Proc. Indian Acad. Sci. (Math. Sci.) Vol. 123, No. 1, February 2013, pp. 19–25.

Density of primes in l-th power residues

R BALASUBRAMANIAN and PREM PRAKASH PANDEY

The Institute of Mathematical Sciences, CIT Campus, Taramani,
Chennai 600 113, India
E-mail: prem.p2506@gmail.com

MS received 25 September 2011; revised 16 November 2011

Abstract. Given a prime number l, a finite set of integers $S = \{a_1, \ldots, a_m\}$ and m many l-th roots of unity $\zeta_l^{r_i}, i = 1, \ldots, m$ we study the distribution of primes $\mathbf{p}$ in $\mathbb{Q}(\zeta_l)$ such that the l-th residue symbol of a_i with respect to $\mathbf{p}$ is $\zeta_l^{r_i}$, for all i. We find out that this is related to the degree of the extension $\mathbb{Q}(a_1^{\frac{1}{l}}, \ldots, a_m^{\frac{1}{l}})/\mathbb{Q}$. We give an algorithm to compute this degree. Also we relate this degree to rank of a matrix obtained from $S = \{a_1, \ldots, a_m\}$. This latter argument enables one to describe the degree $\mathbb{Q}(a_1^{\frac{1}{l}}, \ldots, a_m^{\frac{1}{l}})/\mathbb{Q}$ in much simpler terms.

Keywords. Distribution of primes; higher residue symbols.

1. Introduction

In a recent paper [1] the authors have computed the relative density of primes for which a given finite string $S = \{a_1, \ldots, a_m\}$ of integers are quadratic residues simultaneously. It turns out, via Chebotarev density theorem, that this density is reciprocal to the degree of the multiquadratic extension given by square roots of the finite string of given integers over $\mathbb{Q}$. Given a field K which contains an n-th root of unity and given a finite set of integers $S = \{a_1, \ldots, a_m\}$, one can determine the degree of the extension $K(a_1^{\frac{1}{n}}, \ldots, a_m^{\frac{1}{n}})/K$ using Galois theory (for instance see [8]). In this article, we study the distribution of primes $\mathbf{p}$ of $\mathbb{Q}(\zeta_l)$ modulo where each a_i assumes a preassigned l-th power residue symbol and then relate it to the degree of the extension $\mathbb{Q}(a_1^{\frac{1}{l}}, \ldots, a_m^{\frac{1}{l}})/\mathbb{Q}$. We give two methods to compute the degree of the extension $\mathbb{Q}(a_1^{\frac{1}{l}}, \ldots, a_m^{\frac{1}{l}})/\mathbb{Q}$ and either of the two methods may prove to be useful at a given instance.

In § 2, we use a ramification argument in place of the classical use of the Eisenstein criterion to compute the degree of the extension $\mathbb{Q}(a_1^{\frac{1}{l}}, \ldots, a_m^{\frac{1}{l}})/\mathbb{Q}$. Section 3 deals with the l-th power residue symbols and the study of the distribution of primes $\mathbf{p}$ modulo which take a fixed value for each a_i. In § 4, we define a matrix T and then proceed to relate the degree of the extension to the rank of T. The tools we use are basic in nature [2,4,5] and can be worked out from any basic text on algebraic number theory, but for the sake of completion we will give some of the proofs.

We fix an odd prime l and ζ_l stands for a fixed primitive l-th root of unity.

2. Determination of the degree

To start with, we can assume that a_i''s are l-th power free and none of them is 1.

One has the following:

Lemma 1. *If $a \in \mathbb{Z}$ is not a l-th power then $X^l - a$ is irreducible over $\mathbb{Z}$.*

Lemma 2. *Let $b_1, b_2, \ldots, b_i$ be some integers and b be an intger which is not a l-th power such that there is a prime $q \neq l$ which divides b but does not divide any of b_j. Then $[\mathbb{Q}(b_1^{\frac{1}{l}}, \ldots, b_i^{\frac{1}{l}}, b^{\frac{1}{l}}) : \mathbb{Q}(b_1^{\frac{1}{l}}, \ldots, b_i^{\frac{1}{l}})] = l$.*

Proof. Let us write $L = \mathbb{Q}(b_1^{\frac{1}{l}}, \ldots, b_i^{\frac{1}{l}}, b^{\frac{1}{l}})$ and $K = \mathbb{Q}(b_1^{\frac{1}{l}}, \ldots, b_i^{\frac{1}{l}})$. Since q does not divide b_j for any j, q is unramified in each of $\mathbb{Q}(b_j^{\frac{1}{l}})$ and hence it is unramified in K as well. On the other hand, looking at complex factorization of $X^l - b$ we find that if $X^l - b = f_1(X) f_2(X)$ in $K[X]$ then $f_1(0) = b^{\frac{r}{l}} \zeta_l^c \in K$ for some integers r and c. Since q ramifies in K, we have that the polynomial $X^l - b$ is irreducible in $K[X]$. This proves the lemma. □

Algorithm to compute the degree $[\mathbb{Q}(a_1^{\frac{1}{l}}, \ldots, a_m^{\frac{1}{l}}) : \mathbb{Q}]$

Claim. We can obtain some integers $b_1, \ldots, b_t$ with the following properties:

(1) There is a prime number $q_i | b_i$ which does not divide b_j for $j \neq i$.
(2) None of b_i is a l-th power.
(3) $\mathbb{Q}(a_1^{\frac{1}{l}}, \ldots, a_m^{\frac{1}{l}}) = \mathbb{Q}(b_1^{\frac{1}{l}}, \ldots, b_t^{\frac{1}{l}})$.

We will generate the numbers b_i''s in successive steps. Here the upper index will indicate the number of steps.

Let q_1 be a prime divisor of a_1. We put $b_1^{(1)} = a_1$. For $i > 1$, if $q_1 \nmid a_i$ then we have $b_i^{(1)} = a_i$ and in case $q_1 | a_i$ then we will define $b_i^{(1)}$ as follows:

Let r_1 and r_i be the exponent of q_1 in a_1 and a_i respectively. Without loss of generality, we can assume that $1 \leq r_1, r_i \leq l - 1$. As m_i runs modulo l the numbers $m_i r_1 + r_i$ are distinct modulo l and hence for some choice of m_i we will have $m_i r_1 + r_i = \lambda_i l$ and then we define $b_i^{(1)} = \frac{a_1^{m_i} a_i}{q_1^{\lambda_i l}}$. If any $b_i^{(1)}$ happens to be a l-th power then we will omit it and consider only those $b_i^{(1)}$ which are not l-th powers, say, $b_1^{(1)}, \ldots, b_{s_1}^{(1)}$. Now one has $q_1 | b_1^{(1)}$ and $q_1 \nmid b_i^{(1)}$ for $i > 1$, and $\mathbb{Q}(a_1^{\frac{1}{l}}, \ldots, a_m^{\frac{1}{l}}) = \mathbb{Q}((b_1^{(1)})^{\frac{1}{l}}, \ldots, (b_{s_1}^{(1)})^{\frac{1}{l}})$. Next we set $b_1^{(2)} = b_1^{(1)}, b_2^{(2)} = b_2^{(1)}$ and start with a prime divisor q_2 of $b_2^{(2)}$ and repeat the same process to obtain $b_i^{(2)}$. Suppose this process stops at the k-th step then $b_1^{(k)}, \ldots, b_{s_t}^{(k)}$ are the required numbers. We will put $t = s_t$ and if $p = q_i$ for some i then we call $b_1 = b_i^{(k)}$ and the remaining $t - 1$ numbers can be taken in any order, and if $p \neq q_i$ for some i then we can take any ordering. Now Lemma 1 gives $[\mathbb{Q}(b_1^{\frac{1}{l}}) : \mathbb{Q}] = l$. Then we use Lemma 2 successively to obtain $[\mathbb{Q}(b_1^{\frac{1}{l}}, \ldots, b_t^{\frac{1}{l}}) : \mathbb{Q}] = l^t$, which is the required degree.

3. l-th Power residue symbol

Let p be a prime different from l and f be the inertia degree of p in $\mathbb{Q}(\zeta_l)$. For any prime ideal $\mathbf{p}$ of $\mathbb{Q}(\zeta_l)$ dividing p and an integer $\alpha \in \mathbb{Q}(\zeta_l)$ not contained in $\mathbf{p}$ one has $l|p^f - 1$ and $\alpha^{p^f-1} \equiv 1 \pmod{\mathbf{p}}$. Hence there is an l-th root of unity $\zeta_l^i, 0 < i \leq l$ such that $\alpha^{\frac{p^f-1}{l}} \equiv \zeta_l^i \pmod{\mathbf{p}}$. Since l-th roots of unity are distinct modulo $\mathbf{p}$, there is an unique i and we will define $(\frac{\alpha}{\mathbf{p}})_l = \zeta_l^i$. We state some results on the higher residue symbols [3,7].

Theorem 1 (Kummer's criterion). $(\frac{\alpha}{\mathbf{p}})_l \equiv \alpha^{\frac{p^f-1}{l}} \pmod{\mathbf{p}}$.

Theorem 2. *The l-th power residue symbols are completely multiplicative.*

Theorem 3. $\alpha \in \mathbb{Q}(\zeta_l)$ *is an l-th power modulo* $\mathbf{p}$ *iff* $(\frac{\alpha}{\mathbf{p}})_l = 1$.

Given any ideal $\eth$ of $\mathbb{Q}(\zeta_l)$, we will define $(\frac{\alpha}{\eth})_l = \prod_{\mathbf{p}|\eth}(\frac{\alpha}{\mathbf{p}})_l$ by including multiplicity. For $\beta \in \mathbb{Q}(\zeta_l)$ we will define $(\frac{\alpha}{\beta})_l = (\frac{\alpha}{(\beta)})_l$ where (β) stands for the principal ideal generated by β.

An integer $\alpha \in \mathbb{Q}(\zeta_l)$ is called primary if it is congruent to a rational integer modulo $(1 - \zeta_l)^2$.

Theorem 4 (Eisenstein's reciprocity law). *If α is a primary integer and a is a rational integer both coprime to each other and coprime to l then one has* $(\frac{a}{\alpha})_l = (\frac{\alpha}{a})_l$.

We will now introduce some more terminologies and see an alternate way to define the l-th residue symbol.

Let L/K be a Galois extension of number fields. For an unramified prime $\wp$ of L we will write k_L for the residue field of $\wp$ and k will denote the residue field of $\wp \cap \mathbb{O}_K$. There is an exact sequence [6],

$$0 \longrightarrow D_\wp \longrightarrow \mathrm{Gal}(k_L/k) \longrightarrow 0,$$

where $D_\wp$ is the decomposition group of $\wp$. Let $\sigma_\wp \in \mathrm{Gal}(k_L/k)$ be the Frobenius at $\wp$. Then its inverse image (in the above exact sequence) in $D_\wp$ is called Artin symbol of $\wp$ for the extension L/K and is written as $\left(\frac{\wp}{L/K}\right)$.

We note that if $\wp$ and $\wp'$ are primes in L above the same prime of K then $\left(\frac{\wp}{L/K}\right)$ and $\left(\frac{\wp'}{L/K}\right)$ are the Galois conjugates by an element of $\mathrm{Gal}(L/K)$ which permutes $\wp$ and $\wp'$. In particular, if L/K is abelian then for prime $\mathbf{p} = \wp \cap \mathbb{O}_K$ we can define $\left(\frac{\mathbf{p}}{L/K}\right) = \left(\frac{\wp}{L/K}\right)$.

For any $\sigma \in \mathrm{Gal}(L/K)$, let $P_{L/K}(\sigma)$ denote the set of prime ideals $\mathbf{p}$ in K such that there is a prime ideal $\wp$ of L above $\mathbf{p}$ such that $\left(\frac{\wp}{L/K}\right) = \sigma$.

Theorem 5 (Cebotarev density theorem). *Let* $\sigma \in \mathrm{Gal}(L/K)$, *and C_σ stands for conjugacy class of σ. Then density of $P_{L/K}(\sigma)$ is* $\frac{|C_\sigma|}{[L:K]}$.

In particular, if L/K is abelian then the density of primes $\mathbf{p}$ of K such that $\left(\frac{\mathbf{p}}{L/K}\right) = \sigma$ is $\frac{1}{[L:K]}$.

We have the following:

Lemma 3. *Consider a Galois extension L/K of number fields, and let F be an intermediate field such that F/K is Galois. Then for any unramified prime $\wp$ of L one has $\left(\frac{\wp}{L/K}\right)_{|F} = \left(\frac{\wp\cap\mathbb{O}_F}{L/K}\right)$.*

For a fixed prime l, we want to define the l-th residue symbol $(\frac{a}{p})_l$ for each prime $p \neq l$ and integer a coprime to p. We will write $f_a(X) = X^l - a$ and let K_a denote the splitting field of $f_a(X)$. Then $K_a \supset \mathbb{Q}(\zeta_l)$. For any prime $\mathbf{p}$ of $\mathbb{Q}(\zeta_l)$ above p, we let $\sigma_{\mathbf{p},a} \in \mathrm{Gal}(K_a/\mathbb{Q}(\zeta_l))$ denote the Artin symbol for the prime $\mathbf{p}$ for the extension $K_a/\mathbb{Q}(\zeta_l)$. Then $\sigma_{\mathbf{p},a}(a^{1/l})/a^{1/l}$ is an l-th root of unity and we will define $\left(\frac{a}{\mathbf{p}}\right)_l = \sigma_{\mathbf{p},a}(a^{1/l})/a^{1/l}$.

Lemma 4. *The definition of l-th residue symbol given here and the one given earlier are equivalent.*

Proof. Let f be the inertia degree of $\mathbf{p}$ in the extension $\mathbb{Q}(\zeta_l)/\mathbb{Q}$. Then the Artin symbol $\sigma_{\mathbf{p},a}$ satisfies

$$\sigma_{\mathbf{p},a}(a^{\frac{1}{l}}) \equiv a^{\frac{p^f}{l}} \pmod{\mathbf{p}},$$

$$\text{i.e.} \quad \frac{\sigma_{\mathbf{p},a}(a^{\frac{1}{l}})}{a^{\frac{1}{l}}} \equiv a^{\frac{p^f-1}{l}} \pmod{\mathbf{p}},$$

which proves the lemma. □

The following theorem is well known but we supply a proof for the sake of completeness.

Theorem 6. *If n is not an l-th power of an integer then the estimate*

$$\sum_{\mathbf{p};\mathrm{Norm}(\mathbf{p})\leq x} \left(\frac{n}{\mathbf{p}}\right)_l = o(\pi(x))$$

holds as $x \to \infty$. Here 'Norm' denotes norm map of the extension $\mathbb{Q}(\zeta_l)/\mathbb{Q}$.

Proof. One has

$$\sum_{\mathbf{p};\mathrm{Norm}(\mathbf{p})\leq x} \left(\frac{n}{\mathbf{p}}\right)_l = \sum_{b=1}^{l} \left(\sum_{\mathrm{Norm}(\mathbf{p})\leq x, \sigma_{\mathbf{p},n}=\tau_b} \left(\frac{n}{\mathbf{p}}\right)_l \right),$$

where τ_b is automorphism of K_n which sends $n^{\frac{1}{l}} \longmapsto (\zeta_l)^b n^{\frac{1}{l}}$. Hence

$$\sum_{\mathbf{p};\mathrm{Norm}(\mathbf{p})\leq x} \left(\frac{n}{\mathbf{p}}\right)_l = \sum_{b=1}^{l} \left(\sum_{\mathrm{Norm}(\mathbf{p})\leq x, \sigma_{\mathbf{p},n}=\tau_b} \zeta_l^b \right).$$

Thus we obtain

$$\sum_{\mathbf{p};\mathrm{Norm}(\mathbf{p})\leq x}\left(\frac{n}{\mathbf{p}}\right)_l = \sum_{b=1}^{l}\zeta_l^b\left(\frac{1}{l}\pi(x)+o(\pi(x))\right)$$

$$= \frac{1}{l}\pi(x)\sum_{b=1}^{l}\zeta_l^b + o(\pi(x)) = o(\pi(x)).$$

Because of the nontriviality of the character, the first term is zero. This proves the result. □

Given m elements $\zeta_l^{r_i}$ in μ_l, the group of l-th roots of unity, is not necessarily distinct. We want to determine density of primes $\mathbf{p}$ which satisfy $(\frac{a_i}{\mathbf{p}})_l = \zeta_l^{r_i}$. For this, we will consider the counting function

$$S_x = \frac{1}{ul^m}\sum_{\mathbf{p};\mathrm{Norm}(\mathbf{p})\leq x,\mathbf{p}\notin S}\prod_{k=1}^{m}\left(\prod_{j=1,j\neq r_k}^{l}\left(\zeta_l^j-\left(\frac{a_k}{\mathbf{p}}\right)_l\right)\right).$$

Here S is the set of primes dividing $a_1\ldots a_m$ and u is a unit satisfying

$$ul^m = \prod_{k=1}^{m}\prod_{j=1,j\neq r_k}^{l}(\zeta_l^j-\zeta_l^{r_k}).$$

We note that S_x exactly counts number of primes $\mathbf{p}$ of norm up to x which satisfy $(\frac{a_i}{\mathbf{p}})_l = \zeta_l^{r_i}$ for all i. Note that the choices of r_i can not be arbitrary because of the multiplicativity of l-th power residue symbol, i.e. to say that the assignment $a_i \longrightarrow \zeta_l^{r_i}$ shall be a restriction of some morphism of semigroups $\mathbb{Z}^*/\mathbb{Z}^{*l} \longrightarrow \mu_l$, but the counting function already takes care of this. To show this we note that any multiplicative relation among a_i''s can be brought to the form $\prod_{k=1}^{m} a_i^{c_i} = c^l$ for some integers c_i and c. Now the corresponding relation expected in μ_l is $\prod_{i=1}^{m}\zeta_l^{r_ic_i} = 1$. If this does not hold then it is easy to see from Theorem 3 that for each prime $\mathbf{p}$ there is an i such that $(\frac{a_i}{\mathbf{p}})_l \neq \zeta_l^{r_i}$. Thus if r_i's satisfy the required condition then S_x exactly counts number of primes of norm up to x which satisfy $(\frac{a_i}{\mathbf{p}})_l = \zeta_l^{r_i}$ for all i. In case there is inconsistency among the choices of r_i, then $S_x = 0$.

Now to estimate S_x, we can actually pass down the corresponding counting funtion for b_j''s which will also be denoted by S_x. When we change set $S = \{a_1,\ldots,a_m\}$ to the set $T = \{b_1,\ldots,b_t\}$ as obtained in the algorithm in § 2, then, the given m elements $\zeta_l^{r_i}$ uniquely determine a set of t elements $\zeta_l^{s_j}$ such that $(\frac{a_i}{\mathbf{p}})_l = \zeta_l^{r_i}$, for all $1 \leq i \leq m$ iff $(\frac{b_j}{\mathbf{p}})_l = \zeta_l^{s_j}$ for all $1 \leq j \leq t$. If the conditions $(\frac{a_i}{\mathbf{p}})_l = \zeta_l^{r_i}$, for all $1 \leq i \leq m$ then it will lead to a condition of the form $(\frac{b_j}{\mathbf{p}})_l = \zeta_l^{s_j}$ for all $1 \leq j \leq t$ with b_j as an l-th power and $s_j \neq 0$. Then we can immediately conclude that there is no prime $\mathbf{p}$ satisfying the condition. Studying the counting function with the b_j makes it easier, since there will be only one main term with one root of unity in it (not a sum of roots of unity). Hence, it is enough to study the behaviour of primes

$\mathbf{p}$ which satisfy $(\frac{b_j}{\mathbf{p}})_l = \zeta_l^{s_j}$ for all $1 \leq j \leq t$. Now we consider the counting function

$$S_x = \frac{1}{vl^t} \sum_{\mathbf{p};\mathrm{Norm}(\mathbf{p})\leq x, \mathbf{p}\notin S'} \prod_{k=1}^{t} \left(\prod_{j=1, j\neq r_k}^{l} \left(\zeta_l^j - \left(\frac{b_k}{\mathbf{p}} \right)_l \right) \right).$$

Here S' is the set of primes dividing $b_1 \ldots b_t$ and v is a unit satisfying

$$vl^t = \prod_{k=1}^{t} \prod_{j=1, j\neq s_k}^{l} (\zeta_l^j - \zeta_l^{s_k}).$$

We emphasize that S_x exactly counts number of primes of norm up to x which satisfy $(\frac{a_i}{\mathbf{p}})_l = \zeta_l^{r_i}$ for all i. Because of multiplicativity of l-th power residue symbol one obtains

$$S_x = \frac{1}{ul^t} \sum_{\mathbf{p};\mathrm{Norm}(\mathbf{p})\leq x, \mathbf{p}\notin S'} \sum_{0\leq d_i \leq l-1, n=\prod b_i^{d_i}} \zeta_l^{t_n} \left(\frac{n}{\mathbf{p}} \right)_l \text{ for some integer } t_n.$$

After changing the order of summation, we see here that the main term comes from those n which are of l-th power, by Theorem 6, and if n is not an l-th power then the contribution is $o(\pi(x))$. But from the construction of b_j its clear that no $n \neq 1$ will be an l-th power. Hence, the main term will give, in absolute value, $\frac{1}{l^t}(\pi(x) - |S'|)$. Thus density of the primes $\mathbf{p}$ satisfy $(\frac{b_j}{\mathbf{p}})_l = \zeta_l^{s_j}$ for all $1 \leq j \leq t$ and hence satisfies $(\frac{a_i}{\mathbf{p}})_l = \zeta_l^{r_i}$, for all $1 \leq i \leq m$ is $\frac{1}{l^t}$.

Remark 1.

(1) Note that the density does not depend upon the choice of r_i as long as there is consistency required.

(2) One can also obtain the density of primes $\mathbf{p}$ of $\mathbb{Q}(\zeta_l)$ which satisfy $(\frac{\alpha_i}{\mathbf{p}})_l = \zeta_l^{r_i}$, where α_i are integers of $\mathbb{Q}(\zeta_l)$ and r_i's are as in the Introduction. The above proof may not work in this case. However we see from the second definition of the l-th residue symbol in § 3 that if the requirement $\left(\frac{\alpha_i}{\mathbf{p}}\right)_l = \zeta_l^{r_i}$ is consistent (in the same sense as in § 3) then it uniquely determines an element in $\mathrm{Gal}(\mathbb{Q}(\zeta_l, \alpha_1^{\frac{1}{l}}, \ldots, \alpha_m^{\frac{1}{l}})/\mathbb{Q}(\zeta_l))$, and hence density of such primes $\mathbf{p}$ is $[\mathbb{Q}(\zeta_l, \alpha_1^{\frac{1}{l}}, \ldots, \alpha_m^{\frac{1}{l}}) : \mathbb{Q}(\zeta_l)]^{-1}$.

4. Another way to find the degree

Let $p_1, p_2, \ldots, p_n$ be all the primes dividing $a_1 \ldots a_m$. Let us write λ_{ij} for exact power of p_j dividing a_i. Then we will consider the $m \times n$ matrix T whose (i, j)-th entry is λ_{ij}. Note that for our purpose we can assume that $0 \leq \lambda_{ij} \leq l - 1$.

Lemma 5. *The cardinality of the set* $A = \{(\lambda_i)_{i=1}^m : 0 \leq \lambda_i \leq l-1, \prod_i a_i^{\lambda_i} \in \mathbb{Z}^l\}$ *is a power of* l.

Proof. Consider the $\mathbb{Z}/l\mathbb{Z}$ vector space $(\mathbb{Z}/l\mathbb{Z})^m$ with basis $S = \{a_1, \ldots, a_m\}$. $\mathbb{Z}/l\mathbb{Z}$ acts on $\mathbb{Q}^*/(\mathbb{Q}^*)^l$ by $\alpha \cdot x = x^\alpha$. Consider the map $T\colon (\mathbb{Z}/l\mathbb{Z})^m \longrightarrow \mathbb{Q}^*/(\mathbb{Q}^*)^l$ which sends $a_i \to \bar{a_i}$ and extend it linearly. Then $\sum_i \lambda_i a_i \in \ker T \text{iff} (\lambda_i) \in A$. This proves that $|A|$ is an l-th power. □

As mentioned in [8] the degree $\mathbb{Q}(a_1^{\frac{1}{l}}, \ldots, a_m^{\frac{1}{l}}, \zeta_l)/\mathbb{Q}(\zeta_l)$ is l^m/l^r, where l^r is the cardinality of set A. Now we relate this degree to the rank of the matrix T.

Theorem 7. *The rank of the matrix T is $m - r$.*

Proof. If there are x_i, $1 \le i \le m$ with $0 \le x_i \le l-1$ such that $\prod_{i=1}^m a_i^{x_i} \in \mathbb{Z}^l$. Then for all j we have $x_1\lambda_{1j} + \cdots + x_m\lambda_{mj} = 0(\text{mod } l)$, i.e the row vectors $(\lambda_{i1}, \ldots, \lambda_{in})$, $1 \le i \le m$ in $(\mathbb{Z}/l\mathbb{Z})^n$ are linearly dependent. Conversely, any such linear dependence among row vectors of matrix T will give exactly l many relations of the type in set A. Let r be the rank of the matrix T. After a rearrangement we can assume that the row vectors $(\lambda_{i1}, \ldots, \lambda_{in})$, $1 \le i \le r$ are linearly independent. Then we see that for any choice of x_i, $1 \le i \le r$ with $1 \le x_i \le l-1$ the condition $\prod_{i=1}^r a_i^{x_i} \in \mathbb{Z}^l$ does not hold. On the other hand, for any selection of x_j, $j > r$ we have l many relation of the form $\prod_{i=1}^m a_i^{x_i} \in \mathbb{Z}^l$ (this can be seen by looking at the vectors $(\lambda_{i1}, \ldots, \lambda_{in})$, $1 \le i \le r$ and $x_{r+1}(\lambda_{r+11}, \ldots, \lambda_{r+1n}) + \cdots + x_m(\lambda_{m1}, \ldots, \lambda_{mn})$ which are linearly dependent). This proves the theorem. □

Acknowledgments

The authors would like to thank Professor Kannan Soundararajan for pointing out some mathematical inaccuracies in an earlier draft. Thanks are also due to the anonymous referee for a careful reading of the manuscript and for helping us in improving the presentation.

References

[1] Balasubramanian R, Luca F and Thangadurai R, On the exact degree of $\mathbb{Q}(a_1^{\frac{1}{l}}, \ldots, a_m^{\frac{1}{l}})$ over $\mathbb{Q}$, *Proc. Am. Math. Soc.* **138(7)** (2010) 2283–2288

[2] Cassels J W S and Frohlich A, Algebraic Number Theory (1967) (The London Mathematical Society)

[3] Hilbert David, The Theory of Algebraic Number Fields (1991)

[4] Koch Helmut, Number Theory: Algebraic Numbers and Functions, Graduate Studies in Mathematics, vol. 24 (2000)

[5] Washington Lawrence C, Introduction to Cyclotomic Fields, second edition (1991) (Springer)

[6] Neukirch Jurgen, Algebraic Number Theory (1991) (Springer)

[7] Ram Murty M and Esmonde Jody, Problems in Algebraic Number Theory, Graduate Text in Mathematics (1991)

[8] Weintraub Steven H, Galois Theory (2006) (Springer-Verlag) (Universitext)