SOME DENSITY QUESTIONS AND AN APPLICATION

R. THANGADURAI

Abstract. Let $S = \{a_1, a_2, \cdots, a_\ell\}$ be a finite set of non-zero integers. Recently, R. Balasubramanian *et al.*, ([2], 2010) computed the density of those primes p such that a_i is a quadratic residue (respectively, non-residue) modulo p for every i. As an application of this result, the proved an exact formula for the degree of the multi-quadratic field $\mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \ldots, \sqrt{a_\ell})$ over $\mathbb{Q}$. In this lecture notes, we give an expository of the above result together with all the preliminaries that needed.

1. Introduction

Let $S = \{a_1, a_2, \ldots, a_\ell\}$ be a finite set of non-zero integers.

In 1968, M. Fried [3] answered that there are infinitely many primes p for which a is a quadratic residue modulo p for every $a \in S$. Also, he provided a necessary and sufficient condition for a to be a quadratic non-residue modulo p for every $a \in S$. More recently, S. Wright [13] and [14] also studied this qualitative problem.

For a given prime p, the set of all quadratic non-residue modulo p is a disjoint union of the set of all generators g of $(\mathbb{Z}/p\mathbb{Z})^*$ (which are called primitive roots modulo p) and the complement set contains all the non-residues which are not primitive roots modulo p.

In 1927, E. Artin [1] conjectured the following;

Artin's primitive root conjecture. Let $g \neq \pm 1$ be a square-free integer. Then there are infinitely many primes p such that g is a primitive root modulo p.

Note that it is not even known that for a given square-free integer, $g \neq \pm 1$, there exists a prime p such that g is a primitive root modulo p. The above Artin's conjecture asks for the existence infinitely many such primes. In 1967, Hooley [6] proved this conjecture assuming the (as yet) unresolved genearlized Riemann hypothesis for Dedekind zeta functions of certain number fields. In 1983, R. Gupta and M. R. Murty [4] made the first breakthrough by showing

2000 *Mathematics Subject Classification.* 11A15.
Key words and phrases. Quadratic residues; Galois field; Chebotarev density theorem.

the following: given three prime numbers a, b, c, then at least one of the thirteen numbers

$$\{ac^2, a^3b^2, a^2b, b^3c, b^2c, a^2c^3, ab^3, a^3bc^2, bc^3, a^2b^3c, a^3c, ab^2c^3, abc\}$$

is a primitive root modulo p for infinitely many primes p. Then later Heath-Brown [5] proved that $\{a, b, c\}$ one is primitive root modulo p for infinitely many primes p. Similarly, using the method of Hooley, in 1976, K. R. Matthews [10] found a necessary and sufficient condition for a to be primitive root modulo p for every $a \in S$, under unproved hypothesis.

Analogue question for a non-residue which is not a primitive root modulo a prime is relatively easier to handle. For example, in [11] it is proved that for a given g which is not a perfect square of an integer, there are infinitely many primes p for which g is a quadratic non-residue but not a primitive root modulo p, using the arithmetic of certain number fields. Of course computing the density of such primes is not done yet.

From basic field theory, it is well-known that the degree of the multi-quadratic field

$$\mathbb{K} = \mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \ldots, \sqrt{a_\ell})$$

over $\mathbb{Q}$ is 2^t for some integer $0 \leq t \leq \ell$, depending on the algebraic cancellations among the $\sqrt{a_i}$'s. The arithmetic of multi-quadratic number fields plays a crucial role in the theory of elliptic curves. See for instance Hollinger [7] and Laska-Lorenz [9].

When $a_i = p_i$, distinct prime numbers, then it is well-known that the degree of $[\mathbb{K} : \mathbb{Q}] = 2^\ell = 2^{|S|}$; in our notation, $t = \ell = |S|$. On the other hand, when $S = \{2, 3, 6\}$, the degree of $[\mathbb{K} : \mathbb{Q}] = 2^2 < 2^{|S|}$; thence $t = 2 = |S| - 1$.

In this paper, we provide a complete answer by computing the number t in terms of the given inputs a_i's. Before we state the theorems, we must first present some notations.

Throughout the paper, we write p, q for prime numbers, x for a positive real number, and $\pi(x)$ for the number of primes $p \leq x$. A set P of prime numbers is said to have the *relative density* ε with $0 \leq \varepsilon \leq 1$, if

$$\varepsilon = \lim_{x\to\infty} \frac{|P \cap [1, x]|}{\pi(x)}$$

exits. Also, the following numbers count some special subsets of S.

(i) Let α_S denote the number of subsets T of S, including the empty one, such that $|T|$ is even and $\displaystyle\prod_{s\in T} s = m^2$ for some integer m; hence, $\alpha_S \geq 1$ for every S.

(ii) Let β_S denote the number of subsets T of S such that $|T|$ is odd and $\prod_{s\in T} s = m^2$ for some integer m.

Then the following theorems were proved by R. Balasubramanian, F. Luca and the author [2].

Theorem 1. ([2], 2010) *The relative density of the set of prime numbers p for which a is a quadratic residue modulo p for every $a \in S$ is*

$$\frac{\alpha_S + \beta_S}{2^\ell}.$$

Theorem 2. ([2], 2010) *We have, $\beta_S = 0$ if and only if the density of the set of primes p for which a is a quadratic non-residue modulo p for every $a \in S$ is*

$$\frac{\alpha_S}{2^\ell}.$$

As an application of Theorem 1, we prove:

Theorem 3. ([2], 2010) *For a given finite set S of non-zero integers with $|S| = \ell$, we have,*

$$[\mathbb{K} : \mathbb{Q}] = 2^{\ell-k},$$

where k is the non-negative integer given by $2^k = \alpha_S + \beta_S$. In other words, $t = \ell - k$.

2. Preliminaries

Lemma 1. *We have $\alpha_S + \beta_S = 2^k$ for some integer $k \leq \ell$.*

Proof. Let $V = (\mathbb{Z}/2\mathbb{Z})^\ell$ be the $\mathbb{Z}/2\mathbb{Z}$-vector space having $\mathbf{a}_1, \ldots, \mathbf{a}_\ell$ as a basis. Let W be the $\mathbb{Z}/2\mathbb{Z}$-vector space $\mathbb{Q}^*/(\mathbb{Q}^*)^2$, where the addition modulo 2 is defined as multiplication modulo squares. Let $\tau : V \longmapsto W$ be given by $\tau(\mathbf{a}_i) = a_i \pmod{(\mathbb{Q}^*)^2}$ and extended by linearity. It is then clear that $\{i_1, \ldots, i_j\} \subseteq \{1, \ldots, \ell\}$ is such that $a_{i_1} \cdots a_{i_j}$ is a perfect square of an integer if and only if $\mathbf{a}_{i_1} + \cdots + \mathbf{a}_{i_j} \in \operatorname{Ker}(\tau)$. It now follows immediately that $\alpha_S + \beta_S = 2^k$, where k is the dimension of $\operatorname{Ker}(\tau)$, and $\ell - k$ is the dimension of the image of τ in W. $\square$

For an integer a and odd prime p we write $\left(\frac{a}{p}\right)$ for the Legendre symbol of a with respect to p. Let $n > 1$ be an integer and m be an integer such that $1 \leq m \leq n$ and $(m, n) = 1$. Let $\pi(x, n, m)$ be denote the number of primes $p \leq x$ and $p \equiv m \pmod{n}$ and $\phi(n)$ denote the Euler Phi-function which counts the number of integers m with $1 \leq m \leq n$ and $(m, n) = 1$. Then Siegel-Walfisz theorem states as follows.

Siegel-Walfisz Theorem. (see e.g., [12], Satz 4.8.3) *For any $A > 1$, we have*

$$\pi(x, n, m) = \frac{\pi(x)}{\phi(n)} + O\left(\frac{x}{(\log x)^A}\right)$$

holds for all large enough x.

Proposition 1. *Let n be any integer which is not a perfect square. Then the estimate*

$$\sum_{p \leq x} \left(\frac{n}{p}\right) = o(\pi(x)),$$

holds as $x \to \infty$.

Proof. Define a map

$$\chi : (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow \{\pm 1\}$$

by

$$\chi(m) = \left(\frac{n}{m}\right) \text{ for every } 1 \leq m \leq n, \ (m, n) = 1,$$

where $\left(\frac{n}{m}\right)$ is the Kronecker symbol. Note that when $m = 1$, we define $\chi(1) = 1$. By the multiplicativity of the Kronecker symbol, it is clear that χ is a character modulo n. Hence, by the orthogonality relation, we get

$$\sum_{\substack{1 \leq m \leq n \\ (m,n)=1}} \chi(m) = 0.$$

For simplicity, we define,

$$\sum_{m \pmod{n}^*} := \sum_{\substack{1 \leq m \leq n \\ (m,n)=1}}.$$

Now, consider

$$\sum_{p \leq x} \left(\frac{n}{p}\right) = \sum_{\ell \pmod{n}^*} \sum_{\substack{p \equiv \ell \pmod{n} \\ p \leq x}} \left(\frac{n}{\ell}\right) = \sum_{\ell \pmod{n}^*} \sum_{\substack{p \equiv \ell \pmod{n} \\ p \leq x}} \chi(\ell).$$

By interchanging the summation, we get,

$$\sum_{p \leq x} \left(\frac{n}{p}\right) = \sum_{\ell \pmod{n}^*} \chi(\ell) \pi(x, n; \ell),$$

where $\pi(x, n, \ell)$ denotes the number of primes $p \equiv \ell \pmod{n}$ and $p \leq x$. Walfisz's Theorem implies that for any fixed integer $A > 1$, we have

$$\pi(x, n, \ell) = \frac{\pi(x)}{\phi(n)} + O\left(\frac{x}{(\log x)^A}\right)$$

for every large enough x. Therefore, we get,

$$\sum_{p \leq x} \left(\frac{n}{p}\right) = \frac{\pi(x)}{\phi(n)} \sum_{\ell \pmod{n}^*} \chi(\ell) + O\left(\frac{\phi(n) x}{(\log x)^A}\right).$$

By the orthogonality relation, we, further, get,

$$\sum_{p\le x}\left(\frac{n}{p}\right) = O\left(\frac{\phi(n)x}{(\log x)^A}\right) = o(\pi(x)).$$

Hence the proposition. □

Now, we review the algebraic number theory that are needed to prove the main theorem.

Let $K/\mathbb{Q}$ be a finite extension over $\mathbb{Q}$. That is, K is a field and as a vector space over $\mathbb{Q}$, it is finite dimentional and its dimension is denoted by $[K:\mathbb{Q}]$. Let $\mathcal{O}_K$ be the maximal proper subring of K such that K is the quotient field of $\mathcal{O}_K$. By Dedekind domain theory, it is well-known that $\mathcal{O}_K$ is a Dedekind domain and it is called *ring of integers* of K. For example, when $K=\mathbb{Q}$, $\mathcal{O}_K=\mathbb{Z}$.

In $\mathcal{O}_K$, every ideal $\mathfrak{a}$ is uniquely expressed as a product of prime ideals in it. Let $p\in\mathbb{Q}$ be a rational prime. Then the principal ideal

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_g^{e_g} \tag{*}$$

where $\mathfrak{p}_i$'s are distinct prime ideals of $\mathcal{O}_K$ and $e_j\ge 0$ are integers. Also, it is known that the quotient ring $\mathcal{O}_K/\mathfrak{p}_i$ is a finite field extension over $\mathbb{Z}/p\mathbb{Z}$ and dimension is denoted by f_i's. It is well known result that

$$[K:\mathbb{Q}] = \sum_{i=1}^{g} e_i f_i.$$

In particular, $\displaystyle\sum_{i=1}^{g} e_i \le [K:\mathbb{Q}]$.

A rational prime $p\in\mathbb{Q}$ is said to be

- *ramified* if $e_i\ge 2$ for some i in (*)
- *unramified* if $e_i=1$ for all i in (*)
- *splits completely* if $e_i=1$ and $f_i=1$ for all i in (*); In this case, we get $[K:\mathbb{Q}]=g$.

Note that when K is a quadratic extension over $\mathbb{Q}$, then by the above condition, we have following situations.
(1) $p\mathcal{O}_K=\mathfrak{p}^2$; (ramifies)
(2) $p\mathcal{O}_K=\mathfrak{p}\mathfrak{q}$ with $\mathfrak{p}\ne\mathfrak{q}$; (splits completely)
and (3) $p\mathcal{O}_K=\mathfrak{p}$ (inert)

Proposition 2. *Let d be any square-free integer and let $K=\mathbb{Q}(\sqrt{d})$ be a quadratic extension over $\mathbb{Q}$. Then for any odd prime $p\ge 3$, we have*

(i) *p ramifies in $\mathcal{O}_K$ if and only if $p|d$;*
(ii) *p splits completely in $\mathcal{O}_K$ if and only if $\left(\frac{d}{p}\right)=1$, or d is a square modulo p.*

(iii) *p is inert in $\mathcal{O}_K$ if and only if $\left(\frac{d}{p}\right) = -1$, or d is not a square modulo p.*

Let $K/\mathbb{Q}$ be a finite Galois extension with Galois group $G =$ Gal $(K/\mathbb{Q})$. Let $\mathcal{O}_K$ be the ring of integers of K. First let us recall some groups that are associated with the prime ideals of $\mathcal{O}_K$.

Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$, Then note that for any $\sigma \in G$, if

$$\sigma(\mathfrak{p}) := \{x \in \mathcal{O}_K : x = \sigma(y) \text{ for some } y \in \mathfrak{p}\},$$

then $\sigma(\mathfrak{p})$ is a prime ideal in $\mathcal{O}_K$. We define

$$D_{\mathfrak{p}} := \{\sigma \in G : \sigma\mathfrak{p} = \mathfrak{p}\}.$$

Then $D_{\mathfrak{p}}$ forms a group under composition of maps and becomes a subgroup of G. This subgroup is called the *decomposition group* of G. Let $g = [G : D_{\mathfrak{p}}]$ denote the index of $D_{\mathfrak{p}}$. Then

$$G = \bigcup_{i=1}^{g} \sigma_i D_{\mathfrak{p}},$$

where $\sigma_i(\mathfrak{p}) = \mathfrak{p}_i$, a conjugate of $\mathfrak{p}$. Hence $D_{\mathfrak{p}}$ gives the information about prime $p \in \mathbb{Q}$ splits in K. More precisely, the prime $p \in \mathbb{Q}$ splits into g prime ideals in $\mathcal{O}_K$. If $\sigma \in D_{\mathfrak{p}}$, and $x - y \in \mathfrak{p}$, then

$$\sigma(x-y) = \sigma(x) - \sigma(y) \in \sigma(\mathfrak{p}) = \mathfrak{p}.$$

That is, if

$$\begin{aligned} x &\equiv y \pmod{\mathfrak{p}} \text{ for all } x, y \in \mathcal{O}_K, \text{ then we have} \\ \sigma(x) &\equiv \sigma(y) \pmod{\mathfrak{p}}. \end{aligned}$$

Therefore every $\sigma \in D_{\mathfrak{p}}$ takes congruences class modulo $\mathfrak{p}$ to congruence class modulo $\mathfrak{p}$. This defines an automorphism $\overline{\sigma} \in$ Aut$(\mathcal{O}_K/\mathfrak{p})$. Let $p \in \mathbb{Q}$ be a rational prime number such that $p\mathcal{O}_K \subset \mathfrak{p}$, we have a map

$$D_{\mathfrak{p}} \to \text{ Gal } (\mathcal{O}_K/\mathfrak{p} \mid \mathbb{Z}/p\mathbb{Z}).$$

This automorphism turns out to be surjective. (The surjectivity is non-trivial, see for instance, G. Janusz [8], Algebraic Number fields, pg. 95). The kernal of this surjection is called *Inertia group*, denoted by $I_{\mathfrak{p}}$. Therefore,

$$\begin{aligned} I_{\mathfrak{p}} &= Ker\{D_{\mathfrak{p}} \to \text{ Gal } (\mathcal{O}_K/\mathfrak{p}|\mathbb{Z}/p\mathbb{Z})\} \\ &= \{\sigma \in D_{\mathfrak{p}} : \overline{\sigma} = 1\} \\ &= \{\sigma \in D_{\mathfrak{p}} : \sigma(x) \equiv x \pmod{\mathfrak{p}} \text{ for all } x \in \mathcal{O}_K\} \end{aligned}$$

Therefore,

$$\text{Gal } (\mathcal{O}_K/\mathfrak{p} \mid \mathbb{Z}/p\mathbb{Z}) \cong D_{\mathfrak{p}}/I_{\mathfrak{p}}.$$

It is well-known that $\mathcal{O}_K/\mathfrak{p}$ is a finite extension of the finite field $\mathbb{Z}/p\mathbb{Z}$. Therefore its Galois group Gal $(\mathcal{O}_K/\mathfrak{p} \mid \mathbb{Z}/p\mathbb{Z})$ is cyclic and it is generated by the Frobenious element $\sigma_{\mathfrak{p}}$ which is uniquely determined by the condition

$$\sigma_p(x) \equiv x^p \pmod{\mathfrak{p}} \text{ for all } x \in \mathcal{O}_K.$$

Corresponding to this map, we have an element in $D_{\mathfrak{p}}/I_{\mathfrak{p}}$ which is denoted by $\left[\frac{K/\mathbb{Q}}{\mathfrak{p}}\right]$ and so

$$D_{\mathfrak{p}}/I_{\mathfrak{p}} =< \left[\frac{K/\mathbb{Q}}{\mathfrak{p}}\right] > .$$

Note that if p is unramified, then for all prime ideal $\mathfrak{p}$ such that $p\mathcal{O}_K \subset \mathfrak{p}$, we have $I_{\mathfrak{p}} = \{1\}$. Therefore,

$$D_{\mathfrak{p}} \cong \text{ Gal } (\mathcal{O}_K/\mathfrak{p} \mid \mathbb{Z}/p\mathbb{Z})\,.$$

Hence for all unramified primes p, we have $D_{\mathfrak{p}}$ is cyclic for all prime ideal $p\mathcal{O}_K \subset \mathfrak{p}$ and $\left[\frac{K/\mathbb{Q}}{\mathfrak{p}}\right]$ is unique and completely determined by the condition

$$\left[\frac{K/\mathbb{Q}}{\mathfrak{p}}\right] x \equiv x^p \pmod{\mathfrak{p}} \text{ for all } x \in \mathcal{O}_K.$$

Also, if $\mathfrak{p}, \mathfrak{q}$ are the two prime ideals such that $p\mathcal{O}_K \subset \mathfrak{p}, \mathfrak{q}$, then

$$\left[\frac{K/\mathbb{Q}}{\mathfrak{q}}\right] = \sigma^{-1} \left[\frac{K/\mathbb{Q}}{\mathfrak{p}}\right] \sigma$$

where $\sigma \in \ G$ such that $\sigma(\mathfrak{p}) = \mathfrak{q}$. This is because, for $\sigma \in \ G$ and $\sigma\mathfrak{p} = \mathfrak{q}$, we have,

$$\begin{aligned}
\left[\frac{K/\mathbb{Q}}{\mathfrak{p}}\right] x &\equiv x^p \pmod{\mathfrak{p}} \text{ for all } x \in \mathcal{O}_K \\
\sigma \left[\frac{K/\mathbb{Q}}{\mathfrak{p}}\right] x &\equiv \sigma(x^p) \pmod{\sigma\mathfrak{p}} \text{ for all } x \in \mathcal{O}_K \\
\sigma \left[\frac{K/\mathbb{Q}}{\mathfrak{p}}\right] x &\equiv (\sigma(x))^p \pmod{\mathfrak{q}} \text{ for all } x \in \mathcal{O}_K \\
\sigma \left[\frac{K/\mathbb{Q}}{\mathfrak{p}}\right] \sigma^{-1}(x) &\equiv x^p \pmod{\mathfrak{q}} \text{ for all } x \in \mathcal{O}_K
\end{aligned}$$

In the last step, we replace x by $\sigma^{-1}(x)$. Therefore, $\left[\frac{K/\mathbb{Q}}{\mathfrak{q}}\right] = \sigma \left[\frac{K/\mathbb{Q}}{\mathfrak{p}}\right] \sigma^{-1}$.

Therefore when $\mathfrak{p}$ ranges over the prime ideals of $\mathcal{O}_K$ lying above the rational prime p, the $\left[\frac{K/\mathbb{Q}}{\mathfrak{p}}\right]$ ranges over its conjugacy class in $\mathrm{Gal}(K/\mathbb{Q})$ that depends only on p. Thus, for each rational prime p, we define the Frobenious element, $\sigma_p \in \mathrm{Gal}(K/\mathbb{Q})$, which generates $D_{\mathfrak{p}}/I_{\mathfrak{p}}$ for some prime ideal $\mathfrak{p}$ lying above p.

The following theorem computes the density of primes p such that the corresponding Frobenious element σ_p lies in a given conjugacy class of G. This is a far reaching generalization of Dirichlet's Prime Number Theorem in arithmetic progressions.

Chebotarev's Density Theorem. *Let $\mathbb{K}/\mathbb{Q}$ be a Galois extension with Galois group G. Let C be a given conjugacy class of G. Then the relative density of the set of primes $P = \{p : \sigma_p \in C\}$ is $\dfrac{|C|}{[\mathbb{K} : \mathbb{Q}]}$.*

3. Proof of Theorems

Proof of Theorem 1. Let $\mathcal{P}(S)$ be the set of all distinct prime factors of $a_1 a_2 \cdots a_\ell$. Clearly, $|\mathcal{P}(S)|$ is finite. Let $x > 1$ be a real number. Consider the following counting function

$$S_x = \frac{1}{2^\ell} \sum_{\substack{p \le x \\ p \notin \mathcal{P}(S)}} \left(1 + \left(\frac{a_1}{p}\right)\right) \cdots \left(1 + \left(\frac{a_\ell}{p}\right)\right).$$

Since the Legendre symbol is completely multiplicative, $\left(\dfrac{a_i}{p}\right)\left(\dfrac{a_j}{p}\right) = \left(\dfrac{a_i a_j}{p}\right)$, we see that

$$S_x = \frac{1}{2^\ell} \sum_{\substack{p \le x \\ p \notin \mathcal{P}(S)}} \sum_{\substack{0 \le b_i \le 1 \\ n = a_1^{b_1} \cdots a_\ell^{b_\ell}}} \left(\frac{n}{p}\right) = \sum_{\substack{0 \le b_i \le 1 \\ n = a_1^{b_1} \cdots a_\ell^{b_\ell}}} \frac{1}{2^\ell} \sum_{\substack{p \le x \\ p \notin \mathcal{P}(S)}} \left(\frac{n}{p}\right).$$

Note that if n is a perfect square, then $\left(\dfrac{n}{p}\right) = 1$ for each $p \notin \mathcal{P}(S)$. Thus, for these $\alpha_S + \beta_S$ values of n, the inner sum is

$$\frac{1}{2^\ell} \sum_{\substack{p \le x \\ p \notin \mathcal{P}(S)}} \left(\frac{n}{p}\right) = \frac{1}{2^\ell}(\pi(x) - |\mathcal{P}(S)|).$$

For the remaining values of n (i.e., when n is not a perfect square), we apply Proposition 1 to get

$$\frac{1}{2^\ell} \sum_{\substack{p \le x \\ p \notin \mathcal{P}(S)}} \left(\frac{n}{p}\right) = o(\pi(x)) \qquad \text{as} \quad x \to \infty.$$

Therefore,

$$S_x = \frac{1}{2^\ell}(\alpha_S + \beta_S)(\pi(x) - |\mathcal{P}(S)|) + o(\pi(x))$$

and hence

$$\frac{S_x}{\pi(x)} = \frac{\alpha_S + \beta_S}{2^\ell}\left(1 - \frac{|\mathcal{P}(S)|}{\pi(x)}\right) + o(1).$$

Since $|\mathcal{P}(S)|$ is a finite number and it is elementary to see that as $x \to \infty$, $\pi(x) \to \infty$, we get

$$\lim_{x\to\infty} \frac{S_x}{\pi(x)} = \frac{\alpha_S + \beta_S}{2^\ell}.$$

This completes the proof of Theorem 1. □

This can be applied to the quadratic non-residue case as well. Take

$$S_x = \frac{1}{2^\ell} \sum_{\substack{p\le x \\ p\notin \mathcal{P}(S)}} \left(1 - \left(\frac{a_1}{p}\right)\right) \cdots \left(1 - \left(\frac{a_\ell}{p}\right)\right)$$

and proceed as in the proof of Theorem 1. This yields Theorem 2.

Proof of Theorem 3. It is clear that $\mathbb{K}$ is a 2-elementary abelian extension of $\mathbb{Q}$, so $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) = (\mathbb{Z}/2\mathbb{Z})^t$ for some $1 \le t \le \ell$. In fact, if

$$f(x) = (x^2 - a_1)(x^2 - a_2)\cdots(x^2 - a_\ell) \in \mathbb{Z}[x],$$

then $\mathbb{K}/\mathbb{Q}$ is the splitting field of $f(x)$. Let

$$P := \left\{ p > 2 : \left(\frac{a_1}{p}\right) = \cdots = \left(\frac{a_\ell}{p}\right) = 1 \right\}.$$

By Theorem 1, we know that the density of P is

$$\frac{\alpha_S + \beta_S}{2^\ell} = \frac{1}{2^{\ell-k}}.$$

Now, we shall calculate the relative density of P using Chebotarev's Density Theorem.

Let $p \in P$. We need to calculate the Frobenius element $\sigma_p \in \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$. It is enough to find the action of σ_p on $\sqrt{a_i}$ for each i. Since $p \in P$, a_i is a quadratic residue modulo p, by Proposition 2, we see that p splits completely in $\mathbb{Q}(\sqrt{a_i})$. Therefore, the corresponding $e_i = f_i = 1$. Hence $\mathcal{O}_{\mathbb{Q}(\sqrt{a_i})}/\mathfrak{p}_i = \{0\}$. Therefore σ_p restricted to $\mathbb{Q}(\sqrt{a_i})$ is the identity. In fact this is true for every $i = 1, 2, \cdots, \ell$. Therefore, the Frobenius element $\sigma_p \in \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ satisfies

$$\sigma_p(\sqrt{a_i}) = \sqrt{a_i} \qquad \text{for all } i = 1, 2, \ldots, \ell.$$

Since any element $\alpha \in K$ can written as $\alpha = \sum_{i=1}^{\ell} c_i \sqrt{a_i}$, with $c_i \in \mathbb{Q}$,

$$\sigma_p(\alpha) = \sum_{i=1}^{\ell} c_i \sigma_p(\sqrt{a_i}) = \sum_{i=1}^{\ell} c_i \sqrt{a_i} = \alpha.$$

Thus, σ_p is identity for all $p \in P$. Hence, σ_p is uniquely defined in $\mathrm{Gal}(K/\mathbb{Q})$. By the Chebotarev Density theorem, the relative density of P is

$$\frac{1}{[\mathbb{K} : \mathbb{Q}]} = \frac{1}{2^t}.$$

Thus, we get that $t = \ell - k$, which is what we wanted. □

Example. Let $p_1, p_2, p_3, q_1, q_2, q_3$ be distinct primes. Let

$$S = \{p_1, p_3, p_1p_2, p_2p_3, q_1, q_3, q_1q_2, q_2q_3\}.$$

Observe that $|S| = 8$ and that $\beta_S = 0$. We also see that

$$a_1a_2a_3a_4 = (p_1p_2p_3)^2, \ a_5a_6a_7a_8 = (q_1q_2q_3)^2, \ a_1a_2\cdots a_8 = (p_1p_2p_3q_1q_2q_3)^2$$

are the only nonempty products of even length which are squares. Hence,

$$\alpha_S = 3 + 1 = 4 = 2^2.$$

Thus, the degree of $\mathbb{K}$ over $\mathbb{Q}$ is $\dfrac{\alpha_S}{2^8} = \dfrac{2^2}{2^8} = 2^6$.

Let us verify this using field theory. Let $\mathbb{K}_1 = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_3}, \sqrt{p_1p_2}, \sqrt{p_2p_3})$ and $\mathbb{K}_2 = \mathbb{Q}(\sqrt{q_1}, \sqrt{q_3}, \sqrt{q_1q_2}, \sqrt{q_2q_3})$. It is easy to see that $\mathbb{K}_1 = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3})$ and $\mathbb{K}_2 = \mathbb{Q}(\sqrt{q_1}, \sqrt{q_2}, \sqrt{q_3})$. Since there are no algebraic relations among the p_i's and the q_j's, we see that

$$\mathbb{K} = \mathbb{K}_1\mathbb{K}_2 = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}, \sqrt{q_1}, \sqrt{q_2}, \sqrt{q_3}),$$

and $\mathbb{K}_1 \cap \mathbb{K}_2 = \mathbb{Q}$. Hence, $[\mathbb{K} : \mathbb{Q}] = 2^6$.

Concluding Remarks. One could ask how hard or how easy it is to compute α_S and β_S?

(1) If we use Lemma 1, then it is clear that the image of τ lies in the subspace of W spanned by the prime numbers in $\mathcal{P}(S)$. Thus, we can think of the matrix associated to τ as a matrix A of type $\ell \times r$ with entries from $\{0, 1\}$, where $r = |\mathcal{P}(S)|$. Hence, computing α_S and β_S reduces to computing the kernel of A modulo 2, which is an easy linear algebra problem. Thus, all is needed are the factorizations of $a_1, \ldots, a_\ell$, so computing the values of α_S and β_S fall in the class of integer factorization problems.

(2) For a given real number x, we can easily compute the value of S_x (which comes in the proof of Theorem 1) by computing the Legendre symbols. Hence, we are able to compute the value $\dfrac{S_x}{\pi(x)}$ also. For large value of x, this quotient is an approximation to the density $\dfrac{\alpha_S + \beta_S}{2^\ell} = \dfrac{1}{[\mathbb{K} : \mathbb{Q}]}$. Therefore, the quotient $\pi(x)/S_x$ gives the approximation to the degree $[\mathbb{K} : \mathbb{Q}]$. However, the correct value of x which gives the best approximation comes from Proposition 1, as we use the estimate

$$\sum_{p \le x} \left(\frac{n}{p}\right) = o(\pi(x)).$$

Let $N_n > 1$ be an integer (depending on n) such that for every $x \ge N_n$, the above estimate is true. Let

$$\max\{N_n : n = a_1^{b_1}a_2^{b_2}\cdots a_\ell^{b_\ell} \ne \square, b_i \in \{0, 1\}, a_i \in S\} := N.$$

If we know the explicit value of N, then we can choose an $x > N$ and for this x, we have $\pi(x)/S_x$ is the best approximation to the degree $[\mathbb{K} : \mathbb{Q}]$. However, to find the explicit value of N, we need to know, from the proof of Proposition 1, the information on the least prime size in certain arithmetic progressions.

References

[1] E. Artin, Collected Papers, Addison-Wesley, 1965.

[2] R. Balasubramanian, F. Luca and R. Thangadurai, On the exact degree of $\mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \cdots, \sqrt{a_\ell})$ over $\mathbb{Q}$, To appear in: *Proc. Amer. Math. Soc.*, (2010).

[3] M. Fried, Arithmetical properties of value sets of polynomials, *Acta Arith.*, **15** (1968/69), 91-115.

[4] R. Gupta and M. Ram Murty, A remark on Artin's conjecture, *Invent. Math.* **78** (1984) (1), 127-130.

[5] D. R. Heath-Brown, Artin's conjecture for primitive roots, *Quart. J. Math. Oxford*, (2) **37** (1986), 27-38.

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

[7] C. S. Abel-Hollinger and H. G. Zimmer, Torsion groups of elliptic curves with integral j-invariant over multiquadratic fields, Number-theoretic and algebraic methods in computer science (Moscow, 1993), 69-87, World Sci. Publ., River Edge, NJ, 1995

[8] J. G. Janusz, Algebraic number fields, Second edition, Graduate Studies in Mathematics, **7**, American Mathematical Society, Providence, RI, 1996.

[9] M. Laska and M. Lorenz, Rational points on elliptic curves over $\mathbb{Q}$ in elementary abelian 2-extensions of $\mathbb{Q}$, *J. Reine Angew. Math.*, **355** (1985), 163-172.

[10] K. R. Matthews, A generalisation of Artin's conjecture for primitive roots, *Acta Arith.*, **XXIX** (1976), 113-146.

[11] P. Moree and R. Thangadurai, *Preprint.*

[12] K. Prachar, Primzahlverteilung, Springer, New York, 1957.

[13] S. Wright, Patterns of quadratic residues and nonresidues for infinitely many primes, J. Number Theory, 123 (2007) 120-132.

[14] S. Wright, A combinatorial problem related to quadratic non-residue modulo p, *To appear* Ars Combinatorica.

Department of Mathematics, Harish-Chandra Research Institute, Chhatnag Road, Jhunsi, Allahabad 211019 INDIA

E-mail address, R. Thangadfurai: `thanga@hri.res.in`