#A67 INTEGERS 16 (2016)

AN ANALOGUE OF ARTIN'S PRIMITIVE ROOT CONJECTURE

Pallab Kanti Dey
Harish-Chandra Research Institute, Chhatnag Road, Jhunsi, Allahabad, India
pallabkantidey@gmail.com

Balesh Kumar
Harish-Chandra Research Institute, Chhatnag Road, Jhunsi, Allahabad, India
baleshkumar@hri.res.in

Received: 7/31/14, Accepted: 5/6/16, Published: 10/5/16

Abstract

Let $S = \{a_1, a_2, \dots, a_n\}$ be a set of nonzero integers such that for any nonempty subset T of S, the product of all the elements in T is not a perfect square. Then the density of the set of primes p for which the a_i's are quadratic non-residues modulo p, but not primitive roots modulo p, is at least $\dfrac{1}{2^n(q-1)q^m}$, where m is a non-negative integer with $m \le n$ and q is the least odd prime which does not divide a_i for all $i = 1, 2, \dots, n$.

1. Introduction

Let $S = \{a_1, a_2, \dots, a_n\}$ be a set of nonzero integers which are not perfect squares. In 1968, M. Fried [5] proved that there are infinitely many primes p for which a is a quadratic residue modulo p for every $a \in S$. Further, he provided a necessary and sufficient condition for the a_i's to be quadratic non-residues modulo p. In 2011, R. Balasubramanian, F. Luca and R. Thangadurai [1] calculated the exact density of such primes in Fried's results. More recently, S. Wright ([15, 16]) also considered the above result qualitatively. In 1976, K. R. Matthews [11] proved, assuming the generalized Riemann hypothesis holds, that given nonzero integers $a_1, a_2, \dots, a_n$, there exists a real nonnegative constant $C = C(a_1, a_2, \dots, a_n)$ such that

$$|\{p \le x : \mathrm{ord}_p a_i = p-1, \forall i = 1, 2, \dots, n\}| = C\ \mathrm{li}(x) + O\left(\frac{(\log\log x)^{2^n-1}}{(\log x)^2}\right),$$

where $\mathrm{ord}_p(a_i) = \min\{k \in \mathbb{N} : a_i^k \equiv 1 \pmod p\}$. Matthews [11] generalized the result of Hooley [8] which confirms Artin's primitive root conjecture, under the assumption of generalized Riemann hypothesis. This conjecture is still unsolved. For the state of the art, we refer to a survey article of P. Moree [12].

In this paper, we consider a similar problem for the non-residues which are not primitive roots modulo prime p. It is easy to check that every non-residue modulo prime p is a primitive root modulo p if and only if p is a Fermat prime. Conjecturally, there are only finitely many Fermat primes. Hence for almost all the primes p, the set of non-residues modulo p has an element which is not a primitive root modulo p. The distribution of these residues was considered in [7] and [10]. Here, we prove the following theorem.

Main Theorem. *Let $S = \{a_1, a_2, \ldots, a_n\}$ be a finite set of nonzero integers such that for any nonempty subset T of S, the product of all the elements in T is not a perfect square. Let $q > 2$ be the least prime such that $q \nmid a_1 a_2 \ldots a_n$. Then the density of the set of primes p for which the a_i's are quadratic non-residues but not primitive roots modulo p, is at least $\dfrac{1}{2^n(q-1)q^m}$, where m is a non-negative integer with $m \leq n$.*

2. Preliminaries

We require the following basic results.

Lemma 1 ([13]). *Let a be a nonzero integer and let p and q be odd primes. Then, $p \equiv 1 \pmod q$ and $a^{(p-1)/q} \equiv 1 \pmod p$ if and only if p splits completely in $\mathbb{Q}(\zeta_q, a^{1/q})$, where ζ_q is a primitive q-th root of unity.*

Lemma 2. (Linearly disjointness)

(2.1) ([9]) *Let L and M be finite extensions over $\mathbb{Q}$ and let LM be their compositum over $\mathbb{Q}$. Let p be a rational prime. Then p splits completely in both L and M if and only if p splits completely in LM.*

(2.2) ([3]) *Let L and M be finite extensions over $\mathbb{Q}$ with $L \cap M = \mathbb{Q}$. If one of them is a normal extension over $\mathbb{Q}$, then L and M are linearly disjoint over $\mathbb{Q}$.*

(2.3) ([6]) *Let L and M be finite extensions over $\mathbb{Q}$ and let LM be their compositum over $\mathbb{Q}$. Then $[LM : \mathbb{Q}] = [L : \mathbb{Q}][M : \mathbb{Q}]$ if and only if L and M are linearly disjoint over $\mathbb{Q}$.*

(2.4) ([6]) *Let $\{L_i : i \in I\}$ be a linearly disjoint family of Galois extensions over $\mathbb{Q}$*

and let $\prod_{i \in I} L_i$ *be the compositum of* L_i*'s over* $\mathbb{Q}$*. Then*

$$Gal\left(\prod_{i \in I} L_i/\mathbb{Q}\right) \cong \prod_{i \in I} Gal(L_i/\mathbb{Q}).$$

Lemma 3 ([1]). *Let* $S = \{a_1, a_2, \ldots, a_n\}$ *be a finite set of nonzero integers. Let* α_S *be the number of subsets* T *of* S *including the empty set such that* $|T|$ *is even and* $\prod_{t \in T} t$ *is a perfect square, and let* β_S *be the number of subsets* T *of* S *such that* $|T|$ *is odd and* $\prod_{t \in T} t$ *is a perfect square. If* $K = \mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \ldots, \sqrt{a_n})$*, then we have* $[K : \mathbb{Q}] = 2^{n-k}$*, where* k *is the non-negative integer given by the relation* $2^k = \alpha_S + \beta_S$*.*

Lemma 4 ([14]). *Let* $n_1, n_2, \ldots, n_t$ *be odd positive integers and let* $a_1, a_2, \ldots, a_t$ *be nonzero pairwise co-prime integers where* a_i *is* n_i*-powerfree for all* $i = 1, 2, \ldots, t$*. Then*

$$[\mathbb{Q}(a_1^{1/n_1}, a_2^{1/n_2}, \ldots, a_t^{1/n_t}) : \mathbb{Q}] = n_1 n_2 \ldots n_t.$$

Lemma 5 ([14]). *Let* m *be a nonzero square-free integer. Let*

$$m' = \begin{cases} |m| & \text{if } m \equiv 1 \pmod 4 \\ 4|m| & \text{otherwise.} \end{cases}$$

Then $\mathbb{Q}(\sqrt{m}) \subseteq \mathbb{Q}(\zeta_n)$ *if and only if* n *is a multiple of* m'*.*

Lemma 6 ([4]). *Let* $M = \mathbb{Q}(\sqrt{a})$ *be a quadratic extension over* $\mathbb{Q}$*. Then* p *does not split in* M *if and only if* $\left(\frac{a}{p}\right) = -1$*, where* $\left(\frac{\cdot}{p}\right)$ *denotes the Legendre symbol.*

Theorem 7 ([6]). (Chebotarev Density Theorem) *Let* $K/\mathbb{Q}$ *be a Galois extension with Galois group* $Gal(K/\mathbb{Q})$*. Let* C *be a given conjugacy class in* $Gal(K/\mathbb{Q})$*. For any rational prime* p*, let* σ_p *be the Frobenius element in* $Gal(K/\mathbb{Q})$*. Then the relative density of the set of primes* $\{p \mid \sigma_p \in C\}$ *is* $\frac{|C|}{[K:\mathbb{Q}]}$*.*

To prove our main theorem, we need the following proposition.

Proposition 8. *Let* $a_1, a_2, \ldots, a_n$ *be any distinct nonzero integers and let* p *and* q *be odd primes. Then,* $p \equiv 1 \pmod q$ *and* $a_i^{(p-1)/q} \equiv 1 \pmod p$ *for all* $i = 1, 2, \ldots, n$ *if and only if* p *splits completely in* $\mathbb{Q}(\zeta_q, a_1^{1/q}, a_2^{1/q}, \ldots, a_n^{1/q})$*, where* ζ_q *is a primitive* q*-th root of unity.*

Proof. First we assume that $p \equiv 1 \pmod{q}$ and $a_i^{(p-1)/q} \equiv 1 \pmod{p}$ holds for all $i = 1, 2, \ldots, n$. Then by Lemma 1, p splits completely in $\mathbb{Q}(\zeta_q, a_i^{1/q})$ for all $i = 1, 2, \ldots, n$. Hence by Lemma 2 (2.1), p splits completely in their compositum $\mathbb{Q}(\zeta_q, a_1^{1/q}, a_2^{1/q}, \ldots, a_n^{1/q})$.

Conversely, let us assume that p splits completely in $\mathbb{Q}(\zeta_q, a_1^{1/q}, a_2^{1/q}, \ldots, a_n^{1/q})$. Since it is the compositum of $\mathbb{Q}(\zeta_q, a_1^{1/q})$, $\mathbb{Q}(\zeta_q, a_2^{1/q})$, ... , $\mathbb{Q}(\zeta_q, a_n^{1/q})$, by Lemma 2 (2.1), we see that p splits completely in those subfields of $\mathbb{Q}(\zeta_q, a_1^{1/q}, a_2^{1/q}, \ldots, a_n^{1/q})$. Hence by Lemma 1, we see that $p \equiv 1 \pmod{q}$ and $a_i^{(p-1)/q} \equiv 1 \pmod{p}$ for all $i = 1, 2, \ldots, n$. $\square$

We compute the degree of the extension $\mathbb{Q}(\zeta_q, a_1^{1/q}, a_2^{1/q}, \ldots, a_n^{1/q})$ over $\mathbb{Q}$ for any odd prime q. Denote $\mathbb{Q}(\zeta_q, a_1^{1/q}, a_2^{1/q}, \ldots, a_n^{1/q})$ by $L_{q,n}$. We know that $L_{q,n}$ is a Galois extension over $\mathbb{Q}$ as it is both normal and separable extension over $\mathbb{Q}$.

Lemma 9. $[L_{q,n} : \mathbb{Q}] = (q-1)q^m$*, where* m *is a non-negative integer with* $m \leq n$*.*

Proof. Let $\mathbb{P}$ be the set of all prime numbers. For each $i = 1, 2, \ldots, n$, let $\mathbb{P}_i = \{p \in \mathbb{P} : p \mid a_i\}$. Then $\mathcal{P} = \bigcup_{i=1}^{n} \mathbb{P}_i$ is a finite subset of $\mathbb{P}$ and we let $\mathcal{P} = \{p_1, p_2, \ldots, p_t\}$. Then we see that

$$L_{q,n} \subseteq \mathbb{Q}(\zeta_q, p_1^{1/q}, p_2^{1/q}, \ldots, p_t^{1/q}), \text{ where } p_i \in \mathcal{P} \text{ for all } i = 1, 2, \ldots, t.$$

Let $L'_{q,t} := \mathbb{Q}(p_1^{1/q}, p_2^{1/q}, \ldots, p_t^{1/q})$. Then by Lemma 3, we have, $[L'_{q,t} : \mathbb{Q}] = q^t$. Since $[\mathbb{Q}(\zeta_q) : \mathbb{Q}] = (q-1)$, we see that $L'_{q,t} \cap \mathbb{Q}(\zeta_q) = \mathbb{Q}$. Since $\mathbb{Q}(\zeta_q)/\mathbb{Q}$ is a Galois extension, by Lemma 2 (2.2), we conclude that $\mathbb{Q}(\zeta_q)$ and $L'_{q,t}$ are linearly disjoint over $\mathbb{Q}$. Hence by Lemma 2 (2.3), we have $[L'_{q,t}\mathbb{Q}(\zeta_q) : \mathbb{Q}] = q^t(q-1)$.

Since $L_{q,n} \subseteq L'_{q,t}\mathbb{Q}(\zeta_q)$, we see that $[L_{q,n} : \mathbb{Q}] \mid q^t(q-1)$. Also, since $\mathbb{Q}(\zeta_q) \subseteq L_{q,n}$, we have $(q-1) \mid [L_{q,n} : \mathbb{Q}]$. As $[L_{q,n} : \mathbb{Q}] \leq q^n(q-1)$, we conclude that $[L_{q,n} : \mathbb{Q}] = (q-1)q^m$, where m is a non-negative integer with $m \leq n$. $\square$

Remark. In the paper [2], the following result was proved. *Let* $S = \{a_1, a_2, \ldots, a_n\}$ *be a set of nonzero integers. Then for any odd prime* q*,* $[L_{q,n} : \mathbb{Q}] = (q-1)q^n$*, provided for any nonempty subset* T *of* S*, the product of all the elements in* T *is not a* q*-th power of an integer.* In particular, if a_i's are pairwise coprime square-free integers, we get the same degree as above.

3. Proof of Main Theorem

Let $\mathbb{P}$ be the set of all prime numbers and let $\mathbb{P}_i = \{p \in \mathbb{P} : p \mid a_i\}$ for all $i = 1, 2, \ldots, n$. Then

$$\mathcal{P} = \bigcup_{i=1}^{n} \mathbb{P}_i = \{p_1, p_2, \ldots, p_t\}$$

is a finite subset of $\mathbb{P}$. Let q be the least odd prime such that $q \notin \mathcal{P}$.

Consider the number fields $L_q = \mathbb{Q}(a_1^{1/q}, a_2^{1/q}, \ldots, a_n^{1/q}, \zeta_q)$ and $M_i = \mathbb{Q}(\sqrt{a_i})$ for all $i = 1, 2, \ldots, n$. Since for any nonempty subset T of S, the product of all the elements in T is not a perfect square, we have $[\mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \ldots, \sqrt{a_n}) : \mathbb{Q}] = 2^n$, by Lemma 3. Also from Lemma 2 (2.3), it is clear that the compositum $M_1 \cdots M_{j-1}$ and M_j are linearly disjoint over $\mathbb{Q}$ for $j = 2, 3, \ldots, n$. Hence $\{M_j\}_{j=1}^{n}$ is a linearly disjoint family over $\mathbb{Q}$.

Let $M = M_1 M_2 \cdots M_n$ be the compositum of M_j's over $\mathbb{Q}$. Since the M_j's are Galois extensions over $\mathbb{Q}$, we see that M is a Galois extension over $\mathbb{Q}$. Since $\{M_j\}_{j=1}^{n}$ is a linearly disjoint family of Galois extensions over $\mathbb{Q}$, by Lemma 2 (2.4), we have

$$\mathrm{Gal}(M/\mathbb{Q}) \cong \mathrm{Gal}(M_1/\mathbb{Q}) \times \mathrm{Gal}(M_2/\mathbb{Q}) \times \cdots \times \mathrm{Gal}(M_n/\mathbb{Q}).$$

Now consider the compositum of L_q and M and let $L = L_q M$.

We claim that $L_q \cap M = \mathbb{Q}$. To see this, assume for a contradiction that $L_q \cap M \neq \mathbb{Q}$. Since any subfield of M containing $\mathbb{Q}$ contains a quadratic extension, we see that $\mathbb{Q}(\sqrt{d}) \subseteq L_q \cap M$, where $d = p_1^{n_1} p_2^{n_2} \ldots p_t^{n_t}$ with $n_i = 0$ or 1 for all $i = 1, 2, \ldots, t$. By Lemma 5, $\mathbb{Q}(\sqrt{d}) \nsubseteq \mathbb{Q}(\zeta_q)$. Hence, $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\zeta_q)$ are linearly disjoint over $\mathbb{Q}$. Therefore, $[\mathbb{Q}(\sqrt{d}, \zeta_q) : \mathbb{Q}] = 2(q-1)$. Since $\mathbb{Q}(\sqrt{d}, \zeta_q) \subseteq L_q$ and by Lemma 9, $[L_q : \mathbb{Q}] = q^m(q-1)$ with $m \leq n$, we arrive at a contradiction as $2(q-1) \nmid q^m(q-1)$. So, $L_q \cap M = \mathbb{Q}$.

Since L_q and M both are Galois extensions over $\mathbb{Q}$, by Lemma 2 (2.4),

$$\mathrm{Gal}(L/\mathbb{Q}) \cong \mathrm{Gal}(L_q/\mathbb{Q}) \times \mathrm{Gal}(M/\mathbb{Q}).$$

Thus,

$$\mathrm{Gal}(L/\mathbb{Q}) \cong \mathrm{Gal}(L_q/\mathbb{Q}) \times \mathrm{Gal}(M_1/\mathbb{Q}) \times \cdots \times \mathrm{Gal}(M_n/\mathbb{Q}).$$

Consider the set

$$R = \{p \in \mathbb{P} : p \text{ splits completely in } L_q, p \text{ does not split in } M_i \text{ for all } i = 1, 2, \ldots, n\}.$$

Let p be a prime unramified in L. Then $p \in R$ if and only if the Frobenius element $\sigma_p \in \mathrm{Gal}(L/\mathbb{Q})$ is equal to $(1, -1, -1, \ldots, -1)$. This is because the first projection is trivial if and only if p splits completely in L_q, and the $(i+1)$-th projection is non-trivial if and only if p does not split in M_i and hence it is -1 as its Galois group is of order 2. Also, note that when $\sigma_p = (1, -1, -1, \ldots, -1)$, the conjugacy class of σ_p contains only one element which is nothing but σ_p itself. Therefore, by the Chebotarev Density Theorem (Theorem 7), the density of R is $\frac{1}{[L:\mathbb{Q}]}$.

By Lemma 2 (2.2, 2.3) and the above claim, we conclude that $[L:\mathbb{Q}] = [L_q:\mathbb{Q}][M:\mathbb{Q}] = 2^n q^m (q-1)$, where m is a non-negative integer with $m \leq n$. Therefore, the density of R is $\frac{1}{2^n (q-1) q^m}$.

By Proposition 8, p splits completely in L_q if and only if $p \equiv 1 \pmod q$ and

$$a_i^{(p-1)/q} \equiv 1 \pmod p \text{ for all } i = 1, 2, \ldots, n.$$

Also, by Lemma 6, we have that p does not split in M_i if and only if

$$\left(\frac{a_i}{p}\right) = -1 \text{ for all } i = 1, 2, \ldots, n.$$

Therefore, for any prime p in R, we have that, $a_1, a_2, \ldots, a_n$ are quadratic non-residues but not primitive roots modulo p.

Since the set R is contained in the set of primes for which $a_1, a_2, \ldots, a_n$ are quadratic non-residues but not primitive roots modulo p, the theorem follows. □

Acknowledgement. We would like to thank Prof. R. Thangadurai for discussing this problem and for making necessary corrections throughout this paper. Also we want to thank Bruce Landman for his helpful suggestions for improving this paper.

References

[1] R. Balasubramanian, F. Luca and R. Thangadurai, On the exact degree of $\mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \ldots, \sqrt{a_\ell})$ over $\mathbb{Q}$, *Proc. Amer. Math. Soc.* **138** (2010), 2283-2288.

[2] R. Balasubramanian and P. P. Pandey, Density of primes in ℓ-th power residues, *Proc. Indian Acad. Sci. (Math. Sci.)* **123** (1) (2013), 19-25.

[3] P. M. Cohn, *Basic Algebra, Groups, Rings and Fields*, 2nd Edition, Springer, 2005.

[4] J. Esmonde and M. Ram Murty, *Problems in Algebraic Number Theory*, Vol. 190, Springer-Verlag, 1999.

[5] M. D. Fried, Arithmetical properties of value sets of polynomials, *Acta Arith.* **15** (1968/1969), 91–115.

[6] M. D. Fried and M. Jarden, *Field Arithmetic, A Series of Modern Surveys in Mathematics*, 3rd Edition, Vol. 11, Springer, 2008.

[7] S. Gun, F. Luca, P. Rath, B. Sahu and R. Thangadurai, Distribution of residues modulo p, *Acta Arith.* **129**(4) (2007), 325–333.

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

[9] H. Koch, *Number Theory: Algebraic Numbers and Functions*, Vol. 24, American Mathematical Society, 2000.

[10] F. Luca, I. E. Shparlinski and R. Thangadurai, Quadratic non-residues versus primitive roots mod p, *J. Ramanujan Math. Soc.* **23** (1) (2008), 97–104.

[11] K. R. Matthews, A generalisation of Artin's conjecture for primitive roots, *Acta Arith* **29** (2) (1976), 113–146.

[12] P. Moree, Artin's primitive root conjecture - A survey, *Integers* **12** (2012), 1305–1416.

[13] M. Ram Murty, Artin's conjecture for primitive roots, *Math. Intelligencer* **10** (4) (1988), 59–67.

[14] S. H. Weintraub, *Galois Theory*, 2nd Edition, Springer, 2008.

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

[16] S. Wright, Some enumerative combinatorics arising from a problem on quadratic non-residues, *Australas. J. Combin.* **44** (2009), 301–315.