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

By Koji CHINEN*) and Leo MURATA**)

(Communicated by Heisuke HIRONAKA, M. J. A., Feb. 12, 2003)

Abstract: Let a be a positive integer which is not a perfect h-th power with $h \geq 2$, and $Q_a(x;k,l)$ be the set of primes $p \leq x$ such that the residual order of a in $\mathbf{Z}/p\mathbf{Z}^\times$ is congruent to $l \bmod k$. It seems that no one has ever considered the density of $Q_a(x;k,l)$ for $l \neq 0$ when $k \geq 3$. In this article, the natural densities of $Q_a(x;4,l)$ ($l = 0,1,2,3$) are considered. When $l = 0, 2$, calculations of $\sharp Q_a(x;4,l)$ are simple, and we can get these natural densities unconditionally. On the contrary, the distribution properties of $Q_a(x;4,l)$ for $l = 1,3$ are rather complicated. Under the assumption of Generalized Riemann Hypothesis, we determine completely the natural densities of $\sharp Q_a(x;4,l)$ for $l = 1,3$.

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

1. Introduction. Let $\mathbf{P}$ be the set of all prime numbers.

For a fixed natural number $a \geq 2$, we can define two functions, I_a and D_a, from $\mathbf{P}$ to $\mathbf{N}$:

(1.1)

$$I_a : p \mapsto I_a(p) = |(\mathbf{Z}/p\mathbf{Z})^\times : \langle a \ (\mathrm{mod}\ p)\rangle|$$
(the residual index of a (mod p)),

$$D_a : p \mapsto D_a(p) = \sharp\langle a \ (\mathrm{mod}\ p)\rangle$$
(the residual order of a (mod p) in $(\mathbf{Z}/p\mathbf{Z})^\times$),

where $(\mathbf{Z}/p\mathbf{Z})^\times$ denotes the multiplicative group of all invertible residue classes mod p, $\langle a \ (\mathrm{mod}\ p)\rangle$ denotes the cyclic group generated by $a\,(\mathrm{mod}\ p)$ in $(\mathbf{Z}/p\mathbf{Z})^\times$, and $|\ :\ |$ the index of the subgroup.

We have a simple relation

$$I_a(p)D_a(p) = p - 1, \tag{1.2}$$

but both of these functions fluctuate quite irregularly. C. F. Gauss already noticed that $I_{10}(p) = 1$ happens rather frequently. And the famous Artin's conjecture for primitive roots asks whether the cardinality of the set

$$N_a(x) := \big\{p \leq x;\ I_a(p) = 1\big\} \tag{1.3}$$

tends to ∞ or not as $x \to \infty$. On the assumption of the Generalized Riemann Hypothesis for a certain type of Dedekind zeta functions, C. Hooley [6] succeeded in calculating the natural density of $N_a(x)$. There are various variations of Artin's conjecture, among which two papers Lenstra [8] and Murata [9] considered the surjectivity of the map I_a. For any natural number n, we define

$$N_a(x;n) := \big\{p \leq x;\ I_a(p) = n\big\}. \tag{1.4}$$

Then their results show that, for a square free a with $a \not\equiv 1 \pmod 4$, we have, under GRH, an asymptotic formula

$$\sharp N_a(x;n) \sim C_a^{(n)} \operatorname{li} x \tag{1.5}$$

and $C_a^{(n)} > 0$, where $\operatorname{li} x := \int_2^x (\log t)^{-1} dt$ and the constant $C_a^{(n)}$ depends on a and n. Therefore, for such an a, the map I_a is surjective from $\mathbf{P}$ onto $\mathbf{N}$.

And the surjectivity of the map D_a is also well known. Indeed, except for at most finitely many n's, the map D_a is surjective from $\mathbf{P}$ onto $\mathbf{N}$.

Thus these two maps are surjective for those a's, but between their surjective-properties we notice a big difference. Under GRH, for any $n \in \mathbf{N}$, (1.5) means that

$$I_a^{-1}(n) = \big\{p \in \mathbf{P};\ I_a(p) = n\big\} \tag{1.6}$$

contains infinite elements, but on the contrary, the set

$$D_a^{-1}(n) = \big\{p \in \mathbf{P};\ D_a(p) = n\big\} \tag{1.7}$$

contains only a finite number of elements. In fact, if

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.

$D_a(p) = n$, then

$$n + 1 \le p \le a^n.$$

And recent study on cryptography shows that characterizing D_a is very difficult.

For the purpose of considering the distribution property of the map D_a, here we take an arbitrary natural number $k \ge 2$ and an arbitrary residual class $l \pmod{k}$ and consider the asymptotic behavior of the cardinality of the following set:

$$Q_a(x; k, l) := \{p \le x;\ D_a(p) \equiv l \pmod{k}\}. \tag{1.8}$$

It is more than 40 years ago, W. Sierpinski first considered about this problem and H. Hasse proved, by our notations, that, for odd prime q,

$$\textit{the Dirichlet density of } Q_a(x; q, 0) = \frac{q}{q^2 - 1}$$

([4, 5]). Odoni [10] proved the existence of the natural density of $Q_a(x; q, 0)$, and he obtained a similar results on $Q_a(x; k, 0)$ for a composite square free moduli k.

In this paper we take $k = 4$ and consider the distribution property of $Q_a(x; 4, l)$ for all residue classes $l = 0, 1, 2, 3$. We assume $a \in \mathbf{N}$ is not a perfect h-th power with $h \ge 2$, and put

$$a = a_1 a_2^2, \quad a_1 : \text{ square free}.$$

When $a_1 \equiv 2 \pmod 4$, we define a_1' by

$$a_1 = 2a_1'.$$

With these settings, our results can be stated as follows:

Theorem 1.1. *When $l = 0, 2$, we have*

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

where

$$\delta_0 = \delta_2 = 1/3, \qquad \textit{if } a_1 \ne 2,$$
$$\delta_0 = 5/12 \textit{ and } \delta_2 = 7/24, \qquad \textit{if } a_1 = 2.$$

Theorem 1.2. *We assume GRH. And we define an absolute constant C by*

$$C := \prod_{\substack{p \equiv 3 \pmod 4 \\ p:\text{prime}}} \left(1 - \frac{2p}{(p^2+1)(p-1)}\right) \approx 0.64365. \tag{1.9}$$

Then, for $l = 1, 3$, we have an asymptotic formula

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

and the leading coefficients δ_l $(l = 1, 3)$ are given by the following way:

(I) *If $a_1 \equiv 1, 3 \pmod 4$, then $\delta_1 = \delta_3 = 1/6$.*

(II) *When $a_1 \equiv 2 \pmod 4$,*

(i) *If $a_1' = 1$, i.e., $a = 2 \cdot$ (a square number), then*

$$\delta_1 = \frac{7}{48} - \frac{C}{8}, \quad \delta_3 = \frac{7}{48} + \frac{C}{8}.$$

(ii) *If $a_1' \equiv 1 \pmod 4$ with $a_1' > 1$, then*

(ii-1) *if a_1' has a prime divisor p with $p \equiv 1 \pmod 4$, then $\delta_1 = \delta_3 = 1/6$,*

(ii-2) *if all prime divisors p of a_1' satisfy $p \equiv 3 \pmod 4$, then*

$$\delta_1 = \frac{1}{6} - \frac{C}{8}\prod_{p \mid a_1'}\left(\frac{-2p}{p^3 - p^2 - p - 1}\right),$$
$$\delta_3 = \frac{1}{6} + \frac{C}{8}\prod_{p \mid a_1'}\left(\frac{-2p}{p^3 - p^2 - p - 1}\right).$$

(iii) *If $a_1' \equiv 3 \pmod 4$, then*

(iii-1) *if a_1' has a prime divisor p with $p \equiv 1 \pmod 4$, then $\delta_1 = \delta_3 = 1/6$,*

(iii-2) *if all prime divisors p of a_1' satisfy $p \equiv 3 \pmod 4$, then*

$$\delta_1 = \frac{1}{6} + \frac{C}{8}\prod_{p \mid a_1'}\left(\frac{-2p}{p^3 - p^2 - p - 1}\right),$$
$$\delta_3 = \frac{1}{6} - \frac{C}{8}\prod_{p \mid a_1'}\left(\frac{-2p}{p^3 - p^2 - p - 1}\right).$$

It seems an interesting phenomenon that, in (II)-(ii) and -(iii), the densities δ_1 and δ_3 are controled by whether a_1' has a prime factor p with $p \equiv 1 \pmod 4$ or not. Moreover, we can check easily that, in all cases, we have a *mysterious* inequality

$$\delta_1 \le \delta_3.$$

Remark. The contents of this article appeared in conference proceedings [1–3]. For the full proofs, see *e*-Print archive, http://xxx.lanl.gov/archive/math, article number *math*.NT/0211077 and *math*.NT/0211083.

2. Preliminaries. In this section we introduce some notations and lemmas. For $k \in \mathbf{N}$, 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^e, $q^e || m$ means that $q^e | m$ and $q^{e+1} \nmid m$.

Let K be an algebraic number field. Then we define

(2.1)

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

and

(2.2)

$$\pi^{(1)}(x,K) = \sharp\{\mathfrak{p} : \text{a prime ideal of degree 1 in } K,\ N\mathfrak{p} \le x\}$$

where $N\mathfrak{p}$ is the (absolute) norm of $\mathfrak{p}$. Moreover let L/K be a finite Galois extension. Then for a prime ideal $\mathfrak{p}$ in K, we define the Frobenius symbol by

(2.3)

$$(\mathfrak{p}, L/K) = \left\{ \sigma \in \mathrm{Gal}(L/K);\ \begin{array}{r} \mathfrak{q}^\sigma = \mathfrak{q} \text{ for some prime } \mathfrak{q} \\ \text{in } L \text{ above } \mathfrak{p}, \\ \alpha^\sigma \equiv \alpha^{N\mathfrak{p}} \pmod{\mathfrak{q}} \text{ for all } \alpha \in L \end{array} \right\}.$$

We need the prime ideal theorem for a certain type of Kummer fields:

Theorem 2.1. *For a prime q and $i, j \in \mathbf{N} \cup \{0\}$, we define an extension field*

$$K_{i,j}^{(q)} = \mathbf{Q}(\zeta_{q^i}, \zeta_{q^j}, a^{1/q^j}),$$

and we put

$$n = [K_{i,j}^{(q)} : \mathbf{Q}],$$
$$D = \textit{ the discriminant of } K_{i,j}^{(q)}.$$

Then, under the condition

$$x \ge \exp(10n \log^2 |D|),$$

we have

$$\pi^{(1)}(x, K_{i,j}^{(q)}) = \mathrm{li}\, x + O\big(nxe^{-c\sqrt{\log x}/n^2}\big),$$

where the constant implied by O-symbol and the positive constant c depend only on a and q.

Proof. For the field $K_{i,j}^{(q)}$, we have an estimate

$$|D| \le (n^2|a|)^n.$$

Then Theorems 1.3 and 1.4 of Lagarias-Odlyzko [7] give the desired formula. □

And we need the Chebotarev theorem with GRH:

Theorem 2.2 (Chebotarev density theorem, GRH)**.** *Let K be an algebraic number field, L/K be a finite Galois extension and C be a conjugacy class in $G = \mathrm{Gal}(L/K)$. We define $\pi(x; L/K, C)$ by*

(2.4)

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

Then, under GRH for the field L, we have

(2.5)

$$\pi(x; L/K, C) = \frac{\sharp C}{\sharp G}\,\mathrm{li}\, x + O\left(\frac{\sharp C}{\sharp G}\sqrt{x}\log(d_L x^{n_L}) + \log d_L\right), \quad \textit{as } x \to \infty,$$

where d_L is the discriminant of L and $n_L = [L : \mathbf{Q}]$.

Proof. Lagarias-Odlyzko [7, Theorem 1.1]. □

3. Outline of proof.

Proof of Theorem 1.1. Generally speaking, the condition "$D_a(p) \equiv j \pmod 4$" is rather difficult to handle. So, using the relation (1.2), we transform the condition on $D_a(p)$ into some conditions on $I_a(p)$. First we consider $Q_a(x; 4, 0)$:

(3.1)

$$\begin{aligned} \sharp Q_a(x;4,0) &= \sharp\{p \le x;\ p \equiv 1 \pmod 4\} \\ &\quad - \sum_{j\ge1} \sharp\{p \le x;\ p \equiv 1 \pmod{2^{j+1}},\ 2^j | I_a(p)\} \\ &\quad + \sum_{j\ge1} \sharp\{p \le x;\ p \equiv 1 \pmod{2^{j+2}},\ 2^j | I_a(p)\}. \end{aligned}$$

The first term of the right hand side of (3.1) is calculated by the Siegel-Walfisz theorem. As to the other terms, we note that, when $i \ge j$, "$p \equiv 1 \pmod{2^i}$ and $2^j | I_a(p)$" if and only if p splits completely in the field $K_{i,j}^{(2)}$. So we can use Theorem 2.1 to estimate them. In a similar way to Hooley [6], we obtain

(3.2)

$$\sharp Q_a(x;4,0) = \left\{\frac{1}{\varphi(4)} - \sum_{j\ge1}\left(\frac{1}{[K_{j+1,j}^{(2)} : \mathbf{Q}]} - \frac{1}{[K_{j+2,j}^{(2)} : \mathbf{Q}]}\right)\right\}\mathrm{li}\, x + O\left(\frac{x}{\log x \log\log x}\right).$$

Explicit calculation of the extension degrees in the above formula brings the desired result.

When $l = 2$, we notice that

$$\sharp Q_a(x;4,2) = \sharp Q_a(x;2,0) - \sharp Q_a(x;4,0).$$

We already have the asymptotic formula for $\sharp Q_a(x;4,0)$, and from Odoni's result, we have

$$\sharp Q_a(x;2,0) = \delta\,\mathrm{li}\, x + O\left(\frac{x}{\log x \log\log x}\right),$$

where $\delta = 2/3$ if $a_1 \neq 2$ and $\delta = 17/24$ if $a_1 = 2$. This completes the proof of Theorem 1.1. $\square$

Proof of Theorem 1.2. First we introduce the set

$$N_a(x;k;s \pmod t) := \{p \leq x;\ p \in N_a(x;k),\ p \equiv s \pmod t\}. \tag{3.3}$$

Then, in a similar way to (3.1), we can deduce the following formulas:

$$\begin{aligned} \sharp Q_a(x;4,1) &= \sum_{f\geq 1}\sum_{l\geq 0} \sharp N_a(x; 2^f + l\cdot 2^{f+2}; 1+2^f \pmod{2^{f+2}}) \\ &+ \sum_{f\geq 1}\sum_{l\geq 0} \sharp N_a(x; 3\cdot 2^f + l\cdot 2^{f+2}; 1+3\cdot 2^f \pmod{2^{f+2}}) \end{aligned} \tag{3.4}$$

and

$$\begin{aligned} \sharp Q_a(x;4,3) &= \sum_{f\geq 1}\sum_{l\geq 0} \sharp N_a(x; 3\cdot 2^f + l\cdot 2^{f+2}; 1+2^f \pmod{2^{f+2}}) \\ &+ \sum_{f\geq 1}\sum_{l\geq 0} \sharp N_a(x; 2^f + l\cdot 2^{f+2}; 1+3\cdot 2^f \pmod{2^{f+2}}). \end{aligned} \tag{3.5}$$

As was pointed out in Introduction, the natural density of the set $N_a(x;k)$ is estimated under GRH with an error term in Murata [9]:

$$\begin{aligned} \sharp N_a(x;k) &= \frac{k_0}{\varphi(k_0)} \sum_{d\mid k_0} \frac{\mu(d)}{d} \sum_{n=1}^{\infty} \frac{\mu(n)}{[G_{n,kd} : \mathbf{Q}]} \operatorname{li} x \\ &+ O\left(\{n \log\log x + \log a\} \frac{x}{\log^2 x} \right), \end{aligned} \tag{3.6}$$

where

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

$$G_{n,kd} = \mathbf{Q}(\zeta_n, \zeta_{kd}, a^{1/kn}).$$

This is obtained by considering the decomposition of prime ideals of $K_k = \mathbf{Q}(\zeta_{k_0}, a^{1/k})$ in $G_{n,kd}$, and the prime ideal theorem (under GRH) for $G_{n,kd}$.

The set $N_a(x;k;s \pmod t)$ can be estimated along the same lines, but we must appeal to the Chebotarev density theorem (see Theorem 2.2) instead of the prime ideal theorem to deal with the condition $p \equiv s \pmod t$. For $k = (j+4l)\cdot 2^f$, $s = 1 + i\cdot 2^f$, $t = 2^{f+2}$ with $f \geq 1$, $l \geq 0$, $i = 1$ or 3 and $j = 1$ or 3, we have, under GRH,

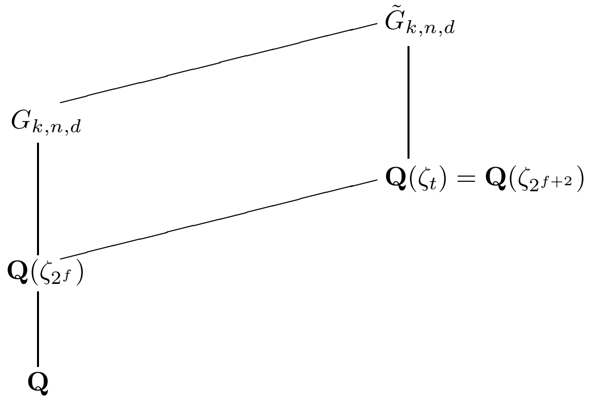
$$\begin{aligned} &\sharp N_a(x;k;s \pmod t) \\ &= \frac{k_0}{\varphi(k_0)} \sum_{d\mid k_0} \frac{\mu(d)}{d} \sum_{n=1}^{\infty} \frac{\mu(n) c_i(k,n,d)}{[\tilde{G}_{n,kd} : \mathbf{Q}]} \operatorname{li} x \\ &+ O\left(\frac{x}{\log^2 x} (\log\log x)^4 \right), \end{aligned} \tag{3.7}$$

where $\tilde{G}_{n,kd} = G_{n,kd}(\zeta_t)$ and the coefficient $c_i(k,n,d)$ is determined in the following way: we consider $\sigma_i^* \in \mathrm{Gal}(\tilde{G}_{n,kd}/K_k)$ satisfying the conditions

$$\begin{cases} 1^\circ & \sigma_i^*|_{G_{n,kd}} = \mathrm{id}. \\ 2^\circ & \sigma_i^*|_{\mathbf{Q}(\zeta_t)} = \sigma_i \end{cases} \tag{3.8}$$

where $\sigma_i \in \mathrm{Gal}(\mathbf{Q}(\zeta_t)/\mathbf{Q})$ is an automorphism determined by $\zeta_t \mapsto \zeta_t^s$. Since there exists at most one σ_i^* with the above conditions, for $i = 1, 3$, we can define

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



If we combine (3.4) and (3.7), after estimation of the error terms we get the asymptotic formula for $\sharp Q_a(x;4,l)$ $(l = 1, 3)$. Now we write $k = (1+4l)\cdot 2^f$ and $k' = (3+4l)\cdot 2^f$. Then we have

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

and the coefficients δ_1 and δ_3 are given by

$$\begin{aligned} \delta_1 &= \sum_{f\geq 1}\sum_{l\geq 0} \frac{k_0}{\varphi(k_0)} \sum_{d\mid k_0} \frac{\mu(d)}{d} \sum_{n} \frac{\mu(n) c_1(k,n,d)}{[\tilde{G}_{k,n,d} : \mathbf{Q}]} \\ &+ \sum_{f\geq 1}\sum_{l\geq 0} \frac{k_0'}{\varphi(k_0')} \sum_{d\mid k_0'} \frac{\mu(d)}{d} \sum_{n} \frac{\mu(n) c_3(k',n,d)}{[\tilde{G}_{k',n,d} : \mathbf{Q}]}, \end{aligned} \tag{3.9}$$

(3.10)

$$\delta_3 = \sum_{f\geq 1}\sum_{l\geq 0}\frac{k_0}{\varphi(k_0)}\sum_{d|k_0}\frac{\mu(d)}{d}\sum_{n}\frac{\mu(n)c_3(k,n,d)}{[\tilde{G}_{k,n,d}:\mathbf{Q}]} + \sum_{f\geq 1}\sum_{l\geq 0}\frac{k_0'}{\varphi(k_0')}\sum_{d|k_0'}\frac{\mu(d)}{d}\sum_{n}\frac{\mu(n)c_1(k',n,d)}{[\tilde{G}_{k',n,d}:\mathbf{Q}]}.$$

In order to calculate these infinite sums, we need the following lemma:

Lemma 3.1. *Let* $\underline{k}$ *be the odd part of* k *and* $\langle a,b\rangle$ *be the least common multiple of* a *and* b. *Then we have*

(i)

$$\sum_{l\geq 0}\frac{k_0}{\varphi(k_0)}\sum_{\substack{d|k_0\\ d:\mathrm{odd}}}\frac{\mu(d)}{d}\sum_{n:\mathrm{odd}}\frac{\mu(n)}{nk\varphi(\langle n,\underline{k}d\rangle)} + (\textit{the same term but } k\to k') = \frac{1}{2^f}.$$

(ii)

$$\sum_{l\geq 0}\frac{k_0}{\varphi(k_0)}\sum_{\substack{d|k_0\\ d:\mathrm{odd}}}\frac{\mu(d)}{d}\sum_{\substack{n:\mathrm{odd}\\ a_1|\langle n,\underline{k}d\rangle}}\frac{\mu(n)}{nk\varphi(\langle n,\underline{k}d\rangle)} + (\textit{the same term but } k\to k') = \begin{cases}\dfrac{1}{2^f} & \textit{if } a_1=1,\\ 0 & \textit{if } a_1>1.\end{cases}$$

We can determine the exact values of $[\tilde{G}_{n,kd}:\mathbf{Q}]$ and $c_i(k,n,d)$ (and the same quantities but $k\to k'$), then we get the desired natural densities. □

References

[1] Chinen, K., and Murata, L.: On a distribution property of the residual orders of a (mod p). Analytic Number Theory — Expectations for the 21st Century —. RIMS Kokyuroku, **1219**, 245–255 (2001). (In Japanese).

[2] Chinen, K., and Murata, L.: On a distribution property of the residual orders of a (mod p). Proceedings of the Conference AC2001 (Algebra and Computation) held at the Tokyo Metropolitan Univ. (2001). (In Japanese). (Published electronically in ftp://tnt.math.metro-u.ac.jp/pub/ac/2001).

[3] Chinen, K., and Murata, L.: On a distribution property of the residual orders of a (mod p), II. New Aspects of Analytic Number Theory. RIMS Kokyuroku, **1274**, 62–69 (2002). (In Japanese).

[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**, 74–76 (1965).

[5] 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).

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

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

[8] Lenstra Jr., H. W.: On Artin's conjecture and Euclid's algorithm in global fields. Invent. Math., **42**, 201–224 (1977).

[9] Murata, L.: A problem analogous to Artin's conjecture for primitive roots and its applications. Arch. Math., **57**, 555–565 (1991).

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