

On a distribution property of the residual order of $a \pmod{p}$ — IV

大阪工業大学 工学部 知念 宏司 (Koji Chinen)
Department of Mathematics, Faculty of Engineering,
Osaka Institute of Technology.

明治学院大学 経済学部 村田 玲音 (Leo Murata)
Department of Mathematics, Faculty of Economics,
Meiji Gakuin University.

1 Introduction

Let $a (\geq 2)$ be a natural number which is not a perfect b -th power with $b \geq 2$. For a prime p not dividing a , we define the number

$$D_a(p) = \# \langle a \pmod{p} \rangle$$

(the order of the class $a \pmod{p}$ in $(\mathbb{Z}/p\mathbb{Z})^\times$)

and consider the set

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

for arbitrary prescribed integers k and l . We denote the natural density of $Q_a(x; k, l)$ by $\Delta_a(k, l)$. To be precise, let

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

where $\pi(x)$ means the number of primes not exceeding x .

In our papers [2] and [9], we considered the case $k = 4$ (See also [1], [4] and [5]). In these papers, we proved under GRH (=Generalized Riemann Hypothesis), the existence of the natural density $\Delta_a(4, l)$ for $l = 0, 1, 2, 3$ and obtained the explicit values of them. Later in [6] and [10], we extended the result to the cases $(k, l) = (q^i, j)$ and $(k, l) = (5, h)$ respectively, where q is an odd prime, $i \geq 2$, $q \nmid j$ and $1 \leq h < 5$.

In this article, we consider the most general case, i.e. k and l are arbitrary integers. We will show two different types of statements according to the value of k :

For our motivation of considering this problem, the reader is referred to [2] or [4]. For some related problems, see [5] or Odoni [11]. The reader who wants to see examples of computer experiments is referred to any of our previously published articles other than [1].

2 The case k is a prime power

In this section we consider the case $k = q^i$ (q is a prime number) and $0 \leq l \leq q^i - 1$ ([3] and [6]). First we assume $i \geq 2$ if q is an odd prime, and $i \geq 3$ if $q = 2$. Then in most cases, we have a certain recurrence formula between $\Delta_a(q^i, l)$ and $\Delta_a(q^{i-1}, l)$ which shows a kind of "local equi-distribution property":

Theorem 2.1 *We assume GRH. Then the density $\Delta_a(q^i, l)$ always exists and we have the following:*

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

(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 l , we have the relation*

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

Part (II) of the above theorem tells us that $\Delta_a(q^{i-1}, l)$ is *equally* divided into q values $\Delta_a(q^i, l')$ ($l' = l + iq^{i-1}$, $0 \leq i \leq q - 1$). We call it "local equi-distribution property". The former two equalities in Part (I) seem a little mysterious and we do not know so far a heuristic explanation for them.

By Theorem 2.1, the calculation of $\Delta_a(q^i, l)$ is reduced to the case $k = 4$ if $q = 2$ (which is already done in [2] and [9]), and to the case $k = q$ if q is an odd prime. We state the result for $k = q$. Let a_1 be the square free part of a , $G = \mathbf{Z}/q\mathbf{Z}^\times$ and let $\hat{G}$ be the character group of G . We denote

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

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

(II) If $q|a_1$, then

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

where $\sum_r$ means a sum over all r ($1 \leq r \leq q-1$) such that $(\frac{hr+1}{q}) = 1$ and $\underline{a}_1$ is the q -free part of a_1 (i.e. $\underline{a}_1 = a_1/q$).

When $q \geq 5$, the constant C_χ is not always a real number. For example, when $q = 5$, we have

$$C_{\chi_0} = 1, \quad C_{\chi_1} = \prod_{p \equiv 2, 3 \pmod{5}} \left(1 - \frac{2p}{(p-1)(p^2+1)} \right) \approx 0.1293079,$$

$$C_{\chi_2} = \prod_{p \equiv 2 \pmod{5}} \left(1 + \frac{p(i-1)}{(p-1)(p^2-i)} \right) \prod_{p \equiv 3 \pmod{5}} \left(1 - \frac{p(i+1)}{(p-1)(p^2+i)} \right) \\ \cdot \prod_{p \equiv 4 \pmod{5}} \left(1 - \frac{2p}{(p-1)(p^2+1)} \right) \approx 0.3640896 + 0.2240411i$$

and $C_{\chi_3} = \overline{C_{\chi_2}}$, where $\hat{G} = \{\chi_0, \chi_1, \$

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

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

The following lemma is the starting point:

Lemma 2.3 *Let $I_a(p) = |(\mathbb{Z}/p\mathbb{Z})^\times : \langle a \pmod{p} \rangle|$, the residual index mod p of a . Then,*

$$\#Q_a(x; q^i, hq^e) = \sum_{\substack{1 \leq r < q^i \\ q \nmid r}} \sum_{f \geq e} \sum_{j \geq 0} \# \{p \leq x; I_a(p) = k, p \equiv 1 + rq^f \pmod{q^{f+i}}\}.$$

This lemma and a similar reasoning to that of [2] allows us to prove the existence of the density $\Delta_a(q^i, l)$ and its expression in infinite series (Theorem 2.4 below). To state the theorem, we need some more notations. We define the following two types of number fields:

$$\begin{aligned} G_{k,n,d} &= \mathbb{Q}(a^{1/kn}, \zeta_{kd}, \zeta_n), \\ \tilde{G}_{k,n,d} &= G_{k,n,d}(\zeta_{q^f+i}). \end{aligned}$$

We take an automorphism $\sigma_r \in \text{Gal}(\mathbb{Q}(\zeta_{q^f+i})/\mathbb{Q})$ 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 $\sigma_r^* \in \text{Gal}(\tilde{G}_{k,n,d}/G_{k,n,d})$ which satisfies $\sigma_r^*|_{\mathbb{Q}(\zeta_{q^f+i})} = \sigma_r$. We can verify that such a σ_r^* is unique if it exists (see [

3 The case k is an arbitrary composite number

In this section we consider the case k is an arbitrary composite number, especially k has at least two distinct prime factors. The main result for this case is the following:

Theorem 3.1 *We assume GRH. Then, for any residue class $l \pmod{k}$, the natural density $\Delta_a(k, l)$ exists and the value of $\Delta_a(k, l)$ is effectively computable.*

We sketch the idea of proof. Let $k = \prod_{i=1}^r p_i^{e_i}$ (factorization into prime factors) and we put $l = h \prod_{i=1}^r p_i^{f_i}$ ($(h, k) = 1$). First we consider the case where l satisfies the condition $p_i^{e_i} \nmid l$ for any i , $1 \leq i \leq r$. Then like Lemma 2.3, we can decompose the set $Q_a(x; k, l)$ as follows:

Lemma 3.2 *Under the above notations, we have*

$$\begin{aligned} \#Q_a(x; k, l) &= \sum_{g_1 \geq f_1} \cdots \sum_{g_r \geq f_r} \sum_{\substack{0 < s < k \\ (s, k) = 1}} \sum_{t \geq 0} \\ &\quad \#\left\{p \leq x ; I_a(p) = m, p \equiv 1 + s \prod_{i=1}^r p_i^{g_i} \pmod{\prod_{i=1}^r p_i^{e_i + g_i}}\right\}, \end{aligned}$$

where

$$m = \left\{ \bar{h}s \pmod{\prod_{i=1}^r p_i^{e_i - f_i}} + t \prod_{i=1}^r p_i^{e_i - f_i} \right\} \prod_{i=1}^r p_i^{g_i - f_i}$$

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

Using this lemma, we can

We know all the values in the left hand sides by our previous results. In the right hand sides, we can calculate all values which are not underlined by the discussion above. So each equation contains only one undecided value, and we can get it by solving the equation.

The case $k = 12$ is the simplest case, but we can show that we can always construct such a "good" system of equations and can determine any $\Delta_a(k, l)$.

References

- [1] Chinen, K. and Murata, L. : On a distribution property of the residual order of $a \pmod{p}$, Proc. Japan Acad. **79** Ser. A (2003), 28-32.
- [2] _____ : On a distribution property of the residual order of $a \pmod{p}$, to appear in J. Number Theory.
- [3] _____ : On a distribution property of the residual order of $a \pmod{p}$ — III, preprint.
- [4] _____ : On a distribution property of the residual order of $a \pmod{p}$ (in Japanese) in *Analytic Number Theory — Expectations for the 21st Century* —, RIMS Kokyuroku **1219** (2001), 245-255.
- [5] _____ : On a distribution property of the residual order of $a \pmod{p}$ (in Japanese) in Proceedings of the Conference *AC2001* (Algebra and Computation) held at the Tokyo Metropolitan Univ. (2001), published electronically in <ftp://tnt.math.metro-u.ac.jp/pub/ac/2001>.
- [6] _____ : On a distribution property of the residual order of $a \pmod{p}$, II (in Japanese) in *New Aspects of Analytic Number Theory*, RIMS Kokyuroku **1274** (2002), 62-69.
- [7] 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. unteilbarer Ordnung mod p ist, Math. Ann. **162** (1965), 74-76.
- [8] _____ : 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.
- [9] Murata, L. and Chinen, K. : On a distribution property of the residual order of $a \pmod{p}$ — II, to appear in J. Number Theory.
- [10] _____ : On a distribution property of the residual order of <