ON THE EXACT DEGREE OF $\mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \dots, \sqrt{a_\ell})$ OVER $\mathbb{Q}$

R. BALASUBRAMANIAN, F. LUCA, AND R. THANGADURAI

(Communicated by Ken Ono)

ABSTRACT. Let $S = \{a_1, a_2, \dots, a_\ell\}$ be a finite set of non-zero integers. In this paper, we give an exact formula for the degree of the multi-quadratic field $\mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \dots, \sqrt{a_\ell})$ over $\mathbb{Q}$. To do this, we compute the relative density of the set of prime numbers p for which all the a_i 's are simultaneously quadratic residues modulo p in two ways.

1. INTRODUCTION

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

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

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

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 Abel-Hollinger [2] and Laska and Lorenz [3].

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 . Before we state the main theorem, we must first present some notation.

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

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

exists. 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 $\prod_{s \in T} s = m^2$ for some integer m ; hence, $\alpha_S \geq 1$ for every S .

Received by the editors September 15, 2009.

2010 *Mathematics Subject Classification*. Primary 11A15.

Key words and phrases. Quadratic residues, Galois field, Chebotarev density theorem.

©2010 American Mathematical Society
 Reverts to public domain 28 years from publication

- (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 .

Now, we can state the main result of our paper.

Theorem 1.1. *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

In 1968, M. Fried [1] 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 $a \in S$. Similarly, in 1976, K. R. Matthews [4] found a necessary and sufficient condition for a to be a primitive root modulo p for every $a \in S$. More recently, S. Wright [5] and [6] also studied this qualitative problem.

Here we consider the quantitative problem as follows. More precisely, we calculate the relative density of those primes p such that a is a quadratic residue (respectively, non-residue) modulo p for every $a \in S$. Let us start with the following result.

Lemma 2.1. *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 $\mathbf{a}_1, \dots, \mathbf{a}_\ell$ 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 $\tau : V \rightarrow W$ be given by $\tau(\mathbf{a}_i) = a_i \pmod{(\mathbb{Q}^*)^2}$ and extended by linearity. It is then clear that $\{i_1, \dots, i_j\} \subseteq \{1, \dots, \ell\}$ is such that $a_{i_1} \cdots a_{i_j}$ is a perfect square of an integer if and only if $\mathbf{a}_{i_1} + \cdots + \mathbf{a}_{i_j} \in \text{Ker}(\tau)$. It now follows immediately that $\alpha_S + \beta_S = 2^k$, where k is the dimension of $\text{Ker}(\tau)$, 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 . The following result is well-known, and we omit its proof.

Lemma 2.2. *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 $x \rightarrow \infty$.

Theorem 2.3. *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*

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

Proof. 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:

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

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

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

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

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

For the remaining values of n (i.e., when n is not a perfect square), we apply Lemma 2.2 to get

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

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 $x \rightarrow \infty$, $\pi(x) \rightarrow \infty$, we get

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

This completes the proof of Theorem 2.3. $\square$

The method adopted to prove Theorem 2.3 can be applied to the quadratic non-residue case as well. Take

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

and proceed as in the proof of Theorem 2.3. This yields the following result:

Theorem 2.4. *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*

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

3. PROOF OF THEOREM 1.1

First, we shall recall Chebotarev's Density Theorem as follows.

Chebotarev's Density Theorem. *Let $\mathbb{K}/\mathbb{Q}$ be a Galois extension with Galois group G . For each prime p , let $\sigma_p \in G$ denote its Frobenius and let C be any conjugacy class of G . Then the relative density of the set of primes $P = \{p : \sigma_p \in C\}$ is $\frac{|C|}{[G : 1]}$.*

Proof of Theorem 1.1. It is clear that $\mathbb{K}$ is a 2-elementary abelian extension of $\mathbb{Q}$, so $\text{Gal}(\mathbb{K}/\mathbb{Q}) = (\mathbb{Z}/2\mathbb{Z})^t$ for some $1 \leq t \leq \ell$. 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 2.3, 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. $\square$

Let $p \in P$. We need to calculate the Frobenius element $\sigma_p \in \text{Gal}(\mathbb{K}/\mathbb{Q})$. 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 and hence p splits completely in $\mathbb{Q}(\sqrt{a_i})$. Therefore σ_p restricted to $\mathbb{Q}(\sqrt{a_i})$ is the identity. In fact this is true for every $i = 1, 2, \dots, \ell$. Therefore, the Frobenius element $\sigma_p \in \text{Gal}(\mathbb{K}/\mathbb{Q})$ satisfies

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

Hence, σ_p is uniquely defined in $\text{Gal}(\mathbb{K}/\mathbb{Q})$. 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. $\square$

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

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

are the only non-empty 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 $\frac{\alpha_S}{2^8} = \frac{2^2}{2^8} = 2^{-6}$.

Let us verify this using field theory. Let $\mathbb{K}_1 = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_3}, \sqrt{p_1 p_2}, \sqrt{p_2 p_3})$ and $\mathbb{K}_2 = \mathbb{Q}(\sqrt{q_1}, \sqrt{q_3}, \sqrt{q_1 q_2}, \sqrt{q_2 q_3})$. 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 is it to compute α_S and β_S ?

(1) If we use Lemma 2.1, 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 that is needed are the factorizations of $a_1, \dots, a_\ell$, so computing the values of α_S and β_S falls 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 2.3) by computing the Legendre symbols. Hence, we are able to compute the value $\frac{S_x}{\pi(x)}$ also. For large values of x , this quotient is an approximation to the density $\frac{\alpha_S + \beta_S}{2^\ell} = \frac{1}{[\mathbb{K} : \mathbb{Q}]}$. 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 Lemma 2.2, as we use the estimate

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

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

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

If we know the explicit value of N , then we can choose an $x > N$ and for this x , we have that $\pi(x)/S_x$ 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 Lemma 2.2, the information on the least prime size in certain arithmetic progressions.

ACKNOWLEDGMENTS

We thank the anonymous referee for a careful reading of a preliminary version of this manuscript and for suggestions which improved the quality of the paper. The second author was supported in part by grants SEP-CONACyT 79685 and PAPIIT 100508. The third author is thankful to Professors O. Ramaré and Piyush Kurur for useful discussions.

REFERENCES

1. M. Fried, *Arithmetical properties of value sets of polynomials*, Acta Arith., **15** (1968/69), 91–115. MR0244150 (39:5467)
2. 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. MR1377742 (97e:11060)
3. 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. MR772489 (86d:11048)
4. K. R. Matthews, *A generalisation of Artin's conjecture for primitive roots*, Acta Arith., **29** (1976), 113–146. MR0396448 (53:313)
5. S. Wright, *Patterns of quadratic residues and nonresidues for infinitely many primes*, J. Number Theory, **123** (2007), 120–132. MR2295434 (2007j:11007)
6. S. Wright, *A combinatorial problem related to quadratic non-residue modulo p* , Ars Combinatoria, to appear.

INSTITUTE OF MATHEMATICAL SCIENCES, C. I. T. CAMPUS, TARAMANI, CHENNAI 600113, INDIA
E-mail address: `balu@imsc.res.in`

MATHEMATICAL INSTITUTE, UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, AP. POSTAL, 61-3 (XANGARI), CP 58089, MORELIA, MICHOACÁN, MEXICO
E-mail address: `fluca@matmor.unam.mx`

DEPARTMENT OF MATHEMATICS, HARISH-CHANDRA RESEARCH INSTITUTE, CHHATNAG ROAD, JHUNSI, ALLAHABAD 211019, INDIA
E-mail address: `thanga@hri.res.in`