

NOTES ON A CHARACTER SUM FOR COUNTING PRIMITIVE ROOTS

SHUGUANG LI

RÉSUMÉ. Pour un nombre naturel n , soit $\lambda(n)$ l'exposant de $(\mathbb{Z}/n\mathbb{Z})^*$ et D le plus grand diviseur libre de carré de $\lambda(n)$. Soit

$$E(n) = \{a \in (\mathbb{Z}/n\mathbb{Z})^* : a^{\lambda(n)/D} \equiv 1 \pmod{n}\}.$$

Si un caractère de Dirichlet est trivial sur $E(n)$, il est appelé caractère élémentaire. En comptant les modules pour une racine primitive a , on arrive à une somme de caractères de la forme $\sum_{\text{ord}(\chi)=d} \chi(a)$, où d est un diviseur de D et les caractères en question sont élémentaires. Dans cet article, on obtient une formule pour cette somme peu importe le module, généralisant un résultat connu pour cette somme dans le cas où $(\mathbb{Z}/n\mathbb{Z})^*$ est cyclique, et conduit à une formulation de la conjecture d'Artin.

ABSTRACT. For a natural number n , let $\lambda(n)$ be the exponent of $(\mathbb{Z}/n\mathbb{Z})^*$ and D the largest squarefree divisor of $\lambda(n)$. Let

$$E(n) = \{a \in (\mathbb{Z}/n\mathbb{Z})^* : a^{\lambda(n)/D} \equiv 1 \pmod{n}\}.$$

A Dirichlet character is called an elementary character if it is trivial on $E(n)$. Counting moduli for a given primitive root a leads to a character sum of the form $\sum_{\text{ord}(\chi)=d} \chi(a)$ where d is a divisor of D and the involved characters are elementary. In this paper, we obtain a formula for the sum for any modulus, which extends a known result of the sum when $(\mathbb{Z}/n\mathbb{Z})^*$ is cyclic, and leads to a formulation for Artin's conjecture.

1. Introduction

Let n be a natural number. The maximum order of the residue classes in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^*$ is known as $\lambda(n)$. The values of $\lambda(n)$ can be easily determined [8] from the prime factorization of n . Indeed, $\lambda(n) = \text{lcm}_{p^e \parallel n} \{\lambda(p^e)\}$ where $p^e \parallel n$ means that p^e divides n but p^{e+1} does not, and $\lambda(p^e) = \varphi(p^e)$, for all prime powers p^e except that $\lambda(2^e) = \frac{1}{2}\varphi(2^e)$ for $e \geq 3$, where we denoted by φ the Euler's totient function. All of the residue classes and the covered integers with order $\lambda(n)$ in the multiplicative group are referred as primitive λ -roots by Carmichael [1]. These are actually primitive roots when $(\mathbb{Z}/n\mathbb{Z})^*$ is cyclic, namely when n equals 2, 4, p^r or $2p^r$ for any odd prime p .

Regarding problems on primitive roots, Artin's conjecture received the most attention. Let a be a fixed integer, and $P_a(x)$ be the number of primes up to x for which a is a primitive root. If the moduli counted in $P_a(x)$ are extended to arbitrary natural

numbers and primitive roots are extended to primitive λ -roots, then the number of such moduli is denoted by $N_a(x)$. Artin conjectured that, if a is not a square nor -1 , then

$$P_a(x) \sim \frac{A(a)x}{\log x}$$

as $x \rightarrow \infty$, where $A(a) > 0$ is a constant depending on a . Hooley [5] proved the conjecture under the assumption of Extended Riemann Hypothesis (ERH) for Dedekind zeta functions over certain Kummerian fields and he explicitly determined $A(a)$. Goldfeld [3] and Stephens [17] proved the conjecture unconditionally on average. It was also proved in [4, 16] that $P_a(x)$ is unbounded for all a not in a set of density 0, although we do not know a single value of a for which $P_a(x)$ has the property. Research on primitive λ -roots reveals a different pattern for $N_a(x)$.

It was proved unconditionally in [12] that the average order of $N_a(x)$ oscillates between a constant multiple of x and $o(x)$ as x increases. Let $\mathcal{E}$ denote the set of integers a which are a power higher than the first power or a square times a member of $\{\pm 1, \pm 2\}$. Then function $N_a(x)$ follows its average order (see [9, 11]) in the sense that

$$\liminf_{x \rightarrow \infty} N_a(x)/x = 0$$

for every integer a , and

$$\limsup_{x \rightarrow \infty} N_a(x)/x > A\varphi(|a|)/|a|$$

under the assumption of the Generalized Riemann Hypothesis (GRH) for all $a \notin \mathcal{E}$, where A is a positive number. It remains open for unconditional result on

$$\limsup_{x \rightarrow \infty} N_a(x)/x,$$

see [11].

In Stephens's work on the average of $P_a(x)$, an important function of characters was introduced. Let χ be a Dirichlet character modulo prime p . Define

$$c(\chi) = \frac{1}{p-1} \sum_a' \chi(a),$$

where the prime symbol in the sum indicates that the sum is taken over all the primitive roots a modulo p . Obviously the function can be extended to arbitrary moduli n with $p-1$ replaced by $\varphi(n)$ and primitive roots replaced by primitive λ -roots. The extended function in turn brings up a few notions that we cannot avoid. Let $\text{rad}(m)$ denote the largest squarefree divisor of m . Let

$$E(n) = \left\{ a \bmod n : a^{\lambda(n)/\text{rad}(\lambda(n))} \equiv 1 \pmod{n} \right\}.$$

Obviously $E(n)$ is a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$. Another way to obtain $E(n)$ is through the factorization of $(\mathbb{Z}/n\mathbb{Z})^*$ into a direct product of cyclic subgroups whose orders are powers of primes. For each prime factor q of $\lambda(n)$, let v_q be the exponent such that $q^{v_q} \parallel \lambda(n)$. Then after replacing each cyclic factor of order q^{v_q} with its subgroup of order q^{v_q-1} , we obtain a factorization of $E(n)$.

We say that a character $\chi \bmod n$ is *elementary* if it is trivial on $E(n)$. Clearly the order of an elementary character is squarefree. In the case where $(\mathbb{Z}/n\mathbb{Z})^*$ is a cyclic

group, this condition is also sufficient. Indeed, if g is a generator of $(\mathbb{Z}/n\mathbb{Z})^*$, then $g^{\text{rad}(\lambda(n))}$ is a generator of $E(n)$. If χ is a character mod n whose order is a factor of $\text{rad}(\lambda(n))$, then $\chi(g^{\text{rad}(\lambda(n))}) = 1$ and χ acts trivially on $E(n)$. If $(\mathbb{Z}/n\mathbb{Z})^*$ is not cyclic, then there are characters mod n whose orders are squarefree, but they are not elementary characters. For example, $(\mathbb{Z}/259\mathbb{Z})^*$ can be factored as a direct product of $(\mathbb{Z}/7\mathbb{Z})^*$ and $(\mathbb{Z}/37\mathbb{Z})^*$. Note that $38 \equiv 3 \pmod{7}$ and $38 \equiv 1 \pmod{37}$, while $113 \equiv 1 \pmod{7}$ and $113 \equiv 2 \pmod{37}$. Since 3 and 2 are primitive roots for 7 and 37 respectively, 38 and 113 generate $(\mathbb{Z}/259\mathbb{Z})^*$. Consider two characters χ_1 and χ_2 modulo 259 so that χ_1 takes 38 to a primitive 6-th root of unity and 113 to 1 while χ_2 takes 113 and 38 to the above roots of unity respectively. Both characters have order 6. But χ_2 is an elementary character while χ_1 is not since $E(259)$ contains the subgroup generated by 38.

Let us use $\Delta_q(n)$ to denote the number of cyclic factors of order q^{v_q} in the above factorization of $(\mathbb{Z}/n\mathbb{Z})^*$. For each squarefree number $h \mid \varphi(n)$, let $\rho_n(h)$ be the number of elementary characters mod n of order h . It is not hard to see that

$$\rho_n(h) = \prod_{q|h} (q^{\Delta_q(n)} - 1).$$

It was proved (see [10]) that

$$(1) \quad \sum_{\chi \bmod n} c(\chi) \chi(a) = \begin{cases} 1 & \text{if } a \text{ is a primitive } \lambda\text{-root mod } n, \\ 0 & \text{otherwise.} \end{cases}$$

We can write

$$N_a(x) = \sum_{n \leq x} \sum_{\chi \bmod n} c(\chi) \chi(a).$$

This formula also holds for $P_a(x)$ if the moduli are restricted to primes and primitive λ -roots are replaced by primitive roots. In [12] we obtained that, for each Dirichlet character χ modulo n ,

$$(2) \quad c(\chi) = \begin{cases} \frac{(-1)^\omega R(n)/\varphi(n)}{\rho_n(\text{ord}(\chi))} & \text{if } \chi \text{ is elementary,} \\ 0 & \text{if } \chi \text{ is not elementary,} \end{cases}$$

where $R(n)$ is the number of primitive λ -roots modulo n and ω is the number of prime factors of $\text{ord}(\chi)$. Thus $c(\chi)$ remains a constant for all of elementary characters with the same order. It would be helpful to obtain a closed form for the sum

$$\sum_{\substack{\chi \bmod n \\ \text{ord}(\chi)=d}} \chi(a)$$

in order to provide an alternative way of counting the moduli in $P_a(x)$ or $N_a(x)$. And it is only necessary to involve elementary characters in the closed form because of (2). The character sum is a Ramanujan sum and was studied in many papers [6, 13, 14, 15]. One can find a nice proof of a closed form for the sum in [14] when the modulus is a prime.

The goal of this paper is to obtain such a closed form for the character sum for arbitrary modulus n . First, let us state the following lemma.

Lemma 1. Let $d > 1$ be a squarefree divisor of $\varphi(p^e)$, where p is a prime and $e \geq 1$. Suppose that a is not divisible by p . We define $\bar{d}$ as the largest divisor of d such that $a \equiv b^{\bar{d}} \pmod{p^e}$ for some integer b if p is an odd prime or $p = 2$ and $e = 2, 3$. When $p = 2$ and $e > 3$, $\bar{d}$ is the largest divisor of $d = 2$ such that $a \equiv \pm 5^{\bar{d}l} \pmod{2^e}$ for some integer l . Then $\bar{d} = \gcd(d, \lambda(p^e)/\text{ord}(a))$.

Thus $\bar{d}$ actually depends on p, e, d and a , although the notation $\bar{d}$ only shows its connection with d . Now we can introduce a closed form for the character sum for the modulus $n = p^e$.

Lemma 2. Let $p, e, d > 1$, a and $\bar{d}$ be the same as before.

(a) We have

$$\sum_{\substack{\chi \pmod{p^e} \\ \text{ord}(\chi)=d}}^{(E)} \chi(a) = \mu\left(\frac{d}{\bar{d}}\right) \varphi(\bar{d})$$

except for $p = 2$ and $e = 3$, where (E) in the sum indicates that the sum is taken over all elementary characters modulo p^e .

(b) If $p = 2$ and $e = 3$, the identity in (a) still holds for $\bar{d} = 1$, and the following identity holds for $\bar{d} = 2$ (namely $a \equiv 1 \pmod{8}$):

$$\sum_{\substack{\chi \pmod{8} \\ \text{ord}(\chi)=2}}^{(E)} \chi(a) = 3.$$

To extend the lemma to arbitrary moduli we need to introduce another notation. Recall that $q^{v_q} \parallel \lambda(n)$ for each prime divisor q of $\lambda(n)$. Let us define

$$s_q = \#\{p^e : p^e \parallel n, q^{v_q} \mid \lambda(p^e) \text{ and } a \not\equiv b^q \pmod{p^e} \text{ for any } b\}$$

for all odd q and $q = 2$ if $16 \nmid n$. When $2^e \parallel n$ and $e > 3$, we define

$$s_2 = \#\{\text{odd } p^e : p^e \parallel n, q^{v_q} \mid \lambda(p^e) \text{ and } a \not\equiv b^q \pmod{p^e} \text{ for any } b\}$$

except in the case where $2^{v_2} \mid \lambda(2^e)$ and $a \not\equiv \pm 5^{2l} \pmod{2^e}$ for any integer l , for which s_2 is equal to 1 plus the above number. Thus s_q is actually a function of n, p^e, q and a , although the notation only shows its connection with prime q . It should be noted that $2^3 = 8$ is counted in s_2 if $8 \parallel n$, $2^{v_2} = \lambda(2^3) = 2$ and $a \not\equiv 1 \pmod{8}$ although, in the factorization of $(\mathbb{Z}/n\mathbb{Z})^*$ into a direct product of cyclic subgroups, $(\mathbb{Z}/8\mathbb{Z})^*$ and $(\mathbb{Z}/2^e\mathbb{Z})^*$ have different structure. This case leads to a different handling of the character sum considered in Lemma 2, and will be dealt with separately.

It should also be noted that the maximum of s_q is the number of powers p^e for which $p^e \parallel n, q^{v_q} \mid \lambda(p^e)$, and the minimum could be 0. For example, when $n = 17 \cdot 109 \cdot 433$, $\lambda(n) = 16 \cdot 27$, $v_2 = 4$ and $v_3 = 3$. It can be verified that, within prime factors of n and $a \in \{2, 3, 7\}$, $a^{\frac{p-1}{q}} \equiv 1 \pmod{p}$ only if $a = 2$ and $q = 2$ for $p = 17, 433$, or $a = 3$ and $q = 2$ for $p = 433$. Thus $s_2 = 0$ for $a = 2$, $s_2 = 1$ for $a = 3$ and $s_2 = 2$ (the maximum of s_2) for $a = 7$. Similarly, $s_3 = 0$ for $a = 2$, $s_3 = 1$ for $a = 19$ and $s_3 = 2$ (the maximum of s_3) for $a = 3$.

Now we can introduce the following theorem as an extension of Lemma 2.

Theorem 3. Let $n > 1$ be a natural number and $a \neq 0$ be an integer. Let d be a squarefree divisor of $\varphi(n)$. Then

$$\sum_{\substack{\chi \bmod n \\ \text{ord}(\chi)=d}}^{(E)} \chi(a) = \left(\prod_{\substack{q|d \\ s_q > 0}} (-1) \right) \left(\prod_{\substack{q|d \\ s_q = 0}} (q^{\Delta_q(n)} - 1) \right).$$

The symbol (E) in the theorem and in part (a) of Lemma 2 is unnecessary when $(\mathbb{Z}/n\mathbb{Z})^*$ is cyclic or p is odd, due to the comment following the definition of elementary character.

As a consequence of Lemma 2 and Theorem 3, we will present an alternative way to count the moduli in $P_a(x)$ or $N_a(x)$. Although Theorem 3 can be used to get a formula for $N_a(x)$, a deep investigation of such an application has yet been carried out.

2. Proof of Lemma 1 and Lemma 2

Proof of Lemma 1. Case I. Let p be an odd prime, or $p = 2$ and $e = 2$. Since $(\mathbb{Z}/p^e\mathbb{Z})^*$ is a cyclic group, $\varphi(p^e) = \lambda(p^e)$ and the following congruences are equivalent:

$$(3) \quad a \equiv b^{\bar{d}} \pmod{p^e} \quad \text{and} \quad a^{\frac{\varphi(p^e)}{\bar{d}}} \equiv 1 \pmod{p^e}$$

for some integer b . The last congruence is equivalent to

$$\text{ord}(a) \mid \varphi(p^e)/\bar{d} \quad \text{or} \quad \bar{d} \mid \varphi(p^e)/\text{ord}(a).$$

Let us write

$$\frac{\varphi(p^e)}{\text{ord}(a)} = \bar{d} \cdot k$$

for some integer k . We must have $\gcd(k, d/\bar{d}) = 1$ since otherwise $\bar{d}$ would not be the largest divisor of d satisfying the congruences in (3). Thus $\bar{d} = \gcd(d, \varphi(p^e)/\text{ord}(a))$.

Case II. Let $p = 2$ and $e \geq 3$. In this case, $d = 2$ is the only squarefree divisor of $\lambda(2^e)$ that is bigger than 1. For $e > 3$, if $\bar{d} = 2$ then

$$a^{\lambda(2^e)/2} \equiv (\pm 5^{2l})^{\lambda(2^e)/2} \equiv 1 \pmod{2^e}.$$

Thus

$$\text{ord}(a) \mid \lambda(2^e)/2 \quad \text{and} \quad \bar{d} = \gcd(d, \lambda(2^e)/\text{ord}(a)).$$

If $\bar{d} = 1$ then l is odd and

$$\text{ord}(a) = \text{ord}(\pm 5^l) = \lambda(2^e).$$

We still have $\bar{d} = \gcd(d, \lambda(2^e)/\text{ord}(a))$.

For $e = 3$, it can be verified directly from $a \equiv b^{\bar{d}} \pmod{8}$ that the above identity about $\bar{d}$ holds. This concludes the proof. $\square$

Proof of Lemma 2. Case I. Let p be an odd prime, or let $p = 2$ and $e = 2$. Then $(\mathbb{Z}/p^e\mathbb{Z})^*$ is a cyclic group. Let g be a generator modulo p^e . We have $a \equiv g^m \pmod{p^e}$ for some positive integer $m \leq \varphi(p^e)$. From the definition of $\bar{d}$, we can take $m = r \cdot \bar{d}$ where $(r, d/\bar{d}) = 1$. Now, if χ is a character modulo p^e with order d , then $\chi(g)$ is a primitive d -th root of unity, and vice versa. So we can write $\chi(g) = e\left(\frac{t}{d}\right)$ for some positive integer $t \in [1, d]$ coprime to d , where $e(u) = e^{2\pi i u}$. By the comment following Theorem 3, we have

$$\begin{aligned} \sum_{\substack{\chi \bmod n \\ \text{ord}(\chi)=d}}^{(E)} \chi(a) &= \sum_{\substack{\chi \bmod n \\ \text{ord}(\chi)=d}} \chi(a) \\ &= \sum_{\substack{1 \leq t \leq d \\ (t,d)=1}} e\left(\frac{r\bar{d}t}{d}\right) \\ &= \sum_{1 \leq t \leq d} e\left(\frac{r\bar{d}t}{d}\right) \sum_{d_1 \mid (t,d)} \mu(d_1) \\ &= \sum_{d_1 \mid d} \mu(d_1) \sum_{\substack{1 \leq t \leq d \\ \bar{d}_1 \mid t}} e\left(\frac{r\bar{d}t}{d}\right) \\ &= \sum_{d_1 \mid d} \mu(d_1) \sum_{1 \leq t_2 \leq d/d_1} e\left(\frac{r\bar{d}t_2}{d_2}\right). \end{aligned}$$

Here $t = t_2 \cdot d_1$ and $d = d_2 \cdot d_1$. Note that, if $d_2 \nmid r\bar{d}$ then the last sum is equal to

$$\left(e\left(\frac{r\bar{d}}{d_2}\right)^{d/d_1} - 1 \right) / \left(e\left(\frac{r\bar{d}}{d_2}\right) - 1 \right) = 0,$$

and, if $d_2 \mid r\bar{d}$, then it is equal to d/d_1 . Since $(r, d/\bar{d}) = 1$, $d/d_1 = d_2 \mid r\bar{d}$ is equivalent to $d/\bar{d} \mid d_1$. Thus,

$$(4) \quad \sum_{\substack{\chi \bmod n \\ \text{ord}(\chi)=d}} \chi(a) = \sum_{\substack{d_1 \mid d \\ d/\bar{d} \mid d_1}} \mu(d_1) \frac{d}{d_1} = d \sum_{\substack{d_1 \mid d \\ d/\bar{d} \mid d_1}} \frac{\mu(d_1)}{d_1}.$$

Furthermore, if we write $d_1 = (d/\bar{d}) \cdot d'$ for some integer d' , then $d_1 \mid d$ is equivalent to $d' \mid \bar{d}$ and the quantity in (4) is equal to

$$\mu(d/\bar{d}) \cdot \bar{d} \sum_{d' \mid \bar{d}} \frac{\mu(d')}{d'} = \mu\left(\frac{d}{\bar{d}}\right) \varphi(\bar{d}).$$

We have proved the lemma for Case I.

Case II. Let $p = 2$ and $e > 3$. In this case $(\mathbb{Z}/2^e\mathbb{Z})^*$ is a direct product of cyclic subgroups of orders respectively equal to 2 and 2^{e-2} (see [2]). In addition, -1 and 5 are generators of the two subgroups. Thus each odd number a verifies

$$a \equiv (-1)^k \cdot 5^l \pmod{2^e},$$

for unique integers $k \bmod 2$ and $l \bmod 2^{e-2}$. Each character mod 2^e can be factored as $\chi_1 \chi_2$, where χ_1 is a character for the subgroup generated by -1 and χ_2 is a character

of the subgroup generated by 5. If χ is elementary, then χ_1 is the principal character since χ needs to be trivial on the subgroup

$$E(2^e) = \{b \bmod 2^e : b^{2^{e-3}} \equiv 1 \bmod 2^e\}.$$

Thus $\chi(a) = \chi_2(5^l) = (-1)^l$. The value of $\chi(a)$ only depends on the parity of l . This proves the lemma for case II.

Case III. Let $p = 2$ and $e = 3$. The above conclusions about $(\mathbb{Z}/2^e\mathbb{Z})^*$ still hold. If χ is an elementary character modulo 8 of order 2, then either $\chi_1(-1) = -1$ or $\chi_2(5) = -1$. Thus there are three such characters in total. Therefore, if $a \equiv 1 \bmod 8$, namely $\bar{d} = 2$, then

$$\sum_{\substack{\chi \bmod 8 \\ \text{ord}(\chi)=2}} \chi(a) = 3.$$

If $a \not\equiv 1 \bmod 8$, namely $\bar{d} = 1$, then either k or l is odd. No matter which parity combination for k and l is considered, the character sum is equal to

$$(-1)^k + (-1)^l + (-1)^{k+l} = -1.$$

We are done for this case and thus for the lemma. $\square$

Remark 4. Note that although it is possible to deal with the character sum in Lemma 2 without restricting χ to elementary characters, the corresponding result will be irrelevant to its application in Theorem 3.

3. Proof of Theorem 3

It would be convenient to introduce some notations and properties related to the structure of $(\mathbb{Z}/n\mathbb{Z})^*$. Let $n = p_1^{e_1} \cdots p_r^{e_r}$, where $p_1 = 2$, $e_1 \geq 0$ and $p_2, \dots, p_r$ are distinct odd primes. Then

$$(\mathbb{Z}/n\mathbb{Z})^* = (\mathbb{Z}/p_1^{e_1}\mathbb{Z})^* \otimes \cdots \otimes (\mathbb{Z}/p_r^{e_r}\mathbb{Z})^*.$$

Using this factorization, each character χ modulo n can be factored as $\chi = \chi_1 \cdots \chi_r$ in the sense that $\chi(a) = \chi_1(a) \cdots \chi_r(a)$, where χ_i is a character mod $p_i^{e_i}$. It should also be noted that if $\chi \bmod n$ is an elementary character and $q \mid \text{ord}(\chi_i)$, then $q^{v_q} \mid \lambda(p_i^{e_i})$ where $q^{v_q} \parallel \lambda(n)$. Conversely, for each set of squarefree natural numbers $d_1, \dots, d_r$ satisfying that $q \mid d_i$ implies $q^{v_q} \mid \lambda(p_i^{e_i})$, any character $\chi = \chi_1 \cdots \chi_r$ with $\text{ord}(\chi_i) = d_i$ is an elementary character modulo n with order $d = [d_1, d_2, \dots, d_r]$, the least common multiple of $d_1, \dots, d_r$. Therefore,

$$\begin{aligned} \sum_{\substack{\chi \bmod n \\ \text{ord}(\chi)=d}}^{(E)} \chi(a) &= \sum_{\substack{(d_1, \dots, d_r): \\ d=[d_1, \dots, d_r] \\ q \mid d_i \Rightarrow q^{v_q} \mid \lambda(p_i^{e_i})}} \sum_{\substack{\chi_i \bmod p_i^{e_i} \\ \text{ord}(\chi_i)=d_i}}^{(E)} \chi_1(a) \cdots \chi_r(a) \\ (5) \quad &= \sum_{\substack{(d_1, \dots, d_r): \\ d=[d_1, \dots, d_r] \\ q \mid d_i \Rightarrow q^{v_q} \mid \lambda(p_i^{e_i})}} \prod_{i=1}^r \left(\sum_{\substack{\chi_i \bmod p_i^{e_i} \\ \text{ord}(\chi_i)=d_i}}^{(E)} \chi_i(a) \right), \end{aligned}$$

where (E) over the sums indicates that the characters involved in the sums are elementary characters for the corresponding moduli.

Note that p_i is an odd prime for $i \geq 2$. By Lemma 2, if $i \geq 2$, the inner sum in (5) is equal to

$$\left(\prod_{\substack{q \mid d_i \\ a \not\equiv b^q \pmod{p_i^{e_i}}}} (-1) \right) \cdot \left(\prod_{\substack{q \mid d_i \\ a \equiv b^q \pmod{p_i^{e_i}}}} \varphi(q) \right).$$

Moreover, χ_1 is an elementary character modulo 2^{e_1} if χ modulo n is an elementary character and $2 \mid \text{ord}(\chi_1)$ (or $d_1 = 2$). By Lemma 2, the above formula for the inner sum in (5) still holds for $i = 1$ (the congruences in the above product formula for the inner sum in (5) should be replaced by $a \not\equiv \pm 5^{2l} \pmod{2^{e_1}}$ and $a \equiv \pm 5^{2l} \pmod{2^{e_1}}$ respectively if $e_1 > 3$) except when $d_1 = 2$, $e_1 = 3$ and $a \equiv 1 \pmod{8}$ for which the corresponding sum is equal to 3. Let us introduce the function $\psi_i(q)$ for each i and each prime $q \mid d$ as follows. For $i \geq 2$, we define

$$\psi_i(q) = \begin{cases} 1 & \text{if } q \nmid d_i, \\ -1 & \text{if } q \mid d_i \text{ but } a \not\equiv b^q \pmod{p_i^{e_i}} \text{ for any } b, \\ \varphi(q) & \text{if } q \mid d_i \text{ and } a \equiv b^q \pmod{p_i^{e_i}} \text{ for some } b. \end{cases}$$

Note that the only possible order for χ_1 is either 1 or 2 if $\chi \pmod{n}$ is elementary. And since $a \equiv b^2 \pmod{2^{e_1}}$ is equivalent to $a \equiv 1 \pmod{2^{e_1}}$ for $e_1 \leq 3$, we define

$$\psi_1(2) = \begin{cases} 3 & \text{if } d_1 = 2 \text{ and } a \equiv 1 \pmod{2^{e_1}} \text{ for } e_1 = 3, \\ -1 & \text{if } d_1 = 2, \text{ but } a \not\equiv 1 \pmod{2^{e_1}} \text{ for } e_1 \leq 3, \text{ or } a \not\equiv \pm 5^{2l} \pmod{2^{e_1}} \\ & \text{for any } l \text{ and } e_1 > 3, \\ 1 & \text{otherwise.} \end{cases}$$

Note that the last case in the definition of $\psi_1(2)$ includes $d_1 = 1$, or $d_1 = 2$ but $a \equiv 1 \pmod{4}$, or $d_1 = 2$ but $a \equiv \pm 5^{2l} \pmod{2^{e_1}}$ for $e_1 > 3$ and some integer l .

Then for each i , we have

$$\sum_{\substack{\chi_i \pmod{p_i^{e_i}} \\ \text{ord}(\chi_i) = d_i}} \chi_i(a) = \prod_{q \mid d} \psi_i(q).$$

Plugging this formula into (5), we have

$$(6) \quad \sum_{\substack{\chi \pmod{n} \\ \text{ord}(\chi) = d}}^{(E)} \chi(a) = \sum_{\substack{(d_1, \dots, d_r): \\ d = [d_1, \dots, d_r] \\ q \mid d_i \Rightarrow q^{v_q} \mid \lambda(p_i^{e_i})}} \prod_{i=1}^r \prod_{q \mid d} \psi_i(q).$$

After the interchange of the order of the double product, we can write the double product as

$$(7) \quad \prod_{q \mid d} (-1)^{s'_q} \varphi(q)^{t'_q} 3^{u_q}.$$

Here s'_q is the number of i 's for which $q \mid d_i$ but $a \not\equiv b^q \pmod{p_i^{e_i}}$ for prime q and any integer b except the count of $i = 1$ in s'_2 when $e_1 > 3$ for which $i = 1$ will be counted in s'_2 if and only if $e_1 > 3$, $2 \mid d_1$, $a \not\equiv \pm 5^{2l} \pmod{p_1^{e_1}}$ for any integer l (namely s'_2 counts $i = 1$ if $d_1 = 2$, $e_1 = 3$ and $a \not\equiv b^2 \pmod{8}$). Moreover, t'_q is the number of i 's for which $q \mid d_i$ and $a \equiv b^q \pmod{p_i^{e_i}}$ for prime q and some integer b except the count of $i = 1$ in t'_2 when $e_1 \geq 3$ for which $i = 1$ will be counted if and only if $e_1 > 3$ and $a \equiv \pm 5^{2l} \pmod{p_1^{e_1}}$ for some integer l (namely t'_2 does not count $i = 1$ even if $d_1 = 2$, $e_1 = 3$ and $a \equiv 1 \pmod{8}$). Finally $u_q = 0$ for all primes q except when $q = 2$, $d_1 = 2$, $e_1 = 3$ and $a \equiv 1 \pmod{8}$ in which case $u_2 = 1$.

Simplifying the sum in (6) is now reduced to counting the number of the products (7) for all possible values of (s'_q, t'_q, u_q) where $q \mid d$.

Obviously, s'_q , t'_q and u_q are functions of $d_1, \dots, d_r$, n , q and a even though the notations only show their dependence on q . Recall that $n = p_1^{e_1} \cdots p_r^{e_r}$ where $p_1 = 2$ and $e_1 \geq 0$. Since s_q is defined before Theorem 3, let us define t_q as the number of i 's such that $q^{v_q} \mid \lambda(p_i^{e_i})$ and $a \equiv b^q \pmod{p_i^{e_i}}$ or $a \equiv \pm 5^{2l} \pmod{p_1^{e_1}}$ in the case of $q = 2$ and $e_1 > 3$ for some integer b or l . But $i = 1$ is excluded from t_2 even if $e_1 = 3$, $2^{v_2} \mid \lambda(p_1^{e_1})$ and $a \equiv 1 \pmod{p_1^{e_1}}$. Then we have $s_q + t_q = \Delta_q(n)$ except $q = 2$, $e_1 = 3$ and $2^{v_2} \mid \lambda(p_1^{e_1})$ for which case $s_2 + t_2 = r - 1 = \Delta_2(n) - 2$ if $a \equiv 1 \pmod{8}$ ($s_2 + t_2 = r$ if $a \not\equiv 1 \pmod{8}$). We also have the ranges for s'_q and t'_q :

$$0 \leq s'_q \leq s_q \quad \text{and} \quad 0 \leq t'_q \leq t_q$$

except $s'_q = 0 = t'_q$ because that is the case where $q \nmid d_i$ for any $i \neq 1$ (when $q = 2$ or $i = 1$, the case to be excluded is $s'_2 = t'_2 = u_2 = 0$). Uniformly, we just need to exclude the case where $s'_q = t'_q = u_q = 0$ since u_q is always 0 if $q \neq 2$. Let us regroup the sum in (6) into a double summation so that the inner sum is over all of $(d_1, d_2, \dots, d_r)$, for which s'_q and t'_q remain the same. Then the inner sum is equal to

$$\prod_{q \mid d} \binom{s_q}{s'_q} (-1)^{s'_q} \binom{t_q}{t'_q} \varphi(q)^{t'_q} 3^{u_q},$$

and (6) can be written as

$$\begin{aligned} \sum_{\substack{\chi \pmod{n} \\ \text{ord}(\chi)=d}}^{(E)} \chi(a) &= \sum_{\substack{(s'_q, t'_q): 0 \leq s'_q \leq s_q \\ 0 \leq t'_q \leq t_q \\ \text{except } s'_q=t'_q=u_q=0}} \prod_{q \mid d} \binom{s_q}{s'_q} (-1)^{s'_q} \binom{t_q}{t'_q} \varphi(q)^{t'_q} 3^{u_q} \\ (8) \quad &= \prod_{q \mid d} \sum_{\substack{0 \leq s'_q \leq s_q \\ 0 \leq t'_q \leq t_q \\ \text{except } s'_q=t'_q=u_q=0}} \binom{s_q}{s'_q} (-1)^{s'_q} \binom{t_q}{t'_q} \varphi(q)^{t'_q} 3^{u_q}. \end{aligned}$$

Note that if $q \neq 2$, the inner sum in (8) is equal to

$$(9) \quad \sum_{\substack{0 \leq s'_q \leq s_q \\ 0 \leq t'_q \leq t_q}} \binom{s_q}{s'_q} (-1)^{s'_q} \binom{t_q}{t'_q} \varphi(q)^{t'_q} - 1 = (1-1)^{s_q} (\varphi(q) + 1)^{t_q} - 1$$

$$= \begin{cases} -1 & \text{if } s_q > 0, \\ q^{\Delta_q(n)} - 1 & \text{if } s_q = 0. \end{cases}$$

When $q = 2$, we will deal with the sum in two cases:

$$\begin{cases} e_1 \neq 3 \text{ or } 4 \mid \lambda(n), \\ e_1 = 3 \text{ and } 2 \parallel \lambda(n). \end{cases}$$

In the first case we have $u_2 = 0$ because either $e_1 \neq 3$ or $e_1 = 3$ but $2^{v_2} \nmid \lambda(2^{e_1}) = 2$, which implies $d_1 \neq 2$. Thus (9) still holds for $q = 2$. Plugging (9) into (8), we get the theorem.

In the second case, $2^{v_2} = 2 \mid \lambda(2^{e_1})$. Then $a \not\equiv 1 \pmod 8$ or $a \equiv 1 \pmod 8$. If $a \not\equiv 1 \pmod 8$, by definition, $u_2 = 0$, t_2 does not count the modulus $2^3 \parallel n$ but s_2 does. The inner sum in (8) for $q = 2$ is still given by (9), which is equal to -1 . Plugging (9) (including the case for $q = 2$) into (8), we get the theorem. If $a \equiv 1 \pmod 8$, by definition, $u_2 = 1$, and both s_2 and t_2 do not count the modulus $2^3 \parallel n$. The modulus n can have elementary characters $\chi = \chi_1 \cdots \chi_r$, for which $2 \mid d_1 = \text{ord}(\chi_1)$. Thus depending on whether or not $2 \mid d_1$, the quantity in (8) can be split into two sums:

$$\begin{aligned} \sum_{\substack{\chi \bmod n \\ \text{ord}(\chi)=d}}^{(E)} \chi(a) &= \sum_{\substack{(s'_q, t'_q): 0 \leq s'_q \leq s_q \\ 0 \leq t'_q \leq t_q \\ \text{except } s'_q=t'_q=0 \text{ if } q \neq 2}} \sum_{q \mid d} 3^1 \cdot \prod \binom{s_q}{s'_q} (-1)^{s'_q} \binom{t_q}{t'_q} \varphi(q)^{t'_q} \\ &\quad + \sum_{\substack{(s'_q, t'_q): 0 \leq s'_q \leq s_q \\ 0 \leq t'_q \leq t_q \\ \text{except } s'_q=t'_q=0}} \sum_{q \mid d} 3^0 \cdot \prod \binom{s_q}{s'_q} (-1)^{s'_q} \binom{t_q}{t'_q} \varphi(q)^{t'_q} \\ &= \sum_{\substack{(s'_q, t'_q): 0 \leq s'_q \leq s_q \\ 0 \leq t'_q \leq t_q \\ \text{except } s'_q=t'_q=0 \text{ if } q \neq 2}} \sum_{q \mid d} 3^1 \cdot \prod \binom{s_q}{s'_q} (-1)^{s'_q} \binom{t_q}{t'_q} \varphi(q)^{t'_q} \\ &\quad + \sum_{\substack{(s'_q, t'_q): 0 \leq s'_q \leq s_q \\ 0 \leq t'_q \leq t_q \\ \text{except } s'_q=t'_q=0 \text{ if } q \neq 2}} \sum_{q \mid d} 3^0 \cdot \prod \binom{s_q}{s'_q} (-1)^{s'_q} \binom{t_q}{t'_q} \varphi(q)^{t'_q} \\ &\quad - \sum_{\substack{q > 2 \text{ and } (s'_q, t'_q): \\ 0 \leq s'_q \leq s_q \text{ and } 0 \leq t'_q \leq t_q \\ \text{except } s'_q=t'_q=0}} \sum_{\substack{q \mid d \\ q > 2}} 3^0 \cdot \prod \binom{s_q}{s'_q} (-1)^{s'_q} \binom{t_q}{t'_q} \varphi(q)^{t'_q}, \end{aligned}$$

where the last two sums after the second equal sign split from the last sum before the second equal sign, depending on whether to exclude the case $s'_2 = t'_2 = 0$ in the sum or not. Then, we get

$$\begin{aligned}
 \sum_{\substack{\chi \bmod n \\ \text{ord}(\chi)=d}}^{(e)} \chi(a) &= \sum_{\substack{(s'_q, t'_q): 0 \leq s'_q \leq s_q \\ 0 \leq t'_q \leq t_q \\ \text{except } s'_q=t'_q=0 \text{ if } q \neq 2}} 4 \cdot \prod_{q|d} \binom{s_q}{s'_q} (-1)^{s'_q} \binom{t_q}{t'_q} \varphi(q)^{t'_q} \\
 (10) \quad &- \sum_{\substack{q>2 \text{ and } (s'_q, t'_q): \\ 0 \leq s'_q \leq s_q \text{ and } 0 \leq t'_q \leq t_q \\ \text{except } s'_q=t'_q=0}} 3^0 \cdot \prod_{\substack{q|d \\ q>2}} \binom{s_q}{s'_q} (-1)^{s'_q} \binom{t_q}{t'_q} \varphi(q)^{t'_q}.
 \end{aligned}$$

Note that here s'_2 and t'_2 do not count the case $i = 1$ because $i = 1$ is dealt with in the factors 3^1 and 3^0 , and the same for s_2 and t_2 . Thus $s_2 + t_2 = r - 1$. Similar to the simplification of the inner sum in (8), we can write the difference of the two sums in (10) as

$$((1-1)^{s_2} (\varphi(2) + 1)^{t_2} \cdot 4 - 1) \cdot \prod_{\substack{q|d \\ q>2}} ((1-1)^{s_q} (\varphi(q) + 1)^{t_q} - 1).$$

Note that if $s_2 = 0$ then $t_2 + 2 = s_2 + t_2 + 2 = r + 1 = \Delta_2(n)$. So the first factor of the last product above is equal to $2^{\Delta_2(n)} - 1$ if $s_2 = 0$, and -1 if $s_2 > 0$. Combining this and (9) with (8) and (10) proves the theorem for the second case. That concludes the proof of the theorem.

4. Formulation of $P_a(x)$ by Lemma 2

As an application of Lemma 2, we would like to present a formula for $P_a(x)$, the number of prime moduli up to x for which a is a primitive root. Recall that, for a squarefree divisor d of $p - 1$, $\bar{d}$ is the largest divisor of d for which $a \equiv b^{\bar{d}} \pmod{p}$ for some integer b . In such a situation, we will write “ p passes $\bar{d}$ -test”.

Since every character modulo p with a squarefree order is elementary, by Lemma 2, we have

$$\sum_{\substack{\chi \bmod p \\ \text{ord}(\chi)=d}} \chi(a) = \mu(d/\bar{d}) \cdot \varphi(\bar{d}).$$

Thus, by (1) and (2), we have

$$\begin{aligned}
 P_a(x) &= \sum_{p \leq x} \sum_{\chi \bmod p} c(\chi) \chi(a) \\
 &= \sum_{p \leq x} \sum_{d \mid p-1} \frac{\mu(d)}{\varphi(d)} \cdot \frac{\varphi(p-1)}{p-1} \sum_{\substack{\chi \bmod p \\ \text{ord}(\chi)=d}} \chi(a) \\
 &= \sum_{p \leq x} \sum_{d \mid p-1} \frac{\mu(d)}{\varphi(d)} \cdot \frac{\varphi(p-1)}{p-1} \cdot \frac{\mu(\bar{d})}{\mu(\bar{d})} \varphi(\bar{d}) \\
 (11) \quad &= \sum_{d \leq x} \frac{\mu^2(d)}{\varphi(d)} \sum_{\bar{d} \mid d} \mu(\bar{d}) \varphi(\bar{d}) \sum_{\substack{p \leq x \\ p \equiv 1 \bmod d \\ p \text{ passes } \bar{d}\text{-test}}} \frac{\varphi(p-1)}{p-1}.
 \end{aligned}$$

We can write

$$\frac{\varphi(p-1)}{p-1} = \frac{\varphi(d)}{d} \cdot \prod_{\substack{q \mid p-1 \\ q \nmid d}} \left(1 - \frac{1}{q}\right),$$

and

$$\prod_{\substack{q \mid p-1 \\ q \nmid d}} \left(1 - \frac{1}{q}\right) = \sum_{\substack{d' \mid p-1 \\ (d', d)=1}} \frac{\mu(d')}{d'}.$$

Since $dd' \mid p-1$ and $p \leq x$, we have that $d' \leq (x-1)/d$. Thus,

$$\begin{aligned}
 P_a(x) &= \sum_{d \leq x} \frac{\mu^2(d)}{d} \sum_{\bar{d} \mid d} \mu(\bar{d}) \varphi(\bar{d}) \sum_{\substack{p \leq x \\ p \equiv 1 \bmod d \\ p \text{ passes } \bar{d}\text{-test}}} \sum_{\substack{d' \mid p-1 \\ (d', d)=1}} \frac{\mu(d')}{d'} \\
 (12) \quad &= \sum_{d \leq x} \frac{\mu^2(d)}{d} \sum_{\bar{d} \mid d} \mu(\bar{d}) \varphi(\bar{d}) \sum_{\substack{d' \leq (x-1)/d \\ (d', d)=1}} \frac{\mu(d')}{d'} \sum_{\substack{p \leq x \\ p \equiv 1 \bmod d \cdot d' \\ p \text{ passes } \bar{d}\text{-test}}} 1.
 \end{aligned}$$

This formula results from a straight application of Lemma 2.

Because of involvement of extra variables d and d' in the formulation for $P_a(x)$, (12) seems to be more complicated than the formula for $P_a(x)$ in Hooley's conditional proof of Artin's conjecture [5] (where only the variable $\bar{d}$ is involved), but there is a factor $\frac{1}{d \cdot d'}$ in front of the inner sum in formula (12), which could have a positive impact in estimation of sums of certain error terms separated from the inner sum. Although the two formulas for $P_a(x)$ are different, the idea to deal with the inner sum of (12) is similar. Hooley splits the inner sum into two sums; one sum takes into account the primes which satisfy the same conditions plus that every prime factor of $\bar{d}$ is less than $\frac{1}{6} \log x$ and the other sum takes into account the rest of primes. The first sum is estimated by an asymptotic formula, which is obtained under assumption of ERH, while the second sum is handled for an upper bound with unconditional arguments.

In order to apply formula (12), we can split the inner sum differently. Note that the primes counted in the inner sum are the primes up to x which split completely in the

field $L = \mathbb{Q}(\sqrt[d]{a}, \sqrt[d \cdot d']{1})$. Let $n_L = [L : \mathbb{Q}]$ and let d_L be the discriminant of L over $\mathbb{Q}$. If we denote the inner sum of (12) by $P(a, x)$, by a result of Lagarias and Odlyzko [7], we have

$$(13) \quad \left| P(a, x) - \frac{\text{li}(x)}{n_L} \right| \leq \frac{\text{li}(x^\beta)}{n_L} + c_1 x \cdot \exp \left(-c_2 \left(\frac{\text{li}(x)}{n_L} \right)^{1/2} \right)$$

for all $x \geq \exp(10n_L \ln^2 d_L)$, where $\text{li}(x) = \int_2^\infty \frac{dt}{\log t}$, c_1 and c_2 are positive constants, and β is a real zero of the Dedekind zeta function of L and in the range

$$1 - \frac{1}{4 \ln d_L} \leq \beta \leq 1 - \frac{1}{c d_L^{1/n_L}}$$

with $c > 0$ being an absolute constant; the requirement of a , for which (13) holds, is that $|a|$ is not a q -th power for any prime factor of $\bar{d}$ or not twice of a square if $q = 2$. It can be determined that n_L is equal to $\bar{d} \cdot \varphi(d \cdot d')$, or to half of the number depending on the structure of a . In order to meet the condition $x \geq \exp(10n_L \ln^2 d_L)$, we would need that n_L or $d \cdot d' \leq (\ln x)^\delta$ for some positive number $\delta < 1/6$. This equivalently splits the inner sum into two sums depending on whether or not $dd' \leq (\ln x)^\delta$ (such a split would be eventually carried out somehow on the summation over d and d'). Let us call them as $\sum_1$ and $\sum_2$. Then $\sum_1$ can be estimated using (13).

However, $\sum_2$ could not be handled using Hooley's argument in [5] because dd' can be close to $(\ln x)^\delta$, way too small from what is handled in [5]. A convenient way is to introduce a conjecture to the inner sum of (12) similar to the Brun-Titchmarsh inequality [18] for the arithmetic progression. That is,

$$(14) \quad \sum_{\substack{p \leq x \\ p \equiv 1 \pmod{dd'} \\ p \text{ passes } \bar{d}\text{-test}}} 1 \ll \frac{\text{li}(x)}{n_L}$$

uniformly for all of $D = dd'$ and x , where the involved constant is an absolute constant. Computations on lower values of D and $\bar{d}$ shows that this constant can be 3 at most. With (14), the above argument would lead to $P_a(x) = A(a)\text{li}(x) + o(\text{li}(x))$ where the constant $A(a)$ is the same as in Hooley's formula for $P_a(x)$ in [5].

Although $N_a(x)$ counts the number of positive moduli $n \leq x$ for which a is a primitive λ -root, $N_a(x)$ shares the same counting mechanism as $P_a(x)$, namely

$$N_a(x) = \sum_{n \leq x} \sum_{\chi \pmod{n}} c(\chi) \chi(a).$$

By formula (2) for $c(\chi)$, we can write

$$N_a(x) = \sum_{n \leq x} \sum_{d \mid \varphi(n)} \frac{\mu(d)}{\rho_n(d)} \cdot \frac{R(n)}{\varphi(n)} \sum_{\substack{\chi \pmod{n} \\ \text{ord}(\chi)=d}}^{(E)} \chi(a),$$

where an application of Theorem 3 to the inner sum of the concerned equation leads to a formula for $N_a(x)$. Because of the complication of the formula in Theorem 3, further investigation is necessary to determine if such a formula could lead to any development of an unconditional estimate for the magnitude of $N_a(x)$.

Acknowledgements. The author is grateful to Pieter Moree and the referee for making valuable comments and suggestions that enriched the article.

REFERENCES

- [1] R. D. Carmichael, *The theory of numbers*, Wiley, New York, 1914.
- [2] H. Davenport, *Multiplicative number theory*, Third edition, Revised and with a preface by Hugh L. Montgomery, Graduate Texts in Mathematics, **74**, Springer-Verlag, New York, 2000, xiv+177 pp.
- [3] M. Goldfeld, *Artin's conjecture on the average*, *Mathematika* **15** (1968), 223–226.
- [4] D. R. Heath-Brown, *Artin's conjecture for primitive roots*, *Quart. J. Math. Oxford Ser. (2)* **37** (1986), no. 145, 27–38.
- [5] C. Hooley, *On Artin's conjecture*, *J. Reine Angew. Math.* **225** (1967), 209–220.
- [6] E. Jensen and M. R. Murty, *Artin's conjecture for polynomials over finite fields*, *Number theory*, 167–181, *Trends Math.*, Birkhäuser, Basel, 2000.
- [7] J. C. Lagarias and A. M. Odlyzko, *Effective versions of the Chebotarev density theorem*, in *Algebraic number fields: L -functions and Galois properties* (Proc. Sympos., Univ. Durham, Durham, 1975), pp. 409–464. Academic Press, London, 1977.
- [8] S. Li, *On Artin's conjecture for composite moduli*, Ph.D. thesis (U. of Georgia), 1998, 115 pp.
- [9] S. Li, *On extending Artin's conjecture to composite moduli*, *Mathematika* **46** (1999), no. 2, 373–390.
- [10] S. Li, *An improvement of Artin's conjecture on average for composite moduli*, *Mathematika* **51** (2004), no. 1-2, 97–109 (2005).
- [11] S. Li and C. Pomerance, *On generalizing Artin's conjecture on primitive roots to composite moduli*, *J. Reine Angew. Math.* **556** (2003), 205–224.
- [12] S. Li and C. Pomerance, *The Artin-Carmichael primitive root problem on average*, *Mathematika* **55** (2009), no. 1–2, 167–176.
- [13] P. J. McCarthy, *Introduction to arithmetical functions*, Universitext, Springer-Verlag, New York, 1986, vii+365 pp.
- [14] P. Moree, *On primes in arithmetic progression having a prescribed primitive root*, *J. Number Theory* **78** (1999), no. 1, 85–98.
- [15] P. Moree, *Asymptotically exact heuristics for (near) primitive roots*, *J. Number Theory* **83** (2000), no. 1, 155–181.
- [16] M. R. Murty, *Artin's conjecture for primitive roots*, *Math. Intelligencer* **10** (1988), no. 4, 59–67.
- [17] P. J. Stephens, *An average result for Artin's conjecture*, *Mathematika* **16** (1969), 178–188.
- [18] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Translated from the second French edition (1995) by C. B. Thomas, *Cambridge Studies in Advanced Mathematics*, **46**, Cambridge University Press, Cambridge, 1995, xvi+448 pp.