Kalyan Chakraborty
Azizul Hoque
Prem Prakash Pandey *Editors*

Class Groups of Number Fields and Related Topics

Springer

Class Groups of Number Fields and Related Topics

Kalyan Chakraborty · Azizul Hoque ·
Prem Prakash Pandey
Editors

Class Groups of Number Fields and Related Topics

Springer

Editors
Kalyan Chakraborty
School of Mathematics
Harish-Chandra Research Institute
Allahabad, Uttar Pradesh, India

Azizul Hoque
School of Mathematics
Harish-Chandra Research Institute
Allahabad, Uttar Pradesh, India

Prem Prakash Pandey
Department of Mathematics
IISER Berhampur
Berhampur, Odisha, India

ISBN 978-981-15-1513-2 ISBN 978-981-15-1514-9 (eBook)
https://doi.org/10.1007/978-981-15-1514-9

Mathematics Subject Classification (2010): 11Rxx, 11Sxx, 13C20

© Springer Nature Singapore Pte Ltd. 2020
This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

To all concerned, who were responsible for the successful completion of ICCGNFRT-2017

Preface

The number theory seminar has been organized, from January 20, 2017, by Algebraic/Algorithmic/Analytic Number Theory Seminar (ANTS) at Harish-Chandra Research Institute, Allahabad, India. This lecture series was started by Kalyan Chakraborty, Azizul Hoque and other members of the group. Prior to the existence of this group, we had decided to hold a series of three conferences on the theme 'Class Groups of Number Fields and Related Topics.' By October 2019, we had organized these three conferences. However, seeing its success and also on the request of all concerned, we have decided to continue this yearly conference.

The first 'International Conference on Class Groups of Number Fields and Related Topics (ICCGNFRT)' was held during September 4–7, 2017, at Harish-Chandra Research Institute, Allahabad, India.

This collection comprises original research papers and survey articles presented at ICCGNFRT-2017. There are 16 chapters on important topics in algebraic number theory and related parts of analytic number theory. These topics include class groups and class numbers of number fields, units, the Kummer–Vandiver conjecture, class number one problem, Diophantine equations, Thue equations, continued fractions, Euclidean number fields, heights, rational torsion points on elliptic curves, cyclotomic numbers, Jacobi sums and Dedekind zeta values.

We are grateful to Springer and its mathematics editor(s), especially Mr. Shamim Ahmad, for publishing this volume.

Allahabad, India
October 2019

Kalyan Chakraborty
Azizul Hoque
Prem Prakash Pandey

Contents

About the Editors

Kalyan Chakraborty is Professor at Harish-Chandra Research Institute (HRI), Allahabad, India, where he also obtained his Ph.D. in Mathematics. Professor Chakraborty was a postdoctoral fellow at IMSc, Chennai, and at Queen's University, Canada, and a visiting scholar at the University of Paris VI, VII, France; Tokyo Metropolitan University, Japan; Universitá Roma Tre, Italy; The University of Hong Kong, Hong Kong; Northwest University and Shandong University, China; Mahidol University, Thailand; Mandalay University, Myanmar; and many more. His broad area of research is number theory, particularly class groups, Diophantine equations, automorphic forms, arithmetic functions, elliptic curves, and special functions. He has published more than 60 research articles in respected journals and two books on number theory, and has been on the editorial boards of various leading journals. Professor Chakraborty is Vice-President of the Society for Special Functions and their Applications.

Azizul Hoque is a national postdoctoral fellow at Harish-Chandra Research Institute (HRI), Allahabad. He earned his Ph.D. in Pure Mathematics from Gauhati University, Guwahati, in 2015. Before joining HRI, Dr. Hoque was Assistant Professor at the Regional Institute of Science and Technology, Meghalaya, and at the University of Science and Technology, Meghalaya. He has visited Hong Kong University, Hong Kong; Northwest University, China; Shandong University, China; Mahidol University, Thailand; and many more. His research has mostly revolved around class groups, Diophantine equations, elliptic curves, zeta values, and related topics, and he has published a considerable number of papers in respected journals. He has been involved in a number of conferences and received numerous national and international grants.

Prem Prakash Pandey is Assistant Professor at the Indian Institute of Science Education and Research (IISER) Berhampur, Odisha. Before that, he was a post-doctoral fellow at HRI, Allahabad, and NISER Bhubaneswar, Odisha. After completing his Ph.D. at the Institute of Mathematical Sciences (IMSc), Chennai, he spent a couple of years at Chennai Mathematical Institute (CMI), Chennai, as a visiting scholar. Dr. Pandey's interests include class groups of number fields, annihilators of class groups, Diophantine equations, and related topics. During his time at HRI, he worked on divisibility problems for class numbers of quadratic fields with Dr. Hoque and Prof. Chakraborty.

Distribution of Residues Modulo p Using the Dirichlet's Class Number Formula

Jaitra Chattopadhyay, Bidisha Roy, Subha Sarkar and R. Thangadurai

1 Introduction

Let p be an odd prime number. A number $a \in \{1, \ldots, p-1\}$ is said to be a *quadratic residue* modulo p, if the congruence

$$x^2 \equiv a \pmod{p}$$

has a solution in $\mathbb{Z}$. Otherwise, a is said to be a *quadratic non-residue* modulo p. The study of distribution of quadratic residues and quadratic non-residues modulo p has been considered with great interest in the literature (see for instance [1, 3–7, 10, 12, 13, 15–25]).

Since $\mathbb{Z}/p\mathbb{Z}$ is a field, the polynomial $X^{p-1} - 1$ has precisely $p-1$ nonzero solutions over $\mathbb{Z}/p\mathbb{Z}$. As p is an odd prime, we see that $X^{p-1} - 1 = (X^{(p-1)/2} + 1)(X^{(p-1)/2} - 1)$ and one can conclude that there are exactly $\frac{p-1}{2}$ quadratic residues as well as non-residues modulo p in the interval $[1, p-1]$.

Question 1 *For an odd prime number p and a given natural number k with $1 \leq k \leq p-1$, we let $S_k = \{a \in \{1, 2, \ldots, p-1\} : a \equiv 0 \pmod{k}\}$ be the subset consisting of all natural numbers which are multiples of k. How many quadratic residues (respectively, non-residues) lie inside S_k?*

J. Chattopadhyay (✉) · B. Roy · S. Sarkar · R. Thangadurai
Harish-Chandra Research Institute, HBNI, Chhatnag Road,
Jhunsi 211019, Allahabad, India
e-mail: jaitrachattopadhyay@hri.res.in

B. Roy
e-mail: bidisharoy@hri.res.in

S. Sarkar
e-mail: subhasarkar@hri.res.in

R. Thangadurai
e-mail: thanga@hri.res.in

© Springer Nature Singapore Pte Ltd. 2020

K. Chakraborty et al. (eds.), *Class Groups of Number Fields and Related Topics*,
https://doi.org/10.1007/978-981-15-1514-9_9

In the literature, there are many papers addressed similar to Question 1 and to name a few, one may refer to [8, 9, 11]. First we shall fix some notations as follows. We denote by $Q(p, S_k)$ (respectively, $N(p, S_k)$) the number of quadratic residues (respectively, quadratic non-residues) modulo p in the subset S_k of the interval $[1, p-1]$.

The standard techniques in analytic number theory answers the above question as

$$Q(p, S_k) = \frac{p-1}{2k} + O(\sqrt{p}\log p) \tag{1}$$

and the same result is true for $N(p, S_k)$ for all k (we shall be proving this fact in this article). However, it might happen that for some primes p, we may have $Q(p, S_k) > N(p, S_k)$ or $Q(p, S_k) < N(p, S_k)$. Using the standard techniques, we could not answer this subtle question. In this article, we shall answer this using the Dirichlet's class number formula for the field $\mathbb{Q}(\sqrt{-p})$, when $k = 2, 3$ or 4. More precisely, we prove the following theorems.

Theorem 1 *Let p be an odd prime. If $p \equiv 3 \pmod 4$, then for any ϵ with $0 < \epsilon < \frac{1}{2}$, we have*

$$Q(p, S_2) - \frac{p-1}{4} \gg_\epsilon p^{\frac{1}{2}-\epsilon}.$$

When the prime $p \equiv 1 \pmod 4$, we have

$$Q(p, S_2) = \frac{p-1}{4}.$$

Corollary 1.1 *Let p be an odd prime and let $\mathcal{O}$ be the set of all odd integers in $[1, p-1]$. If $R = N(p, S_2)$ or $R = Q(p, \mathcal{O})$, then for any ϵ with $0 < \epsilon < \frac{1}{2}$, we have*

$$\frac{p-1}{4} - R \gg_\epsilon p^{\frac{1}{2}-\epsilon}, \text{ if } p \equiv 3 \pmod 4.$$

When the prime $p \equiv 1 \pmod 4$, we have

$$R = \frac{p-1}{4}.$$

Theorem 2 *Let p be an odd prime. If $p \equiv 1, 11 \pmod{12}$, then for any ϵ with $0 < \epsilon < \frac{1}{2}$, we have*

$$Q(p, S_3) - \frac{p-1}{6} \gg_\epsilon p^{\frac{1}{2}-\epsilon}.$$

When $p \equiv 5, 7 \pmod{12}$, in this method, we do not get any finer information other than in (1).

Corollary 1.2 *Let p be an odd prime. If $p \equiv 1, 11 \pmod{12}$, then for any ϵ with $0 < \epsilon < \frac{1}{2}$, we have*

$$\frac{p-1}{6} - N(p, S_3) \gg_\epsilon p^{\frac{1}{2}-\epsilon}.$$

Theorem 3 *Let p be an odd prime. Then, for $p \equiv 3 \pmod 8$, we have*

$$Q(p, S_4) = \frac{1}{2}\left[\frac{p-1}{4}\right].$$

Also, for any $0 < \epsilon < \frac{1}{2}$, we have

$$Q(p, S_4) - \frac{p-1}{8} \gg_\epsilon p^{\frac{1}{2}-\epsilon}, \text{ if } p \equiv 1 \pmod 4,$$

and

$$Q(p, S_4) - \frac{1}{2}\left[\frac{p-1}{4}\right] \gg_\epsilon p^{\frac{1}{2}-\epsilon}; \text{ if } p \equiv 7 \pmod 8.$$

Corollary 1.3 *Let p be an odd prime. Then, for $p \equiv 3 \pmod 8$, we have*

$$N(p, S_4) = \frac{1}{2}\left[\frac{p-1}{4}\right].$$

Also, for any $0 < \epsilon < \frac{1}{2}$, we have

$$\frac{p-1}{8} - N(p, S_4) \gg_\epsilon p^{\frac{1}{2}-\epsilon}; \text{ if } p \equiv 1 \pmod 4,$$

and

$$\frac{1}{2}\left[\frac{p-1}{4}\right] - N(p, S_4) \gg_\epsilon p^{\frac{1}{2}-\epsilon}; \text{ if } p \equiv 7 \pmod 8.$$

Using Theorems 1 and 3, we conclude the following corollary.

Corollary 1.4 *Let p be an odd prime such that $p \equiv 3 \pmod 8$. Then for any ϵ with $0 < \epsilon < \frac{1}{2}$, we have*

$$Q(p, S_2 \backslash S_4) - \frac{1}{2}\left\lfloor\frac{p-1}{4}\right\rfloor \gg_\epsilon p^{\frac{1}{2}-\epsilon}.$$

2 Preliminaries

In this section, we shall state many useful results as follows.

Theorem 4 (Polya–Vinogradov) *Let p be any odd prime and χ be a non-principal Dirichlet character modulo p. Then, for any integers $0 \leq M < N \leq p-1$, we have*

$$\left|\sum_{m=M}^{N} \chi(m)\right| \leq \sqrt{p} \log p.$$

Let us define the following counting functions as follows. Let

$$f(x) = \frac{1}{2}\left(1 + \left(\frac{x}{p}\right)\right) \text{ for all } x \in (\mathbb{Z}/p\mathbb{Z})^* \tag{2}$$

and

$$g(x) = \frac{1}{2}\left(1 - \left(\frac{x}{p}\right)\right) \text{ for all } x \in (\mathbb{Z}/p\mathbb{Z})^* \tag{3}$$

where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol. Then, we have

$$f(x) = \begin{cases} 1; \text{ if } x \text{ is a quadratic residue} \pmod{p}, \\ 0; \text{ otherwise.} \end{cases}$$

and

$$g(x) = \begin{cases} 1; \text{ if } x \text{ is a quadratic non-residue} \pmod{p}, \\ 0; \text{ otherwise.} \end{cases}$$

In the following lemma, we prove the "expected" result.

Lemma 1 *For an integer $k \geq 1$ and an odd prime p, let $S_k = kI$ where I is the interval $I = \{1, 2, \ldots, [(p-1)/k]\}$. Then*

$$Q(p, S_k) = \frac{1}{2}\left[\frac{p-1}{k}\right] + \frac{1}{2}\left(\frac{k}{p}\right)\sum_{m=1}^{(p-1)/k}\left(\frac{m}{p}\right) \tag{4}$$

and hence

$$Q(p, S_k) = \frac{1}{2}\left[\frac{p-1}{k}\right] + O(\sqrt{p}\log p).$$

The same expressions hold for $N(p, S_k)$ as well.

Proof We prove for $Q(p, S_k)$ and the proof of $N(p, S_k)$ follows analogously. Let ψ_k be the characteristic function for S_k which is defined as

$$\psi_k(m) = \begin{cases} 1; & \text{if } m \in S_k, \\ 0; & \text{if } m \notin S_k. \end{cases}$$

Now, by (2), we see that

$$Q(p, S_k) = \sum_{m \in S_k} f(m) = \sum_{m=1}^{p-1} \psi_k(m) f(m) = \frac{1}{2} \sum_{m=1}^{p-1} \psi_k(m) \left(1 + \left(\frac{m}{p}\right)\right)$$
$$= \frac{1}{2}\left[\frac{p-1}{k}\right] + \frac{1}{2}\left(\frac{k}{p}\right) \sum_{m=1}^{(p-1)/k} \left(\frac{m}{p}\right), \tag{5}$$

which proves (4). Then, by Theorem 4, we get

$$Q(p, S_k) = \frac{1}{2}\left[\frac{p-1}{k}\right] + O(\sqrt{p}\log p).$$

This finishes the proof. □

Let $q > 1$ be a positive integer and let ψ be a nontrivial quadratic character modulo q. Let $L(s, \psi) = \sum_{n=1}^{\infty} \frac{\psi(n)}{n^s}$ be the Dirichlet L-function associated to ψ. Since ψ is a nontrivial homomorphism, $L(s, \psi)$ admits the following Euler product expansion:

$$L(s, \psi) = \prod_{p \nmid q} \left(1 - \frac{\psi(p)}{p^s}\right)^{-1}$$

for all complex number s with $\Re(s) > 1$. This, in particular, shows that $L(s, \psi) > 0$ for all real number $s > 1$. By continuity, it follows that $L(1, \psi) \geq 0$. Dirichlet proved that $L(1, \psi) \neq 0$ in order to prove the infinitude of prime numbers in an arithmetic progression. Hence, it follows that $L(1, \psi) > 0$ for all nontrivial quadratic character ψ. Since $L(1, \psi) > 0$, it is natural to expect some nontrivial lower bound as a function of q. This is what was proved by Landau–Siegel in the following theorem. The proof can be found in [14].

Theorem 5 *Let $q > 1$ be a positive integer and ψ be a nontrivial quadratic character modulo q. Then for each $\epsilon > 0$, there exists a constant $C(\epsilon) > 0$ such that*

$$L(1, \psi) > \frac{C(\epsilon)}{q^\epsilon}.$$

The following lemma is crucial for our discussions. This lemma connects the sum of Legendre symbols and the Dirichlet L-function associated with Legendre symbol via the famous Dirichlet class number formula for the quadratic field. For an odd prime p, the Legendre symbol $\left(\frac{\cdot}{p}\right) = \chi_p(\cdot)$ is a quadratic Dirichlet character modulo p. We also define a character

$$\chi_4(n) = \begin{cases} (-1)^{(n-1)/2}; & \text{if } n \text{ is odd}, \\ 0; & \text{otherwise}. \end{cases}$$

Then one can define the Dirichlet character χ_{4p} as $\chi_{4p}(n) = \chi_4(n)\chi_p(n)$ for any odd prime p and similarly, we can define $\chi_{3p}(n) = \chi_3(n)\chi_p(n)$ for any odd prime $p > 3$. Clearly, χ_{4p} and χ_{3p} are nontrivial and real quadratic Dirichlet characters.

Lemma 2 *(See for instance, Page 151, Theorem 7.2 and 7.4 in [24]) Let $p > 3$ be an odd prime and for any real number $\ell \geq 1$, we define*

$$S(1, \ell) = \sum_{1 \leq m < \ell} \chi_p(m). \tag{6}$$

Then we have the following equalities.

(1) For a prime $p \equiv 3 \pmod 4$, we have

$$S(1, p/2) = \frac{\sqrt{p}}{\pi}\big(2 - \chi_p(2)\big) L(1, \chi_p),$$

where $L(1, \chi_p)$ is the Dirichlet L-function; Also, we have

$$S(1, p/3) = \frac{\sqrt{p}}{2\pi}(3 - \chi_p(3))L(1, \chi_p).$$

(2) For a prime $p \equiv 1 \pmod 4$, we have

$$S(1, p/3) = \frac{\sqrt{3p}}{2\pi} L(1, \chi_{3p});$$

Also, we have

$$S(1, p/4) = \frac{\sqrt{p}}{\pi} L(1, \chi_{4p}).$$

Now, we need the following lemma, which deals with the vanishing sums of Legendre symbols. This was proved in [2]. For more such relations one may refer to [8].

Lemma 3 *[2] Let p be an odd prime. Then the following equalities hold true.*

(1) If $p \equiv 1 \pmod 4$, then we have $\displaystyle\sum_{n=1}^{(p-1)/2} \left(\frac{n}{p}\right) = 0.$

(2) If $p \equiv 3 \pmod 8$, then we have $\displaystyle\sum_{n=1}^{\lfloor p/4 \rfloor} \left(\frac{n}{p}\right) = 0.$

(3) If $p \equiv 7 \pmod 8$, then we have $\displaystyle\sum_{\lceil p/4 \rceil}^{\lfloor p/2 \rfloor} \left(\frac{n}{p}\right) = 0.$

3 Proof of Theorem 1

Let p be a given odd prime. We want to estimate the quantity $Q(p, S_2)$. Therefore, by (5), we get

$$Q(p, S_2) = \frac{1}{2}\left[\frac{p-1}{2}\right] + \frac{1}{2}\left(\frac{2}{p}\right)\sum_{n=1}^{(p-1)/2}\left(\frac{n}{p}\right). \tag{7}$$

Now, we consider three cases as follows.

Case 1. $p \equiv 1 \pmod 4)$

In this case, since $\sum_{n=1}^{(p-1)/2}\left(\frac{n}{p}\right) = 0$, by Lemma 3 (1), the Eq. (7) reduces to

$$Q(p, S_2) = \frac{p-1}{4},$$

which is as desired.

Case 2. $p \equiv 3 \pmod 8$

By Lemma 2 (1) and by (7), we get

$$Q(p, S_2) = \frac{1}{2}\left[\frac{p-1}{2}\right] + \frac{\sqrt{p}}{\pi}\big(2 - \chi_p(2)\big)\, L(1, \chi_p).$$

In this case, we know that $\left(\frac{2}{p}\right) = -1$. Therefore, we get

$$Q(p, S_2) = \frac{1}{2}\left[\frac{p-1}{2}\right] + 3\frac{\sqrt{p}}{\pi}L(1, \chi_p).$$

Let ϵ be any real number such that $0 < \epsilon < \frac{1}{2}$. Then by Theorem 5, we get

$$Q(p, S_2) - \frac{1}{2}\left[\frac{p-1}{2}\right] \gg_\epsilon p^{\frac{1}{2}-\epsilon},$$

as desired.

Case 3. $p \equiv 7 \pmod 8$.

Since $p \equiv 7 \pmod 8$, we know that $\left(\frac{2}{p}\right) = 1$. Therefore, by Lemma 2 (1) and by (7), we get

$$Q(p, S_2) = \frac{1}{2}\left[\frac{p-1}{2}\right] + \frac{\sqrt{p}}{\pi}L(1, \chi_p) = \frac{1}{2}\left[\frac{p-1}{2}\right] + \frac{\sqrt{p}L(1, \chi_p)}{\pi}.$$

Let ϵ be any real number such that $0 < \epsilon < \frac{1}{2}$. Then by Theorem 5 we get

$$Q(p, S_2) - \frac{1}{2}\left[\frac{p-1}{2}\right] \gg_{\epsilon} p^{\frac{1}{2}-\epsilon}$$

which proves the theorem. □

4 Proof of Theorem 2

Let p be a given odd prime. We want to estimate the quantity $Q(p, S_3)$. Therefore, by (5), we get,

$$Q(p, S_3) = \frac{1}{2}\left[\frac{p-1}{3}\right] + \left(\frac{3}{p}\right) \sum_{n=1}^{(p-1)/3} \left(\frac{n}{p}\right). \tag{8}$$

Now, we consider the following cases.

Case 1. $p \equiv 1 \pmod{12}$

Note that, in this case, we have $\left(\frac{3}{p}\right) = 1$. By (8) and by Lemma 2 (2), we get

$$\begin{aligned} Q(p, S_3) - \frac{1}{2}\left(\frac{p-1}{3}\right) &= \frac{1}{2}\frac{\sqrt{3p}}{2\pi} L(1, \chi_3\chi_p) \\ &\geq \frac{\sqrt{3p}}{4\pi}\frac{C(\epsilon)}{(3p)^{\epsilon}} \\ &\gg_{\epsilon} p^{\frac{1}{2}-\epsilon}, \end{aligned}$$

for any given $0 < \epsilon < \frac{1}{2}$ in Theorem 5.

Case 2. $p \equiv 11 \pmod{12}$

In this case, we have, $\left(\frac{3}{p}\right) = 1$. Then again by (8) and by Lemma 2 (1), we get

$$Q(p, S_3) = \frac{1}{2}\left[\frac{p-1}{3}\right] + \frac{1}{2}\frac{\sqrt{3p}}{2\pi}(3 - \chi_p(3))L(1, \chi_p).$$

Hence

$$Q(p, S_3) - \frac{1}{2}\left[\frac{p-1}{3}\right] \gg_{\epsilon} p^{\frac{1}{2}-\epsilon},$$

for any $0 < \epsilon < \frac{1}{2}$ in Theorem 5. □

5 Proof of Theorem 3

At first, using the Eq. (5), we note that

$$Q(p,S_4)=\frac{1}{2}\left[\frac{p-1}{4}\right]+\frac{1}{2}\left(\frac{4}{p}\right)\sum_{m=1}^{(p-1)/4}\left(\frac{m}{p}\right)=\frac{1}{2}\left[\frac{p-1}{4}\right]+\frac{1}{2}\sum_{m=1}^{(p-1)/4}\left(\frac{m}{p}\right). \tag{9}$$

Case 1. $p \equiv 1 \pmod 4$

Now, we apply Lemma 2 (2) in (9) and we get

$$Q(p,S_4)=\frac{1}{2}\left(\frac{p-1}{4}\right)+\frac{1}{2}\frac{\sqrt{p}}{\pi}L(1,\chi_4\chi_p).$$

Hence

$$Q(p,S_4)-\frac{p-1}{8}\gg_\epsilon p^{\frac{1}{2}-\epsilon},$$

for any $0<\epsilon<\frac{1}{2}$ in Theorem 5.

Case 2. $p \equiv 3 \pmod 8$

In this case, we apply Lemma 3 (2) which says that $\displaystyle\sum_{n=1}^{[(p-1)/4]}\left(\frac{m}{p}\right)=0$. Hence, by (9), we get

$$Q(p,S_4)=\frac{1}{2}\left[\frac{p-1}{4}\right].$$

Case 3. $p \equiv 7 \pmod 8$

First note that by Lemma 3 (3), we have

$$\sum_{\frac{p-1}{4}<m<\frac{p-1}{2}}\left(\frac{m}{p}\right)=0.$$

Therefore, the Eq. (9) can be rewritten as

$$\begin{aligned}Q(p,S_4)&=\frac{1}{2}\left[\frac{p-1}{4}\right]+\frac{1}{2}\sum_{1\le m\le (p-1)/4}\left(\frac{m}{p}\right)+\frac{1}{2}\sum_{(p-1)/4\le m\le (p-1)/2}\left(\frac{m}{p}\right)\\&=\frac{1}{2}\left[\frac{p-1}{4}\right]+\frac{1}{2}\sum_{m=1}^{\frac{p-1}{2}}\left(\frac{m}{p}\right).\end{aligned}$$

Now, by Lemma 2 (1), we get

$$Q(p, S_4) = \frac{1}{2}\left[\frac{p-1}{4}\right] + \frac{1}{2}\frac{\sqrt{p}}{\pi}L(1, \chi_p).$$

Hence

$$Q(p, S_4) - \frac{1}{2}\left[\frac{p-1}{4}\right] \gg_\epsilon p^{\frac{1}{2}-\epsilon},$$

for any $0 < \epsilon < \frac{1}{2}$ in Theorem 5. This proves the result. □

Acknowledgements We thank Professor V. Kumar Murty for going through the manuscript very carefully and for a suggestion to clear our doubts.

References

1. A. Brauer, Űber Sequenzen von Potenzresten. Sitzungsberichte der Preubischen Akademie der Wissenschaften 9–16 (1928)
2. B.C. Berndt, S. Chowla, Zero sums of the legendre symbol. Nordisk Mat. Tidskr. **22**, 5–8 (1974)
3. L. Carlitz, Sets of primitive roots. Compos. Math. **13**, 65–70 (1956)
4. A. Gica, Quadratic residues of certain types. Rocky Mt. J. Math. **36**, 1867–1871 (2006)
5. S. Gun, B. Ramakrishnan, B. Sahu, R. Thangadurai, Distribution of quadratic non-residues which are not primitive roots. Math. Bohem. **130**(4), 387–396 (2005)
6. S. Gun, F. Luca, P. Rath, B. Sahu, R. Thangadurai, Distribution of residues modulo p. Acta Arith. **129**(4), 325–333 (2007)
7. M. Hausman, Primitive roots satisfying a coprime condition. Amer. Math. Monthly **83**, 720–723 (1976)
8. W. Johnson, K.J. Mitchell, Symmetries for sums of the legendre symbol. Pac. J. Math. **59**(1), 117–124 (1977)
9. B. Karaivanov, T.S. Vassilev, On certain sums involving the Legendre symbol. Integers **16**, A14 (2016)
10. W. Kohnen, An elementary proof of the theory of quadratic residues. Bull. Korean Math. Soc. **45** (2), 273–275 (2008)
11. A. Laradji, M. Mignotte, N. Tzanakis, Elementary trigonometric sums related to quadratic residues. Elem. Math. **67**, 51–60 (2012)
12. F. Luca, I.E. Shparlinski, R. Thangadurai, Quadratic non-residue verses primitive roots modulo p. J. Ramanujan Math. Soc. **23**(1), 97–104 (2008)
13. F. Luca, R. Thangadurai, Distribution of Residues Modulo p - II, to appear in the Ramanujan Mathematical Society Lecture Notes Series (2011)
14. H. Montgomery, R. Vaughan, *Multiplicative Number Theory I Classical Theory* (Cambridge University Press, Cambridge, 2007)
15. L. Moser, On the equation $\phi(n) = \pi(n)$. Pi Mu Epsilon J. 101–110 (1951)
16. P. Pollack, The least prime quadratic non-residue in a prescribed residue class mod 4. J. Number Theory **187**, 403–414 (2018)
17. M. Szalay, On the distribution of the primitive roots mod p (in Hungarian). Mat. Lapok **21**, 357–362 (1970)
18. M. Szalay, On the distribution of the primitive roots of a prime. J. Number Theory **7**, 183–188 (1975)
19. J. Tanti, R. Thangadurai, Distribution of residues and primitive roots. Proc. Indian Acad. Sci. **123**(2), 203–211 (2013)

20. E. Vegh, Primitive roots modulo a prime as consecutive terms of an arithmetic progression. J. Reine Angew. Math. **235**, 185–188 (1969)
21. E. Vegh, Arithmetic progressions of primitive roots of a prime. II, ibid. **244**, 108–111 (1970)
22. E. Vegh, A note on the distribution of the primitive roots of a prime. J. Number Theory **3**, 13–18 (1971)
23. E. Vegh, Arithmetic progressions of primitive roots of a prime. III. J. Reine Angew. Math. **256**, 130–137 (1972)
24. S. Wright, Quadratic residues and non-residues: selected topics. *Lecture notes in Mathematics*, vol. 2171. (Springer, 2016)
25. A. Weil, On the Riemann hypothesis. Proc. Nat. Acad. Sci. USA **27**, 345–347 (1941)