}; md; 1 + vk' \pmod{k''}; n) \\ = \pi(x; \tilde{G}_{m,n,d}/K_m, \{\sigma^*\}) + O(m^2\sqrt{x}), \end{aligned}$$

where

$$\pi(x; L/K, C) = \sharp \left\{ \mathfrak{p} : \begin{array}{l} \text{a prime ideal in } K, \text{ unramified in } L, \\ (\mathfrak{p}, L/K) = C, N\mathfrak{p} \leq x \end{array} \right\}$$

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

We can estimate  $[\tilde{G}_{m,n,d} : K_m]$  and the discriminant  $d_{\tilde{G}_{m,n,d}}$  of  $\tilde{G}_{m,n,d}$  as follows:

$$[\tilde{G}_{m,n,d} : K_m] = \delta \frac{d}{m_0 \varphi((n, m_0))} \cdot mn\varphi(n)$$

and

$$\log |d_{\tilde{G}_{m,n,d}}| \ll (mnd)^3 \log(mnd),$$

where  $\delta$  and the constant implied by  $\ll$  depends only on  $a$ ,  $k$  and  $l$  (the proof is similar to [1, Lemma 4.6]). This estimate is based on Lagarias-Odlyzko [6].

By Lemma 2.1,  $\sharp Q_a(x; k, l)$  is the infinite sum of  $\sharp N_a(x; m; 1 + vk' \pmod{k''})$ 's, and the above results show that each  $\sharp N_a(x; m; 1 + vk' \pmod{k''})$  is the sum of  $\pi(x; \tilde{G}_{m,n,d}/K_m, \{\sigma^*\})$  plus error terms. The sum of these main terms gives rise to the main term  $\Delta_a(k, l) \times \text{li}(x)$ . And, in a similar way as in [1], we can estimate the sum of the error terms by  $O(x \log^{-1} x \log \log^{-1} x)$ , completing the proof.  $\square$

### 3. Existence of the Density — $l$ being divisible by some $p_i^{e_i}$

In this section, we shall prove the following result:

**Theorem 3.1.** *If  $l$  is divisible by some  $p_i^{e_i}$ , then  $Q_a(x; k, l)$  has the natural density  $\Delta_a(k, l)$  and we can calculate it effectively.*

We prove this theorem by induction on  $r$  — the number of distinct prime factors of  $k$ .

For  $k = p_1^{e_1}$ , our assertion is true by [2].

For  $k = \prod_{i=1}^r p_i^{e_i}$  — the general case — we assume, without loss of generality,

$$\prod_{p_i^{e_i} | l} p_i^{e_i} = p_1^{e_1} \dots p_s^{e_s}.$$

If  $s = 0$  (i.e.  $l$  is not divisible by any  $p_i^{e_i}$ ), our assertion is true by Theorem 2.2, and so we assume  $s \geq 1$  and put  $l_0 = p_1^{e_1} \dots p_s^{e_s}$ .

Write

$$l = m_0 + n_0 \frac{k}{l_0}, \quad 0 \leq m_0 < \frac{k}{l_0}$$

and consider the decomposition:

$$Q_a\left(x; \frac{k}{l_0}, m_0\right) = \bigcup_{n=0}^{l_0-1} Q_a\left(x; k, m_0 + n \frac{k}{l_0}\right). \quad (3.1)$$

For  $j \geq s + 1$ , since  $p_j^{e_j} | \frac{k}{l_0}$  and  $p_j^{e_j} \nmid l$ , then for any  $n$ ,  $p_j^{e_j}$  does not divide  $m_0 + n \frac{k}{l_0}$ . So we have, for any  $n$ ,

$$\#\left\{j : p_j^{e_j} \mid m_0 + n \frac{k}{l_0}\right\} \leq s.$$

Moreover the condition

$$\#\left\{j : p_j^{e_j} \mid m_0 + n \frac{k}{l_0}\right\} = s$$

is satisfied, if and only if,

$$\left\{j : p_j^{e_j} \mid m_0 + n \frac{k}{l_0}\right\} = \{1, 2, \dots, s\} \quad \text{and } n = n_0.$$

In fact,  $\{j : p_j^{e_j} | m_0 + n_0 \frac{k}{l_0}\} = \{1, 2, \dots, s\}$  is clear, and if  $\#\{j : p_j^{e_j} | m_0 + n' \frac{k}{l_0}\} = s$  for some  $n'$ , then  $l_0$  divides both  $m_0 + n' \frac{k}{l_0}$  and  $m_0 + n_0 \frac{k}{l_0}$ , thus  $n' = n_0$ . Therefore, except for  $Q_a(x; k, l)$ , all other  $Q_a(x; k, m_0 + n \frac{k}{l_0})$  appearing in (3.1) satisfy

$$\#\left\{j : p_j^{e_j} \mid m_0 + n \frac{k}{l_0}\right\} < s,$$

and for those  $Q_a(x; k, m_0 + n \frac{k}{l_0})$  we know the existence of its natural density, from the induction hypothesis. And, also from the induction hypothesis, the set on the left hand side of (3.1) has its density. Then we can conclude that  $Q_a(x; k, l)$  has its natural density.

This proof provides an *algorithm* to determine the density  $\Delta_a(x; k, l)$ , but it is difficult to write down the pervading formula in general. In the next section, we will present a numerical example and clarify the contents of Theorem 3.1.

#### 4. Some numerical examples

We take  $a = 5$  and  $k = 12 = 2^2 \cdot 3^1$ . Unconditionally, we have  $\Delta_5(12, 0) = 1/4$ .

For such an  $l$  with  $2^2 \nmid l$  and  $3 \nmid l$ , we can apply Theorem 2.2, and get the densities :

$$\Delta_5(12, 1), \Delta_5(12, 2), \Delta_5(12, 5), \Delta_5(12, 7), \Delta_5(12, 10), \Delta_5(12, 11).$$

First we state the results for these densities. We can determine the value  $c_v(m, n, d)$  in Theorem 2.2 similarly to [2, Section 3]:

**Proposition 4.1.** *We assume GRH and let  $a = 5$ ,  $k = 12$ . Then we have the following:*

(I) *When  $l = 1, 5, 7, 11$ , the value  $c_v(m, n, d)$  in (2.3) is given as follows:*

(i) *If  $g_1 \geq 1$  and  $g_2 \geq 1$ ,*

$$c_v(m, n, d) = \begin{cases} 1, & \text{if } 2 \nmid d \text{ and } 3 \nmid d, \\ 0, & \text{otherwise.} \end{cases}$$

(ii) *If  $g_1 \geq 1$  and  $g_2 = 0$ , then  $c_v(m, n, d) = 1$  if and only if*

(a)  $2 \nmid d, 3 \nmid n, g_1: \text{ odd}, v \equiv 5 \pmod{6}$  or

(b)  $2 \nmid d, 3 \nmid n, g_1: \text{ even}, v \equiv 1 \pmod{6}$ ,

*and  $c_v(m, n, d) = 0$  in all other cases.*

(II) *When  $l = 2, 10$ , the value  $c_v(m, n, d)$  in (2.3) is given as follows:*

(i) *If  $g_1 \geq 1$  and  $g_2 \geq 1$ ,*

$$c_v(m, n, d) = \begin{cases} 1, & \text{if } 3 \nmid d, \\ 0, & \text{otherwise.} \end{cases}$$

(ii) *If  $g_1 \geq 1$  and  $g_2 = 0$ , then  $c_v(m, n, d) = 1$  if and only if*

(a)  $3 \nmid n, g_1: \text{ odd}, v \equiv 5 \pmod{6}$  or

(b)  $3 \nmid n, g_1: \text{ even}, v \equiv 1 \pmod{6}$ ,

*and  $c_v(m, n, d) = 0$  in all other cases.*

We can also calculate the extension degree  $[\tilde{G}_{m,n,d} : \mathbf{Q}]$  (see [2, Lemma 3.3]). In the following lemma,  $\langle m_1, \dots, m_n \rangle$  means the least common multiple of  $m_1, \dots, m_n$ .



**Lemma 4.2.**

$$[\tilde{G}_{m,n,d} : \mathbf{Q}] = \begin{cases} mn\varphi(\langle md, n, 2^{g_1+2}3^{g_2+1} \rangle), \\ \frac{1}{2}mn\varphi(\langle md, n, 2^{g_1+2}3^{g_2+1} \rangle), \end{cases}$$

where the latter case happens if and only if  $mn$  is even and  $5 \mid \langle md, n \rangle$ .

Now we can transform the series (2.3) for  $a = 5$ ,  $k = 12$  and  $l = 1, 2, 5, 7, 10, 11$  into an expression involving some Euler products. The proof is similar to [7, Section 5] (see also [2, Section 4]):

**Theorem 4.3.** *Let  $\chi$  be a nontrivial character of  $(\mathbf{Z}/6\mathbf{Z})^\times$ . We define the constant  $C_\chi$  by*

$$\begin{aligned} C_\chi &= \prod_{\substack{p:\text{prime} \\ p \neq 2,3}} \left( 1 - \frac{p(1 - \chi(p))}{(p-1)(p^2 - \chi(p))} \right) \\ &= \prod_{\substack{p:\text{prime} \\ p \equiv 5 \pmod{6}}} \left( 1 - \frac{-2p}{(p-1)(p^2+1)} \right) \approx 0.86989. \end{aligned}$$

Then under GRH, we have the following:

(I) For  $l = 1, 5, 7, 11$ ,

$$\Delta_5(12, l) = \frac{1}{96} + \frac{1}{120} \left( 5 - \chi(l) \frac{126}{47} C_\chi \right).$$

(II) For  $l = 2, 10$ ,

$$\Delta_5(12, 6 \pm 4) = \frac{5}{48} \pm \frac{109}{1880} C_\chi.$$

Theoretical approximate values are

$$\begin{aligned} \Delta_5(12, 1) &= \Delta_5(12, 7) = \frac{5}{96} - \frac{21}{940} C \approx 0.03265, \\ \Delta_5(12, 5) &= \Delta_5(12, 11) = \frac{5}{96} + \frac{21}{940} C \approx 0.07151, \\ \Delta_5(12, 2) &= \frac{5}{48} - \frac{109}{1880} C \approx 0.053732, \\ \Delta_5(12, 10) &= \frac{5}{48} + \frac{109}{1880} C \approx 0.154602. \end{aligned}$$

For the remaining values of  $l$ , i.e. for  $l = 3, 4, 6, 8$  and  $9$ , we have by Theorem 3.1,

$$\begin{aligned}\Delta_5(12, 3) &= \Delta_5(4, 3) - \Delta_5(12, 7) - \Delta_5(12, 11) = \frac{1}{16}, \\ \Delta_5(12, 6) &= \Delta_5(4, 2) - \Delta_5(12, 2) - \Delta_5(12, 10) = \frac{1}{8}, \\ \Delta_5(12, 9) &= \Delta_5(4, 1) - \Delta_5(12, 1) - \Delta_5(12, 5) = \frac{1}{16},\end{aligned}$$

and

$$\begin{aligned}\Delta_5(12, 4) &= \Delta_5(3, 1) - \Delta_5(12, 1) - \Delta_5(12, 7) - \Delta_5(12, 10) = \frac{1}{6} - \frac{5}{376}C, \\ \Delta_5(12, 8) &= \Delta_5(3, 2) - \Delta_5(12, 2) - \Delta_5(12, 5) - \Delta_5(12, 11) = \frac{1}{24} + \frac{5}{376}C.\end{aligned}$$

Consequently, we can determine all densities.

Numerical data seem to be well-matched with these theoretical densities. In the table below,  $\Delta_5(x; 12, l) = \#\mathbb{Q}_5(x; 12, l)/\pi(x)$  at  $x = 179424673$  ( $10^7$  th prime).

**Table 1.** Experimental densities  $\Delta_5(x; 12, l)$ .

$j$	0	1	2	3	4	5
theoretical	0.125000	0.032650	0.053732	0.062500	0.155099	0.071517
experimental	0.124955	0.032617	0.053689	0.062416	0.154655	0.071531
$j$	6	7	8	9	10	11
theoretical	0.125000	0.032650	0.053234	0.062500	0.154601	0.071517
experimental	0.125067	0.032665	0.053736	0.062595	0.154542	0.071532

**Remark 2.** When considering  $\Delta_a(12, l)$ , one may expect that one would encounter the multiplicative characters mod 12, but in the above example, only the character mod 6 appeared. This is caused by the fact that  $c_v(m, n, d)$  is determined by the condition of  $v \pmod{6}$ . We have already come across similar phenomena in our previous papers. For example, in [7], we needed the nontrivial character mod 4 in general, which give rise to the absolute constant  $C$  (see [7, Theorem 1.2]), but in some cases, we obtained the densities  $\Delta_a(4, 1) = \Delta_a(4, 3) = 1/6$  (under GRH) and  $C$  did not appear. We can explain this “vanishing” of the absolute constant from the same viewpoint. Thus, if we take  $a = 10$  for example, then  $c_v(m, n, d)$  is *not* determined by the condition of  $v \pmod{6}$ . Indeed, when  $l = 1, 5, 7, 11$ ,  $c_v(m, n, d) = 1$  happens in the following cases:

- (I) If  $g_2 \geq 1$ ,
- (i)  $g_1 \geq 3; 2, 3 \nmid d$ ,

- (ii)  $g_1 = 2; 2 \nmid d; 5 \nmid \langle md, n \rangle,$
- (iii-a)  $g_1 = 1; 2, 3 \nmid d; 5 \nmid \langle md, n \rangle,$
- (iii-b)  $g_1 = 1; 2, 3 \nmid d; 5 \mid \langle md, n \rangle, \begin{cases} g_2 : \text{odd}, & r = 1, 5, \\ g_2 : \text{even}, & r = 7, 11. \end{cases}$

(II) If  $g_2 = 0,$

- (i)  $g_1 \geq 3, 2 \nmid d, 3 \nmid n, \begin{cases} g_1 : \text{odd}, & r \equiv 5 \pmod{6}, \\ g_1 : \text{even}, & r \equiv 1 \pmod{6}, \end{cases}$
- (ii)  $g_1 = 2, 2 \nmid d, 3 \nmid n, 5 \nmid \langle md, n \rangle, r \equiv 1 \pmod{6},$
- (iii-a)  $g_1 = 1, 2 \nmid d, 3 \nmid n, 5 \nmid \langle md, n \rangle, r \equiv 5 \pmod{6},$
- (iii-b)  $g_1 = 1, 2 \nmid d, 3 \nmid n, 5 \mid \langle md, n \rangle, r = 11.$

In such cases, it happens that  $\Delta_a(12, l)$ 's are indeed determined mod 12. We can observe it from the following experimental results:

**Table 2.** Experimental densities  $\Delta_{10}(x; 12, l).$

$l$	0	1	2	3	4	5
$\Delta_{10}(x; 12, l)$	0.124991	0.028384	0.062410	0.062506	0.148836	0.075796
$l$	6	7	8	9	10	11
$\Delta_{10}(x; 12, l)$	0.125061	0.034013	0.059552	0.062442	0.145885	0.070125

**Remark 3.** We notice that the distribution property of  $\Delta_5(12, j)$  are complicated.

When

$$j \pmod{12} = j_1 \pmod{4} \times j_2 \pmod{3}$$

in  $\mathbf{Z}/12\mathbf{Z} \cong \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$ , we naïvely expect

$$\Delta_5(12, j) = \Delta_5(4, j_1)\Delta_5(3, j_2)$$

— local multiplicity —, but the following examples show that the distribution is not so simple.

$$1 \begin{cases} \Delta_5(3, 0) = \frac{3}{8} \\ \Delta_5(3, 1) = \frac{3}{8} \\ \Delta_5(3, 2) = \frac{1}{4} \end{cases}$$

$$\Delta_5(4, 1) = \frac{1}{6} \begin{cases} \Delta_5(12, 9) = \frac{1}{16} \\ \Delta_5(12, 1) = \frac{5}{96} - \frac{21}{940}C \\ \Delta_5(12, 5) = \frac{5}{96} + \frac{21}{940}C \end{cases}$$

## References

- [1] K. Chinen and L. Murata, *On a distribution property of the residual order of  $a \pmod{p}$* , J. Number Theory **105** (2004), 60–81.
- [2] K. Chinen and L. Murata, *On a distribution property of the residual order of  $a \pmod{p}$  — III*, preprint.
- [3] 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  $\pmod{p}$  ist*, Math. Ann. **162** (1965), 74–76.
- [4] H. Hasse, *Über die Dichte der Primzahlen  $p$ , für die eine vorgegebene ganzrationale Zahl  $a \neq 0$  von gerader bzw. ungerader Ordnung  $\pmod{p}$  ist*, Math. Ann. **166** (1966), 19–23.
- [5] C. Hooley, *On Artin's conjecture*, J. Reine Angew. Math. **225** (1967), 209–220.
- [6] J. C. Lagarias and A. M. Odlyzko, *Effective versions of the Chebotarev density theorem*, in : Algebraic Number Fields (Durham, 1975), Academic Press, London, 1977, 409–464.
- [7] L. Murata and K. Chinen, *On a distribution property of the residual order of  $a \pmod{p}$  — II*, J. Number Theory **105** (2004), 82–100.
- [8] R. W. Odoni, *A conjecture of Krishnamurthy on decimal periods and some allied problems*, J. Number Theory **13** (1981), 303–319.



<http://www.springer.com/978-0-387-30414-4>

Number Theory

Tradition and Modernization

Zhang, W.; Tanigawa, Y. (Eds.)

2006, XXII, 234 p., Hardcover

ISBN: 978-0-387-30414-4