NOTES ON THE NUMBER OF PRIMITIVE λ-ROOTS MOD n AND ITS MULTIPLICATIVE PROPERTIES

Benjamin Huang
Department of Physics, UC Berkeley, Berkeley, California
benhua476@berkeley.edu

Shuguang Li
Department of Mathematics, University of Hawaii, Hilo, Hawaii,
shuguang@hawaii.edu

Received: 8/17/23, Revised: 7/29/24, Accepted: 3/17/25, Published: 4/25/25

Abstract

Let $n > 1$ be a positive integer. An integer a is called *a primitive λ-root mod n* if $\gcd(a, n) = 1$ and a has the maximum multiplicative order modulo n. Let $R(n)$ be the number of primitive λ-roots mod n. We show that $R(mn) \geq R(m)R(n)$ whenever $\gcd(m, n) = 1$. We also find the necessary and sufficient conditions for the equality to hold. Additional numerical data about the function $R(n)$ are included at the end of the paper.

1. Introduction

Throughout the article, we use n and a to denote integers with $n > 1$, and we use p and q to denote prime numbers. It is not hard to see that if $\gcd(a, n) = 1$, then $a^e \equiv 1 \mod n$ for some positive integers e. The least such integer is called the *multiplicative order* of $a \bmod n$, and is denoted by $l_a(n)$. Note that $l_a(n)$ is also the multiplicative order of the residue class $\bmod n$ containing a in $(\mathbb{Z}/n\mathbb{Z})^*$. For any fixed modulus n, the largest value of $l_a(n)$ is denoted by $\lambda(n)$. An integer a is called a *primitive λ-root modulo n* if $\gcd(a, n) = 1$ and $l_a(n) = \lambda(n)$. We may also call the corresponding residue class mod n containing such integers a primitive λ-root $\bmod n$. The primitive λ-root modulo n was initially introduced by Carmichael [1] in 1914. He also found that $\lambda(p^r) = \phi(p^r)$, where ϕ is Euler-ϕ function, except when $p = 2$ with $r > 2$, for which case $\lambda(2^r) = \frac{1}{2}\phi(2^r)$. When $n = 2, 4, p^r$ or $2p^r$ where p is an odd prime, it is well-known that $(\mathbb{Z}/n\mathbb{Z})^*$ is a cyclic group and $\lambda(n) = \phi(n)$. In this case, any integer a, for which $l_a(n) = \phi(n)$, is called a *primitive root mod n*. Thus a primitive λ-root $\bmod n$ is a primitive root $\bmod n$ in this case. So primitive λ-root $\bmod n$ is a generalization of the primitive root $\bmod n$.

DOI: 10.5281/zenodo.15283681

Let us count primitive λ-roots $\bmod n$ from two perspectives. First let us fix the integer a and count the number of moduli n up to x, for which a is a primitive λ-root. We denote this number by $N_a(x)$. Then let us fix the modulus n and count the number of primitive λ-roots $a \bmod n$. We denote the second number by $R(n)$. Although the functions $N_a(x)$ and $R(n)$ count primitive λ-roots from two different perspectives, they are connected through the average of $N_a(x)$. Li [5] proved that, for $x > e^3$ and $y \geq \exp\left((\ln x)^{3/4}\right)$, we have

$$\frac{1}{y}\sum_{a\leq y} N_a(x) = \sum_{n\leq x}\frac{R(n)}{n} + O(x\cdot\exp(-E(x,y)), \tag{1}$$

where $E(x,y) \gg \frac{5}{16}(\ln x)^{\frac{1}{2}}$ for some absolute constant and all $y \geq \exp\left((\ln x)^{3/4}\right)$. So the magnitude of $\sum_{n\leq x} R(n)/n$ helps to understand the average order of function $N_a(x)$. Li [3] proved that there exists a positive constant c_1 such that $\sum_{n\leq x} R(n)/n \geq c_1 x$ on a unbounded set of x, and $\sum_{n\leq x} R(n)/n = o(x)$ on another unbounded set of x. The behavior of the average order of $N_a(x)$ is matched by the behavior of individual $N_a(x)$ in the following sense. Let $\mathcal{E}$ denote the set of integers which are a power with an exponent larger than 1, or a square times either -1 or ± 2. According to the results of Li [4] and Pomerance [6], if $a \notin \mathcal{E}$, the individual $N_a(x)/x$ oscillates between 0 and another positive constant c_2 depending on a, as x gets large. In the estimate of $\sum_{n\leq x} R(n)/n$, we only used a basic formula for $R(n)$, which will be presented below. Any other arithmetic properties of $R(n)$ are not only interesting to the function, but may also be helpful for sharpening or better understanding the above results.

One objective of the paper is to explore numerically the values of $R(n)/n$ over a small interval of x to see whether or not there is an oscillation of $\sum_{n\leq x} R(n)/n$ within such an interval. The result is presented in the last section. The data of $R(n)$ from the last section also helps us in shaping our main theorem below.

Another objective of the paper is to investigate the multiplicativity of $R(n)$. An arithmetic function $f(n)$ is called a *multiplicative function* if $f(mn) = f(m)f(n)$ whenever $\gcd(m,n) = 1$. If $R(n)$ is a multiplicative function, then the estimate of $\sum_{n\leq x}\frac{R(n)}{n}$ may be obtained easier, and one may get a sharper estimate for the above sum and some other functions related to $R(n)$ as one can see in Schoenberg [9]. Unfortunately, we do not have such privilege to deal with the functions because one can easily find a counterexample, which shows that $R(n)$ is not a multiplicative function. Then we may ask how likely or unlikely $R(mn) = R(m)R(n)$ when $\gcd(m,n) = 1$. This is the other question that we want to solve in this paper. To answer this question, we need to bring up a formula for $R(n)$, for which we need to introduce several notions.

For $n > 1$ and prime p, if p^v divides n but p^{v+1} does not divide n, we denote the division by $p^v \| n$. When $n = 2$, $\lambda(n) = 1$ and $R(n) = 1$. When $n > 2$, $\lambda(n) > 1$. Let q be a prime divisor of $\lambda(n)$. Then for a unique integer $v \geq 1$, we have $q^v \| \lambda(n)$.

Note that the exponent v depends on both q and n. Let $\Delta_q(n) := \#\{\text{prime } p : p^e \| n \text{ and } q^v | \lambda(p^e)\}$ where $q^v \| \lambda(n)$, except the case $2^3 \| n$ and $2 \| \lambda(n)$, for which $\Delta_2(n) := 1 + \#\{\text{prime } p : \ p | n\}$. It should be pointed out that q^v is the maximum order of the cyclic subgroups of $(\mathbb{Z}/n\mathbb{Z})^*$ with prime power orders for prime q, and $\Delta_q(n)$ is the number of cyclic subgroups of order q^v in the factorization of $(\mathbb{Z}/n\mathbb{Z})^*$ into the direct product of cyclic subgroups of prime power orders. Martin [7] and Li [2] proved independently that

$$R(n) = \phi(n) \prod_{q|\lambda(n)} \left(1 - \frac{1}{q^{\Delta_q(n)}}\right). \tag{2}$$

We obtain the following result.

Theorem 1. *Let $m, n > 1$ with $\gcd(m, n) = 1$. We have $R(mn) \geq R(m)R(n)$, where the equality holds if and only if $m = 2$ and n is odd, or $n = 2$ and m is odd.*

2. Preliminary Results

From (2), we have

$$\frac{R(n)}{\phi(n)} = \prod_{q|\lambda(n)} \left(1 - \frac{1}{q^{\Delta_q(n)}}\right).$$

Note that $\Delta_q(n) > 0$ if and only if $q|\lambda(n)$. If $q \nmid \lambda(n)$, we define $\Delta_q(n) = 0$. If $q \nmid \lambda(n)$, q does not appear in the product. We can also say that the contribution of the prime q to the above product is 1. So it is easier and more effective to introduce a new function for each prime q.

Let

$$h_q(n) = \begin{cases} 1 - \frac{1}{q^{\Delta_q(n)}}, & \text{if } \Delta_q(n) > 0 \\ 1, & \text{if } \Delta_q(n) = 0. \end{cases} \tag{3}$$

It is easy to see that

$$\frac{R(n)}{\phi(n)} = \prod_{\text{prime } q} h_q(n). \tag{4}$$

Lemma 1. *Let $m, n > 1$ with $\gcd(m, n) = 1$. Then $\lambda(mn) = \operatorname{lcm}(\lambda(m), \lambda(n))$.*

Proof. The result can be deduced easily from the following identity:

$$\lambda(n) = \operatorname{lcm}_{p^e \| n}\{\lambda(p^e)\},$$

which is obtained in Carmichael [1]. □

Lemma 2. *Suppose that $m, n > 1$ and $\gcd(m, n) = 1$. Then, for any prime divisor q of $\lambda(mn)$, we have*

$$h_q(mn) \geq h_q(m)h_q(n)$$

where the strict inequality holds if and only if one of the following conditions holds:

(*i*) $\Delta_q(mn) > \Delta_q(m) > 0$,

(*ii*) $\Delta_q(mn) > \Delta_q(n) > 0$,

(*iii*) $\Delta_q(m) > 0$, $\Delta_q(n) > 0$ *and* $\Delta_q(mn)$ *is equal to one of the two integers.*

Proof. Since $q|\lambda(mn)$, we have $q^v \| \lambda(mn)$ for some $v > 0$. By Lemma 1, q^v divides one of $\lambda(m)$ or $\lambda(n)$. Without loss of generality, let us assume that $q^v|\lambda(m)$. Actually we have $q^v \| \lambda(m)$. By the definition of Δ_q, we have that

$$\Delta_q(m) := \#\{\text{prime } p : \ p^e \| m \text{ and } q^v | \lambda(p^e)\}$$

except $8\|m$ and $q = 2\|\lambda(m)$ or $v = 1$. In the meantime,

$$\Delta_q(mn) := \#\{\text{prime } p : \ p^e \| mn \text{ and } q^v | \lambda(p^e)\}.$$

Since $\gcd(m, n) = 1$, we have that $\Delta_q(mn) \geq \Delta_q(m) \geq 1$. In the case $8\|m$ and $2\|\lambda(m)$, all the odd prime factors p of m and n must be in the arithmetic progression $p \equiv 3 \mod 4$. Thus,

$$\begin{aligned} \Delta_2(mn) &= 1 + \#\{\text{prime } p : \ p|mn\} \\ &= 1 + \#\{\text{prime } p : \ p|m\} + \#\{\text{prime } p : \ p|n\} \\ &= \Delta_2(m) + \Delta_2(n). \end{aligned}$$

We still have that $\Delta_q(mn) \geq \Delta_q(m) \geq 1$. Therefore, for any $q|\lambda(mn)$, we have

$$h_q(mn) = 1 - \frac{1}{q^{\Delta_q(mn)}} \geq 1 - \frac{1}{q^{\Delta_q(m)}} = h_q(m) \geq h_q(m)h_q(n),$$

because $1 \geq h_q(n)$ by the definition of h_q.

Next let us deal with the strict inequality. It is not hard to see that if one of the three conditions holds, then $h_q(mn) > h_q(m)h_q(n)$. Conversely, assume that $h_q(mn) > h_q(m)h_q(n)$. If the condition (*i*) or (*ii*) holds, then we are done. So we only need to consider the case that both conditions (*i*) and (*ii*) fail. Since $q|\lambda(mn)$, we can assume that $q^v \| \lambda(mn)$ for some $v > 0$. By Lemma 1, $q^v|\lambda(m)$ or $q^v|\lambda(n)$. Without loss of generality, let us assume that $q^v|\lambda(m)$. Then $\Delta_q(m) > 0$. Since condition (*i*) fails, we must have $\Delta_q(mn) = \Delta_q(m)$. Thus $h_q(mn) = h_q(m) = 1 - 1/q^{\Delta_q(m)}$, and inequality $h_q(mn) > h_q(m)h_q(n)$ yields that

$$1 > h_q(n),$$

which yields that $\Delta_q(n) > 0$. We obtain the condition (*iii*). We have proved the lemma. □

3. Proof of the Main Theorem

Proof of Theorem 1. Since $\gcd(m,n)=1$, we have that $\phi(mn)=\phi(m)\phi(n)$. Therefore, we only need to prove that

$$\frac{R(mn)}{\phi(mn)} \geq \frac{R(m)}{\phi(m)}\frac{R(n)}{\phi(n)}, \tag{5}$$

and the sufficient and necessary conditions for the equality.

For each $q|\lambda(mn)$, we have $h_q(mn) \geq h_q(m)h_q(n)$ by Lemma 2. We obtain (5) by identity (4).

Next let us prove the conditions for the equality to hold. If $m=2$ and n is odd, then $R(m)=1$ and $R(2n)=R(n)$. So we have $R(mn)=R(m)R(n)$. This can also be obtained by using the isomorphism between $(\mathbb{Z}/(2n)\mathbb{Z})^*$ and $(\mathbb{Z}/n\mathbb{Z})^*$. The equality holds similarly for the case where m is odd and $n=2$.

Conversely assume that $m,n>2$ and $\gcd(m,n)=1$. We will show that $R(mn)\neq R(m)R(n)$. Since we have proved (5), we only need to show that $R(mn)>R(m)R(n)$, which is equivalent to

$$\frac{R(mn)}{\phi(mn)} > \frac{R(m)}{\phi(m)}\frac{R(n)}{\phi(n)}. \tag{6}$$

`Case 1:` $m>2$ and $n>2$ are both odd. In this case, 2 is a divisor of $\lambda(m)$ and $\lambda(n)$. Let us assume that $2^{v_1}\|\lambda(m)$ and $2^{v_2}\|\lambda(n)$. Without loss of generality, we may assume that $v_1\leq v_2$. If $v_1<v_2$, then $2^{v_2}\|\lambda(mn)$ by Lemma 1. And $\Delta_2(mn)=\Delta_2(n)>0$ by the definition of Δ_2. But $\Delta_2(m)>0$, so by Lemma 2, we obtain $h_2(mn)>h_2(m)h_2(n)$. By Lemma 2 again, we have (6). If $v_1=v_2$, then $\Delta_2(mn)=\Delta_2(m)+\Delta_2(n)$ because $2^{v_1}\|\lambda(m), 2^{v_1}\|\lambda(n), 2^{v_1}\|\lambda(mn)$ and $\gcd(mn)=1$. By Lemma 2, we still obtain $h_2(mn)>h_2(m)h_2(n)$ and (6). Therefore, we have $R(mn)>R(m)R(n)$.

`Case 2:` $m>2$ and $n>2$ have the opposite parity. Without loss of generality, we can assume that m is even and n is odd. Since $m,n>2$, it follow easily that 2 is a divisor of $\lambda(m)$ and $\lambda(n)$. Let v_1 and v_2 be the same as in case 1. By the definition of Δ_2, we have that

$$\Delta_2(m) := \#\{\text{prime } p:\ p^e\|m \text{ and } 2^{v_1}|\lambda(p^e)\} \tag{7}$$

except that $8\|m$ and $2\|\lambda(m)$ (or $v_1=1$). This formula can also apply to $\Delta_2(n)$ with v_1 replaced by v_2.

If $v_1<v_2$, then $v_2\geq 2$. We can apply (7) to mn and get

$$\Delta_2(mn) := \#\{\text{prime } p:\ p^e\|mn \text{ and } 2^{v_2}|\lambda(p^e)\}.$$

Note that we replace v_1 in (7) by v_2 because $2^{v_2}\|\lambda(mn)=\operatorname{lcm}(\lambda(m),\lambda(n))$ by Lemma 1. Thus we have $\Delta_2(mn)=\Delta_2(n)>0$, and in the meantime $\Delta_2(m)>0$.

By Lemma 2, we obtain (6). Similarly, if $v_1 > v_2$, then $\Delta_2(mn) = \Delta_2(m) > 0$, and obviously $\Delta_2(n) > 0$. We still obtain (6).

If $v_1 = v_2$, then $2^{v_1} \| \lambda(m), 2^{v_1} \| \lambda(n)$, and $2^{v_1} \| \lambda(mn)$. If $v_1 > 1$ or 8 is not the maximum power of 2 that divides m, we have, by applying (7) to mn, that $\Delta_2(mn) = \Delta_2(m) + \Delta_2(n)$. We obtain (6) by Lemma 2.

If $v_1 = 1$ and $8 \| m$, then $\Delta_2(mn) = 1 + \#\{\text{prime } p : \ p|mn\} = \Delta_2(m) + \Delta_2(n)$. By Lemma 2, we obtain Inequality (6). Therefore, we have proved the theorem. □

4. Numerical Values $R(n)$ within Small Intervals

One of our objectives is to investigate $\sum_{n \le x} \frac{R(n)}{n}$ numerically to see whether or not it oscillates as x gets large. However, due to the complexity of $\Delta_q(n)$ and $R(n)$ as shown in (2), it is impossible to carry out calculations of $\Delta_q(n)$, $R(n)$, and $\sum_{n \le x} \frac{R(n)}{n}$ by hand. We implemented an algorithm for calculating $R(n)$, and we ran some computations regarding functions $y = \frac{R(n)}{n}$, $y = \sum_{n \le x} \frac{R(n)}{n}$ and $y = R(mn) - R(m)R(n)$. Our calculations show that $y = \sum_{n \le x} \frac{R(n)}{n}$ does not show significant oscillations over small intervals of x as one can see in Figure 1.

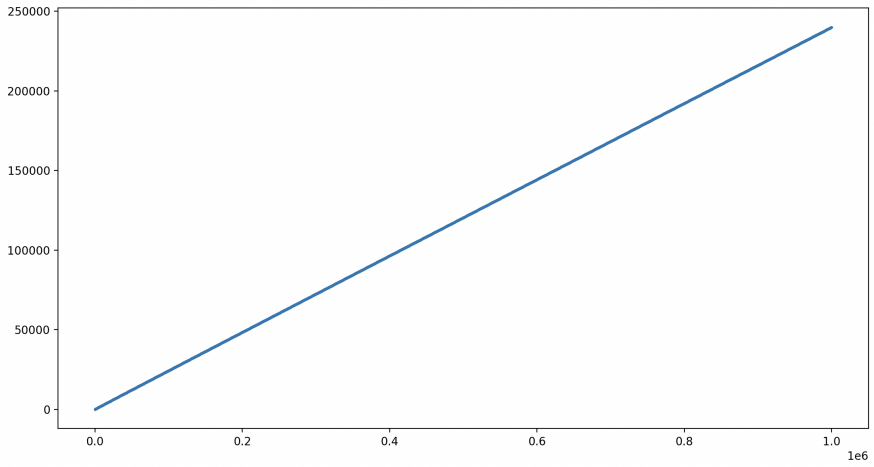

Figure 1: y=$\sum_{n \le x} \frac{R(n)}{n}$, $2 \le x \le 1,000,000$

Figure 1 shows that $y = \sum_{n \le x} \frac{R(n)}{n} \approx kx$ for some constant $k < 1/4$. However, $\frac{R(n)}{n}$ does show violent oscillation between 0 and 1 as in the next figure.

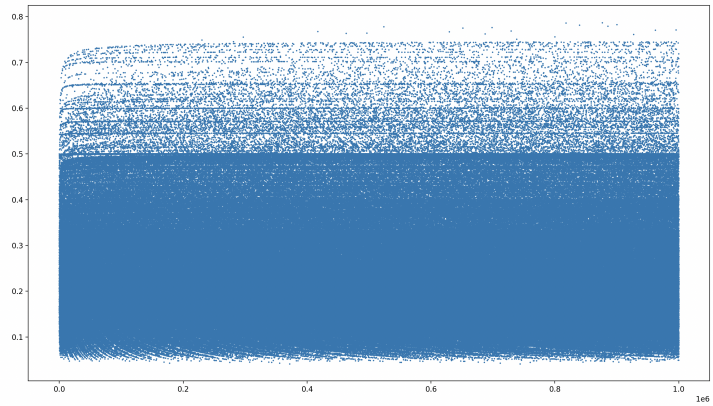

Figure 2: y=$R(n)/n$, $2 \leq n \leq 1,000,000$

From Figure 2, it can be implied that the function $y = \sum_{n \leq x} \frac{R(n)}{n}$ is more like a linear function. First, it can be noticed that the graph of $y = \frac{R(n)}{n}$ is formed by points in the region $1 \leq n \leq 1,000,000$ and $0 \leq y \leq 1$. Secondly, these points are almost evenly distributed horizontally, but unevenly distributed vertically. However, they are dense in the vertical zone $0.045 \leq y \leq 0.5$. This dense zone does not have any significant vertical shifts or oscillations. Thus, when we take the sum of $R(n)/n$ for $1 \leq n \leq x$, function $y = \sum_{n \leq x} \frac{R(n)}{n} \approx kx$ for some constant k. This indicates that we do not see oscillation of $\frac{1}{x} \sum_{n \leq x} \frac{R(n)}{n}$ between a positive number and 0 as x increases from $x = 2$ to $x = 1,000,000$. Our computer has a hard time verifying the data of $R(n)/n$ beyond the above range.

However, when we zoom into a smaller interval, the graph of $y = \frac{R(n)}{n}$ contains some interesting curve patterns as shown in Figure 3, which we cannot explain yet.

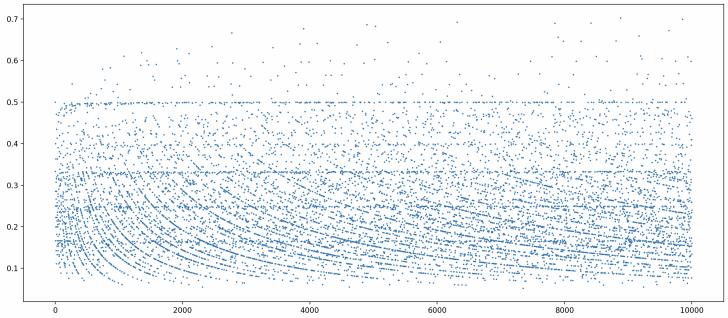

Figure 3: y=$R(n)/n$, $2 \leq n \leq 10,000$

Figure 4 below is a numerical verification of Theorem 1 because all the points of $y = R(mn) - R(m)R(n)$ with $\gcd(m, n) = 1$ are on or above the mn-plane or the plane $y = 0$. It can also be seen that when $m = 2$ or $n = 2$, the points on the graph of the function are on the plane $y = 0$. Due to visual effects, the lines on the plane may not look like the line $m = 2$ and $y = 0$ or the line $n = 2$ and $y = 0$. Figure 5 shows the lines with better visual effects.

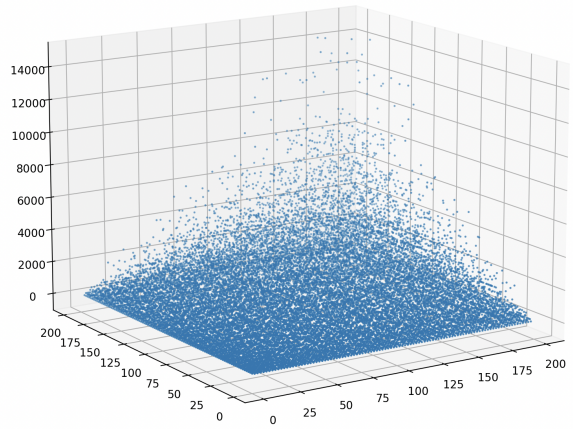

Figure 4: $y = R(mn) - R(m) \cdot R(n)$, $0 \leq m, n \leq 200$

Figure 5 only shows the points of the graph of the function $y = R(mn) - R(m)R(n)$ with $\gcd(m, n) = 1$ that are on the plane $y = 0$. One can see that $R(mn) - R(m)R(n) = 0$ if and only if one of m and n is 2 and the other is an odd number.

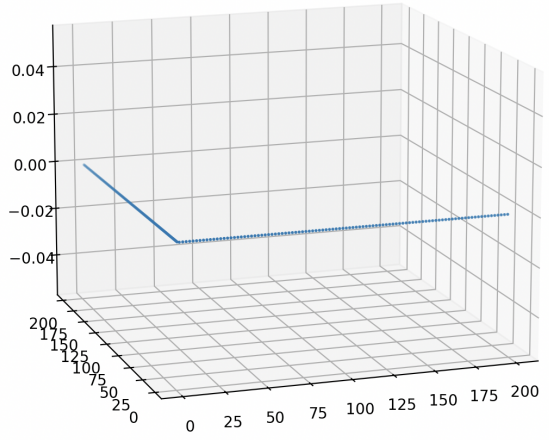

Figure 5: $y = R(mn) - R(m) \cdot R(n)$ and $y = 0$

Acknowledgements. We would like to thank Carl Pomerance for his invaluable comments on this paper. We also want to thank the referee's valuable suggestions, which led to important improvements in the results.

References

[1] R.D. Carmichael, *The Theory of Numbers*, Wiley, New York, 1914.

[2] S. Li, On the number of elements with maximal order in the multiplicative group modulo n, *Acta Arith.* **86** (1998), 113-132.

[3] S. Li, Artin's conjecture on average for composite moduli, *J. Number Theory* **84** (2000), 93-118.

[4] S. Li, On extending Artin's conjecture to composite moduli, *Mathematika* **46** (1999), 373-390.

[5] S. Li, An improvement of Artin's conjecture on average for composite moduli, *Mathematika* **51** (2004), 97-109.

[6] S. Li and C. Pomerance, On generalizing Artin's conjecture on primitive roots to composite moduli, *J. Reine Angew. Math.* **556** (2003), 205-224.

[7] G. Martin, The least prime primitive root and the shifted sieve, *Acta Arith.* **80** (1997), 277-288.

[8] C. Pomerance, On the distribution of amicable numbers, *J. Reine Angew. Math.* **293/294** (1977), 217-222.

[9] I.J. Schoenberg, On asymptotic distributions of arithmetical functions, *Trans. Amer. Math. Soc.* **39** (1936), 315-330.