COMPOSITIO MATHEMATICA

ZHANG WENPENG

On a problem of D. H. Lehmer and its generalization

Compositio Mathematica, tome 86, n° 3 (1993), p. 307-316

<http://www.numdam.org/item?id=CM_1993__86_3_307_0>

Compositio Mathematica **86**: 307–316, 1993.

On a problem of D. H. Lehmer and its generalization*

ZHANG WENPENG
Department of Mathematics, Northwest University, Xi'an, China

Received 6 January 1992; accepted 4 June 1992

Keywords: Congruence equation; D. H. Lehmer problem; Asymptotic formula; Prime power.

Abstract. Let $q > 2$ be an odd number. For each integer x with $0 < x < q$ and $(q, x) = 1$, we define $\bar{x}$ by $x\bar{x} \equiv 1 \pmod{q}$ and $0 < \bar{x} < q$. Let $r(q)$ be the number of integers x with $0 < x < q$ for which x and $\bar{x}$ are of opposite parity. The main purpose of this paper is to give an asymptotic formula for $r(q)$ for odd numbers q of certain special types.

1. Introduction

For any odd number $n > 2$ and integer $0 < x < n$ with $(n, x) = 1$, we know that there exists one and only one $\bar{x}$ with $0 < \bar{x} < n$ such that $x\bar{x} \equiv 1 \pmod{n}$. Let $r(n)$ be the number of cases in which x and $\bar{x}$ are of opposite parity. E.g., for $n = 13$, $(x, \bar{x}) = (1, 1), (2, 7), (3, 9), (4, 10), (5, 8), (6, 11), (12, 12)$ so $r(13) = 6$. For $n = p$ a prime, D. H. Lehmer [1] asks us to find $r(p)$ or at least to say something nontrivial about. It is known that $r(p) \equiv 2$ or $0 \pmod 4$ according as $p \equiv \pm 1 \pmod 4$. About this problem, it seems that none can obtain any advance at present. The main purpose of this paper is to study the asymptotic properties of $r(n)$ for odd numbers n of certain special types. The constants implied by the O-symbols and the symbols $\ll$, $\gg$ used in this paper do not depend on any parameter, unless otherwise indicated. By using estimates for character sums and Kloosterman sums, we prove the following two theorems:

THEOREM 1. *Let $\alpha > 0$ be an integer and p an odd prime. Then we have*

$$r(p^\alpha) = \tfrac{1}{2}p^{\alpha-1}(p-1) + O(p^{\alpha/2}\ln^3(p^\alpha)).$$

THEOREM 2. *Let p* and *q* be two distinct odd primes. *Then*

$$r(pq) = \tfrac{1}{2}(p-1)(q-1) + O((pq)^{1/2}\ln^2(pq))$$

We conjecture that for every odd integer n and every $\varepsilon > 0$,

$$r(n) = \tfrac{1}{2}\phi(n) + O(n^{1/2+\varepsilon})$$

where $\phi(n)$ is Euler's function.

*Project supported by the National Natural Science Foundation of China.

2. Several lemmas

To complete the proofs of the theorems, we need several lemmas. First we have:

LEMMA 1. *Let $q > 2$ be an odd number. Then*

$$y(q) = \frac{1}{2}\phi(q) - \frac{2}{\phi(q)} \sum_{\chi(-1)=-1} \chi(4) \left(\sum_{q=1}^{(q-1)/2} \chi(a) \right)^2$$

where the summation is over all odd characters mod q.

Proof. From the definition of $r(q)$ and the orthogonality of characters we get:

$$\begin{aligned} y(q) &= \frac{1}{2} \sum_{\substack{a=1 \\ ab \equiv 1(q)}}^{q-1} \sum_{b=1}^{q-1} (1 - (-1)^{a+b}) \\ &= \frac{1}{2}\phi(q) - \frac{1}{2} \sum_{\substack{a=1 \\ ab \equiv 1(q)}}^{q-1} \sum_{b=1}^{q-1} (-1)^{a+b} \\ &= \frac{1}{2}\phi(q) - \frac{1}{2\phi(q)} \sum_{\chi \bmod q} \left(\sum_{a=1}^{q-1} (-1)^a \chi(a) \right)^2 \\ &= \frac{1}{2}\phi(q) - \frac{1}{2\phi(q)} \sum_{\chi \neq \chi^0} \left(\sum_{a=1}^{q-1} (-1)^a \chi(a) \right)^2 \end{aligned} \tag{1}$$

where $\Sigma_{\chi \neq \chi^0}$ denotes the summation over all nonprincipal characters mod q. Now if $\chi(-1) = 1$ and $\chi \neq \chi^0$, then we have

$$\begin{aligned} \sum_{a=1}^{q-1} (-1)^a \chi(a) &= \sum_{a=1}^{(q-1)/2} \chi(2a) - \sum_{a=1}^{(q-1)/2} \chi(2a-1) \\ &= \sum_{a=1}^{(q-1)/2} \chi(2a) - \sum_{a=1}^{(q-1)/2} \chi(q-2a) \\ &= \sum_{a=1}^{(q-1)/2} \chi(2a) - \sum_{a=1}^{(q-1)/2} \chi(2a) = 0 \end{aligned} \tag{2}$$

If $\chi(-1) = -1$, then we have

$$\begin{aligned} \sum_{a=1}^{q-1} (-1)^a \chi(a) &= \sum_{a=1}^{(q-1)/2} \chi(2a) - \sum_{a=1}^{(q-1)/2} \chi(q-2a) \\ &= \sum_{a=1}^{(q-1)/2} \chi(2a) + \sum_{a=1}^{(q-1)/2} \chi(2a) = 2 \sum_{a=1}^{(q-1)/2} \chi(2a) \end{aligned} \tag{3}$$

By combining (1), (2) and (3) we immediately deduce that

$$y(q) = \frac{1}{2}\phi(q) - \frac{2}{\phi(q)} \sum_{\chi(-1)=-1} \left(\sum_{a=1}^{(q-1)/2} \chi(2a) \right)^2$$

This completes the proof of lemma 1. □

LEMMA 2. *Let $q > 2$. Then for each primitive odd character $\chi \bmod q$ we have:*

$$\sum_{a \leqslant q/2} \chi(a) = \frac{\tau(\chi)}{\pi i} (2 - \bar{\chi}(2)) L(1, \bar{\chi}) + O(1)$$

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

Proof. From G. Pólya [2] we know that for any primitive character $\bmod q$ and real numbers U and V with $U < V$ we have

$$\sum_{uq < n \leqslant Vq} \chi(n) = \tau(\chi) \sum_{0 < |h| \leqslant H} \bar{\chi}(h) \frac{e(-hU) - e(-hV)}{2\pi i h} + O\left(1 + \frac{q \ln q}{H}\right), \tag{4}$$

where $e(x) = e^{2\pi i x}$, $\tau(\chi) = \Sigma_{a=1}^{q} \chi(a) e(a/q)$.

Taking $U = 0$ and $V = 1/2$ in (4), and noticing that $\chi(-1) = -1$, we get:

$$\begin{aligned}
\sum_{1 \leqslant a \leqslant q/2} \chi(a) &= \frac{\tau(\chi)}{2\pi i} \sum_{0 < |h| \leqslant H} \frac{\bar{\chi}(h)(1 - e(-h/2))}{h} + O\left(1 + \frac{q \ln q}{H}\right) \\
&= \frac{\tau(\chi)}{\pi i} \sum_{1 \leqslant h \leqslant H} \frac{\bar{\chi}(h)(1 - \cos(\pi h))}{h} + O\left(1 + \frac{q \ln q}{H}\right) \\
&= \frac{\tau(\chi)}{\pi i} \left[\sum_{h \leqslant H} \frac{\bar{\chi}(h)}{h} + \sum_{h \leqslant H/2} \frac{\bar{\chi}(2h-1)}{2h-1} - \sum_{h \leqslant H/2} \frac{\bar{\chi}(2h)}{2h} \right] \\
&\quad + O(1 + H^{-1} q \ln q) \\
&= \frac{\tau(\chi)}{\pi i} \left[2 \sum_{h \leqslant H} \frac{\bar{\chi}(h)}{h} - \bar{\chi}(2) \sum_{h \leqslant H/2} \frac{\bar{\chi}(h)}{h} \right] + O\left(1 + \frac{q \ln q}{H}\right)
\end{aligned}$$

By letting $H \to \infty$ in the above formula and noticing that

$$\lim_{H \to \infty} \sum_{h \leqslant H} \frac{\bar{\chi}(h)}{h} = L(1, \bar{\chi}),$$

we immediately deduce:

$$\sum_{1 \leqslant n \leqslant q/2} \chi(n) = \frac{\tau(\chi)}{\pi i}(2 - \bar{\chi}(2))L(1, \bar{\chi}) + 0(1).$$

This proves lemma 2. □

LEMMA 3. *Let m, n, q be integers with $q > 1$. Then*

$$S(m, n; q) = \sum_{\substack{d(\bmod q) \\ (d,q)=1}} \exp\left(m\frac{\bar{d}}{q} + n\frac{d}{q}\right) \ll (m, n, q)^{1/2} q^{1/2} d(q),$$

where $d\bar{d} \equiv 1 \pmod q$, $d(q)$ is the divisor function, and (m, n, q) denotes the greatest common factor of m, n and q.

Proof. (See reference [3]).

LEMMA 4. *Let $q > 2$. Then for any integer b we have*

$$\sum_{\chi(-1)=-1} \tau^2(\chi)\chi(b)L^2(1, \bar{\chi}) \ll q^{2/3} d(q) \ln^2 q.$$

Proof. First for any integer r with $(r, q) = 1$ we have

$$\begin{aligned}\sum_{\chi(-1)=-1} \chi(y) &= \frac{1}{2}\sum_{\chi}(\chi(y) - \chi(-1)\chi(y)) \\ &= \frac{1}{2}\sum_{\chi}\chi(y) - \frac{1}{2}\sum_{\chi}\chi(-y) \\ &= \begin{cases} \frac{1}{2}\phi(q), & y \equiv 1 (\bmod q); \\ -\frac{1}{2}\phi(q), & y \equiv -1 (\bmod q); \\ 0, & \text{otherwise.} \end{cases} \end{aligned} \tag{5}$$

Now let y be a real number with $y > q^2$ and put $A(y, \chi) = \Sigma_{q^2 < n \leqslant y} d(n)\chi(n)$ for $\chi \neq \chi^0$. Then from the well-known Pólya-Vinogradov inequality (See Theorem 13.15 of [4]) we may get

$$\begin{aligned} A(y, \chi) &= \sum_{q^2 < mn \leqslant y} \chi(mn) = 2 \sum_{m \leqslant \sqrt{y}} \sum_{(q^2/m) < n \leqslant y/m} \chi(mn) \\ &\quad - \sum_{\substack{m \leqslant \sqrt{y} \\ mn > q^2}} \sum_{n \leqslant \sqrt{y}} \chi(mn) \ll \sqrt{yq} \ln q \end{aligned} \tag{6}$$

From (6) and Abel's summation we can easily deduce that

$$L^2(1, \bar{\chi}) = \sum_{n \leqslant q^2} \frac{d(n)\bar{\chi}(n)}{n} + \int_{q^2}^{\infty} \frac{A(y, \bar{\chi})}{y^2}\, dy$$

$$= \sum_{n \leqslant q^2} \frac{d(n)\bar{\chi}(n)}{n} + O(q^{-1/2} \ln q) \tag{7}$$

If $(b, q) > 1$ then $\chi(b) = 0$ and in this case it is clear that lemma 4 holds. Now we suppose that $(b, q) = 1$. It is known that for primitive characters $\chi \pmod q$ we have $|\tau(\chi)| = q^{1/2}$, while for nonprimitive characters $\chi \pmod q$ with $\chi \neq \chi^0$ we have $|\tau(\chi)| \leqslant q^{1/2}$. Therefore,

$$\sum_{\chi \neq \chi^0} |\tau(\chi)|^2 \ll q^2.$$

From this inequality, (5), (7) and the definition of Gauss sum, we get:

$$\sum_{\chi(-1)=-1} \tau^2(\chi)\chi(b)L^2(1, \bar{\chi})$$

$$= \sum_{a=1}^{q-1} \sum_{c=1}^{q-1} \sum_{n \leqslant q^2} \frac{d(n)}{n} \sum_{\chi(-1)=-1} \chi(a)\chi(b)\chi(c)\bar{\chi}(n) \exp\left(\frac{a+c}{q}\right)$$

$$+ O\left(q^{-1/2} \ln q \sum_{\chi \neq \chi^0} |\tau(\chi)|^2\right)$$

$$= \sum_{n \leqslant q^2}{}' \frac{d(n)}{n} \sum_{a=1}^{q-1} \sum_{c=1}^{q-1} \sum_{\chi(-1)=-1} \chi(abc\bar{n}) \exp\left(\frac{a+c}{q}\right) + O\left(q^{3/2} \ln q\right)$$

$$= \frac{1}{2}\phi(q) \sum_{n \leqslant q^2}{}' \frac{d(n)}{n} \sum_{\substack{a=1 \\ abc \equiv n(q)}}^{q-1} \sum_{c=1}^{q-1}{}' \exp\left(\frac{a+c}{q}\right) + O(q^{3/2} \ln q)$$

$$- \frac{1}{2}\phi(q) \sum_{n \leqslant q^2}{}' \frac{d(n)}{n} \sum_{\substack{a=1 \\ abc \equiv -n(q)}}^{q-1}{}' \sum_{c=1}^{q-1}{}' \exp\left(\frac{a+c}{q}\right)$$

$$= \frac{1}{2}\phi(q) \sum_{n \leqslant q^2}{}' \frac{d(n)}{n} \left(S(1, \bar{bn}; q) - S(1, -\bar{bn}; q)\right) + O(q^{3/2} \ln q) \tag{8}$$

where the definition of $S(m, n; q)$ is as in lemma 3. From the estimate $\sum_{n \leqslant N} d(n)/n \ll \ln^2 N$, (8) and lemma 3, we may immediately deduce that

$$\sum_{\chi(-1)=-1} \tau^2(\chi)\chi(b)L^2(1, \bar{\chi}) \ll q^{3/2} d(q) \ln^2 q.$$

This completes the proof of lemma 4. □

LEMMA 5. *For every integer $\alpha > 0$ and every odd prime p, we have the recursive formula*

$$\left|\sum_{\chi_{p^\alpha}(-1)=-1}\left(\sum_{a=1}^{(p^\alpha-1)/2}\chi(2a)\right)^2\right| = \left|\sum_{\chi_{p^{\alpha-1}}(-1)=-1}\left(\sum_{a=1}^{(p^{\alpha-1}-1)/2}\chi(2a)\right)^2\right| + O(p^{3\alpha/2}\ln^3(p^\alpha))$$

Proof. From the properties of characters we know that any non-primitive odd character $\chi \bmod p^\alpha$ is a nonprincipal odd character mod $p^{\alpha-1}$. Thus we have

$$\sum_{\chi_{p^\alpha}(-1)=-1}\left(\sum_{a=1}^{(p^\alpha-1)/2}\chi(2a)\right)^2 = \sum_{\chi_{p^\alpha}(-1)=-1}^{*}\left(\sum_{a=1}^{(p^\alpha-1)/2}\chi(2a)\right)^2 + \sum_{\chi_{p^{\alpha-1}}(-1)=-1}\left(\sum_{a=1}^{(p^\alpha-1)/2}\chi(2a)\right)^2 \tag{9}$$

From the periodicity of $\chi_{p^{\alpha-1}}(n)$ we deduce that

$$\begin{aligned}&\sum_{\chi_{p^{\alpha-1}}(-1)=-1}\left(\sum_{a=1}^{(p^\alpha-1)/2}\chi(2a)\right)^2\\ &= \sum_{\chi_{p^{\alpha-1}}(-1)=-1}\left(\sum_{k=0}^{[(p-1)/2]-1}\sum_{kp^{\alpha-1}<a\leqslant(k+1)p^{\alpha-1}}\chi(2a) + \sum_{[(p-1)/2]p^{\alpha-1}<a\leqslant p^\alpha/2}\chi(2a)\right)^2\\ &= \sum_{\chi_{p^{\alpha-1}}(-1)=-1}\left(\sum_{1\leqslant a\leqslant p^{\alpha-1}/2}\chi(2a)\right)^2\end{aligned} \tag{10}$$

By applying lemmas 2 and 4 and using that for primitive characters mod q we have $|\tau(\chi)| = q^{1/2}$ and $|L(1,\chi)| \ll \ln q$, we get:

$$\begin{aligned}&\sum_{\chi_{p^\alpha}(-1)=-1}^{*}\left(\sum_{a=1}^{(p^\alpha-1)/2}\chi(2a)\right)^2 = \sum_{\chi_{p^\alpha}(-1)=-1}^{*}\chi(4)\left(\sum_{a=1}^{(p^\alpha-1)/2}\chi(a)\right)^2\\ &= \sum_{\chi_{p^\alpha}(-1)=-1}^{*}\chi(4)\left(\frac{\tau(\chi)}{\pi i}(2-\bar\chi(2))L(1,\bar\chi)+O(1)\right)^2\\ &= -\sum_{\chi_{p^\alpha}(-1)=-1}^{*}\frac{\tau^2(\chi)}{\pi^2}(2\chi(2)-1)^2L^2(1,\bar\chi)+O(p^{3\alpha/2}\ln(p^\alpha))\\ &= -\sum_{\chi_{p^\alpha}(-1)=-1}\frac{\tau^2(\chi)}{\pi^2}(2\chi(2)-1)^2L^2(1,\bar\chi)+O(p^{3\alpha/2}\ln(p^\alpha))\\ &\ll p^{3\alpha/2}d(p^\alpha)\ln^2(p^\alpha) \ll p^{3\alpha/2}\ln^3(p^\alpha)\end{aligned} \tag{11}$$

where we have used the identity:

$$\sum_{1\leqslant a\leqslant p^\alpha} \chi_{p\alpha-1}(a)\exp\left(\frac{a}{p^\alpha}\right)$$
$$= \sum_{b=0}^{p-1}\sum_{a=1}^{p\alpha-1} \chi_{p\alpha-1}(p^{\alpha-1}b+a)\exp\left(\frac{bp^{\alpha-1}+a}{p\alpha}\right)$$
$$= \sum_{a=1}^{p^{\alpha-1}} \chi_{p^{\alpha-1}}(a)\exp\left(\frac{a}{p\alpha}\right)\sum_{b=0}^{p-1}\exp\left(\frac{b}{p}\right) = 0.$$

Thus for all nonprimitive odd characters mod p^α we have

$$\frac{\tau^2(\chi)}{\pi^2}(2\chi(2)-1)^2L^2(1,\bar{\chi}) = 0 \tag{12}$$

By combining (9), (10) and (11) we immediately get lemma 5.

3. Proof of the theorems

In this section, we shall complete the proofs of the theorems. First we prove theorem 1. Notice that

$$\sum_{\chi_p(-1)=-1}\left(\sum_{a=1}^{(p-1)/2}\chi(2a)\right)^2$$
$$= \sum_{\chi_p(-1)=-1}\chi(4)\left(\frac{\tau(\chi)}{\pi i}(2-\bar{\chi}(2))L(1,\bar{\chi})+O(1)\right)^2$$
$$= -\sum_{\chi_p(-1)=-1}\frac{\tau^2(\chi)}{\pi^2}(2\chi(2)-1)^2L^2(1,\bar{\chi})+O(p^{3/2}\ln p)$$
$$\ll p^{3/2}\ln^2 p.$$

From lemma 5 we easily deduce, by using induction on α, that for $\alpha > 1$,

$$\sum_{\chi_{p\alpha}(-1)=-1}\left(\sum_{a=1}^{(p\alpha-1)/2}\chi(2a)\right)^2 \ll p^{3\alpha/2}\ln^3(p^\alpha)$$

From this and lemma 1 we get

$$y(p^\alpha) = \frac{1}{2}\phi(p^\alpha) - \frac{2}{\phi(p^\alpha)}\sum_{\chi_{p\alpha}(-1)=-1}\left(\sum_{a=1}^{(p\alpha-1)/2}\chi(2a)\right)^2$$
$$= \frac{1}{2}\phi(p^\alpha)+O(p^{\alpha/2}\ln^3(p^\alpha)).$$

This completes the proof of theorem 1. □

Now we prove theorem 2. Let p and q be distinct odd primes. Every nonprimitive character mod pq can be expressed as either $\chi_p^0\chi_q$ or $\chi_p\chi_q^0$. From this and lemma 1 we get

$$\begin{aligned} y(pq) &= \tfrac{1}{2}\phi(pq) - \frac{2}{\phi(qp)} \sum_{\chi_{pq}(-1)=-1} \left(\sum_{a=1}^{(pq-1)/2} \chi(2a) \right)^2 \\ &= \tfrac{1}{2}(p-1)(q-1) - \frac{2}{\phi(pq)} \sum_{\chi_{pq}(-1)=-1}{}^{*} \left(\sum_{a=1}^{(pq-1)/2} \chi(2a) \right)^2 \\ &\quad - \frac{2}{\phi(pq)} \sum_{\chi_q(-1)=-1} \left(\sum_{a=1}^{(pq-1)/2} \chi_p^0(2a)\chi_q(2a) \right)^2 \\ &\quad - \frac{2}{\phi(pq)} \sum_{\chi_p(-1)=-1} \left(\sum_{a=1}^{(pq-1)/2} \chi_p(2a)\chi_q^0(2a) \right)^2 \end{aligned} \tag{13}$$

From lemma 2 and lemma 4 we get

$$\begin{aligned} &\sum_{\chi_p(-1)=-1} \left(\sum_{a=1}^{(pq-1)/2} \chi_p(2a)\chi_q^0(2a) \right)^2 \\ &= \sum_{\chi_p(-1)=-1} \left(\sum_{a=1}^{(pq-1)/2} \chi_p(2a) - \sum_{a=1}^{(p-1)/2} \chi_p(2aq) \right)^2 \\ &= \sum_{\chi_p(-1)=-1} \left((\chi_p(2) - \chi_p(2q)) \sum_{a=1}^{(p-1)/2} \chi_p(a) \right)^2 \\ &= \sum_{\chi_p(-1)=-1} \chi_p(4)(1-\chi_p(q))^2 \left(\sum_{a=1}^{(p-1)/2} \chi_p(a) \right)^2 \\ &= \sum_{\chi_p(-1)=-1} \chi_p(4)(1-\chi_p(q))^2 \left(\frac{\tau(\chi_p)}{\pi i}(2-\bar{\chi}(2))L(1,\bar{\chi}) + O(1) \right)^2 \\ &\ll p^{3/2}\ln^2 p. \end{aligned} \tag{14}$$

Similarly we can deduce that

$$\sum_{\chi_q(-1)=-1} \left(\sum_{a=1}^{(pq-1)/2} \chi_p^0(2a)\chi_q(2a) \right)^2 \ll q^{3/2}\ln^2 q \tag{15}$$

Notice that if χ is a character mod pq of the form $\chi_p^0\chi_q$, then

$$\tau(\chi) = \sum_{a=1}^{pq} \chi_p(a)\chi_q^0(a)\exp\left(\frac{a}{pq}\right)$$

$$= \sum_{a=1}^{pq} \chi_p(a)\exp\left(\frac{a}{pq}\right) - \sum_{a=1}^{p} \chi_p(aq)\exp\left(\frac{a}{p}\right)$$

$$= \sum_{a=1}^{p}\sum_{b=1}^{q} \chi_p(aq+bp)\exp\left(\frac{a}{p}+\frac{b}{q}\right) - \sum_{a=1}^{p-1} \chi_p(aq)\exp\left(\frac{a}{p}\right)$$

$$= \left(\sum_{a=1}^{p} \chi_p(aq)\exp\left(\frac{a}{p}\right)\right)\left(\sum_{b=1}^{q} \exp\left(\frac{b}{q}\right)\right) - \chi_p(q)\tau(x_p)$$

$$= -\chi_p(q)\tau(\chi_p) \tag{16}$$

Similarly, if χ is of the form $\chi_p^0\chi_q$, then

$$\tau(\chi) = \sum_{a=1}^{pq} \chi_q(a)\chi_p^0(a)\exp\left(\frac{a}{pq}\right) = -\chi_q(p)\tau(\chi_q) \tag{17}$$

Thus from Lemma 2 and lemma 4 we get

$$\sum_{\chi_{pq}(-1)=-1}^{*} \left(\sum_{a=1}^{(pq-1)/2} \chi(2a)\right)^2$$

$$= \sum_{\chi_{pq}(-1)=-1}^{*} \chi(4)\left[\frac{\tau(\chi)}{\pi i}(2-\bar{\chi}(2))L(1,\bar{\chi}) + O(1)\right]^2$$

$$= \sum_{\chi_{pq}(-1)=-1}^{*} (2\chi(2)-1)^2 \frac{\tau^2(\chi)}{-\pi^2} L^2(1,\bar{\chi}) + O((pq)^{3/2}\ln(pq))$$

$$= \sum_{\chi_{pq}(-1)=-1} (2\chi_p(2)-1)^2 \frac{\tau^2(\chi)}{-\pi^2} L^2(1,\bar{\chi}) + O((pq)^{3/2}\ln(pq))$$

$$+ \sum_{\chi_p(-1)=-1} (2\chi_p(2)-1)^2 \frac{\tau^2(\chi_p\chi_q^0)}{\pi^2} L^2(1,\bar{\chi}_p\bar{\chi}_q^0)$$

$$+ \sum_{\chi_q(-1)=-1} (2\chi_q(2)-1)^2 \frac{\tau^2(\chi_q\chi_p^0)}{\pi^2} L^2(1,\bar{\chi}_q\bar{\chi}_p^0)$$

$$= -\sum_{\chi_{pq}(-1)=-1} (2\chi(2)-1)^2 \frac{\tau^2(\chi)}{\pi^2} L^2(1,\bar{\chi}) + O((pq)^{3/2}\ln(pq))$$

$$+ \sum_{\chi_p(-1)=-1} (2\chi_p(2)-1)^2 \frac{\chi_p^2(q)\tau^2(\chi_p)}{\pi^2}\left(1-\frac{\bar{\chi}_p(q)}{q}\right)^2 L^2(1,\bar{\chi}_p)$$

$$+ \sum_{\chi_q(-1)=-1} (2\chi_q(2)-1)^2 \frac{\chi_q^2(p)\tau^2(\chi_q)}{\pi^2}\left(1-\frac{\bar{\chi}_q(p)}{p}\right)^2 L^2(1,\bar{\chi}_q)$$

$$\ll (pq)^{3/2}\ln^2(pq). \tag{18}$$

By combining (13), (14), (15), (18), we arrive at

$$y(pq) = \tfrac{1}{2}(p-1)(q-1) + O((pq)^{1/2}\ln^2(pq)).$$

This completes the proof of theorem 2. □

Acknowledgment

The author expresses his gratitude to the referee for helpful comments.

References

1. Richard K. Guy, *Unsolved Problems in Number Theory*, Springer-Verlag, 1981, pp. 139–141.
2. G. Pólya, Über die Verteilung der quadratischen Reste und Nichtreste, *Göttinger Nachrichten*, 1918, pp. 21–29.
3. T. Estermann, On Kloosterman's sum, *Mathematika*, 8 (1961), pp. 83–86.
4. Apostol, Tom M., *Introduction to Analytic Number Theory*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1976.