

Hybrid mean value on the difference between a quadratic residue and its inverse modulo p

By LIU HUANING (Xi'an) and ZHANG WENPENG (Xi'an)

Abstract. The main purpose of this paper is using the generalized Bernoulli numbers, Gauss sums and the mean value theorems of Dirichlet L -functions to study the asymptotic property of the difference between a quadratic residue and its inverse modulo p (a prime), and give an interesting hybrid mean value formula.

1. Introduction

Let $q > 2$ and c are two integers with $(c, q) = 1$. For each integer $1 \leq a \leq q$ with $(a, q) = 1$, we know that there exists one and only one integer $1 \leq b \leq q$ with $(b, q) = 1$ such that $ab \equiv c \pmod{q}$. Let

$$M(q, k, c) = \sum_{\substack{a=1 \\ ab \equiv c \\ \pmod{q}}}^q \sum_{\substack{b=1 \\ \pmod{q}}}^q (a - b)^{2k},$$

where $\sum_{a=1}^q$ denotes the summation over all a such that $(a, q) = 1$. In [3], the second author used the estimates for Kloosterman sums and trigonometric sums to obtain a sharp asymptotic formula for $M(q, k, c)$, and prove the following:

Mathematics Subject Classification: 11L05, 11A07.

Key words and phrases: modular inverses, Bernoulli numbers, Gauss sums.

This work is supported by the N.S.F. and P.N.S.F. of P.R. China.

Proposition 1. *Let $q > 2$ and c are two integers with $(c, q) = 1$. Then for any positive integer k , we have the asymptotic formula*

$$M(q, k, c) = \frac{1}{(2k+1)(k+1)} \phi(q) q^{2k} + O\left(4^k q^{\frac{4k+1}{2}} d^2(q) \ln^2 q\right),$$

where $\phi(q)$ is the Euler function, and $d(q)$ is the divisor function.

The error term in Proposition 1 is the best possible. In fact for $k = 1$, let

$$M(q, 1, c) = \frac{1}{6} \phi(q) q^2 + \frac{1}{3} q \prod_{p|q} (1-p) + F(q, 1, c),$$

where $\prod_{p|q}$ denotes the product over all distinct prime divisors of q . The second author [5] used the properties of Dedekind sums and Cochrane sums to give a sharp mean value formula for $F(q, 1, c)$. That is the following:

Proposition 2. *For any integer $q > 2$, we have the asymptotic formula*

$$\sum_{c=1}^q{}' F^2(q, 1, c) = \frac{5}{36} q^3 \phi^3(q) \prod_{p^\alpha || q} \frac{\frac{(p+1)^3}{p(p^2+1)} - \frac{1}{p^{3\alpha-1}}}{1 + \frac{1}{p} + \frac{1}{p^2}} + O\left(q^5 \exp\left(\frac{4 \ln q}{\ln \ln q}\right)\right),$$

where $\prod_{p^\alpha || q}$ denotes the product over all prime divisors of q with $p^\alpha | q$ and $p^{\alpha+1} \nmid q$.

Now we consider the difference between a quadratic residue and its inverse modulo q . Let

$$N(q, k, c) = \sum_{\substack{a=1 \\ a \in A \\ ab \equiv c}}^q{}' \sum_{\substack{b=1 \\ b \in A \\ \text{mod } q}}^q{}' (a-b)^{2k},$$

where A denotes the set of all quadratic residues modulo q . Denote

$$\begin{aligned} N(q, k, c) &= \frac{1}{2\phi(q)} \sum_{a=1}^q{}' \sum_{b=1}^q{}' (a-b)^{2k} \\ &\quad + \frac{1}{\phi(q)} \sum_{a=1}^q{}' \sum_{b=1}^q{}' \chi_2(b) (a-b)^{2k} + E(q, k, c), \end{aligned}$$

where χ_2 is the quadratic character modulo q .

It is interesting that there exists some relation between $E(q, k, c)$ and the classical Kloosterman sums

$$K(m, n; q) = \sum_{a=1}^q{}' e\left(\frac{ma + n\bar{a}}{q}\right),$$

where $e(y) = e^{2\pi iy}$, $\bar{a}$ is defined by the equation $a\bar{a} \equiv 1 \pmod{q}$. In this paper, we use the generalized Bernoulli numbers, Gauss sums and the mean value theorems of Dirichlet L -functions to study the hybrid mean value of $\sum_{\substack{c=1 \\ c \in A}}^{p-1} E(p, k, c)K(c, 1; p)$, and give an interesting asymptotic formula.

That is, we shall prove the following:

Theorem 1. *For any prime $p \geq 5$ and integer $k \geq 1$, we have the following:*

$$\begin{aligned} & \sum_{\substack{c=1 \\ c \in A}}^{p-1} E(p, k, c)K(c, 1; p) \\ &= 2p^{2k+2} \sum_{n=2}^{2k-2} C_{2k}^n \sum_{m=1}^{\lfloor \frac{n}{2} \rfloor} \sum_{l=1}^{\lfloor \frac{2k-n}{2} \rfloor} \frac{C_n^{2m-1} C_{2k-n}^{2l-1} (2m-1)!(2l-1)!}{(-1)^{n+m+l} (2\pi)^{2m+2l}} \\ & \quad - 2p^{2k+2} \sum_{n=1}^{2k-1} C_{2k}^n \sum_{m=0}^{\lfloor \frac{n-1}{2} \rfloor} \sum_{l=0}^{\lfloor \frac{2k-n-1}{2} \rfloor} \frac{C_n^{2m} C_{2k-n}^{2l} (2m)!(2l)!}{(-1)^{n+m+l} (2\pi)^{2m+2l+2}} + O(p^{2k+\frac{3}{2}+\epsilon}), \end{aligned}$$

where $C_n^m = \frac{n!}{m!(n-m)!}$ is the combinatorial number, ϵ is any fixed positive number, and $[y]$ denotes the greatest integer not more than y .

For general integers $q \geq 5$ and $k \geq 1$, whether there exists an asymptotic formula for

$$\sum_{\substack{c=1 \\ c \in A}}^q{}' E(q, k, c)K(c, 1; q)$$

is an open problem.

2. Some lemmas

To complete the proof of Theorem 1, we need the following lemmas.

Lemma 1. *Let q be a positive integer, then for any character χ modulo q we have*

$$\sum_{\substack{c=1 \\ c \in A}}^q \bar{\chi}(c) K(c, 1; q) = \frac{1}{2} \tau^2(\bar{\chi}) + \frac{1}{2} \tau^2(\bar{\chi} \chi_2),$$

where $\tau(\chi) = \sum_{a=1}^q \chi(a) e(\frac{a}{q})$ is the Gauss sum.

PROOF. Noting that (see Lemma 2 of [6])

$$\sum_{c=1}^q \bar{\chi}(c) K(c, 1; q) = \tau^2(\bar{\chi}),$$

so we have

$$\begin{aligned} \sum_{\substack{c=1 \\ c \in A}}^q \bar{\chi}(c) K(c, 1; q) &= \frac{1}{2} \sum_{c=1}^q [1 + \chi_2(c)] \bar{\chi}(c) K(c, 1; q) \\ &= \frac{1}{2} \tau^2(\bar{\chi}) + \frac{1}{2} \tau^2(\bar{\chi} \chi_2). \end{aligned}$$

This proves Lemma 1. □

Lemma 2. *Let integers $q > 2$ and $n > 0$, then for any primitive character χ modulo q we have*

$$\sum_{a=1}^q a^n \chi(a) = \begin{cases} 2q^n \tau(\chi) \sum_{m=1}^{\lfloor \frac{n}{2} \rfloor} \frac{C_n^{2m-1} (2m-1)! L(2m, \bar{\chi})}{(-1)^{m+1} (2\pi)^{2m}}, & \text{if } \chi(-1) = 1; \\ 2q^n \tau(\chi) \sum_{m=0}^{\lfloor \frac{n-1}{2} \rfloor} \frac{C_n^{2m} (2m)! L(2m+1, \bar{\chi})}{(-1)^{m+1} (2\pi)^{2m+1}}, & \text{if } \chi(-1) = -1, \end{cases}$$

where $L(s, \chi)$ is the Dirichlet L -function corresponding to χ .

PROOF. Usually, the generalized Bernoulli numbers $B_{k,\chi}$ are defined as following:

$$\sum_{a=1}^q \chi(a) \frac{te^{at}}{e^{qt} - 1} = \sum_{k=0}^{\infty} \frac{B_{k,\chi}}{k!} t^k.$$

Let

$$B_{n,\chi}(x) = \sum_{k=0}^n C_n^k B_{k,\chi} x^{n-k},$$

then from [1] we know that

$$\begin{aligned} \sum_{a=1}^q a^n \chi(a) &= \frac{1}{n+1} (B_{n+1,\chi}(q) - B_{n+1,\chi}(0)) \\ &= \frac{1}{n+1} \sum_{k=0}^n C_{n+1}^k B_{k,\chi} q^{n+1-k}. \end{aligned} \quad (1)$$

For $\chi(-1) = 1$, from (1) we have

$$\sum_{a=1}^q a^n \chi(a) = \frac{1}{n+1} \sum_{m=1}^{\lfloor \frac{n}{2} \rfloor} C_{n+1}^{2m} B_{2m,\chi} q^{n+1-2m}. \quad (2)$$

Noting that (see [1])

$$L(2m, \bar{\chi}) = \frac{(-1)^{m+1} \tau(\bar{\chi})}{2(2m)!} \left(\frac{2\pi}{q} \right)^{2m} B_{2m,\chi} \quad (3)$$

for any positive integer m , so from (2) and (3) we have

$$\sum_{a=1}^q a^n \chi(a) = 2q^n \tau(\chi) \sum_{m=1}^{\lfloor \frac{n}{2} \rfloor} \frac{C_n^{2m-1} (2m-1)! L(2m, \bar{\chi})}{(-1)^{m+1} (2\pi)^{2m}}, \quad \text{if } \chi(-1) = 1.$$

For $\chi(-1) = -1$, it follows from (1) that

$$\sum_{a=1}^q a^n \chi(a) = B_{1,\chi} q^n + \frac{1}{n+1} \sum_{m=1}^{\lfloor \frac{n-1}{2} \rfloor} C_{n+1}^{2m+1} B_{2m+1,\chi} q^{n-2m}. \quad (4)$$

Noting that (see [1])

$$B_{1,\chi} = \frac{i\tau(\chi)L(1,\bar{\chi})}{\pi}, \quad (5)$$

and for any positive integer m ,

$$L(2m+1, \bar{\chi}) = \frac{i(-1)^m \tau(\bar{\chi})}{2(2m+1)!} \left(\frac{2\pi}{q}\right)^{2m+1} B_{2m+1,\chi}, \quad (6)$$

now combining (4), (5) and (6) we have

$$\sum_{a=1}^q a^n \chi(a) = 2q^n \tau(\chi) \sum_{m=0}^{\lfloor \frac{n-1}{2} \rfloor} \frac{C_n^{2m}(2m)! L(2m+1, \bar{\chi})}{(-1)^{m+1} (2\pi)^{2m+1} i}, \quad \text{if } \chi(-1) = -1.$$

This completes the proof of Lemma 2. $\square$

Lemma 3. *Let q and r be integers with $q \geq 2$ and $(r, q) = 1$, χ be a Dirichlet character modulo q . Then we have the identities*

$$\sum_{\chi \bmod q}^* \chi(r) = \sum_{d|(q, r-1)} \mu\left(\frac{q}{d}\right) \phi(d)$$

and

$$J(q) = \sum_{d|q} \mu(d) \phi\left(\frac{q}{d}\right),$$

where $\sum_{\chi \bmod q}^*$ denotes the summation over all primitive characters modulo q , $\mu(n)$ is the Möbius function and $J(q)$ denotes the number of primitive characters mod q .

PROOF. This is Lemma 3 of [4]. $\square$

Lemma 4. *Let q be any integer with $q > 2$, and $u, v \geq 1$ be real numbers. Then we have*

$$\begin{aligned} \text{(I)} \quad & \sum_{\chi(-1)=1}^* L(u, \bar{\chi}) L(v, \bar{\chi}) = \frac{J(q)}{2} + O(q^\epsilon); \\ \text{(II)} \quad & \sum_{\chi(-1)=-1}^* L(u, \bar{\chi}) L(v, \bar{\chi}) = \frac{J(q)}{2} + O(q^\epsilon). \end{aligned}$$

PROOF. We only prove (II), since similarly we can deduce (I). For any non-principal character χ modulo q , and parameter $N \geq q$, applying Abel's identity we have

$$\begin{aligned} L(u, \bar{\chi}) &= \sum_{n=1}^{+\infty} \frac{\bar{\chi}(n)}{n^u} = \sum_{1 \leq n \leq N} \frac{\bar{\chi}(n)}{n^u} + u \int_N^{+\infty} \frac{\sum_{N < n \leq y} \bar{\chi}(n)}{y^{u+1}} dy \\ &= \sum_{1 \leq n \leq N} \frac{\bar{\chi}(n)}{n^u} + O\left(\frac{\sqrt{q} \log q}{N^u}\right). \end{aligned} \quad (7)$$

Let $\sigma_\alpha(n) = \sum_{d|n} d^\alpha$. For $(a, q) = 1$, by Lemma 3 we have

$$\begin{aligned} \sum_{\chi(-1)=-1}^* \chi(a) &= \frac{1}{2} \sum_{\chi \bmod q}^* (1 - \chi(-1))\chi(a) = \frac{1}{2} \sum_{\chi \bmod q}^* \chi(a) - \frac{1}{2} \sum_{\chi \bmod q}^* \chi(-a) \\ &= \frac{1}{2} \sum_{d|(q, a-1)} \mu\left(\frac{q}{d}\right) \phi(d) - \frac{1}{2} \sum_{d|(q, a+1)} \mu\left(\frac{q}{d}\right) \phi(d). \end{aligned}$$

Therefore

$$\begin{aligned} &\sum_{\chi(-1)=-1}^* L(u, \bar{\chi}) L(v, \bar{\chi}) \\ &= \sum_{\chi(-1)=-1}^* \left(\sum_{1 \leq n \leq N} \frac{\bar{\chi}(n)}{n^u} + O\left(\frac{\sqrt{q} \log q}{N^u}\right) \right) \left(\sum_{1 \leq m \leq N} \frac{\bar{\chi}(m)}{m^v} + O\left(\frac{\sqrt{q} \log q}{N^v}\right) \right) \\ &= \sum_{\chi(-1)=-1}^* \sum_{1 \leq n \leq N} \sum_{1 \leq m \leq N} \frac{\bar{\chi}(n) \bar{\chi}(m)}{n^u m^v} + O\left(\frac{q^{\frac{3}{2}} \log^2 q}{N}\right) \\ &= \sum_{1 \leq k \leq N^2} \frac{\sigma_{u-v}(k)}{k^u} \sum_{\chi(-1)=-1}^* \bar{\chi}(k) + O\left(\frac{q^{\frac{3}{2}} \log^2 q}{N}\right) \\ &= \frac{1}{2} \sum_{\substack{1 \leq k \leq N^2 \\ (k, q)=1}} \frac{\sigma_{u-v}(k)}{k^u} \sum_{d|(q, k-1)} \mu\left(\frac{q}{d}\right) \phi(d) \\ &\quad - \frac{1}{2} \sum_{\substack{1 \leq k \leq N^2 \\ (k, q)=1}} \frac{\sigma_{u-v}(k)}{k^u} \sum_{d|(q, k+1)} \mu\left(\frac{q}{d}\right) \phi(d) + O\left(\frac{q^{\frac{3}{2}} \log^2 q}{N}\right) \end{aligned}$$

$$\begin{aligned}
&= \frac{1}{2} \sum_{d|q} \mu\left(\frac{q}{d}\right) \phi(d) \sum_{\substack{1 \leq k \leq N^2 \\ (k,q)=1 \\ k \equiv 1 \pmod{d}}} \frac{\sigma_{u-v}(k)}{k^u} \\
&\quad - \frac{1}{2} \sum_{d|q} \mu\left(\frac{q}{d}\right) \phi(d) \sum_{\substack{1 \leq k \leq N^2 \\ (k,q)=1 \\ k \equiv -1 \pmod{d}}} \frac{\sigma_{u-v}(k)}{k^u} + O\left(\frac{q^{\frac{3}{2}} \log^2 q}{N}\right) \\
&= \frac{J(q)}{2} + O\left(\sum_{d|q} \phi(d) \sum_{1 \leq l \leq \frac{N^2-1}{d}} \frac{\sigma_{u-v}(ld+1)}{(ld+1)^u}\right) \\
&\quad + O\left(\sum_{d|q} \phi(d) \sum_{1 \leq l \leq \frac{N^2+1}{d}} \frac{\sigma_{u-v}(ld-1)}{(ld-1)^u}\right) + O\left(\frac{q^{\frac{3}{2}} \log^2 q}{N}\right) \\
&= \frac{J(q)}{2} + O\left(\frac{q^{\frac{3}{2}} \log^2 q}{N}\right) + O(N^\epsilon).
\end{aligned}$$

Now taking $N = q^{\frac{3}{2}}$ in above, we immediately get

$$\sum_{\chi(-1)=-1}^* L(u, \bar{\chi}) L(v, \bar{\chi}) = \frac{J(q)}{2} + O(q^\epsilon).$$

This proves Lemma 4. $\square$

Lemma 5. *Let q be an odd prime power and let F be the field $GF(q)$. Let $f(y)$ be a non-constant polynomial over F which decomposes into the product of m distinct linear factors. Then, for the quadratic character χ ,*

$$\left| \sum_{y \in F} \chi(f(y)) \right| \leq (m-1)q^{\frac{1}{2}}.$$

PROOF. This is the well-known estimate for character sums, due to WEIL [2]. $\square$

Lemma 6. *Let prime $p \geq 5$, $u, v \geq 1$ be real numbers, χ_2 be the quadratic character modulo p . Then we have*

$$(I) \quad \sum_{\substack{\chi \neq \chi_0 \\ \chi(-1)=1}} \tau^2(\bar{\chi}\chi_2) \tau^2(\chi) L(u, \bar{\chi}) L(v, \bar{\chi}) \ll p^{\frac{5}{2}+\epsilon};$$

$$(II) \quad \sum_{\chi(-1)=-1} \tau^2(\overline{\chi}\chi_2)\tau^2(\chi)L(u,\overline{\chi})L(v,\overline{\chi}) \ll p^{\frac{5}{2}+\epsilon}.$$

PROOF. We only prove (II), since similarly we can deduce (I). From the properties of Gauss sums we have

$$\begin{aligned} \tau(\overline{\chi}\chi_2)\tau(\chi) &= \sum_{a=1}^{p-1} \overline{\chi}(a)\chi_2(a)e\left(\frac{a}{p}\right) \sum_{b=1}^{p-1} \chi(b)e\left(\frac{b}{p}\right) \\ &= \sum_{a=1}^{p-1} \chi_2(a)e\left(\frac{a}{p}\right) \sum_{b=1}^{p-1} \chi(b)e\left(\frac{ba}{p}\right) \\ &= \sum_{b=1}^{p-1} \chi(b) \sum_{a=1}^{p-1} \chi_2(a)e\left(\frac{a(1+b)}{p}\right) \\ &= \tau(\chi_2) \sum_{b=1}^{p-1} \chi(b)\chi_2(1+b), \end{aligned}$$

therefore

$$\begin{aligned} \tau^2(\overline{\chi}\chi_2)\tau^2(\chi) &= \tau^2(\chi_2) \sum_{a=1}^{p-1} \chi(a)\chi_2(1+a) \sum_{b=1}^{p-1} \chi(b)\chi_2(1+b) \\ &= \tau^2(\chi_2) \sum_{b=1}^{p-1} \chi(b) \sum_{a=1}^{p-1} \chi_2(1+a)\chi_2(1+b\overline{a}). \end{aligned}$$

Noting that for $(ab, p) = 1$, by the orthogonality relations for character sums modulo p we have

$$\sum_{\chi(-1)=-1} \chi(a)\overline{\chi}(b) = \begin{cases} \frac{1}{2}(p-1), & \text{if } a \equiv b \pmod{p}; \\ -\frac{1}{2}(p-1), & \text{if } a \equiv -b \pmod{p}; \\ 0, & \text{otherwise.} \end{cases} \quad (8)$$

Then for parameter $N \geq p$, by (7) and (8) we get

$$\sum_{\chi(-1)=-1} \tau^2(\overline{\chi}\chi_2)\tau^2(\chi)L(u,\overline{\chi})L(v,\overline{\chi})$$

$$\begin{aligned}
&= \sum_{\chi(-1)=-1} \tau^2(\bar{\chi}\chi_2) \tau^2(\chi) \sum_{1 \leq n \leq N} \sum_{1 \leq m \leq N} \frac{\bar{\chi}(n)\bar{\chi}(m)}{n^u m^v} + O\left(\frac{p^{\frac{7}{2}} \log^2 p}{N}\right) \\
&= \tau^2(\chi_2) \sum_{1 \leq k \leq N^2} \frac{\sigma_{u-v}(k)}{k^u} \sum_{b=1}^{p-1} \sum_{a=1}^{p-1} \chi_2(1+a) \chi_2(1+b\bar{a}) \sum_{\chi(-1)=-1} \chi(b) \bar{\chi}(k) \\
&\quad + O\left(\frac{p^{\frac{7}{2}} \log^2 p}{N}\right) \\
&= \frac{\tau^2(\chi_2)(p-1)}{2} \sum_{\substack{1 \leq k \leq N^2 \\ (k,p)=1}} \frac{\sigma_{u-v}(k)}{k^u} \sum_{\substack{b=1 \\ b \equiv k \pmod p}}^{p-1} \sum_{a=1}^{p-1} \chi_2(1+a) \chi_2(1+b\bar{a}) \\
&\quad - \frac{\tau^2(\chi_2)(p-1)}{2} \sum_{\substack{1 \leq k \leq N^2 \\ (k,p)=1}} \frac{\sigma_{u-v}(k)}{k^u} \sum_{\substack{b=1 \\ b \equiv -k \pmod p}}^{p-1} \sum_{a=1}^{p-1} \chi_2(1+a) \chi_2(1+b\bar{a}) \\
&\quad + O\left(\frac{p^{\frac{7}{2}} \log^2 p}{N}\right).
\end{aligned}$$

On the other hand, by Lemma 5 we can get

$$\begin{aligned}
\sum_{a=1}^{p-1} \chi_2(1+a) \chi_2(1+b\bar{a}) &= \sum_{a=1}^{p-1} \chi_2(a^2) \chi_2(1+a) \chi_2(1+b\bar{a}) \\
&= \sum_{a=1}^{p-1} \chi_2(a) \chi_2(a^2 + ab + a + b) \ll p^{\frac{1}{2}}.
\end{aligned}$$

So we have

$$\begin{aligned}
&\sum_{\chi(-1)=-1} \tau^2(\bar{\chi}\chi_2) \tau^2(\chi) L(u, \bar{\chi}) L(v, \bar{\chi}) \\
&\ll p^{\frac{5}{2}} \sum_{1 \leq k \leq N^2} \frac{\sigma_{u-v}(k)}{k^u} + \frac{p^{\frac{7}{2}} \log^2 p}{N} \ll p^{\frac{5}{2}} N^\epsilon + \frac{p^{\frac{7}{2}} \log^2 p}{N}.
\end{aligned}$$

Now taking $N = p$ in above, we immediately get

$$\sum_{\chi(-1)=-1} \tau^2(\bar{\chi}\chi_2) \tau^2(\chi) L(u, \bar{\chi}) L(v, \bar{\chi}) \ll p^{\frac{5}{2}+\epsilon}.$$

This completes the proof of Lemma 6. $\square$

Lemma 7. *Let prime $p > 2$, $u, v \geq 1$ be real numbers, χ_2 be the quadratic character modulo p . Then we have*

$$(I) \quad \sum_{\substack{\chi \neq \chi_0 \\ \chi(-1)=1}} \tau(\bar{\chi})\tau(\chi\chi_2)L(u, \bar{\chi})L(v, \bar{\chi}\chi_2) \ll p^{\frac{3}{2}+\epsilon};$$

$$(II) \quad \sum_{\chi(-1)=-1} \tau(\bar{\chi})\tau(\chi\chi_2)L(u, \bar{\chi})L(v, \bar{\chi}\chi_2) \ll p^{\frac{3}{2}+\epsilon}.$$

PROOF. We only prove (II), since similarly we can deduce (I). From the properties of Gauss sums we have

$$\begin{aligned} \tau(\bar{\chi})\tau(\chi\chi_2) &= \sum_{a=1}^{p-1} \bar{\chi}(a)e\left(\frac{a}{p}\right) \sum_{b=1}^{p-1} \chi(b)\chi_2(b)e\left(\frac{b}{p}\right) \\ &= \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \chi(b)\chi_2(b)\chi_2(a)e\left(\frac{a(1+b)}{p}\right) \\ &= \tau(\chi_2) \sum_{b=1}^{p-1} \chi(b)\chi_2(b)\chi_2(1+b). \end{aligned}$$

Let $\tau_\alpha(n) = \sum_{d|n} \chi_2(d)d^\alpha$. Then for $N \geq p$, by (7) and (8) we get

$$\begin{aligned} &\sum_{\chi(-1)=-1} \tau(\bar{\chi})\tau(\chi\chi_2)L(u, \bar{\chi})L(v, \bar{\chi}\chi_2) \\ &= \sum_{\chi(-1)=-1} \tau(\bar{\chi})\tau(\chi\chi_2) \sum_{1 \leq n \leq N} \sum_{1 \leq m \leq N} \frac{\bar{\chi}(n)\bar{\chi}(m)\chi_2(m)}{n^u m^v} + O\left(\frac{p^{\frac{5}{2}} \log^2 p}{N}\right) \\ &= \tau(\chi_2) \sum_{1 \leq k \leq N^2} \frac{\tau_{u-v}(k)}{k^u} \sum_{b=1}^{p-1} \chi_2(b)\chi_2(1+b) \sum_{\chi(-1)=-1} \chi(b)\bar{\chi}(k) + O\left(\frac{p^{\frac{5}{2}} \log^2 p}{N}\right) \\ &= \frac{\tau(\chi_2)(p-1)}{2} \sum_{\substack{1 \leq k \leq N^2 \\ (k,p)=1}} \frac{\tau_{u-v}(k)}{k^u} \sum_{\substack{b=1 \\ b \equiv k \pmod{p}}}^{p-1} \chi_2(b)\chi_2(1+b) \\ &\quad - \frac{\tau(\chi_2)(p-1)}{2} \sum_{\substack{1 \leq k \leq N^2 \\ (k,p)=1}} \frac{\tau_{u-v}(k)}{k^u} \sum_{\substack{b=1 \\ b \equiv -k \pmod{p}}}^{p-1} \chi_2(b)\chi_2(1+b) + O\left(\frac{p^{\frac{5}{2}} \log^2 p}{N}\right) \end{aligned}$$

$$\ll p^{\frac{3}{2}} \sum_{1 \leq k \leq N^2} \frac{\tau_{u-v}(k)}{k^u} + \frac{p^{\frac{5}{2}} \log^2 p}{N} \ll p^{\frac{3}{2}} N^\epsilon + \frac{p^{\frac{5}{2}} \log^2 p}{N}.$$

Now taking $N = p$ in above, we immediately get

$$\sum_{\chi(-1)=-1} \tau(\bar{\chi}) \tau(\chi \chi_2) L(u, \bar{\chi}) L(v, \bar{\chi} \chi_2) \ll p^{\frac{3}{2}+\epsilon}.$$

This proves Lemma 7. □

3. Proof of Theorem 1

In this section, we complete the proof of Theorem 1. For any prime $p \geq 5$ and integer $k \geq 1$, from the definition of $N(p, k, c)$ we have

$$\begin{aligned} N(p, k, c) &= \sum_{\substack{a=1 \\ a \in A \\ ab \equiv c \pmod{p}}}^{p-1} \sum_{\substack{b=1 \\ b \in A}}^{p-1} (a-b)^{2k} \\ &= \frac{1}{4} \sum_{\substack{a=1 \\ ab \equiv c \pmod{p}}}^{p-1} \sum_{\substack{b=1}}^{p-1} (1 + \chi_2(a))(1 + \chi_2(b))(a-b)^{2k} \\ &= \frac{1}{4} \sum_{\substack{a=1 \\ ab \equiv c \pmod{p}}}^{p-1} \sum_{\substack{b=1}}^{p-1} (a-b)^{2k} + \frac{1}{2} \sum_{\substack{a=1 \\ ab \equiv c \pmod{p}}}^{p-1} \sum_{\substack{b=1}}^{p-1} \chi_2(b)(a-b)^{2k} \\ &\quad + \frac{1}{4} \sum_{\substack{a=1 \\ ab \equiv c \pmod{p}}}^{p-1} \sum_{\substack{b=1}}^{p-1} \chi_2(a)\chi_2(b)(a-b)^{2k} \\ &= \frac{1}{2(p-1)} \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} (a-b)^{2k} + \frac{1}{(p-1)} \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \chi_2(b)(a-b)^{2k} \\ &\quad + \frac{1}{2(p-1)} \sum_{\chi \neq \chi_0} \bar{\chi}(c) \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \chi(a)\chi(b)(a-b)^{2k} \\ &\quad + \frac{1}{2(p-1)} \sum_{\chi^2 \neq \chi_0} \bar{\chi}(c) \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \chi(a)\chi(b)\chi_2(b)(a-b)^{2k}. \end{aligned}$$

That is,

$$\begin{aligned} E(p, k, c) &= \frac{1}{2(p-1)} \sum_{\chi \neq \chi_0} \bar{\chi}(c) \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \chi(a) \chi(b) (a-b)^{2k} \\ &\quad + \frac{1}{2(p-1)} \sum_{\chi^2 \neq \chi_0} \bar{\chi}(c) \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \chi(a) \chi(b) \chi_2(b) (a-b)^{2k}. \end{aligned}$$

Then from Lemma 1 we have

$$\begin{aligned} &\sum_{\substack{c=1 \\ c \in A}}^{p-1} E(p, k, c) K(c, 1; p) \\ &= \frac{1}{2(p-1)} \sum_{\chi \neq \chi_0} \left[\frac{\tau^2(\bar{\chi})}{2} + \frac{\tau^2(\bar{\chi}\chi_2)}{2} \right] \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \chi(a) \chi(b) (a-b)^{2k} \\ &\quad + \frac{1}{2(p-1)} \sum_{\chi^2 \neq \chi_0} \left[\frac{\tau^2(\bar{\chi})}{2} + \frac{\tau^2(\bar{\chi}\chi_2)}{2} \right] \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \chi(a) \chi(b) \chi_2(b) (a-b)^{2k} \\ &= \frac{1}{4(p-1)} \sum_{\chi \neq \chi_0} \tau^2(\bar{\chi}) \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \chi(a) \chi(b) (a-b)^{2k} \\ &\quad + \frac{1}{4(p-1)} \sum_{\chi \neq \chi_0} \tau^2(\bar{\chi}\chi_2) \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \chi(a) \chi(b) (a-b)^{2k} \\ &\quad + \frac{1}{2(p-1)} \sum_{\chi^2 \neq \chi_0} \tau^2(\bar{\chi}) \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \chi(a) \chi\chi_2(b) (a-b)^{2k} \\ &= \Omega_1 + \Omega_2 + \Omega_3. \end{aligned} \tag{9}$$

Noting that $J(p) = p-2$, every non-principal character χ modulo p is a primitive character mod p , and

$$\sum_{a=1}^{p-1} \chi(a) = 0, \quad \text{if } \chi \neq \chi_0, \quad \sum_{a=1}^{p-1} a\chi(a) = 0, \quad \text{if } \chi(-1) = 1,$$

then by Lemma 2 and Lemma 4 we have

$$\begin{aligned}
\Omega_1 &= \frac{1}{4(p-1)} \sum_{\substack{\chi \neq \chi_0 \\ \chi(-1)=1}} \tau^2(\bar{\chi}) \sum_{n=2}^{2k-2} C_{2k}^n (-1)^n \left[\sum_{a=1}^{p-1} a^n \chi(a) \right] \left[\sum_{b=1}^{p-1} b^{2k-n} \chi(b) \right] \\
&\quad + \frac{1}{4(p-1)} \sum_{\chi(-1)=-1} \tau^2(\bar{\chi}) \sum_{n=1}^{2k-1} C_{2k}^n (-1)^n \left[\sum_{a=1}^{p-1} a^n \chi(a) \right] \left[\sum_{b=1}^{p-1} b^{2k-n} \chi(b) \right] \\
&= \frac{p^{2k+2}}{(p-1)} \sum_{\substack{\chi \neq \chi_0 \\ \chi(-1)=1}} \sum_{n=2}^{2k-2} C_{2k}^n \sum_{m=1}^{\lfloor \frac{n}{2} \rfloor} \sum_{l=1}^{\lfloor \frac{2k-n}{2} \rfloor} \\
&\quad \times \frac{C_n^{2m-1} C_{2k-n}^{2l-1} (2m-1)! (2l-1)! L(2m, \bar{\chi}) L(2l, \bar{\chi})}{(-1)^{n+m+l} (2\pi)^{2m+2l}} \\
&\quad - \frac{p^{2k+2}}{(p-1)} \sum_{\chi(-1)=-1} \sum_{n=1}^{2k-1} C_{2k}^n \sum_{m=0}^{\lfloor \frac{n-1}{2} \rfloor} \sum_{l=0}^{\lfloor \frac{2k-n-1}{2} \rfloor} \\
&\quad \times \frac{C_n^{2m} C_{2k-n}^{2l} (2m)! (2l)! L(2m+1, \bar{\chi}) L(2l+1, \bar{\chi})}{(-1)^{n+m+l} (2\pi)^{2m+2l+2}} \\
&= 2p^{2k+2} \sum_{n=2}^{2k-2} C_{2k}^n \sum_{m=1}^{\lfloor \frac{n}{2} \rfloor} \sum_{l=1}^{\lfloor \frac{2k-n}{2} \rfloor} \frac{C_n^{2m-1} C_{2k-n}^{2l-1} (2m-1)! (2l-1)!}{(-1)^{n+m+l} (2\pi)^{2m+2l}} \\
&\quad - 2p^{2k+2} \sum_{n=1}^{2k-1} C_{2k}^n \sum_{m=0}^{\lfloor \frac{n-1}{2} \rfloor} \sum_{l=0}^{\lfloor \frac{2k-n-1}{2} \rfloor} \frac{C_n^{2m} C_{2k-n}^{2l} (2m)! (2l)!}{(-1)^{n+m+l} (2\pi)^{2m+2l+2}} \\
&\quad + O(p^{2k+1+\epsilon}). \tag{10}
\end{aligned}$$

Similarly, from Lemma 2 and Lemma 6 we also have

$$\Omega_2 = \frac{1}{4(p-1)} \sum_{\substack{\chi \neq \chi_0 \\ \chi(-1)=1}} \tau^2(\bar{\chi} \chi_2) \sum_{n=2}^{2k-2} C_{2k}^n (-1)^n \left[\sum_{a=1}^{p-1} a^n \chi(a) \right] \left[\sum_{b=1}^{p-1} b^{2k-n} \chi(b) \right]$$

$$\begin{aligned}
& + \frac{1}{4(p-1)} \sum_{\chi(-1)=-1} \tau^2(\bar{\chi}\chi_2) \sum_{n=1}^{2k-1} C_{2k}^n (-1)^n \left[\sum_{a=1}^{p-1} a^n \chi(a) \right] \left[\sum_{b=1}^{p-1} b^{2k-n} \chi(b) \right] \\
& = \frac{p^{2k}}{(p-1)} \sum_{n=2}^{2k-2} C_{2k}^n \sum_{m=1}^{\lfloor \frac{n}{2} \rfloor} \sum_{l=1}^{\lfloor \frac{2k-n}{2} \rfloor} \frac{C_n^{2m-1} C_{2k-n}^{2l-1} (2m-1)!(2l-1)!}{(-1)^{n+m+l} (2\pi)^{2m+2l}} \\
& \quad \times \sum_{\substack{\chi \neq \chi_0 \\ \chi(-1)=1}} \tau^2(\bar{\chi}\chi_2) \tau^2(\chi) L(2m, \bar{\chi}) L(2l, \bar{\chi}) \\
& \quad - \frac{p^{2k}}{(p-1)} \sum_{n=1}^{2k-1} C_{2k}^n \sum_{m=0}^{\lfloor \frac{n-1}{2} \rfloor} \sum_{l=0}^{\lfloor \frac{2k-n-1}{2} \rfloor} \frac{C_n^{2m} C_{2k-n}^{2l} (2m)!(2l)!}{(-1)^{n+m+l} (2\pi)^{2m+2l+2}} \\
& \quad \times \sum_{\chi(-1)=-1} \tau^2(\bar{\chi}\chi_2) \tau^2(\chi) L(2m+1, \bar{\chi}) L(2l+1, \bar{\chi}) \\
& \ll p^{2k+\frac{3}{2}+\epsilon}. \tag{11}
\end{aligned}$$

Now we calculate Ω_3 . If $p \equiv 1 \pmod{4}$, then $\chi_2(-1) = 1$. So from Lemma 2 and Lemma 7 we have

$$\begin{aligned}
\Omega_3 & = \frac{1}{2(p-1)} \sum_{\substack{\chi^2 \neq \chi_0 \\ \chi(-1)=1}} \tau^2(\bar{\chi}) \sum_{n=2}^{2k-2} C_{2k}^n (-1)^n \left[\sum_{a=1}^{p-1} a^n \chi(a) \right] \left[\sum_{b=1}^{p-1} b^{2k-n} \chi\chi_2(b) \right] \\
& \quad + \frac{1}{2(p-1)} \sum_{\chi(-1)=-1} \tau^2(\bar{\chi}) \sum_{n=1}^{2k-1} C_{2k}^n (-1)^n \left[\sum_{a=1}^{p-1} a^n \chi(a) \right] \left[\sum_{b=1}^{p-1} b^{2k-n} \chi\chi_2(b) \right] \\
& = \frac{2p^{2k+1}}{(p-1)} \sum_{n=2}^{2k-2} C_{2k}^n \sum_{m=1}^{\lfloor \frac{n}{2} \rfloor} \sum_{l=1}^{\lfloor \frac{2k-n}{2} \rfloor} \frac{C_n^{2m-1} C_{2k-n}^{2l-1} (2m-1)!(2l-1)!}{(-1)^{n+m+l} (2\pi)^{2m+2l}} \\
& \quad \times \sum_{\substack{\chi^2 \neq \chi_0 \\ \chi(-1)=1}} \tau(\bar{\chi}) \tau(\chi\chi_2) L(2m, \bar{\chi}) L(2l, \bar{\chi}\chi_2) \\
& \quad + \frac{2p^{2k+1}}{(p-1)} \sum_{n=1}^{2k-1} C_{2k}^n \sum_{m=0}^{\lfloor \frac{n-1}{2} \rfloor} \sum_{l=0}^{\lfloor \frac{2k-n-1}{2} \rfloor} \frac{C_n^{2m} C_{2k-n}^{2l} (2m)!(2l)!}{(-1)^{n+m+l} (2\pi)^{2m+2l+2}}
\end{aligned}$$

$$\begin{aligned}
& \times \sum_{\chi(-1)=-1} \tau(\bar{\chi})\tau(\chi\chi_2)L(2m+1, \bar{\chi})L(2l+1, \bar{\chi}\chi_2) \\
& \ll p^{2k+\frac{3}{2}+\epsilon}. \tag{12}
\end{aligned}$$

On the other hand, if $p \equiv 3 \pmod{4}$, then $\chi_2(-1) = -1$. By Lemma 2 and Lemma 7 we also have

$$\begin{aligned}
\Omega_3 &= \frac{1}{2(p-1)} \sum_{\substack{\chi \neq \chi_0 \\ \chi(-1)=1}} \tau^2(\bar{\chi}) \sum_{n=2}^{2k-2} C_{2k}^n(-1)^n \left[\sum_{a=1}^{p-1} a^n \chi(a) \right] \left[\sum_{b=1}^{p-1} b^{2k-n} \chi\chi_2(b) \right] \\
&+ \frac{1}{2(p-1)} \sum_{\substack{\chi \neq \chi_2 \\ \chi(-1)=-1}} \tau^2(\bar{\chi}) \sum_{n=1}^{2k-1} C_{2k}^n(-1)^n \left[\sum_{a=1}^{p-1} a^n \chi(a) \right] \left[\sum_{b=1}^{p-1} b^{2k-n} \chi\chi_2(b) \right] \\
&= \frac{2p^{2k+1}}{(p-1)} \sum_{n=2}^{2k-2} C_{2k}^n \sum_{m=1}^{\lfloor \frac{n}{2} \rfloor} \sum_{l=0}^{\lfloor \frac{2k-n-1}{2} \rfloor} \frac{C_n^{2m-1} C_{2k-n}^{2l} (2m-1)!(2l)!}{(-1)^{n+m+l} (2\pi)^{2m+2l+1} i} \\
&\quad \times \sum_{\substack{\chi \neq \chi_0 \\ \chi(-1)=1}} \tau(\bar{\chi})\tau(\chi\chi_2)L(2m, \bar{\chi})L(2l+1, \bar{\chi}\chi_2) \\
&- \frac{2p^{2k+1}}{(p-1)} \sum_{n=1}^{2k-1} C_{2k}^n \sum_{m=0}^{\lfloor \frac{n-1}{2} \rfloor} \sum_{l=1}^{\lfloor \frac{2k-n}{2} \rfloor} \frac{C_n^{2m} C_{2k-n}^{2l-1} (2m)!(2l-1)!}{(-1)^{n+m+l} (2\pi)^{2m+2l+1} i} \\
&\quad \times \sum_{\substack{\chi \neq \chi_2 \\ \chi(-1)=-1}} \tau(\bar{\chi})\tau(\chi\chi_2)L(2m+1, \bar{\chi})L(2l, \bar{\chi}\chi_2) \ll p^{2k+\frac{3}{2}+\epsilon}. \tag{13}
\end{aligned}$$

Now combining formulae (9)–(13), we immediately get Theorem 1.

Acknowledgments

The authors express their gratitude to the referee for his very helpful comments in improving this paper.

References

- [1] T. MASAO, On certain character sums, *Acta Arithmetica* **LV** (1990), 229–232.
- [2] A. WEIL, Sur les courbes algébriques et les variétés qui s'en déduisent, *Actualités Sci. Ind.* **1041** (1948).
- [3] WENPENG ZHANG, On the difference between an integer and its inverse modulo n , *Journal of Number Theory* **52** (1995), 1–6.
- [4] WENPENG ZHANG, On a Cochrane sum and its hybrid mean value formula, *Journal of Mathematical Analysis and Applications* **267** (2002), 89–96.
- [5] WENPENG ZHANG, On the difference between an integer and its inverse modulo n (II), *Science in China (Series A)* **46** (2003), 229–238.
- [6] WENPENG ZHANG and HUANING LIU, A Note on the Cochrane Sum and its Hybrid Mean Value Formula, *Journal of Mathematical Analysis and Applications* **288** (2003), 646–659.

LIU HUANING
DEPARTMENT OF MATHEMATICS
NORTHWEST UNIVERSITY
XI'AN, SHAANXI
P.R. CHINA

E-mail: hnliu@nwu.edu.cn

ZHANG WENPENG
DEPARTMENT OF MATHEMATICS
NORTHWEST UNIVERSITY
XI'AN, SHAANXI
P.R. CHINA

E-mail: wpzhang@nwu.edu.cn

(Received March 3, 2005; revised May 9, 2005)