Chin. Ann. Math.
27B(5), 2006, 549–552
DOI: 10.1007/s11401-005-0105-0

Chinese Annals of Mathematics, Series B

Distribution of Primitive λ-Roots of Composite Moduli II***

Zhiyong ZHENG* Todd COCHRANE**

(*Dedicated to Professor Wang Yuan on the occasion of his 75th birthday*)

Abstract We improve estimates for the distribution of primitive λ-roots of a composite modulus q yielding an asymptotic formula for the number of primitive λ-roots in any interval I of length $|I| \gg q^{\frac{1}{2}+\epsilon}$. Similar results are obtained for the distribution of ordered pairs (x, x^{-1}) with x a primitive λ-root, and for the number of primitive λ-roots satisfying inequalities such as $|x - x^{-1}| \leq B$.

Keywords λ-Roots, Primitive roots
2000 MR Subject Classification 11L03, 11L07

1 Introduction

Let q be a positive integer with prime factorization $q = 2^e p_1^{e_1} \cdots p_k^{e_k}$ and $G(q)$ be the multiplicative group of reduced residue classes (mod q). Let $\lambda(q)$ be the maximum order of any element of $G(q)$,

$$\lambda(q) = [\lambda(2^e), \lambda(p_1^{e_1}), \cdots, \lambda(p_k^{e_k})], \tag{1.1}$$

where

$$\lambda(p^e) = \begin{cases} \phi(p^e), & \text{if } p \text{ is odd or } p = 2,\ e \leq 2, \\ \dfrac{1}{2}\phi(p^e), & \text{if } p = 2 \text{ and } e \geq 3. \end{cases} \tag{1.2}$$

The function λ, introduced by Carmichael [2], is called the Carmichael λ-function. Any element of order $\lambda(q)$ is called a primitive λ-root of $G(q)$, and the set of all primitive λ-roots is denoted by $H(q)$. It is not hard to show that the number of primitive λ-roots satisfies

$$\frac{\phi(q)}{\log\log q} \ll \phi(\phi(q)) \leq |H(q)| \ll \phi(q) \tag{1.3}$$

(see for instance [4] or [5]). Li [4] established that $\limsup\limits_{q\to\infty} \frac{|H(q)|}{\phi(q)} = 1$ and $\liminf\limits_{q\to\infty} \frac{|H(q)|\log\log(q)}{\phi(q)} = e^{-\gamma}$ with γ Euler's constant, while Müller and Schlage-Puchta [5] proved that the set of q for which $|H(q)| = \phi(\phi(q))$ has density zero.

Manuscript received March 28, 2005.
*Department of Mathematical Sciences, Tsinghua University, Beijing 100084, China.
E-mail: zzheng@math.tsinghua.edu.cn
**Department of Mathematics, Kansas State University, Manhattan, Kansas 66506, USA.
E-mail: cochrane@math.ksu.edu
***Project supported by the National Natural Science Foundation of China (No.19625102) and the 973 Project of the Ministry of Science and Technology of China.

Our interest here is in the distribution of primitive λ-roots for a fixed modulus. In [6] we established that the primitive λ-roots were uniformly distributed. To be specific, let $I \subset \mathbb{Z}/q\mathbb{Z}$ be an interval $I = \{a+1, a+2, \cdots, a+M\}$ of size $|I| = M \leq q$ and let $\tau(q)$ denote the number of divisors of q. We proved that if $\tau(q) \ll 1$, then for any positive ϵ,

$$|H(q) \cap I| = \frac{|I|}{q}|H(q)| + O_\epsilon(q^{\frac{\tau(q)}{1+\tau(q)}+\epsilon}). \tag{1.4}$$

Here, we sharpen the error term and eliminate the restriction on $\tau(q)$.

Theorem 1.1 *For any positive integer q and interval I,*

$$|H(q) \cap I| = \frac{|I|}{q} \cdot |H(q)| + O_\epsilon(q^{\frac{1}{2}+\epsilon}). \tag{1.5}$$

The theorem yields an asymptotic formula for $|H(q) \cap I|$ for intervals of size $|I| \gg q^{\frac{1}{2}+\epsilon}$. Instead of appealing to the Erdös-Turan inequality for uniform distributions as we did in [6], our proof here uses elementary properties of finite Fourier series.

We turn next to the joint distribution of the pairs (x, x^{-1}) with $x \in H(q)$. Such distributions were first studied by Beck and Khan [1] for the case of prime moduli. More generally, let a, b, c, d be integers with $(ad-bc, q) = 1$ and I, J be any intervals in $\mathbb{Z}/q\mathbb{Z}$ with characteristic functions χ_I, χ_J. Our interest is in determining the number of primitive λ-roots x with $ax + bx^{-1} \in I$ and $cx + dx^{-1} \in J$.

Theorem 1.2 *For any positive q, integers a, b, c, d with $(ad - bc, q) = 1$ and intervals I, J we have*

$$\sum_{x \in H(q)} \chi_I(ax + bx^{-1})\chi_J(cx + dx^{-1}) = \frac{|I|}{q}\frac{|J|}{q} \cdot |H(q)| + O_\epsilon(q^{\frac{2}{3}+\epsilon}). \tag{1.6}$$

Taking $a = 1,\ b = 0,\ c = 0,\ d = 1$, we obtain a count on the number of primitive λ-roots x with $x \in I$ and $x^{-1} \in J$. Taking $I = \{-B, -B+1, \cdots, B\}$, $J = \{1, 2, \cdots, q\}$, $a = 1,\ b = -1,\ c = 0,\ d = 1$, we obtain that the number of primitive λ-roots x with $|x - x^{-1}| \leq B$ is $\frac{2B+1}{q} \cdot |H(q)| + O_\epsilon(q^{\frac{2}{3}+\epsilon})$. Theorem 1.1 is just a special case of Theorem 1.2 letting $J = \{1, 2, \cdots, q\}$, $a = 1,\ b = 0,\ c = 0,\ d = 1$, but with a sharper error term.

2 Lemmas

Throughout the paper, big "Oh" and "$\ll$" indicate constants depending on ϵ. The theorems follow from estimates of the exponential sums $\sum_{x \in H(q)} e_q(yx)$, $\sum_{x \in H(q)} e_q(m_1 x + m_2 x^{-1})$, over the set of primitive λ-roots, where $e_q(x) = e^{\frac{2\pi i x}{q}}$, which in turn follow from estimates of the Gauss sum $G(y, \chi) = \sum_{x=1}^{p^e} \chi(x) e_{p^e}(yx)$, and twisted Kloosterman sum $K(m_1, m_2, \chi) = \sum_{x=1}^{p^e} \chi(x) e_{p^e}(m_1 x + m_2 x^{-1})$, where χ is a multiplicative character $(\mathrm{mod}\ p^e)$.

Lemma 2.1 *For any integer y and positive ϵ,*

$$\Big| \sum_{x \in H(q)} e_q(yx) \Big| \ll (q, y)^{\frac{1}{2}} q^{\frac{1}{2}+\epsilon}.$$

Proof By Lemma 3 and equation (22) of [6], we have for any y and χ,

$$|G(y,\chi)| \le (y,p^e)^{\frac12} p^{\frac{e}{2}}. \tag{2.1}$$

Also, from equation (16) of [6] we have

$$\sum_{x\in H(q)} e_q(yx) = \sum_{\substack{d_i|\lambda(p_i^{e_i})\\ 0\le i\le k}}^{*} \prod_{i=0}^{k}\Big(\sum_{\delta_i|d_i}\frac{d_i\mu(\delta_i)}{\delta_i\lambda(p_i^{e_i})} \sum_{\exp(\chi_i)=\frac{\delta_i\lambda(p_i^{e_i})}{d_i}} G(y_i,\chi_i)\Big),$$

where $\sum^*$ means the sum over all d_i such that $[d_0,d_1\cdots,d_k]=\lambda(q)$ and $y_i=yn_i$ with the n_i defined by $\sum\limits_{i=0}^{k} n_i\frac{q}{p_i^{e_i}}=1$. Using $\tau(n)\ll n^{\epsilon}$ we obtain from (2.1) that

$$\sum_{x\in H(q)} e_q(yx) \le \sum_{\substack{d_i|\lambda(p_i^{e_i})\\ 0\le i\le k}}^{*} \prod_{i=0}^{k}\tau(d_i)(y,p_i^{e_i})^{\frac12}p_i^{\frac{e_i}{2}} \ll (y,q)^{\frac12}q^{\frac12+\epsilon}. \tag{2.2}$$

Lemma 2.2 *For any integers m_1,m_2,*

$$\Big|\sum_{x\in H(q)} e_q(m_1x+m_2x^{-1})\Big| \ll (m_1,m_2,q)^{\frac13}q^{\frac23+\epsilon}.$$

Proof For any prime power p^e and multiplicative character $\chi \pmod{p^e}$, by [6, Lemma 5] we have $|K(m_1,m_2,\chi)|\le c_p(m_1,m_2,p^e)^{\frac13}p^{\frac{2e}{3}}$, where $c_2=4\sqrt{2}$ and $c_p=2$ for $p>2$. This is a generalization of the classical Estermann-Weil bound (see [3]) to arbitrary characters χ. Also, by equation (17) of [6],

$$\Big|\sum_{x\in H(q)} e_q(m_1x+m_2x^{-1})\Big| = \sum_{\substack{d_i|\lambda(p_i^{e_i})\\ 0\le i\le k}}^{*} \prod_{i=0}^{k}\Big(\sum_{\delta_i|d_i}\frac{d_i\mu(\delta_i)}{\delta_i\lambda(p_i^{e_i})} \sum_{\exp(\chi_i)=\frac{\delta_i\lambda(p_i^{e_i})}{d_i}} K(m_i',m_i'',\chi_i)\Big),$$

where $\sum^*$ is as defined above, χ_i runs through the set of multiplicative characters $\pmod{p_i^{e_i}}$ and $m_i'=n_im_1$, $m_i''=n_im_2$ with the n_i as above. Thus

$$\Big|\sum_{x\in H(q)} e_q(m_1x+m_2x^{-1})\Big| \ll \sum_{\substack{d_i|\lambda(p_i^{e_i})\\ 0\le i\le k}}^{*} \prod_{i=0}^{k}\tau(d_i)c_{p_i}(m_1,m_2,p_i^{e_i})^{\frac13}p_i^{\frac{2e_i}{3}} \ll (m_1,m_2,q)^{\frac13}q^{\frac23+\epsilon}.$$

3 Proof of Theorem 1.1

Let $I=\{a+1,\cdots,a+M\}$ be an interval of residue classes $\pmod q$ and χ_I its characteristic function with finite Fourier expansion

$$\chi_I(x) = \sum_{y=0}^{q-1} a(y)e_q(yx), \tag{3.1}$$

where $e_q(yx)=e^{\frac{2\pi iyx}{q}}$, $a(0)=\frac{M}{q}$ and

$$a(y) = q^{-1}e_q\Big(-\Big(a+\frac{M}{2}+\frac12\Big)y\Big)\frac{\sin(\pi My/q)}{\sin(\pi y/q)} \qquad \text{for } y=1,\cdots,q-1. \tag{3.2}$$

Using $|\sin(\pi x)| \geq 2x$ for $0 \leq x \leq \frac{1}{2}$ we have

$$|a(y)| = |a(q-y)| \leq \frac{1}{2y} \quad \text{for } y = 1, 2, \cdots, \left[\frac{q}{2}\right]. \tag{3.3}$$

Then

$$\sum_{x \in H(q)} \chi_I(x) = \sum_{x \in H(q)} \sum_{y=0}^{q-1} a(y) e_q(yx) = \frac{M}{q}|H(q)| + \text{Error} \tag{3.4}$$

with $\text{Error} = \sum\limits_{y=1}^{q-1} a(y) \sum\limits_{x \in H(q)} e_q(yx)$.

By Lemma 2.1 we have $|\text{Error}| \leq \sum\limits_{y=1}^{q-1} |a(y)| \Big| \sum\limits_{x \in H(q)} e_q(yx) \Big| \ll q^{\frac{1}{2}+\epsilon} \sum\limits_{d|q, d \neq q} d^{\frac{1}{2}} \sum\limits_{(y,q)=d} |a(y)|$.

Next, using (3.3) and $\tau(q) \ll q^{\epsilon}$, we obtain $|\text{Error}| \ll q^{\frac{1}{2}+\epsilon} \sum\limits_{d|q, d \neq q} d^{\frac{1}{2}} \sum\limits_{k=1}^{\frac{q}{2d}} \frac{1}{dk} \ll q^{\frac{1}{2}+\epsilon} \sum\limits_{d|q, d \neq q} d^{-\frac{1}{2}}$ $\ll q^{\frac{1}{2}+\epsilon}$.

4 Proof of Theorem 1.2

Let a, b, c, d be integers with $(ad - bc, q) = 1$ and I, J be intervals of size $|I| = M \leq q$, $|J| = N \leq q$ in $\mathbb{Z}/q\mathbb{Z}$ with characteristic functions $\chi_I(x) = \sum\limits_{y=0}^{q-1} a(y) e_q(yx)$, $\chi_J(x) = \sum\limits_{z=0}^{q-1} b(z) e_q(zx)$. Then

$$\sum_{x \in H(q)} \chi_I(ax + bx^{-1}) \chi_J(cx + dx^{-1}) = \frac{MN}{q^2}|H(q)| + \text{Error} \tag{4.1}$$

with

$$\text{Error} = \sum_{(y,z) \neq (0,0)} a(y) b(z) \sum_{x \in H(q)} e_q((ay + cz)x + (by + dz)x^{-1})). \tag{4.2}$$

Now, since $(ad - bc, q) = 1$, the mapping $(y, z) \to (ay + cz, by + dz)$ is invertible modulo q and so $(ay + cz, by + dz, q) = (y, z, q)$ for any integers y, z. By Lemma 2.2 we then have

$$\begin{aligned} |\text{Error}| &\ll q^{\frac{2}{3}+\epsilon} \sum_{d|q, d \neq q} d^{\frac{1}{3}} \sum_{(y,z,q)=d} |a(y)||b(z)| \ll q^{\frac{2}{3}+\epsilon} \sum_{d|q, d \neq q} d^{\frac{1}{3}} \sum_{k=1}^{\frac{q}{d}} \sum_{l=1}^{\frac{q}{d}} \frac{1}{dk} \frac{1}{dl} \\ &\ll q^{\frac{2}{3}+\epsilon} \sum_{d|q, d \neq q} d^{-\frac{4}{3}} \ll q^{\frac{2}{3}+\epsilon}. \end{aligned}$$

References

[1] Beck, J. and Khan, M. R., On the Uniform Distribution of Inverses modulo n, *Period. Math. Hungar.*, **44**(2), 2002, 147–155.

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

[3] Estermann, T., On Kloosterman's sums, *Mathematika*, **8**, 1961, 83–86.

[4] Li, S., On the Number of Elements with Maximal Order in the Multiplicative Group modulo n, *Acta Arith.*, **86**(2), 1998, 113–132.

[5] Müller, T. and Schlage-Puchta, J-C., On the number of primitive λ-roots, *Acta Arith.*, **115**(3), 2004, 217–223.

[6] Zheng, Z., Xia, L. and Cochrane, T., Distribution of λ-roots of composite moduli, *Manuscripta Math.*, 2004, to appear.