On a distribution property of the residual order of a (mod p), (2)

By Koji CHINEN*) and Leo MURATA**)

(Communicated by Heisuke HIRONAKA, M. J. A., Nov. 12, 2004)

Abstract: Let a be a positive integer which is not a perfect b-th power with $b \geq 2$, and $Q_a(x;k,l)$ be the set of primes $p \leq x$ such that the residual order of a (mod p) in $\mathbf{Z}/p\mathbf{Z}^*$ is congruent to l (mod k). In this paper, which is a sequel of our previous paper [1], under the assumption of the Generalized Riemann Hypothesis, we prove that for any residue class l (mod 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.

Key words: Residual order; Artin's conjecture (for primitive root).

1. This is a sequel of our previous paper [1].

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 $0 \leq j \leq k$. For a prime p with $p \nmid a$, we define the number

$$D_a(p) = \sharp\langle a \pmod p\rangle$$

(the multiplicative order of the class a (mod p) in $(\mathbf{Z}/p\mathbf{Z})^\times$), and consider the set

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

In [1], we considered the case $k = 4$. We assumed the Generalized Riemann Hypothesis (GRH), then in Theorem 1.1 we proved that any $Q_a(x;4,j)$ has the natural density $\Delta_a(4,j)$, and in Theorem 1.2 we obtained their explicit values. For the full proofs, see [2] and [7].

In this paper, we extend our previous result to more general cases:

1° $k = q^r$, a prime power,

2° k is a composite number which has at least two distinct prime factors.

For these results, see also [3] and [4].

First we can prove the existence of the natural density of $Q_a(x;k,j)$ for general residue classes:

Theorem 1. *We assume GRH, and assume a is not a perfect b-th power with $b \geq 2$. Then, for any residue class j (mod k), the set $Q_a(x;k,j)$ has the natural density $\Delta_a(k,j)$, and the values of $\Delta_a(k,j)$ are effectively computable.*

Remark. When $j = 0$, we can prove this result unconditionally. See also [5, 6] and [8].

When $k'|k$ and $j \equiv j' \pmod{k'}$, then $Q_a(x;k,j) \subset Q_a(x;k',j')$. Then we are interested in what sort of relations we can find between $\Delta_a(k,j)$ and $\Delta_a(k',j')$.

1° The case $k = q^r$, a prime power.

It is clear that, for any $r \geq 1$,

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

Then, it is natural to expect "equi-distribution property", i.e. for any t,

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

And, when r is not "very small", we have above "equi-distribution property".

Theorem 2. *We assume GRH.*

(I) *When q is an odd prime, if $r \geq 2$, then for an arbitrary j, we have*

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

(II) *When $q = 2$, if $r \geq 4$, then for any j, we have the same relation.*

It seems an interesting phenomenon that, for the remaining cases — when r is "very small" — we find some irregularity. Let a_1 be the square free part of a, and for each Dirichlet character χ mod q we define an absolute constant

2000 Mathematics Subject Classification. Primary 11N05; Secondary 11N25, 11R18.

*) Department of Mathematics, Faculty of Engineering, Osaka Institute of Technology, 5-16-1, Omiya, Asahi-ku, Osaka 535-8585.

**) Department of Mathematics, Faculty of Economics, Meiji Gakuin University, 1-2-37 Shirokanedai, Minato-ku, Tokyo 108-8636.

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

Theorem 3. *Let q be an odd prime, $1 \le j \le q-1$, and we assume GRH.*
(I) *If $q \nmid a_1$, then*

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

where

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

(II) *If $q|a_1$, then*

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

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

Theorem 4. *When $q = 2$ and $r = 3$, under GRH, we have*

$$\Delta_a(8,2) = \Delta_a(4,3), \quad \Delta_a(8,6) = \Delta_a(4,1)$$

and unless $j = 2, 6$,

$$\Delta_a(8,j) = \frac{1}{2}\Delta_a(4,j).$$

For $q = 2$ and $r = 2$, see [1].

It is most likely that the constants C_χ which appear in Theorem 3 are not real numbers, and we are interested in the fact that the real constant $\Delta_a(q^r, j)$ is expressed as a combination of these complex constants.

2° k is a composite number which has at least two distinct prime factors.

In the general case, we proved in Theorem 1 that, under GRH, the natural density $\Delta_a(k,j)$ exists, and when k and j are given, we can compute the density effectively. But, taking account of Theorem 3, we can recognize that the explicit form of those densities are very complicated. So here we describe some typical points on the distribution properties of $\Delta_a(k,j)$'s.

Now we take $k = 12 = 2^2 \cdot 3$.

Theorem 5. *We assume GRH, and we take $a = 5$. We define the absolute constant C by*

$$C = \prod_{\substack{p:\text{prime}\\ p\neq 2,3}} \frac{p^3-p^2-p+\chi(p)}{(p-1)(p^2-\chi(p))} \approx 0.86989,$$

where χ is the nontrivial Dirichlet character mod 6. *Then we have*

$$\Delta_5(12,0) = \frac{1}{8},$$
$$\Delta_5(12,1) = \Delta_5(12,7) = \frac{5}{96} - \frac{21}{940}C,$$
$$\Delta_5(12,2) = \frac{5}{48} - \frac{109}{1880}C,$$
$$\Delta_5(12,3) = \Delta_5(12,9) = \frac{1}{16}$$
$$\Delta_5(12,4) = \frac{1}{6} - \frac{5}{376}C,$$
$$\Delta_5(12,5) = \Delta_5(12,11) = \frac{5}{96} + \frac{21}{940}C,$$
$$\Delta_5(12,6) = \frac{1}{8},$$
$$\Delta_5(12,8) = \frac{1}{24} + \frac{5}{376}C,$$
$$\Delta_5(12,10) = \frac{5}{48} + \frac{109}{1880}C.$$

We compare these theoretical densities with experimental densities $\pi(x)^{-1}Q_5(x;12,j)$ with $x = 179424673$ — $\pi(179424673) = 10^7$ (p. 184, Table I).

We find that these theoretical densities are quite well-matched with experimental densities.

On the other hand, we notice that the distribution property of $\Delta_5(12,j)$ are very 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.

Table I.

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

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

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

$$\Delta_5(1,0)=1 \begin{cases} \Delta_5(4,0)=\dfrac{1}{3} \\ \Delta_5(4,1)=\dfrac{1}{6} \\ \Delta_5(4,2)=\dfrac{1}{3} \\ \Delta_5(4,3)=\dfrac{1}{6} \end{cases} ;$$

$$\Delta_5(3,2)=\frac{1}{4} \begin{cases} \Delta_5(12,8)=\dfrac{1}{24}+\dfrac{5}{376}C \\ \Delta_5(12,5)=\dfrac{5}{96}+\dfrac{21}{940}C \\ \Delta_5(12,2)=\dfrac{5}{48}-\dfrac{109}{1880}C \\ \Delta_5(12,11)=\dfrac{5}{96}+\dfrac{21}{940}C. \end{cases}$$

We can prove a similar result for other values of a. For other examples, see [4].

2. We sketch our proofs briefly. Let

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

be the primary decomposition of k, where p_i's are distinct primes, $e_i \geq 1$, and consider the set $Q_a(x;k,j)$. Further we put

$$j = h \prod_{i=1}^{r} p_i^{f_i}, \qquad (h,k)=1.$$

Making use of these expressions of k and j, here we define a set of integers uniquely defined by k:

$$J = \{j \in \mathbf{N};\ 0 \leq j < k,\ f_i \leq e_i - 1 \text{ for all } i\ (1 \leq i \leq r)\},$$

i.e. J is the set of j's satisfying the condition "$p_i^{e_i} \nmid j$ for any i".

1st step. When $j \in J$.

Let $I_a(p)$ be the residual index of $a \pmod p$, i.e. $I_a(p) = |(\mathbf{Z}/p\mathbf{Z})^\times : \langle a \pmod p \rangle|$. In [2] and [7], we use the following method: in order to calculate the density $\Delta_a(4,1)$, first we decompose the set $Q_a(x;4,1)$ into the form

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

We calculated all cardinal numbers of those sets which appeared in the right hand side.

In this 1st step, this method is effective again.

Here we introduce some new notations. For $(g_1,\ldots,g_r)$ with $g_1 \geq f_1, \ldots, g_r \geq f_r$, we put

$$k' = \prod_{i=1}^{r} p_i^{g_i}$$

and for $m, n \in \mathbf{N}$, we define the following two types of number fields:

$$G_{m,n,d} = \mathbf{Q}(a^{1/mn}, \zeta_{md}, \zeta_n),$$
$$\tilde{G}_{m,n,d} = G_{m,n,d}(\zeta_{kk'}).$$

We take an automorphism $\sigma_v \in \mathrm{Gal}(\mathbf{Q}(\zeta_{kk'})/\mathbf{Q})$ 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 $\sigma_v^* \in \mathrm{Gal}(\tilde{G}_{m,n,d}/G_{m,n,d})$ which satisfies $\sigma_v^*|_{\mathbf{Q}(\zeta_{kk'})} = \sigma_v$. We can verify that such a σ_v^* is unique if it exists (see [1, Lemma 4.3]). Furthermore we put

$$m = \left\{ \overline{h}v \Big(\mathrm{mod} \prod_{i=1}^{r} p_i^{e_i - f_i} \Big) + t \prod_{i=1}^{r} p_i^{e_i - f_i} \right\} \cdot \prod_{i=1}^{r} p_i^{g_i - f_i},$$

where $t \geq 0$ and $\overline{h}h \equiv 1 \ \big(\mathrm{mod} \prod_{i=1}^{r} p_i^{e_i - f_i}\big)$. Then we can prove, similarly to [2, §4], the following result:

Proposition 6. *We assume GRH. We have*

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

as $x \to \infty$, where

$$(2.1)\quad \Delta_a(k,l) = \sum_{g_1 \geq f_1} \cdots \sum_{g_r \geq f_r} \sum_{\substack{0<v<k \\ (v,k)=1}} \sum_{t \geq 0} \frac{m}{\varphi(m)} \sum_{d|m} \frac{\mu(d)}{d} \sum_{n=1}^{\infty} \frac{\mu(n) c_v(m,n,d)}{[\tilde{G}_{m,n,d} : \mathbf{Q}]},$$

where

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

The series in the right hand side of (2.1) *always converge.*

We apply this proposition to the special case $k = q^r$, then we obtain Theorems 2–4. For detailed calculations of $[\tilde{G}_{mn,nd} : \mathbf{Q}]$ and $c_v(m,n,d)$, see [3].

2nd Step. When $j \notin J$.

For such an j, we can prove the following result:

Proposition 7. *We assume GRH. When $j \notin J$, then $Q_a(x; k, j)$ has a natural density $\Delta_a(k, j)$, and $\Delta_a(k, j)$ is expressed as a linear combination of*

$$\Delta_a(k, j) \text{ with } j \in J \text{ and } \Delta_a(k', j) \text{ with } k' < k.$$

We state the outline of proof. When $k = p_1^{e_1}$, then our assertion is true by [3]. When $k = \prod_{i=1}^{r} p_i^{e_i}$ — the general case — then we assume, without loss of generality,

$$\prod_{p_i^{e_i} | j} p_i^{e_i} = p_1^{e_1} \cdots p_s^{e_s}, \quad e_i \geq 1.$$

We denote this number by j_0. If $j \notin J$, we can express j in the form

$$j = m_0 + n_0 \frac{k}{j_0} \quad \Big(0 \leq m_0 < \frac{k}{j_0},\ 0 \leq n_0 \leq j_0 - 1 \Big)$$

and we consider the identity

$$Q_a\Big(x; \frac{k}{j_0}, m_0\Big) = \bigcup_{n=0}^{j_0 - 1} Q_a\Big(x; k, m_0 + n\frac{k}{j_0}\Big).$$

We can show that, by induction on the number of distinct prime factors of k, all the densities except for $\Delta_a(k, m_0 + n_0(k/j_0))$ exist and are computable from Proposition 6, and so is $\Delta_a(k, m_0 + n_0(k/j_0))$ from the identity above.

Combining Propositions 6 and 7, we complete the proof of Theorem 1.

Now, as a typical example, we take $a = 5$, $k = 12$, and let us calculate the densities $\Delta_5(12, j)$, $j = 0, 1, \ldots, 11$.

1° Unconditionally we have $\Delta_5(12, 0) = 1/4$.

2° For such an j with $2^2 \nmid j$ and $3 \nmid j$, we can apply Proposition 6, and get the densities

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

Here we need the exact values of the extension degrees $[\tilde{G}_{m,n,d} : \mathbf{Q}]$, and we must determine $c_v(m,n,d)$ completely.

3° For the remaining values of j, we have by Proposition 7,

$$\Delta_a(3,1) = \Delta_a(12,1) + \underline{\Delta_a(12,4)} + \Delta_a(12,7) + \Delta_a(12,10),$$
$$\Delta_a(3,2) = \Delta_a(12,2) + \Delta_a(12,5) + \underline{\Delta_a(12,8)} + \Delta_a(12,11),$$
$$\Delta_a(4,1) = \Delta_a(12,1) + \Delta_a(12,5) + \underline{\Delta_a(12,9)},$$
$$\Delta_a(4,2) = \Delta_a(12,2) + \underline{\Delta_a(12,6)} + \Delta_a(12,10),$$
$$\Delta_a(4,3) = \underline{\Delta_a(12,3)} + \Delta_a(12,7) + \Delta_a(12,11).$$

The densities to be found are the underlined ones, and they can be computed from this system of equations. Consequently, we can determine all densities, which proves our Theorem 5.

References

[1] Chinen, K., and Murata, L.: On a distribution property of the residual order of $a \pmod p$. Proc. Japan Acad., **79A**, 28–32 (2003).

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

[3] Chinen, K., and Murata, L.: On a distribution property of the residual order of $a \pmod p$. III. (Preprint).

[4] Chinen, K., and Murata, L.: On a distribution property of the residual order of $a \pmod p$. IV. (Preprint).

[5] 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**, 74–76 (1965).

[6] Hasse, H.: 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**, 19–23 (1966).

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

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