Title	On the number of lattice points in the square $\|x\|+\|y\|\leq u$ with a certain congruence condition
Author(s)	Yamamoto, Yoshihiko
Citation	Osaka Journal of Mathematics. 1980, 17(1), p. 9-21
Version Type	VoR
URL	https://doi.org/10.18910/8615
rights	
Note	

ON THE NUMBER OF LATTICE POINTS IN THE SQUARE |x|+|y|≦u WITH A CERTAIN CONGRUENCE CONDITION

Yoshihiko YAMAMOTO*)

0. Introduction. Let $a(u; p, q)$ denote the number of lattice points $(x, y) \in \mathbf{Z}^2$ such that (i) $|x|+|y| \leqq u$ (ii) $x+py \equiv 0 \pmod{q}$, where u, p, and q are given positive integers. It is easy to see that $a(u; p, q)$ is determined only by p modulo q, if q is fixed. Let p' be another positive integer. We always assume $(p, q)=(p', q)=1$ in the following, where $(,)$ means the greatest common divisor. It is easy to see that we have $a(u; p, q)=a(u; p', q)$ for every positive integer u if $p \equiv \pm p'$ or $pp' \equiv \pm 1 \pmod{q}$. We will prove, in the present paper, that the converse is valid:

Theorem 1. *Suppose* $a(u; p, q)=a(u; p', q)$ *for every positive integer* u. *Then* $p \equiv \pm p'$ *or* $pp' \equiv \pm 1 \pmod{q}$.

Our problem is related with a problem in differential geometry, and gives an answer to it. Consider a 3-dimensional lens space with fundamental group of order q. We ask whether the spectrum of the Laplacian characterizes the space as a riemannian manifold. This geometric problem can be reduced to a problem in number theory. A special case of our theorem, where q is of the form l^n or $2 \cdot l^n$ (l a prime number), has been shown (cf. Ikeda-Yamamoto [3]). Now our Theorem 1 gives a complete affirmative answer to the above geometric problem (see Section 7 below).

If a lattice point (x, y) satisfies the conditions (i) and (ii), so does the point $(-x, -y)$. Denote by $b(u; p, q)$ the number of lattice points (x, y) such that (i') $x \geqq 0$ and $x+|y|=u$ (ii) $x+py \equiv 0 \pmod{q}$. Then we see easily that Theorem 1 is equivalent to

Theorem 2. *Suppose* $b(u; p, q)=b(u; p', q)$ *for every positive integer* u. *Then* $p \equiv \pm p'$ *or* $pp' \equiv \pm 1 \pmod{q}$.

We introduce rational functions $F_j(X)$ $(0 \leqq j \leqq q-1)$;

$$F_j(X) = \frac{1}{(1-\zeta^j X)(1-\zeta^{pj}X)} + \frac{1}{(1-\zeta^j X)(1-\zeta^{-pj}X)},$$

where $\zeta = e^{2\pi i/q}$, a primitive q-th root of unity. The function $F_j(X)$ has the following expansion in X;

$$F_j(X) = (\sum_{x=0}^{\infty} \zeta^{jx}X^x)(\sum_{y=0}^{\infty} \zeta^{pjy}X^y) + (\sum_{x=0}^{\infty} \zeta^{jx}X^x)(\sum_{y=0}^{\infty} \zeta^{-pjy}X^y)$$

$$= \sum_{x,y=0}^{\infty} \zeta^{j(x+py)}X^{x+y} + \sum_{x,y=0}^{\infty} \zeta^{j(x-py)}X^{x+y}.$$

Put $G(X) = \sum_{j=0}^{q-1} F_j(X)$. Since $\sum_{j=0}^{q-1} \zeta^{jx} = q$ if $x \equiv 0 \pmod q$, $= 0$ otherwise; we see easily that the power series expansion of $G(X)$ is given by

$$G(X) = 2q + q\sum_{u=1}^{\infty} X^{qu} + q\sum_{u=1}^{\infty} b(u; p, q)X^u.$$

Define $F_j'(X)$ and $G'(X)$ in the same way, replacing p by p'. Then, theorem 2 is equivalent to

Theorem 3. *If $G(X) = G'(X)$, then we have $p \equiv \pm p'$ or $pp' \equiv \pm 1 \pmod q$.*

We shall prove theorem 3 in the rest of the paper.

1. Residues of $G(X)$. By the definition, we see $G(X)$ has a pole of order at most two at $X = 1, \zeta, \cdots, \zeta^{q-1}$. The point $X = \zeta^k$ is the pole of order two if and only if $k \equiv \pm kp \pmod q$ i.e. $k \equiv 0 \pmod{r_1}$ or $k \equiv 0 \pmod{r_2}$, where we put $r_1 = \dfrac{q}{(p-1, q)}$ and $r_2 = \dfrac{q}{(p+1, q)}$. Clearly $(p-1, p+1, q) = 1$ or 2 according as q is odd or even. We put

$$(1\text{-}1) \qquad \begin{cases} (p-1, q) = \varepsilon u_1, \\ (p+1, q) = \varepsilon u_2, \end{cases}$$

then $(u_1, u_2) = 1$ and $q = \varepsilon u_1 u_2 r$, where $\varepsilon = 1$ if q is odd, $\varepsilon = 2$ if q is even. The singular part of Laurent expansion of $G(X)$ at $X = \zeta^{-k}$ is as follows;

$$(1\text{-}2) \quad \begin{cases} \dfrac{2}{(1-\zeta^k X)^2} & (u_1 r \,|\, k \text{ and } u_2 r \,|\, k), \\[2ex] \dfrac{1}{(1-\zeta^k X)^2} + \left(\dfrac{1}{1-\zeta^{-k(p+1)}} + \dfrac{1}{1-\zeta^{-k(s+1)}}\right)\dfrac{1}{1-\zeta^k X} \\[1ex] \qquad\qquad\qquad\qquad\qquad (u_1 r \nmid k \text{ and } u_2 r \,|\, k), \\[2ex] \dfrac{1}{(1-\zeta^k X)^2} + \left(\dfrac{1}{1-\zeta^{k(p-1)}} + \dfrac{1}{1-\zeta^{k(s-1)}}\right)\dfrac{1}{1-\zeta^k X} \\[1ex] \qquad\qquad\qquad\qquad\qquad (u_1 r \,|\, k \text{ and } u_2 r \nmid k), \\[2ex] \left(\dfrac{1}{1-\zeta^{k(p-1)}} + \dfrac{1}{1-\zeta^{k(s-1)}} + \dfrac{1}{1-\zeta^{-k(p+1)}} + \dfrac{1}{1-\zeta^{-k(s+1)}}\right)\dfrac{1}{1-\zeta^k X} \\[1ex] \qquad\qquad\qquad\qquad\qquad (u_1 r \nmid k \text{ and } u_2 r \nmid k), \end{cases}$$

where s is an integer such that $ps \equiv 1 \pmod{q}$, which is fixed in the following.

Lemma 1 (Chowla [2], Baker-Birch-Wirsing [1]). *Let $c_1, \cdots, c_{q-1}$ be rational numbers such that $c_j = 0$ if $(j, q) \neq 1$ and $c_j = -c_{q-j}$ $(j = 1, \cdots, q-1)$. If*

$$(1\text{-}3) \qquad \sum_{j=1}^{q-1} \frac{c_j}{1 - \zeta^j} = 0 \,,$$

then $c_j = 0$ for all j.

Proof. Operating the automorphism $\sigma_k \colon \zeta \mapsto \zeta^k$ of the q-th cyclotomic field $Q(\zeta)$ over Q to (1-3), we get

$$(1\text{-}4) \qquad \sum_{j=1}^{q-1} \frac{c_j}{1 - \zeta^{jk}} = 0 \qquad \text{for every } k, \quad (k, q) = 1.$$

We can canonically extend the sequence $c_1, \cdots, c_{q-1}$ to an infinite sequence $\{c_j\}_{j \in Z}$ periodically with period q, satisfying $c_j = 0$ if $(j, q) \neq 1$ and $c_{-j} = -c_j$. Then, from (1-4), we have

$$(1\text{-}5) \qquad \sum_{j=1}^{q-1} \frac{c_{jk}}{1 - \zeta^j} = 0 \qquad \text{for } k \in Z \,.$$

Let χ be a Dirichlet character modulo q and put $d_j = \sum_{k=1}^{q-1} \chi(k) c_{jk}$. Then we get

$$(1\text{-}6) \qquad d_j = \bar{\chi}(j) d_1 \quad \text{and}$$

$$
(1\text{-}7) \qquad
\begin{aligned}
\sum_{j=1}^{q-1} \frac{d_j}{1 - \zeta^j} &= \sum_{j=1}^{q-1} \frac{1}{1 - \zeta^j} \sum_{k=1}^{q-1} \chi(k) c_{jk} \\
&= \sum_{k=1}^{q-1} \chi(k) \sum_{j=1}^{q-1} \frac{c_{jk}}{1 - \zeta^j} \\
&= 0 \,.
\end{aligned}
$$

Clearly $d_1 = 0$ if χ is even; $\chi(-j) = \chi(j)$. In case χ is odd; $\chi(-j) = -\chi(j)$; we have, from (1-6),

$$
(1\text{-}8) \qquad
\begin{aligned}
\sum_{j=1}^{q-1} \frac{d_j}{1 - \zeta^j} &= d_1 \sum_{j=1}^{q-1} \frac{\bar{\chi}(j)}{1 - \zeta^j} \\
&= d_1 \sum_{j=1}^{q-1} \bar{\chi}(j) \left(\frac{1}{2} + \frac{1}{2} \cot \frac{j\pi}{q} \right) \\
&= \frac{d_1}{2} \sum_{j=1}^{q-1} \bar{\chi}(j) \cot \frac{j\pi}{q} \\
&= \frac{q d_1}{\pi} L(1, \bar{\chi}) \,,
\end{aligned}
$$

where $L(s, \bar{\chi})$ is the Dirichlet's L-function. Since $L(1, \bar{\chi}) \neq 0$, by Dirichlet's theorem, we get, from (1-7) and (1-8), that $d_1 = 0$ in case χ is odd, too. There-

fore $\sum\limits_{j=1}^{q-1} \chi(j)c_j=0$ for any character χ, hence $c_j=0$ for every j.   q.e.d.

Corollary. *The* $\dfrac{1}{2}\varphi(q)$ *values of cotangent* $\cot\dfrac{k\pi}{q}$, $0<k<\dfrac{q}{2}$ *and* $(k, q)=1$, *are linearly independent over* Q.

In fact, since $\cot\dfrac{k\pi}{q}=\dfrac{i}{1-\zeta^k}-\dfrac{i}{1-\zeta^{q-k}}$, we get the linear independency of above cotangents directly from lemma 1.

2. Proof of Theorem 3. We may safely assume that $q>4$, since theorem 1 is trivial for $q=1, 2, 3$ and 4. Assume $G(X)=G'(X)$, then $G(X)$ and $G'(X)$ have the same Laurent expansion at every $X=\zeta^{-k}$. From (1-2), we get easily, after exchanging p' and $-p'$ if necessary;

$$(2\text{-}1)\qquad \begin{cases} (p-1, q) = (p'-1, q) \ \text{ and} \\ (p+1, q) = (p'+1, q)\,, \end{cases}$$

and

$$(2\text{-}2)\qquad \frac{1}{1-\zeta^{k(p-1)}}+\frac{1}{1-\zeta^{k(s-1)}}+\frac{1}{1-\zeta^{-k(p+1)}}+\frac{1}{1-\zeta^{-k(s+1)}}$$

$$=\frac{1}{1-\zeta^{k(p'-1)}}+\frac{1}{1-\zeta^{k(s'-1)}}+\frac{1}{1-\zeta^{-k(p'+1)}}+\frac{1}{1-\zeta^{-k(s'+1)}}\,,$$

for every integer k satisfying $k\not\equiv 0\ (\text{mod } u_1r)$ and $k\not\equiv 0\ (\text{mod } u_2r)$, where s' is an integer such that $p's'\equiv 1\ (\text{mod } q)$. So we put

$$(2\text{-}3)\qquad \begin{cases} (p-1, q) = (p'-1, q) = \varepsilon u_1\,, \\ (p+1, q) = (p'+1, q) = \varepsilon u_2\,, \\ q = \varepsilon u_1 u_2 r \ \text{ and } \ (u_1, u_2) = 1\,, \\ \varepsilon = 2 \ \text{if } q \text{ is even, } \varepsilon = 1 \text{ otherwise.} \end{cases}$$

Since $(p-1, q)=(s-1, q)$ and $(p+1, q)=(s+1, q)$, we put

$$(2\text{-}4)\qquad \begin{cases} p-1 = \varepsilon u_1 a \ \text{ and } \ p'-1 = \varepsilon u_1 a'\,, \\ s-1 = \varepsilon u_1 b \qquad\quad s'-1 = \varepsilon u_1 b'\,, \\ p+1 = \varepsilon u_2 c \qquad\quad p'+1 = \varepsilon u_2 c'\,, \\ s+1 = \varepsilon u_2 d \qquad\quad s'+1 = \varepsilon u_2 d'\,, \end{cases}$$

where a, b, a' and b' are integers prime to u_2r and c, d, c' and d' are those prime to u_1r. Put

$$I_k = \cot\frac{(p-1)k\pi}{q}+\cot\frac{(s-1)k\pi}{q}-\cot\frac{(p+1)k\pi}{q}-\cot\frac{(s+1)k\pi}{q}$$

$$= \cot \frac{ak\pi}{u_2 r} + \cot \frac{bk\pi}{u_2 r} - \cot \frac{ck\pi}{u_1 r} - \cot \frac{dk\pi}{u_1 r}$$

and

$$I'_k = \cot \frac{(p'-1)k\pi}{q} + \cot \frac{(s'-1)k\pi}{q} - \cot \frac{(p'+1)k\pi}{q} - \cot \frac{(s'+1)k\pi}{q}$$

$$= \cot \frac{a'k\pi}{u_2 r} + \cot \frac{b'k\pi}{u_2 r} - \cot \frac{c'k\pi}{u_1 r} - \cot \frac{d'k\pi}{u_1 r} .$$

Then we get, from (2-2),

$$(2\text{-}5) \qquad\qquad I_k = I'_k$$

for every integer k satisfying $k \not\equiv 0 \pmod{u_1 r}$ and $k \not\equiv 0 \pmod{u_2 r}$. It is sufficient that we prove the theorem in the following cases:

    (1) $q=odd$ or $2\|q$; $u_1 = u_2 = 1$,
    (2)   (i) $q=odd$ or $2\|q$; $u_1 \geqq 3$,
          (ii) $4\|q$; $u_1 \geqq 3$,
          (iii) $8|q$; $u_1 = even (\geqq 2)$,
    (3) $4\|q$; $u_1 = 2$ and $u_2 = 1$,

since the transposition of u_1 and u_2 is induced by replacing p and p' by $-p$ and $-p'$ respectively.

    3. **Case 1:** $q=odd$ or $2\|q$; $u_1 = u_2 = 1$ ($q = \mathcal{E} r$ and $r=odd$).
    From (2-5), we have $I_1 = I'_1$ i.e.

$$(3\text{-}1) \qquad \cot \frac{a\pi}{r} + \cot \frac{b\pi}{r} - \cot \frac{c\pi}{r} - \cot \frac{d\pi}{r}$$

$$= \cot \frac{a'\pi}{r} + \cot \frac{b'\pi}{r} - \cot \frac{c'\pi}{r} - \cot \frac{d'\pi}{r} .$$

We can apply Corollary of Lemma 1 to (3-1), since a, b, c, d, a', b', c' and d' are all prime to r.

    Lemma 2. $I_1 \neq 0$.

    Proof. Assume $I_1 = 0$. We see, by the Corollary, at least one of the following congruences must hold:

$$\begin{cases} a \equiv -b \pmod{r} & (1) \\ a \equiv c \pmod{r} & (2) \\ a \equiv d \pmod{r} & (3). \end{cases}$$

Case (1): Multiplied by $\mathcal{E}$, we have $p - 1 \equiv -(s-1) \pmod{q}$. So $p(p-1) \equiv$

$-p(s-1)\equiv p-1$ (mod q). Hence $(p-1)^2\equiv 0$ (mod q), so that $\mathcal{E}r\,|\,(\mathcal{E}a)^2$. Hence $r\,|\,\mathcal{E}$, since $(a,r)=1$. As r is odd, $r=1$ i.e. $q=\mathcal{E}\leq 2$, a contradiction with $q>4$.

Case (2): We have $p-1\equiv p+1$ (mod q), hence $2\equiv 0$ (mod q) i.e. $q\,|\,2$, a contradiction with $q>4$.

Case (3): We also have $b\equiv c$ (mod r); so $p-1\equiv s+1$ and $s-1\equiv p+1$ (mod q); hence $p-s\equiv 2\equiv -2$ (mod q) i.e. $q\,|\,4$; this contradicts $q>4$ again.   q.e.d.

By Lemma 2, we see that one of a, b, $-c$ and $-d$ is congruent to a', b', $-c'$ or $-d'$ modulo r, that is, multiplied by $\mathcal{E}$, the sets $\{p-1, s-1, -p-1, -s-1\}$ and $\{p'-1, s'-1, -p'-1, -s'-1\}$ have non-empty intersection in the residue classes modulo q ($=\mathcal{E}r$). This implies Theorem 3.

4. Case 2: (i) $q=$ odd or $2\|q$; $u_1\geq 3$ ($q=\mathcal{E}u_1u_2r$ and u_1, u_2, r are all *odd*).

(ii) $4\|q$; $u_1\geq 3$ ($q=2u_1u_2r$, $2\|u_1u_2$ and $r=$ odd).

(iii) $8\,|\,q$; $u_1=$ even ($q=2u_1u_2r$, $4\,|\,u_1r$ and $u_2=$ odd).

Take an integer k such that (a) $k\equiv -1$ (mod u_2r); (b) $(k, u_1r)=1$ and $k\not\equiv -1$ (mod l^e) for every odd prime divisor l of u_1, $e=\mathrm{ord}_l(u_1r)$ i.e. $l^e\|u_1r$; if in case (iii), we further add (b)' $k\not\equiv -1$ (mod 2^f), $f=\mathrm{ord}_2(u_1r)$. The existence of such k is assured by the assumption on u_1. It follows from (2-5) that $I_1+I_k=I_1'+I_k'$. Hence we have:

$$(4\text{-}1) \qquad \cot\frac{c\pi}{u_1r}+\cot\frac{d\pi}{u_1r}+\cot\frac{ck\pi}{u_1r}+\cot\frac{dk\pi}{u_1r}$$

$$=\cot\frac{c'\pi}{u_1r}+\cot\frac{d'\pi}{u_1r}+\cot\frac{c'k\pi}{u_1r}+\cot\frac{d'k\pi}{u_1r}.$$

Now we can apply Corollary of Lemma 1 to (4-1). In the first place, we have

Lemma 3. *The following* (1) *or* (2) *do not hold in* (4-1):

(1) $c\equiv -d$ (mod u_1r), $c'\equiv -d'$, $ck\equiv -dk$, or $c'k\equiv -d'k$ (mod u_1r).

(2) $c\equiv -ck$ (mod u_1r), $d\equiv -dk$, $c'\equiv -c'k$, or $d'\equiv -d'k$ (mod u_1r).

Proof. If $c\equiv -d$ (mod u_1r), we have, both hand sides multiplied by $\mathcal{E}u_2$, $p+1\equiv -(s+1)$ (mod q), so that $p(p+1)\equiv -(1+p)$ (mod q). Since $(p+1, q)=\mathcal{E}u_2$, we have $p\equiv -1$ (mod u_1r). Hence $u_1r\,|\,(p+1)$ i.e. $u_1r\,|\,\mathcal{E}u_2c$. Since $(u_1r, c)=(u_1, u_2)=1$, we have $u_1\,|\,\mathcal{E}$. This is possible only in case (iii) with $u_1=\mathcal{E}=2$, so that $r\,|\,u_2$. Hence r is odd, this contradicts $4\,|\,u_1r$. If $c\equiv -ck$ (mod u_1r), then $k\equiv -1$ (mod u_1r), this contradicts the choice of k. In the same way, we see that the other congruences are also impossible.   q.e.d.

It is easy to see $p\equiv p'$ or $p\equiv s'$ (mod q) if either c or d (resp. ck or dk) is congruent to c' or d' (resp. $c'k$ or $d'k$) modulo u_1r. Hence we may assume that neither c nor d (resp. ck nor dk) is congruent to c' or d' (resp. $c'k$ or $d'k$) modulo u_1r. Then we see, by Corollary of Lemma 1 and by Lemma 3, that only the

following cases may be possible in (4-1), after transposing p and s (resp. p' and s') if necessary:

  (A) $c \equiv -dk$, $d \equiv -ck$, $c' \equiv -d'k$ and $d' \equiv -c'k$ (mod u_1r).
  (B) $c \equiv -dk$, $c' \equiv -d'k$, $d \equiv c'k$ and $d' \equiv ck$ (mod u_1r).
  (C) $c \equiv c'k$, $d \equiv d'k$, $c' \equiv ck$ and $d' \equiv dk$ (mod u_1r).
  (D) $c \equiv c'k$, $d \equiv d'k$, $c' \equiv dk$ and $d' \equiv ck$ (mod u_1r).

Case (A):

From $c \equiv -dk$ and $d \equiv -ck$ (mod u_1r) follows $p+1 \equiv -(s+1)k$ and $s+1 \equiv -(p+1)k$ (mod q), so that $p \equiv s \equiv -k$ (mod u_1r) and $k^2 \equiv 1$ (mod u_1r). As $k \equiv -p \equiv -1$ (mod u_1), we have $k \equiv -1$ (mod l^e) for every odd prime divisor l of u_1, which contradicts the choice of k. Hence u_1 must be a power of 2, and this is possible only in case (iii). Then we have $k \equiv -p \equiv -1$ (mod 4) and $k^2 \equiv 1$ (mod 2^f), so that $k \equiv -1$ (mod 2^{f-1}). Furthermore we have $f \geq 3$ since, by the choice of k, we have $p \equiv -k \not\equiv 1$ (mod 2^f) while $p \equiv 1$ (mod 4). On the other hand, we have $(u_1r, u_2) = 1$, since $p \equiv -k \equiv 1$ (mod r) and $p \equiv -1$ (mod u_2). Therefore we get $p \equiv -k \equiv 1 \left(\text{mod } \dfrac{u_1r}{2} \right)$, $p \equiv -k \not\equiv 1$ (mod u_1r) and $p \equiv -1$ (mod u_2). In the same way, from $c' \equiv -d'k$ and $d' \equiv -c'k$ (mod u_1r), we have $p' \equiv 1 \left(\text{mod } \dfrac{u_1r}{2} \right)$, $p' \not\equiv 1$ (mod u_1r) and $p' \equiv -1$ (mod u_2). We see each one of p and p' is congruent to $1 + \dfrac{u_1r}{2}$ or $1 - \dfrac{u_1r}{2}$ (mod $2u_1r$), hence $p \equiv p'$ or $p \equiv s'$ (mod $2u_1r$), since we have $f \geq 3$ and $\left(1 + \dfrac{u_1r}{2} \right) \left(1 - \dfrac{u_1r}{2} \right) \equiv 1$ (mod $2u_1r$). As $p \equiv s \equiv p' \equiv s' \equiv -1$ (mod u_2), $q = 2u_1u_2r$ and $(2u_1r, u_2) = 1$, we have $p \equiv p'$ or $p \equiv s'$ (mod q).

Case (B):

From $c \equiv -dk$ and $c' \equiv -d'k$ (mod u_1r) follows $p \equiv p' \equiv -k$ (mod u_1r). That $p \equiv -k \equiv 1$ (mod r) and $p \equiv -1$ (mod u_2) implies $(u_1r, u_2) = 1$ or 2. From $d \equiv c'k$ (mod u_1r) follows $s+1 \equiv (p'+1)k$ (mod q). So $p+1 \equiv p(s+1) \equiv p(p'+1)k \equiv p(p+1)(-p) \equiv -(p+1)p^2$ (mod u_1r). Hence $(p+1)(p^2+1) \equiv \varepsilon u_2c(p^2+1) \equiv 0$ (mod u_1r) i.e. $\varepsilon(p^2+1) \equiv 0$ (mod u_1r). We have $p^2 \equiv -1$ (mod l) if there is an odd prime divisor l of u_1, while $p^2 \equiv 1$ (mod l) since $p \equiv 1$ (mod u_1). Therefore u_1 must be a power of 2, this is possible only in case (iii). Then $p^2 \equiv -1$ (mod 2^{f-1}), so that $f = 2$ since $f \geq 2$ by the assumption of (iii). As $p \equiv -k$ (mod u_1r), $p \equiv 1$ (mod εu_1) and $u_1r \equiv \varepsilon u_1 \equiv 0$ (mod 4), we have $k \equiv -1$ (mod 2^f), which contradicts the choice of k. Therefore case (B) is impossible.

Case (C) and (D):

We claim $pp' \equiv 1$ (mod q) in these cases. From $c \equiv c'k$ and $d \equiv d'k$ (mod u_1r) follows $p+1 \equiv (p'+1)k$ and $s+1 \equiv (s'+1)k$ (mod q), so that $p'(1+p) \equiv p(1+p')k \equiv p(p+1)$ (mod q), hence we get $p \equiv p'$ (mod u_1r). Since $p \equiv p' \equiv 1$ (mod εu_1), we have $2 \equiv 2k$ (mod εu_1), so $k \equiv 1$ (mod u_1), while $k \equiv -1$ (mod u_2r).

Hence we see $(u_1, u_2r)=1$ or 2.   Let l be a prime divisor of q.   It is enough to prove $pp'\equiv 1$ (mod $l^{\mathrm{ord}_l(q)}$).

In case l=an odd prime:
Since $p\equiv p'$ (mod u_1r), we get $p-p'=(p+1)-(p'+1)\equiv\mathcal{E}u_2(c-c')\equiv\mathcal{E}u_2c'(k-1)\equiv 0$ (mod u_1r), so that

(4-2) $o(u_2)+o(c')+o(k-1)\geq o(u_1)+o(r)$, where $o(\ )=\mathrm{ord}_l(\ )$.

(a)   If $l|u_1$, then $l\!\!\not|\,u_2r$ and $o(u_1)=o(q)$.   Since $p\equiv p'\equiv 1$ (mod $\mathcal{E}u_1$), we have $pp'\equiv 1$ (mod $l^{o(q)}$).
(b)   If $l|(u_2, r)$, then $l\!\!\not|\,u_1$ and $k\equiv -1\not\equiv 1$ (mod l) therefore from (4-2) $o(q)=o(u_2)+o(r)$.   Since $c\equiv c'k\equiv -c'$ (mod r) and $o(u_2)\geq o(r)$, we get $pp'=(\mathcal{E}u_2c-1)(\mathcal{E}u_2c'-1)=\mathcal{E}^2u_2^2cc'-\mathcal{E}u_2(c+c')+1\equiv 1$ (mod $l^{o(q)}$).
(c)   If $l|u_2$ and $l\!\!\not|\,r$, then $l\!\!\not|\,u_1$ and $o(q)=o(u_2)$.   Since $p\equiv p'\equiv -1$ (mod $\mathcal{E}u_2$), we have $pp'\equiv 1$ (mod $l^{o(q)}$).
(d)   If $l|r$ and $l\!\!\not|\,u_2$, then $l\!\!\not|\,u_1$ and $0=o(u_2)<o(u_1)+o(r)=o(r)$, this is impossible since we have from (4-2), $o(u_2)\geq o(u_1)+o(r)$.

In case l=2:
It is enough to prove only in case (ii) and (iii).
(a)   Case (ii); we see $4\|q$ and $p\equiv p'\equiv 1$ or -1 (mod 4) according as u_1 is even or u_2 is even.   Hence $pp'\equiv 1$ (mod 4).
(b)   Case (iii); we have $o(q)=o(u_1)+o(r)+1\geq 3$ and $o(u_1)=1$.   We get $\mathrm{Min}(o(u_1), o(r))\leq 1$ since $k\equiv 1$ (mod u_1) and $k\equiv -1$ (mod u_2r).
(b-1)   If $o(r)=0$, then we have $o(q)=o(u_1)+1$ and $p\equiv p'\equiv 1$ (mod $2u_1$), so that $pp'\equiv 1$ (mod $2^{o(q)}$).
(b-2)   If $o(r)=1$, then $o(q)=o(u_1)+2$.   Since $o(p-1)=o(p'-1)=o(u_1)+1=o(q)-1$, we have $p\equiv p'\equiv 1+2^{o(q)-1}$ (mod $2^{o(q)}$), so that $pp'\equiv 1$ (mod $2^{o(q)}$).
(b-3)   If $o(u_1)=1$, then $o(q)=o(r)+2\geq 3$.   Since we have $p+1\equiv(p'+1)k$ (mod $2^{o(q)}$) and $p\equiv p'$ (mod $2^{o(u_1r)}$), we get $p+1\equiv(p+1)k$ (mod $2^{o(q)-1}$).   Hence $k\equiv 1$ (mod $2^{o(r)}$), while $k\equiv -1$ (mod $2^{o(u_2r)}$).   So we have $1\equiv -1$ (mod $2^{o(r)}$), so that $o(r)\leq 1$.   Since $o(q)\geq 3$, we get $o(r)=1$ and $o(q)=3$.   It follows from $o(p-1)=o(p'-1)=2$ that $p\equiv p'\equiv 5$ (mod 8), hence $pp'\equiv 1$ (mod 2^3).
   This completes the proof in Case 2.

5.   Case 3: $4\|q$; $u_1=2$ and $u_2=1$ ($q=4r$ and $r=odd>1$).
We see

$$I_1 \ = \cot\frac{a\pi}{r}+\cot\frac{b\pi}{r}-\cot\frac{c\pi}{2r}-\cot\frac{d\pi}{2r},$$

$$I_{r+1}= \cot\frac{a\pi}{r}+\cot\frac{b\pi}{r}-\cot\frac{(c+r)\pi}{2r}-\cot\frac{(d+r)\pi}{2r}.$$

By the duplication formula of cotangent, we get

$$I_1 + I_{r+1}$$
$$= 2\left(\cot\frac{a\pi}{r} + \cot\frac{b\pi}{r} - \cot\frac{c\pi}{r} - \cot\frac{d\pi}{r}\right).$$

From (2-5), $I_1 + I_{r+1} = I_1' + I_{r+1}'$. Halving both hand sides, we have

$$(5\text{-}1) \qquad \cot\frac{a\pi}{r} + \cot\frac{b\pi}{r} - \cot\frac{c\pi}{r} - \cot\frac{d\pi}{r}$$

$$= \cot\frac{a'\pi}{r} + \cot\frac{b'\pi}{r} - \cot\frac{c'\pi}{r} - \cot\frac{d'\pi}{r}.$$

Now we can apply Corollary of Lemma 1 to (5-1). In the first place we have

Lemma 4. *The following* (1), (2) *or* (3) *do not hold in* (5-1):

(1) $a \equiv -b$, $c \equiv -d$, $a' \equiv -b'$, or $c' \equiv -d'$ (mod r).
(2) $a \equiv c$ and $b \equiv d$ (mod r) or $a' \equiv c'$ and $b' \equiv d'$ (mod r).
(3) $a \equiv d$ and $b \equiv c$ (mod r) or $a' \equiv d'$ and $b' \equiv c'$ (mor r).

Proof. (1) If $a \equiv -b$ (mod r), we have $4a \equiv -4b$ (mod q), i.e. $p-1 \equiv -(s-1)$ (mod q). Hence $p(p-1) \equiv -(1-p)$ (mod q), so that $p \equiv 1$ (mod r) since $(p-1, q) = 4$. This implies $r=1$, i.e. $q=4$, a contradiction with $q>4$.
(2) If $a \equiv c$ and $b \equiv d$ (mod r), we have $4a \equiv 4c$ and $4b \equiv 4d$ (mod $4r$), i.e. $p-1 \equiv 2(p+1)$ and $s-1 \equiv 2(s+1)$ (mod $4r$). Hence we get $p \equiv s \equiv -3$ (mod $4r$). Then $1 \equiv ps \equiv 9$ (mod $4r$), i.e. $r=1$ or $r=2$, a contradiction with $q>4$ and $r=$odd.
(3) If $a \equiv d$ and $b \equiv c$ (mod r), we have $p-1 \equiv 2(s+1)$ and $s-1 \equiv 2(p+1)$ (mod $4r$). Multiplied by p, we have $p(p-1) \equiv 2(1+p)$ and $1-p \equiv 2p(p+1)$ (mod $4r$), i.e. $p^2 - 3p - 2 \equiv 0$ and $2p^2 + 3p - 1 \equiv 0$ (mod $4r$). Hence $3p^2 - 3 \equiv 3(p-1)(p+1) \equiv 0$ (mod $4r$). We have $3(p+1) \equiv 0$ (mod r), so that $3 \equiv 0$ (mod r), since $(p-1, 4r)=4$ and $(p+1, 4r)=2$. As $r \geq 3$, we have $r=3$ and $q=4r=12$. Since $p^2 \equiv 1$ (mod 12), $p^2 - 3p - 2 \equiv 0$ (mod 12) implies $3p \equiv -1$ (mod 12), a contradiction.
The other cases can be checked in the same way. q.e.d.

It is easy to see $p \equiv p'$ or $p \equiv s'$ (mod q) if either a or b (resp. c or d) is congruent to a' or b' (resp. c' or d') modulo r. Hence we may assume that neither a nor b (resp. c nor d) is congruent to a' or b' (resp. c' or d') modulo r. Then, we see, by Corollary of Lemma 1 and by Lemma 4, that only the following cases may be possible in (5-1), after trasnposing p and s (resp. p' and s') if necessary:

(A) $a \equiv c$, $a' \equiv c'$, $b \equiv -d'$ and $b' \equiv -d$ (mod r).
(B) $a \equiv d$, $a' \equiv d'$, $b \equiv -c'$ and $b' \equiv -c$ (mod r).
(C) $a \equiv c$, $a' \equiv d'$, $b \equiv -c'$ and $b' \equiv -d$ (mod r).

(D) $a \equiv -c'$, $b \equiv -d'$, $a' \equiv -c$ and $b' \equiv -d$ (mod r).

(E) $a \equiv -c'$, $b \equiv -d'$, $a' \equiv -d$ and $b' \equiv -c$ (mod r).

Case (A):

From $a \equiv c$ and $a' \equiv c'$ (mod r) follows $p \equiv p' \equiv -3$ (mod q) (c.f. the proof of Lemma 4. (2)).

Case (B):

From $b \equiv -c'$ and $b' \equiv -c$ (mod r) follows $s-1 \equiv -2(p'+1)$ and $s'-1 \equiv -2(p+1)$ (mod q), so that $2p'+s \equiv -1$ and $2p+s' \equiv -1$ (mod q). Hence we have $2pp'+1 \equiv -p$ and $2pp'+1 \equiv -p'$ (mod q), so that $p \equiv p'$ and

(5-2) $2p^2+p+1 \equiv 0$ (mod q).

On the other hand, from $a \equiv d$ (mod r), we have $p-1 \equiv 2(s+1)$ (mod q), so that

(5-3) $p^2-3p-2 \equiv 0$ (mod q).

From (5-2) and (5-3), we have $7p \equiv -5$ (mod q). Then $0 \equiv 7^2(p^2-3p-2) \equiv (7p)^2-21(7p)-98 \equiv 32$ (mod q), so that $q|32$ i.e. $r|8$, a contradiction with $r=odd >1$.

Case (C):

We have $p-1 \equiv 2(p+1)$, $p'-1 \equiv 2(s'+1)$, $s-1 \equiv -2(p'+1)$ and $s'-1 \equiv -2(s+1)$ (mod q). Hence $p \equiv -3$, $p'-2s' \equiv 3$, $2p'+s \equiv -1$ and $2s+s' \equiv -1$ (mod q). From the last three congruences, we get $6 \equiv 2(p'-2s') \equiv 2p'-4s' \equiv -s-1-4(-2s-1) \equiv 7s+3$ (mod q), so that $7s \equiv 3$ (mod q) i.e. $3p \equiv 7$ (mod q). Since $p \equiv -3$ (mod q), we have $7 \equiv 3p \equiv -9$ (mod q). Hence $q|16$ i.e. $r|4$, a contradiction.

Case (D):

From $a \equiv -c'$ and $a' \equiv -c$ (mod r) follows $p-1 \equiv -2(p'+1)$ and $p'-1 \equiv -2(p+1)$ (mod q), so that $p+2p' \equiv 2p+p' \equiv -1$ (mod q). Hence $p \equiv p'$ and $3p \equiv -1$ (mod q). From $b \equiv -d'$ and $b' \equiv -d$ (mod r), we get, in the same way, $3s \equiv -1$ (mod q). Therefore $9 \equiv (3p)(3s) \equiv (-1)^2 \equiv -1$ (mod q), so that $q|8$ i.e. $r|2$, a contradiction.

Case (E):

From $a' \equiv -d$ and $b' \equiv -c$ (mod r) follows $p'-1 \equiv -2(s+1)$ and $s'-1 \equiv -2(p+1)$ (mod q), so that $p'+2s \equiv -1$ and $s'+2p \equiv -1$ (mod q). Hence $pp'+2 \equiv -p$ and $1+2pp' \equiv -p'$ (mod q). Eliminating pp', we have

(5-4) $2p-p' \equiv -3$ (mod q).

On the other hand, from $a \equiv -c'$ (mod r), we have

(5-5) $p+2p' \equiv -1$ (mod q).

From (5-4) and (5-5), we have $5p \equiv -7$ and $5p' \equiv 1 \pmod{q}$. Since $5^2(pp'+2)$ $\equiv 5^2(-p) \pmod{q}$, we have $-7+50 \equiv 35 \pmod{q}$, so that $q \mid 8$, a contradiction.

This completes the proof in Case 3 and completes the proof of Theorem 3 also.

6. Appendix. We can prove Theorem 3, without Lemma 1, or without non-vanishing of Dirichlet's L-functions at $s=1$, directly from (2-5) in case q is a prime number $\geqq 7$.

Assume q is prime $\geqq 7$. Let $K = Q(\zeta)$, a cyclotomic field of degree $q-1$, and $\mathcal{O}$ be the ring of algebraic integers of K. Then the prime q is totally ramified in K, more precisely, the principal ideal $(q) = q\mathcal{O}$ in $\mathcal{O}$ is the $(q-1)$-th power of prime ideal $(\lambda) = \lambda\mathcal{O}$; $(q) = (\lambda)^{q-1}$, where $\lambda = 1-\zeta$ and the residue class field $\mathcal{O}/(\lambda)$ is isomorphic to Z/qZ. We have

$$
\begin{aligned}
1-\zeta^k &= 1-(1-\lambda)^k \\
&= \lambda \sum_{j=1}^{k} \binom{k}{j}(-\lambda)^{j-1} \\
&= \lambda k \sum_{j=0}^{k-1} \binom{k-1}{j} \frac{(-\lambda)^j}{j+1} \\
&= \lambda k \left(1 - \frac{k-1}{2}\lambda + \frac{(k-1)(k-2)}{6}\lambda^2 - \frac{(k-1)(k-2)(k-3)}{24}\lambda^3 \right. \\
&\quad \left. + \frac{(k-1)(k-2)(k-3)(k-4)}{120}\lambda^4 - \cdots \right)
\end{aligned}
$$

for $k = 1, 2, \cdots, q-1$. Hence

$$
\begin{aligned}
(6\text{-}1) \quad \frac{\lambda}{1-\zeta^k} &= \frac{1}{k}\left(\sum_{j=0}^{k-1}\binom{k-1}{j}\frac{(-\lambda)^j}{j+1}\right)^{-1} \\
&= \frac{1}{k}\left(1 + \frac{k-1}{2}\lambda + \frac{k^2-1}{12}\lambda^2 + \frac{k^2-1}{24}\lambda^3 \right. \\
&\quad \left. - \frac{(k^2-1)(k^2-19)}{720}\lambda^4 - \cdots \right),
\end{aligned}
$$

where the last series, as is easily seen from the fact that each $\binom{k-1}{j}\frac{1}{j+1} = \frac{1}{k}\binom{k}{j+1}$ is a λ-adic integer, converges λ-adically for $k=1,\cdots,q-1$. From (2-5), we have

$$
(6\text{-}2) \qquad \lambda I_1 = \lambda I_1'.
$$

As $\frac{\lambda}{1-\zeta^k}$ belongs to $\mathcal{O}$ for $k=1,\cdots,q-1$, both λI_1 and $\lambda I_1'$ are also in $\mathcal{O}$. Let

$$
\begin{cases}
\lambda I_1 = g_0 + g_1\lambda + g_2\lambda^2 + g_3\lambda^3 + g_4\lambda^4 + \cdots . \\
\lambda I_1' = g_0' + g_1'\lambda + g_2'\lambda^2 + g_3'\lambda^3 + g_4'\lambda^4 + \cdots .
\end{cases}
$$

be the λ-adic expansions of λI_1 and $\lambda I_1'$ respectively, where the representatives g_k and g_k' of $\mathcal{O}/(\lambda)$ are taken from $\{0, 1, \cdots, q-1\}$. From (6-2), we have

(6-3) $$g_k \equiv g_k' \pmod{q} \text{ for } k = 0, 1, \cdots.$$

From (6-1), we get,

$$g_0 \equiv \sum_k \frac{1}{k} \equiv \frac{1}{p-1} + \frac{1}{s-1} - \frac{1}{p+1} - \frac{1}{s+1}$$

$$\equiv \frac{1}{p-1} + \frac{p}{1-p} - \frac{1}{p+1} - \frac{p}{1+p}$$

$$\equiv -2 \pmod{q},$$

$$g_1 \equiv \frac{1}{2} \sum_k \left(1 - \frac{1}{k}\right) \equiv 2 - (-1) \equiv 3 \pmod{q},$$

$$g_2 \equiv \frac{1}{12} \sum_k \left(k - \frac{1}{k}\right) \equiv -\frac{1}{6} \pmod{q},$$

$$g_3 \equiv \frac{1}{24} \sum_k \left(k - \frac{1}{k}\right) \equiv -\frac{1}{12} \pmod{q},$$

$$g_4 \equiv -\frac{1}{720} \sum_k \left(k^3 - 20k + \frac{19}{k}\right) \equiv \frac{1}{120}(p^2 + s^2) - \frac{19}{360} \pmod{q},$$

where the summation is taken for $k = p-1, s-1, -p-1$ and $-s-1$, especially we see

$$\sum_k k = (p-1) + (s-1) - (p+1) - (s+1) = -4$$

$$\sum_k k^3 = (p-1)^3 + (s-1)^3 - (p+1)^3 - (s+1)^3$$

$$= -6(p^2 + s^2) - 4.$$

In the same way, we get

$$g_0' \equiv -2 \pmod{q},$$

$$g_1' \equiv 3 \pmod{q},$$

$$g_2' \equiv -\frac{1}{6} \pmod{q},$$

$$g_3' \equiv -\frac{1}{12} \pmod{q} \text{ and}$$

$$g_4' \equiv \frac{1}{120}(p'^2 + s'^2) - \frac{19}{360} \pmod{q}.$$

Comparing the case $k=4$ in (6-3), we have

(6-4) $$p^2 + s^2 \equiv p'^2 + s'^2 \pmod{q}.$$

Since $ps \equiv p's' \equiv 1 \pmod{q}$, we have, from (6-4),

$$\begin{cases} (p+s)^2 \equiv (p'+s')^2 \pmod{q} \\ (p-s)^2 \equiv (p'-s')^2 \pmod{q}, \end{cases}$$

hence

(6-5) $$\begin{cases} p+s \equiv \pm(p'+s') \pmod{q} \\ p-s \equiv \pm(p'-s') \pmod{q}, \end{cases}$$

where the signs are taken independently.   Then we see easily, from (6-5), that

$$p \equiv \pm p' \text{ or } p \equiv \pm s' \pmod{q}.$$

Thus we get Theorem 3 for prime $q \geq 7$.

7. Spectrum of 3-dimensional lens spaces.
In the course of the proof of Theorem 3, we have shown the following

Proposition. *Let q, p and p' be as in Section 0.   Assume we have (2-1) and (2-2).   Then $p \equiv \pm p'$ or $pp' \equiv \pm 1 \pmod{q}$.*

This proposition was the essential part of the proof of "Main Theorem" in [3] (cf. Lemma 4.4, Proposition 4.6), though only the case $q = l^n$ or $2 \cdot l^n$ had been shown there.   Now we have proved completely

Theorem. *Let q be a positive integer.   If two 3-dimensional lens spaces with fundamental group of order q are isospectral, then they are isometric to each other.*

References

[1]   A. Baker, B.J. Birch and E.A. Wirsing: *On a problem of Chowla*, J. Number Theory **5** (1973), 224–236.

[2]   S. Chowla: *A special infinite series,* Norske Vid. Selsk. Forh. **37** (1964), 85–87.

[3]   A. Ikeda and Y. Yamamoto: *On the spectra of 3-dimensional lens spaces,* Osaka J. Math. **16** (1979), 447–469.

Departmenf of Mathematics
Osaka University
Toyonaka, Osaka 560, Japan