Ikeda, A. and Yamamoto, Y.
Osaka J. Math.
16 (1979), 447-469

ON THE SPECTRA OF 3-DIMENSIONAL LENS SPACES

AKIRA IKEDA AND YOSHIHIKO YAMAMOTO

(Received July 28, 1978)

Introduction. Let (M,g) be a compact connected riemannian manifold and Δ the Laplacian acting on the space of differentiable functions on M. We denote by $\mathrm{Spec}(M,g)$ the set of all eigenvalues of Δ;

$$\mathrm{Spec}(M,g) = \{0 = \lambda_0 < \lambda_1 \leqq \lambda_2 \leqq \cdots \leqq \lambda_i \leqq \cdots\},$$

where each λ_i is written a number of times equal to its multiplicity. We call it *the spectrum* of (M,g). Two riemannian manifolds (M,g) and (N,h) are said to be *isospectral* to each other if $\mathrm{Spec}(M,g)=\mathrm{Spec}(N,h)$. What are determined by the spectrum of (M,g)? This problem have been studied by many people; as in Berger [2], Colin de Verdiere [6], Duistermaat-Guillemin [7], MaKean-Singer [8], Sakai [9], Tanno [11] and so on. For example, the spectrum of (M,g) determines the dimension of M, the volume of (M,g) and the lengths of closed geodesics of (M,g) etc.

We are interested in the riemannian manifolds of positive constant curvature, and consider whether they are determined by their spectra. Berger (for $n=2,3$) and Tanno (for $n=4,5,6$) have shown that the standard sphere S^n and the standard real projective space $P^n(\boldsymbol{R})$ are completely characterized by their spectra as riemannian manifolds. The lens spaces are familiar examples of compact riemannian manifold of positive constant curvature. Recently, Tanaka [10] have shown that if a 3-dimensional compact riemannian manifold is isospectral to a lens space with fundamental group of order q, then the manifold is isometric to one of the 3-dimensional lens spaces with fundamental group of order q. In particular a 3-dimensional homogeneous lens space is characterized by its spectrum as a riemannian manifold.

Now, we state our Main Theorem.

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

This theorem will be shown here in this paper only for $q=l^\nu$, $2l^\nu$ and 2^ν where l is an odd prime and $\nu \geqq 1$. In case of any composite number q, the

second auther will give a proof in the forthcoming paper [14]. From the above theorem and the result due to Tanaka, we have

Theorem. *A 3-dimensional lens space is completely characterized by its spectrum as a riemannian manifold.*

REMARK. Tanaka announced in his paper [10] that he obtained the above main theorem for q=odd primes and 2-times odd primes.

Our proof is as follows:

First, we shall construct the generating function associated to the spectrum of a $2n+1$-dimensional lens space of constant curvature 1 (see in **1**), i.e.,

$$F(z) = \sum_{k=0}^{\infty} (\dim E_{k(k+2n)}) z^k ,$$

where the space $E_{k(k+2n)}$ denotes the eigenspace with eigenvalue $k(k+2n)$ (see more precisely (1.7)).

By the definition, the spectrum of the lens space determines the generating function and the converse is also true.

Next, we shall consider only the 3-dimensional case, and calculate the residues of the generating functions at suitable points. Applying Key Lemma (Lemma 5.3) to the above residues, we shall prove our Main Theorem for $q=l^\nu$, $2l^\nu$ and 2^ν, case by case (see in **6**,**7**,**8** and **9**).

Lemma 5.3 plays an important role in this paper. It asserts a linear independence of the values of cotangent over the rational number field $\boldsymbol{Q}$. It will be proved using a result in number theory obtained by Chowla [4] and Baker-Birch-Wirsing [1].

The generating function can be defined also for any Clifford-Klein spherical form S^n/G, where G is a finite subgroup of fixed points free isometries. We believe that the generating functions plays an important role studying the spectra of these manifolds.

1. Lens spaces

Let $\boldsymbol{C}^{n+1}$ be the space of $(n+1)$-tuples $(z_0, z_1, \cdots, z_n)$ of complex numbers with the standard flat kähler metric $ds^2 = \sum_{k=0}^{n} dz_i \cdot d\bar{z}_i$. Let q be a positive integer and $p_0, p_1, \cdots, p_n$ integers prime to q. Put $\gamma = \exp 2\pi\sqrt{-1}/q$. We define an isometry g of $\boldsymbol{C}^{n+1}$ by

$$g: (z_0, z_1, \cdots, z_n) \to (\gamma^{p_0} z_0, \gamma^{p_1} z_1, \cdots, \gamma^{p_n} z_n) . \tag{1.1}$$

g generates a cyclic subgroup G of the unitary group $U(n+1)$;

$$G = \{g^k\}_{k=0,\cdots,q-1} . \tag{1.2}$$

Let S^{2n+1} be the unit sphere centered at the origin of $\boldsymbol{C}^{n+1}$. The elements $g^k(0<k<q)$ act on S^{2n+1} without fixed points. The sphere S^{2n+1} is the universal covering manifold of the differentiable manifold S^{2n+1}/G. Let π be the covering projection of S^{2n+1} onto S^{2n+1}/G;

$$\pi\colon S^{2n+1} \to S^{2n+1}/G\,. \tag{1.3}$$

S^{2n+1}/G has a unique riemannian metric such that π gives a local isometry of S^{2n+1} onto S^{2n+1}/G. This riemannian manifold S^{2n+1}/G shall be called a lens space and denoted by $L(q:p_0,\cdots,p_n)$. By the definition, for any $(n+1)$-tuples $(p_0,\cdots,p_n)$, $(p_0',\cdots,p_n')$ of integers prime to q such that $p_i'\equiv p_i \pmod q$ $(i=0,\cdots,n)$, the lens space $L(q:p_0',\cdots,p_n')$ is isometric to $L(q;p_0,\cdots,p_n)$.

Proposition 1.1. *Let $L(q:p_0,\cdots,p_n)$ and $L(q:p_0',\cdots,p_n')$ be lens spaces. Suppose there exist an integer l and numbers $\varepsilon_i\in\{-1,1\}$ $(i=0,1,\cdots,n)$ such that $(p_0',\cdots,p_n')$ is a permutation of $(\varepsilon_0 lp_0,\cdots,\varepsilon_n lp_n)$ (mod q). Then $L(q:p_0,\cdots,p_n)$ is isometric to $L(q:p_0',\cdots,p_n')$.*

Proof. The isometry of S^{2n+1} onto S^{2n+1} defined by the map

$$(z_0,\cdots,z_i,\cdots,z_n)\to(z_0,\cdots,\bar{z}_i,\cdots,z_n) \tag{1.4}$$

(resp.

$$(z_0,\cdots,z_n)\to(z_{\sigma(0)},\cdots,z_{\sigma(n)})\,, \tag{1.5}$$

where σ is a permutation) induces an isometry of $L(q:p_0,\cdots,p_n)$ onto $L(q:p_0,\cdots,-p_i,\cdots,p_n)$ (resp. $L(q:p_{\sigma(0)},\cdots,p_{\sigma(n)})$). Since g^l is a generator of G, the lens space $L(q:lp_0,\cdots,lp_n)$ is identical to $L(q:p_0,\cdots,p_n)$. Now Proposition 1.1 follows easily from these facts. q.e.d.

REMARK. The following fact is known (see M.M. Cohen [5]). Let $L(q:p_0,\cdots,p_n)$ and $L(q:p_0',\cdots,p_n')$ be lens spaces. Then $L(q:p_0,\cdots,p_n)$ is homeomorphic to $L(q:p_0',\cdots,p_n')$ if and only if there exist an integer l and numbers $\varepsilon_i\in\{-1,1\}$ such that $(p_0',\cdots,p_n')$ is a permutation of $(\varepsilon_0 lp_0,\cdots,\varepsilon_n lp_n)$ (mod q). From this, especially the converse of Proposition 1.1 is also true.

A riemannian manifold M is said to be homogeneous if the isometry group of M acts transitively on it.

Proposition 1.2 (see J.A. Wolf [13]). *The riemannian manifold $L(q:p_0,\cdots,p_n)$ is homogeneous if and only if for any i and j, $0\leqq i,j\leqq n$, it satisfies either $p_i\equiv p_j$ (mod q) or $p_i\equiv -p_j$ (mod q). Furthermore two homogeneous lens spaces with same order of fundamental groups are isometric to each other.*

In the following, we denote by $C^\infty(M)$ the space of all differentiable functions on a manifold M and also denote by $\tilde{\Delta}$ the Laplacian acting on $C^\infty(S^{2n+1})$.

For a lens space $L(q:p_0,\cdots,p_n)$, the Laplacian of $L(q:p_0,\cdots,p_n)$ is denoted by $\Delta_{L(q:p_0,\cdots,p_n)}$ or simply Δ. For any nonnegative real number λ, we define the spaces $\tilde{E}_\lambda$ and E_λ by

$$\tilde{E}_\lambda = \{f\in C^\infty(S^{2n+1}): \tilde{\Delta}f = \lambda f\}\,, \tag{1.6}$$

$$E_\lambda = \{f\in C^\infty(L(q:p_0,\cdots,p_n)): \Delta f = \lambda f\}\,. \tag{1.7}$$

The following lemma is elementary.

Lemma 1.3. (1) *For any $f\in C^\infty(L(q:p_0,\cdots,p_n))$, we have*

$$\tilde{\Delta}(\pi^*f) = \pi^*(\Delta f)\,. \tag{1.8}$$

(2) *For any G-invariant function F on S^{2n+1}, there exists a unique function $f\in C^\infty(L(q:p_0,\cdots,p_n))$ such that*

$$F = \pi^*f\,. \tag{1.9}$$

Corollary 1.4. *Let $(\tilde{E}_\lambda)_G$ be the space of all G-invariant functions of $\tilde{E}_\lambda$. Then have*

$$\dim E_\lambda = \dim (\tilde{E}_\lambda)_G\,. \tag{1.10}$$

Proof. By Lemma 1.3, we can see easily that for any eigenfunction f of Δ with an eigenvalue λ, there exists a unique eigenfunction F of $\tilde{\Delta}$ with the same eigenvalue λ such that F is G-invariant and $F=\pi^*f$, and conversely, for any G-invariant eigenfunction F of $\tilde{\Delta}$ with eigenvalue λ, there exists a unique eigenfunction f of Δ with eigenvalue λ such that $F=\pi^*f$. These facts imply (1.10). q.e.d.

2. Spectrum of S^{2n+1}

Let Δ_0 be the Laplacian on the space $\boldsymbol{C}^{n+1}$ with respect to the flat kähler metric. Put $r^2=\sum_{i=0}^{n} z_i\bar{z}_i$. We denote by P^k the space of homogeneous polynomials of degree k with respect to $z_0,z_1,\cdots,z_n,\bar{z}_0,\bar{z}_1,\cdots,\bar{z}_n$ and H^k the subspace of P^k consisting of harmonic polynomials on $\boldsymbol{C}^{n+1}$;

$$H^k = \{f\in P^k: \Delta_0 f = 0\}\,. \tag{2.1}$$

Each unitary transformation of $\boldsymbol{C}^{n+1}$ induces canonically a linear isomorphism of P^k, thus P^k is canonically a $U(n+1)$-module.

Proposition 2.1. *The space H^k is $U(n+1)$-invariant, and the $U(n+1)$-module P^k has the direct sum decomposition*;

$$P^k = H^k\oplus r^2P^{k-2}\,. \tag{2.1}$$

The injection map $i: S^{2n+1} \to \boldsymbol{C}^{n+1}$ *induces a linear map* $i^*: C^\infty(\boldsymbol{C}^{n+1}) \to C^\infty(S^{2n+1})$. *The image* $i^*(H^k)$ *is denoted by* $\mathcal{H}^k$.

Proposition 2.2. $\mathcal{H}^k$ *is an eigenspace of* Δ *on* S^{2n+1} *with eigenvalue* $k(k+2n)$ *and* $\sum_{k=0}^{\infty} \mathcal{H}^k$ *is dense in* $C^\infty(S^{2n+1})$ *by the uniform convergence topology. Moreover,* $\mathcal{H}^k$ *is isomorphic to* H^k *as* $U(n+1)$*-modules by the* i^*.

For the proofs of Proposition 2.1 and 2.2, see in [2].

By Corollary 1.4 and Proposition 2.2, we have

Corollary 2.3. *Let* $L(q:p_0,\cdots,p_n)$ *be a lens space and* $\mathcal{H}^k_G$ *the space of all* G*-invariant functions in* $\mathcal{H}^k$ *where* $G=\{g^k\}_{k=0,1,\cdots,q-1}$. *Then we have*

$$\dim E_{k(k+2)} = \dim \mathcal{H}^k_G \,. \tag{2.3}$$

Moreover, for any integer k *such that* $\dim \mathcal{H}^k_G \neq 0$, $k(k+2n)$ *is an eigenvalue of* Δ *on* $L(q:p_0,\cdots,p_n)$ *with multiplicity* $\dim \mathcal{H}^k_G$ *and no other eigenvalues appear in the spectrum of* Δ.

3. Generating function associated to the spectrum of $L(q:p_0,\cdots,p_n)$

Let $L(q:p_0,\cdots,p_n)$ be a lens space and G the cyclic subgroup of $U(n+1)$ corresponding to it as in **1**. We regard the spaces P^k, H^k and $\mathcal{H}^k$ as G-modules. Let χ_k (resp. $\tilde{\chi}_k$) be the character of the G-module P^k (resp. H^k). Then by Proposition 2.1, we have

$$\chi_k = \tilde{\chi}_k - \tilde{\chi}_{k-2} \,, \tag{3.1}$$

where $\tilde{\chi}_{-t}=0$ for $t>0$, since r^2 is invariant by G. The space P^k has a base consisting of all monomials of the form

$$z^I \cdot \bar{z}^J = (z_0)^{i_0} \cdots (z_n)^{i_n} \cdot (\bar{z}_0)^{j_0} \cdots (\bar{z}_n)^{j_n} \,, \tag{3.2}$$

where $i_0,\cdots,i_n,j_0,\cdots,j_n \geqq 0$ and $i_0+\cdots+i_n+j_0+\cdots+j_n=k$. Let g be the generator of G and $\gamma=\exp 2\pi\sqrt{-1}/q$ as in **1**. Then for any monomial $z^I \cdot \bar{z}^J$, we have

$$g^l(z^I \cdot \bar{z}^J) = \gamma^{l(i_0p_0+\cdots+i_np_n-j_0p_0-\cdots-j_np_n)} z^I \cdot \bar{z}^J \,. \tag{3.3}$$

Consider the formal expansion of

$$\prod_{i=0}^{n} (1+\gamma^{p_i l}z+\gamma^{2p_i l}z^2+\cdots)(1+\gamma^{-p_i l}z+\gamma^{-2p_i l}z^2+\cdots) \,. \tag{3.4}$$

Then it is easy to see that $\tilde{\chi}_k(g^l)$ is equal to the z^k's coefficient of (3.4). On the domain $\{z\in\boldsymbol{C}: |z|<1\}$, the above power series converges to the function

$$\frac{1}{\prod_{i=0}^{n}(1-\gamma^{p_i l}z)(1-\gamma^{-p_i l}z)}. \tag{3.5}$$

Now, we consider the generating function $F(z)$ associated to the infinite series $\{\dim E_{k(n+2k)}\}_{k=0}^{\infty}$, *i.e.*,

$$F(z)=\sum_{k=0}^{\infty}(\dim E_{k(k+2n)})z^k. \tag{3.6}$$

By Corollary 1.4, the generating function $F(z)$ determines the spectrum of $L(q:p_0,\cdots,p_n)$, so that we shall call the function $F(z)$ the generating function associated to the spectrum of $L(q:p_0,\cdots,p_n)$. Now, consider another lens space $L(q':p_0',\cdots,p_n')$ and denote by $E(z)$ the generating function associated to the spectrum of $L(q':p_0',\cdots,p_n')$. Then we have

Proposition 3.1. *The lens space $L(q;p_0,\cdots,p_n)$ is isospectral to $L(q':p_0',\cdots,p_n')$ if and only if*

$$F(z)=E(z). \tag{3.7}$$

Theorem 3.2. *Let $L(q:p_0,\cdots,p_n)$ be a lens space and $F(z)$ the generating function associated to the spectrum of $L(q:p_0,\cdots,p_n)$. Then $F(z)$ has the following form on the the domain $\{z\in\boldsymbol{C}:|z|<1\}$;*

$$F(z)=\frac{1}{q}\sum_{l=0}^{q-1}\frac{1-z^2}{\prod_{i=0}^{n}(1-\gamma^{p_i l}z)(1-\gamma^{-p_i l}z)}. \tag{3.8}$$

Proof. By Corollary 2.3, we have

$$F(z)=\sum_{k=0}^{\infty}(\dim \mathcal{H}_G^k)z^k. \tag{3.9}$$

On the other hand by Proposition 2.2 and (3.1), we have

$$\dim \mathcal{H}_G^k=\frac{1}{q}\sum_{l=0}^{q-1}(\tilde{\chi}_k(g^l)-\tilde{\chi}_{k-2}(g^l)). \tag{3.10}$$

Note that, for a nontrivial irreducible representation of G, the sum $\sum_{g\in G}\chi(g)$ of its character is zero.

By (3.5), (3.9) and (3.10), we have on the domain $\{z\in\boldsymbol{C}:|z|<1\}$

$$\begin{aligned}qF(z)&=q\sum_{k=0}^{\infty}(\dim \mathcal{H}_G^k)z^k\\&=\sum_{l=0}^{q-1}\sum_{k=0}^{\infty}(\tilde{\chi}_k(g^l)z^k-\tilde{\chi}_{k-2}(g^l)z^k)\\&=\sum_{l=0}^{q-1}\frac{1-z^2}{\prod_{i=0}^{n}(1-\gamma^{p_i l}z)(1-\gamma^{-p_i l}z)}.\end{aligned}$$

q.e.d.

$F(z)$ can be considered as a meromorphic function on the whole complex plane $\boldsymbol{C}$. Any pole of $F(z)$ is an *q-th* root of one. Especially, $F(z)$ has a pole of order $(2n+1)$ at $z=1$, and

$$\lim_{z\to 1}(1-z)^{2n+1}F(z)=\frac{2}{q}. \tag{3.11}$$

Thus, we have proved

Corollary 3.3. *Assume $L(q:p_0,\cdots,p_n)$ is isospectral to $L(q':p_0',\cdots,p_n')$. Then we have*

$$q=q'.$$

Corollary 3.4. *Assume $L(q:p_0,\cdots,p_n)$ is a homogeneous lens space and isospectral to $L(q:p_0',\cdots,p_n')$. Then $L(q:p_0',\cdots,p_n')$ is homogeneous and isometric to $L(q:p_0,\cdots,p_n)$.*

Proof. Let $F(z)$ be the generating function associated to the spectrum of $L(q:p_0,\cdots,p_n)$. Then $F(z)$ has a pole of order $(n+1)$ or $(2n+1)$ at $z=$any *q-th* root of one if and only if for any $i,j(0\leqq i,j\leqq n)$, we have either $p_i\equiv p_j \pmod q$ or $p_i\equiv -p_j \pmod q$. By proposition 1.2, this condition holds if and only if $L(q:p_0,\cdots,p_n)$ is homogeneous. By our assumption and Proposition 3.1, the generating function associated to the spectrum of $L(q:p_0',\cdots,p_n')$ has also the same condition as $F(z)$ so that $L(q:p_0',\cdots,p_n')$ is homogeneous. By Proposition 1.2, this space is isometric to $L(q:p_0,\cdots,p_n)$. q.e.d.

REMARK. M. Tanaka [10] obtained Corollary 3.4 for 3-dimensional lens spaces.

4. Three dimensional case

Hereafter in this paper, we consider only 3-dimensional lens spaces. Let $L(q:p_0,p_1)$ be a lens space. Choosing a suitable generator for its defining cyclic group G, we may assume $p_0=1$. From now on, a lens space $L(q:1,p)$ is simply denoted by $L(q:p)$. Assume two lens spaces $L(q:p_1)$ and $L(s:p_2)$ are isospectral to each other. Then by Corollary 3.3, we have $q=s$. Moreover, assume $p_1\not\equiv\pm 1 \pmod q$. Then by Corollary 3.4, we have also $p_2\not\equiv\pm 1 \pmod q$.

Now, we rewrite Proposition 1.1 for 3-dimensional lens spaces.

Proposition 4.1. *Let $L(q:p_1)$ and $L(q:p_2)$ be 3-dimensional lens spaces. Then, the lens space $L(q:p_1)$ is isometric to $L(q:p_2)$ if either*

$$p_1\pm p_2\equiv 0 \pmod q, \tag{4.1}$$

or

$$p_1p_2\equiv\pm 1 \pmod q. \tag{4.2}$$

Proof. By Proposition 1.1, $L(q:p_1)$ is isometric to $L(q:p_2)$ if there exists an integer l such that
either

$$\begin{cases} l \equiv \pm 1 & (\mathrm{mod}\ q) \\ lp_1 \equiv \pm p_2 & (\mathrm{mod}\ q)\,, \end{cases} \tag{4.3}$$

or

$$\begin{cases} l \equiv \pm p_2 & (\mathrm{mod}\ q) \\ lp_1 \equiv \pm 1 & (\mathrm{mod}\ q)\,. \end{cases} \tag{4.4}$$

Now, it is easily seen that (4.3) (resp. (4.4)) is equivalent to (4.1) (resp. (4.2)). This proves Proposition 4.1. q.e.d.

For two integers a and b, we denote by (a,b) the greatest common divisor of a and b.

Lemma 4.2. *Let q be a positive integer $\geqq 2$ and p an integer prime to q. Choose an integer p^* satisfying $pp^* \equiv 1$ (mod q). Then have*

$$(p+1, q) = (p^*+1, q) \tag{4.5}$$

and

$$(p-1, q) = (p^*-1, q)\,. \tag{4.6}$$

Proof. Since p is prime to q, we have

$$(p^*+1, q) = (p(p^*+1), q) = (p+1, q)$$

and

$$(p^*-1, q) = (p(p^*-1), q) = (p-1, q)\,, \qquad \text{q.e.d.}$$

The following lemma is easy to see.

Lemma 4.3. *Let q,p and p^* be as in Lemma* 4.2. *Let k be an integer such that*

$$(p+1)k \equiv 0 \quad (\mathrm{mod}\ q) \tag{4.7}$$

and

$$(p-1)k \equiv 0 \quad (\mathrm{mod}\ q)\,. \tag{4.8}$$

Then we have

$$(p^*+1)k \equiv 0 \quad (\mathrm{mod}\ q) \tag{4.9}$$

and

$$(p^*-1)k \equiv 0 \quad (\mathrm{mod}\ q)\,. \tag{4.10}$$

Lemma 4.4. *Suppose $L(q:p_1)$ is isospectral to $L(q:p_2)$ and $p_1 \not\equiv \pm 1$ (mod q). Then we have*

either

$$\begin{cases}(p_1-1, q) = (p_2-1, q)\\ (p_1+1, q) = (p_2+1, q)\end{cases} \tag{4.11}$$

or

$$\begin{cases}(p_1+1, q) = (p_2-1, q)\\ (p_1-1, q) = (p_2+1, q)\,.\end{cases} \tag{4.12}$$

Moreover the greatest common divisor $((p_1-1,q),(p_1+1,q))$ *is equal to* 1 *or* 2. *When* q *is odd (resp. even), it is necessarily* 1 *(resp.* 2*).*

Proof. The last statement is easy to see, since $(p_1+1)-(p_1-1)=2$ and p_1 is odd for even q.

Now, we shall give a proof of Lemma 4.4 in the case q is odd. Let $F_1(z)$ (resp. $F_2(z)$) be the generating function associated to the spectrum of $L(q:p_1)$ (resp. $L(q:p_2)$). By our assumption and Proposition 3.1, $F_1(z)=F_2(z)$. It is clear that if $F_1(z)$ has a pole of order 2 at γ^k $(0<k<q)$, then k must satisfy either $(p_1+1)k\equiv 0 \pmod q$ or $(p_1-1)k\equiv 0 \pmod q$. Conversely, if k satisfies either $(p_1+1)k\equiv 0 \pmod q$ or $(p_1-1)k\equiv 0 \pmod q$, then $F_1(z)$ has a pole of order 2 at $z=\gamma^k$. In fact, if k satisfies $(p_1+1)k\equiv 0 \pmod q$ (resp. $(p_1-1)k\equiv 0 \pmod q$), then we have

$$\lim_{z\to\gamma^k}(z-\gamma^k)^2F_1(z) = \frac{2}{q(\gamma^{-2k}-1)} \neq 0$$

(resp.

$$\lim_{z\to\gamma^k}(z-\gamma^k)^2F_1(z) = \frac{2}{q(\gamma^{2k}-1)} \neq 0)\,.$$

By this fact, we can see easily that if $(p_1+1,q)=(p_1-1,q)=1$, then $(p_2+1,q)=(p_2-1,q)=1$.

Now, assume $d_1=(p_1+1,q)>1$. Then at $z=\gamma^{q/d_1}$, $F_1(z)$ has a pole of order 2. Since $F_1(z)=F_2(z)$, $F_2(z)$ has also a pole of order 2 at γ^{q/d_1}. Hence, we have either $(p_2+1)\frac{q}{d_1}\equiv 0 \pmod q$ or $(p_2-1)\frac{q}{d_1}\equiv 0 \pmod q$. Therefore d_1 is a divisor of either $d_2=(p_2+1,q)$ or $e_2=(p_2-1,q)$. We may assume d_1 is a divisor of d_2. Since $d_2\geqq d_1>1$, we can apply the same argument as the above and we see that d_2 is a divisor of either d_1 or $e_1=(p_1-1,q)$. If d_2 is a divisor of d_1, then we have $d_2=d_1$. Suppose d_2 is a divisor of e_1. Since d_1 is a divisor of d_2, d_1 is a divisor of e_1. Since $d_1>1$, this contradicts the last statement in our Lemma 4.4. If $e_1>1$ (resp. $e_2>1$), then in the same way as before, we have either $e_1=e_2$ or $e_1=d_2$ (resp. $e_2=d_1$). But the latter condition contradicts also the last statement in our Lemma 4.4. Thus we have Lemma 4.4 when q is odd. By slight modification of the above argument, we can prove Lemma 4.4 when q is even. q.e.d.

The following corollary can be obtained easily by using Lemma 4.4.

Corollary 4.5. *Let $L(q:p_1)$ and $L(q:p_2)$ be as in Lemma* 4.4. *Let k be an integer such that*

$$(p_1+1)k\equiv 0 \pmod q \tag{4.13}$$

and

$$(p_1-1)k\equiv 0 \pmod q . \tag{4.14}$$

Then we have

$$(p_2+1)k\equiv 0 \pmod q \tag{4.15}$$

and

$$(p_2-1)k\equiv 0 \pmod q . \tag{4.16}$$

Proposition 4.6. *Let $L(q:p_1)$ and $L(q:p_2)$ be as in Lemma* 4.4. *Then for any integer k satisfying* (4.13) *and* (4.14), *we have*

$$\begin{aligned}(4.17)\qquad &\frac{1}{1-\gamma^{-(p_1+1)k}}-\frac{1}{1-\gamma^{-(p_1-1)k}}+\frac{1}{1-\gamma^{-(p_1^*+1)k}}-\frac{1}{1-\gamma^{-(p_1^*-1)k}}\\ &=\frac{1}{1-\gamma^{-(p_2+1)k}}-\frac{1}{1-\gamma^{-(p_2-1)k}}+\frac{1}{1-\gamma^{-(p_2^*+1)k}}-\frac{1}{1-\gamma^{-(p_2^*-1)k}} .\end{aligned}$$

Proof. Let k be an integer satisfying (4.13) and (4.14). Then by multiplying (4.13) and (4.14) by p_1^*, we have $(p_1^*+1)k\equiv 0 \pmod q$ and $(p_1^*-1)k\equiv 0 \pmod q$. We calculate the residue of $F_1(z)$ at $z=\gamma^k$.

$$\begin{aligned}&\lim_{z\to\gamma^k}(z-\gamma^k)F_1(z)\\ &=\frac{1}{q}\lim_{z\to\gamma^k}(z-\gamma^k)\sum_{l=0}^{q-1}\frac{1-z^2}{(1-\gamma^{p_1 l}z)(1-\gamma^{-p_1 l}z)(1-\gamma^l z)(1-\gamma^{-l}z)}\\ &=-\frac{2}{q}\left\{\frac{\gamma^k}{(1-\gamma^{(p_1+1)k})(1-\gamma^{-(p_1-1)k})}+\frac{\gamma^k}{(1-\gamma^{(p_1^*+1)k})(1-\gamma^{-(p_1^*-1)k})}\right\}\\ &=\frac{2}{q}\left\{\frac{\gamma^k}{\gamma^{(p_1+1)k}(1-\gamma^{-(p_1+1)k})(1-\gamma^{-(p_1-1)k})}\right.\\ &\qquad\left.+\frac{\gamma^k}{\gamma^{(p_1^*+1)k}(1-\gamma^{-(p_1^*+1)k})(1-\gamma^{-(p_1^*-1)k})}\right\}\\ &=-\frac{2}{q}\frac{\gamma^k}{\gamma^{(p_1+1)k}(\gamma^{-(p_1-1)k}-\gamma^{-(p_1+1)k})}\left\{\frac{1}{1-\gamma^{-(p_1+1)k}}-\frac{1}{1-\gamma^{-(p_1-1)k}}\right\}\\ &\quad-\frac{2}{q}\frac{\gamma^k}{\gamma^{(p_1^*+1)k}(\gamma^{-(p_1^*-1)k}-\gamma^{-(p_1^*+1)k})}\left\{\frac{1}{1-\gamma^{-(p_1^*+1)k}}-\frac{1}{1-\gamma^{-(p_1^*-1)k}}\right\}\\ &=-\frac{2}{q}\frac{\gamma^k}{(\gamma^{2k}-1)}\left\{\frac{1}{1-\gamma^{-(p_1+1)k}}-\frac{1}{1-\gamma^{-(p_1-1)k}}+\frac{1}{1-\gamma^{-(p_1^*+1)k}}-\frac{1}{1-\gamma^{-(p_1^*-1)k}}\right\} .\end{aligned}$$

Since $F_1(z)=F_2(z)$, we have the similar result for $F_2(z)$. Now, we obtain (4.17) q.e.d.

Corollary 4.7. *Let $L(q:p_1)$, $L(q:p_2)$ and k be as in Corollary* 4.5. *Then we have*

$$\begin{aligned}(4.18)\quad &\cot\frac{\pi}{q}(p_1+1)k-\cot\frac{\pi}{q}(p_1-1)k+\cot\frac{\pi}{q}(p_1^*+1)k-\cot\frac{\pi}{q}(p_1^*-1)k\\ &-\cot\frac{\pi}{q}(p_2+1)k+\cot\frac{\pi}{q}(p_2-1)k-\cot\frac{\pi}{q}(p_2^*+1)k+\cot\frac{\pi}{q}(p_2^*-1)k=0.\end{aligned}$$

Proof. Using an elementary formula;

$$\cot\theta=-\sqrt{-1}\left(1-\frac{2}{1-e^{-2\sqrt{-1}\theta}}\right),$$

we can obtain easily (4.18) from (4.17). q.e.d.

5. Key Lemma

In this section we shall give a key Lemma to show our Main Theorem. We denote by $\boldsymbol{Q}$ the field of rational numbers and by Φ_q the *q-th* cyclotomic polynomical. The following theorem is due to S. Chowla [4], and A. Baker, B.J. Birch and E.A. Wirsing [1].

Theorem 5.1. *If f is a nonvanishing function defined on the integers with algebraic numbers such that* (i) *for any integer r, $f(r+q)=f(r)$,* (ii) *$f(r)=0$ if $1<(r,q)<q$ and* (iii) *Φ_q is irreducible over $\boldsymbol{Q}(f(1),\cdots,f(q))$, then*

$$(5.1)\qquad \sum_{n=1}^{\infty}\frac{f(n)}{n}\neq 0.$$

Let $\Gamma(z)$ be the Gamma-function. Define $\psi(z)=\dfrac{\Gamma'(z)}{\Gamma(z)}$, where $\Gamma'(z)=\dfrac{d}{dz}\Gamma(z)$. Then we have

$$(5.2)\qquad \psi(1-z)-\psi(z)=\pi\cot\pi z,$$

(see p. 240 in [12]).
The generalized Zeta-function

$$\zeta(s,a)=\sum_{n=0}^{\infty}\frac{1}{(n+a)^s},$$

where a is a constant with $0<a\leqq 1$, is absolutely convergent and holomorphic function on $\{s\in\boldsymbol{C}: Re\ s>1\}$. It satisfies

$$(5.3)\qquad \zeta(s,a)-\frac{1}{s-1}=-\psi(a)+o(s-1),$$

where $\lim_{s\to 1}\frac{o(s-1)}{s-1}=0$, (see p. 271 in [2] [12]).

Lemma 5.2. *Let* $\{a_n\}_{n=1}^{\infty}$ *be an infinite sequence of complex numbers. Assume the sums* $A_n=\sum_{k=1}^{n} a_k$ *are bounded. Then the series*

$$h(s)=\sum_{n=1}^{\infty}\frac{a_n}{n^s}$$

converges for all real $s>0$. *For any* $\delta>0$, *its convergence is uniform in the interval* $[\delta, \infty)$, *so that the function* $h(s)$ *is continuous on* $(0, \infty)$.

Proof. See p. 331 in [3].

Under the above preparations, we give our key lemma.

Lemma 5.3. *Let* q *be an arbitrary natural number. Then the real numbers*

$$\{\cot\frac{\pi}{q}k: 1\leqq k<\frac{q}{2}, (k, q)=1\}$$

are linearly independent over $\boldsymbol{Q}$.

Proof. Let f be a nonvanishing function defined on the integers with rational numbers such that (i) for any integer, r, $f(r+q)=f(r)$, (ii) $f(r)=0$ if $1<(r,q)<q$ and (iii) $f(r)+f(q-r)=0$, where $1\leqq r<q$. Then the function f satisfies the assumption for f in Theorem 5.1, so that we have

$$\sum_{n=1}^{\infty}\frac{f(n)}{n}\neq 0\,. \tag{5.4}$$

On the other hand, using (i) and (iii), we see easily that the sequence $\{f(n)\}_{n=1}^{\infty}$ satisfies the assumption in Lemma 5.2. Thus the function

$$h(s)=\sum_{n=1}^{\infty}\frac{f(n)}{n^s} \tag{5.5}$$

is continuous on the interval $(0, \infty)$.
Using (5.2), (5.3) and the conditions for f, we have for real $s>1$,

$$\begin{aligned}\sum_{n=1}^{\infty}\frac{f(n)}{n^s}&=\sum_{m=1}^{q}\sum_{n=0}^{\infty}\frac{f(m)}{(nq+m)^s}\\&=\frac{1}{q^s}\sum_{m=1}^{q}f(m)\sum_{n=0}^{\infty}\frac{1}{\left(n+\frac{m}{q}\right)^s}\\&=\frac{1}{q^s}\sum_{m=1}^{q}f(m)\left\{\frac{1}{s-1}-\psi\left(\frac{m}{q}\right)+o(s-1)\right\}\end{aligned} \tag{5.6}$$

$$= \frac{\pi}{q^s} \sum_{1 \leqq m < (q/2)} f(m) \cot \frac{\pi}{q} m + 0(s-1) .$$

By the continuity of $h(s)$ at $s=1$, we have

$$\sum_{n=1}^{\infty} \frac{f(n)}{n} = \frac{\pi}{q} \sum_{1 \leqq m < (q/2)} f(m) \cot \frac{\pi}{q} \neq 0 . \tag{5.7}$$

The numbers $f(m)$ $(1 \leqq m < \frac{q}{2}, (m, q)=1)$ can take any rational numbers. This implies Lemma 5.3. q.e.d.

6. Proof of Main Theorem for odd prime q

In the following sections, we shall give a proof of our Main Theorem stated in the introduction for the case where q is an odd prime, $l^\nu (\nu \geqq 2)$, $2l^\nu (\nu \geqq 1)$ or $2^\nu (\nu \geqq 1)$ (l is an odd prime).

Lemma 6.1. *Main Theorem holds when* $q \leqq 10$.

Proof. Suppose $q \leqq 10$. Then the equivalence classes related by (4.3) and (4.4) are at most two classes. One is homogeneous and the other, if exists, is not. By Corollary 3.4, if two inequivalence classes appear, these are not isospectral to each other. q.e.d.

In the following, we assume $L(q:p_1)$ is isospectral to $L(q:p_2)$ and $q>10$ and also assume $p_1, p_2 \not\equiv \pm 1 \pmod q$.

Consider the formula (4.18). Note that if we have a θ with $\cot \pi\theta < 0$, then we can take $-\cot \pi\phi$ instead of $\cot \pi\theta$ with $0 < \phi < \frac{1}{2}$ and $\phi \equiv -\theta \pmod 1$, because of

$$\cot \pi(1-\theta) = -\cot \pi\theta . \tag{6.1}$$

Proof of Main Theorem for odd prime q

Assume q is an odd prime. By Proposition 4.1, it is sufficient to show that either $p_1 \equiv \pm p_2 \pmod q$ or $p_1 \equiv \pm p_2^* \pmod q$. Substituting $k=1$ (which satisfies (4.13) and (4.14)) in the formula (4.18), we have

$$\begin{aligned} &\cot \frac{\pi}{q}(p_1+1) - \cot \frac{\pi}{q}(p_1-1) + \cot \frac{\pi}{q}(p_1^*+1) - \cot \frac{\pi}{q}(p_1^*-1) \\ &- \cot \frac{\pi}{q}(p_2+1) + \cot \frac{\pi}{q}(p_2-1) - \cot \frac{\pi}{q}(p_2^*+1) + \cot \frac{\pi}{q}(p_2^*-1) = 0 . \end{aligned} \tag{6.2}$$

Assume $p_1 \not\equiv \pm p_2$ and $p_1 \not\equiv \pm p_2^* \pmod q$. Applying Lemma 5.3 to (6.2), only the following cases are possible

$$p_1+1 \equiv p_1-1 \pmod q , \tag{6.3}$$

$$p_1+1\equiv-(p_1^*+1) \pmod q, \tag{6.4}$$

$$p_1+1\equiv p_1^*-1 \pmod q. \tag{6.5}$$

It is clear that (6.3) can not happen. Suppose the case (6.4). We multiply both side by p_1. Then we have $p_1^2+p_1\equiv-(1+p_1) \pmod q$. Therefore we have $(p_1+1)^2\equiv 0 \pmod q$. Since q is an odd prime and $p_1\not\equiv -1 \pmod q$, this leads a contradiction.

Next, we consider the case (6.5). In this case we obtain also

$$p_1-1\equiv p_1^*+1 \pmod q. \tag{6.6}$$

Subtracting (6.6) from (6.5) both side separately, we obtain

$$2\equiv -2 \pmod q. \tag{6.7}$$

This contradicts our assumption $q>10$. q.e.d.

7. Proof of Main Theorem for $q=l^\nu$ (l is an odd prime and $\nu\geqq 2$)

In the case $(p_1+1, q)=(p_1-1, q)=1$, we can prove in the same way as in **6.**

Since $L(q:p_1)$ (resp. $L(q:p_2)$) is isometric to $L(q:q-p_1)$ (resp. $L(q:q-p_2)$), by Lemma 4.4, we may assume

$$(p_1+1, q) = (p_2+1, q) = l^\mu, \tag{7.1}$$

where $\nu>\mu\geqq 1$.
Since l is an odd prime, we have $(p_1-1, q)=1$. Therefore by Lemma 4.2, we have

$$\begin{cases}(p_1+1, q) = (p_1^*+1, q) = (p_2+1, q) = (p_2^*+1, q) = l^\mu \\ (p_1-1, q) = (p_1^*-1, q) = (p_2-1, q) = (p_2^*-1, q) = 1\,. \end{cases} \tag{7.2}$$

Since $k=1$ and $k=l^{\nu-\mu}-1$ satisfy (4.13) and (4.14), by Corollary 4.7, we have

$$\begin{aligned}&\cot\frac{\pi}{q}(p_1+1)-\cot\frac{\pi}{q}(p_1-1)+\cot\frac{\pi}{q}(p_1^*+1)-\cot\frac{\pi}{q}(p_1^*-1)\\ &-\cot\frac{\pi}{q}(p_2+1)+\cot\frac{\pi}{q}(p_2-1)-\cot\frac{\pi}{q}(p_2^*+1)+\cot\frac{\pi}{q}(p_2^*-1)=0\,,\end{aligned} \tag{7.3}$$

$$\begin{aligned}&-\cot\frac{\pi}{q}(p_1+1)-\cot\frac{\pi}{q}(p_1-1)k-\cot\frac{\pi}{q}(p_1^*+1)-\cot\frac{\pi}{q}(p_1^*-1)k\\ &+\cot\frac{\pi}{q}(p_2+1)+\cot\frac{\pi}{q}(p_2-1)k+\cot\frac{\pi}{q}(p_2^*+1)+\cot\frac{\pi}{q}(p_2^*-1)k=0\,,\end{aligned} \tag{7.4}$$

where $k=l^{\nu-\mu}-1$.

Taking the sum of (7.3) and (7.4), we have

$$(7.5)\quad -\cot\frac{\pi}{q}(p_1-1)-\cot\frac{\pi}{q}(p_1-1)k-\cot\frac{\pi}{q}(p_1^*-1)-\cot\frac{\pi}{q}(p_1^*-1)k$$
$$+\cot\frac{\pi}{q}(p_2-1)+\cot\frac{\pi}{q}(p_2-1)k+\cot\frac{\pi}{q}(p_2^*-1)+\cot\frac{\pi}{q}(p_2^*-1)k=0\,.$$

Since k is prime to q, all the integers p_1-1, $(p_1-1)k$, p_1^*-1, $(p_1^*-1)k$, p_2-1, $(p_2-1)k$, p_2^*-1 and $(p_2^*-1)k$ are prime to q. Suppose $p_1\not\equiv\pm p_2 \pmod q$ and $p_1\not\equiv\pm p_2^* \pmod q$. Then applying Lemma 5.3 to (7.5), only the following cases are possible;

$$(7.6)\qquad p_1-1\equiv-(p_1-1)k \pmod q\,,$$

$$(7.7)\qquad p_1-1\equiv-(p_1^*-1) \pmod q\,,$$

$$(7.8)\qquad p_1-1\equiv-(p_1^*-1)k \pmod q\,,$$

$$(7.9)\qquad p_1-1\equiv(p_2-1)k \pmod q\,,$$

$$(7.10)\qquad p_1-1\equiv(p_2^*-1)k \pmod q\,.$$

In case (7.6), we obtain $(p_1-1)(k+1)\equiv0 \pmod q$. Since p_1-1 is prime to q, $k+1=l^{\nu-\lambda}$ and $\nu>\nu-\mu\geqq1$, the case (7.6) can not happen.

In case (7.7), in the same way as in case (6.4), we obtain $(p_1-1)^2\equiv0 \pmod q$. This contradicts the facts $(p_1-1,\ q)=1$ and $p_1\not\equiv-1 \pmod q$.

Next, we consider the case (7.8). Multiplying by p_1 both side in (7.8), we obtain $(p_1-1)(p_1-k)\equiv0 \pmod q$. Hence, we have

$$(7.11)\qquad p_1\equiv k \pmod q\,.$$

By the same argument for p_2 as in the cases (7.6) and (7.7), we have either

$$(7.12)\qquad p_2-1\equiv-(p_2^*-1)k \pmod q$$

or

$$(7.13)\qquad p_2-1\equiv(p_1-1)k \pmod q\,.$$

In case (7.12), in the same way as before, we get

$$(7.14)\qquad p_2\equiv k \pmod q\,.$$

Together this with (7.10), we have

$$(7.15)\qquad p_1\equiv p_2 \pmod q\,.$$

This contradicts our assumption $p_1\not\equiv p_2 \pmod q$.

In case (7.13), by the same argument for p_2 as in the cases (7.6) and (7.7),

we have

$$(p_2^*-1)\equiv-(p_2-1)k \pmod{q}. \tag{7.16}$$

Using this and in the same way as before, we get

$$p_2^*\equiv k \pmod{q}. \tag{7.17}$$

Together this with (7.11), we have

$$p_1\equiv p_2^* \pmod{q}. \tag{7.18}$$

Thus we have a contradiction.

By the above arguments, we see;

(7.19) *Each two members of the first four terms (resp. the second four terms) in* (7.5) *do not cancel to each other.*

Next, we consider the case (7.9). Then by (7.19), we have either

$$(p_1-1)k\equiv p_2-1 \pmod{q} \tag{7.20}$$

or

$$(p_1-1)k\equiv p_2^*-1 \pmod{q}. \tag{7.21}$$

Together (7.9) with (7.20), we obtain $k^2\equiv 1 \pmod{q}$. Hence, we have

$$(k+1)(k-1)\equiv 0 \pmod{q}. \tag{7.22}$$

Since $\nu>\nu-\mu\geqq 1$ and l is odd, $(k-1)$ is prime to l and $0<(k+1)<q$. Thus the case (7.20) can not happen.

Now, we assume (7.9) and (7.21). Then, by our assumption and (7.19), we have

$$(p_1^*-1)\equiv(p_2^*-1)k \pmod{q} \tag{7.23}$$

Substituting (7.9) to (7.21) and (7.21) to (7.23) respectively, we have

$$(p_2-1)k^2\equiv(p_2^*-1) \pmod{q} \tag{7.24}$$

and

$$(p_1^*-1)\equiv(p_1-1)k^2 \pmod{q} \tag{7.25}$$

respectively.
From (7.24) and (7.25), in the same way as before, we have

$$p_2^*\equiv -k^2 \pmod{q} \tag{7.26}$$

and

$$p_1\equiv -k^2 \pmod{q} \tag{7.27}$$

respectively.
Therefore, we have

$$p_1 \equiv p_2^* \pmod{q}, \tag{7.28}$$

which contradicts our assumption. Thus, the case (7.9) can not happen.

In the same way as for the above, we can see the case (7.10) can not happen. q.e.d.

8. Proof of Main Theorem for $q=2l^\nu$ (l is an odd prime and $\nu \geqq 1$)

First, we consider the case

$$(p_1+1, q) = (p_1-1, q) = 2. \tag{8.1}$$

Since $k=1$ satisfies (4.13) and (4.14), by Corollary 4.7, we have

$$\begin{aligned} &\cot\frac{\pi}{q_0}\frac{p_1+1}{2} - \cot\frac{\pi}{q_0}\frac{p_1-1}{2} + \cot\frac{\pi}{q_0}\frac{p_1^*+1}{2} - \cot\frac{\pi}{q_0}\frac{p_1^*-1}{2} \\ &- \cot\frac{\pi}{q_0}\frac{p_2+1}{2} + \cot\frac{\pi}{q_0}\frac{p_2-1}{2} - \cot\frac{\pi}{q_0}\frac{p_2^*+1}{2} + \cot\frac{\pi}{q_0}\frac{p_2^*-1}{2} = 0, \end{aligned} \tag{8.2}$$

where $q_0=l^\nu$.
By (8.1), Lemma 4.2 and Lemma 4.4, all the integers $\frac{p_1\pm 1}{2}$, $\frac{p_1^*\pm 1}{2}$, $\frac{p_2\pm 1}{2}$ and $\frac{p_2^*\pm 1}{2}$ are prime to q_0. Applying Lemma 5.3 to (8.2), in the same way as in 6, we see either $p_1 \equiv \pm p_2 \pmod{q_0}$ or $p_1 \equiv \pm p_2^* \pmod{q_0}$. Since all the integers p_1, p_1^*, p_2 and p_2^* must be odd, we have either $p_1 \equiv \pm p_2 \pmod{q}$ or $p_1 \equiv \pm p_2^* \pmod{q}$, which proves our Main Theorem in this case.

Next, we consider the case where one of the integers (p_1+1) and (p_1-1) is divisible by l. Since $L(q:p_1)$ (resp. $L(q:p_2)$) is isometric to $L(q:q-p_1)$ (resp. $L(q:q-p_2)$), by Lemma 4.4, we may assume

$$\begin{cases} (p_1+1, q) = (p_2+1, q) = 2l^\mu \\ (p_1-1, q) = (p_2-1, q) = 2, \end{cases} \tag{8.3}$$

where $\nu > \mu \geqq 1$.
Substituting by $k=1$ and $k=l^{\nu-\mu}-1$ (which satisfy (4.13) and (4.14)) in (4.18), and taking their sum, we obtain

$$\begin{aligned} &-\cot\frac{\pi}{q_0}\frac{p_1-1}{2} - \cot\frac{\pi}{q_0}\frac{p_1-1}{2}k - \cot\frac{\pi}{q_0}\frac{p_1^*-1}{2} - \cot\frac{\pi}{q_0}\frac{p_1^*-1}{2}k \\ &+\cot\frac{\pi}{q_0}\frac{p_2-1}{2} + \cot\frac{\pi}{q_0}\frac{p_2-1}{2}k + \cot\frac{\pi}{q_0}\frac{p_2^*-1}{2} + \cot\frac{\pi}{q_0}\frac{p_2^*-1}{2}k = 0, \end{aligned} \tag{8.4}$$

where $k=l^{\nu-\mu}-1$.

By (8.3) and Lemma 4.2, all the integers $\frac{p_1-1}{2}$, $\frac{p_1-1}{2}k$, $\frac{p_1^*-1}{2}$, $\frac{p_1^*-1}{2}k$, $\frac{p_2-1}{2}$, $\frac{p_2-1}{2}k$, $\frac{p_2^*-1}{2}$ and $\frac{p_2^*-1}{2}k$ are prime to q_0. Applying Lemma 5.3 to (8.4), in the same way as in **7**, we see either $p_1\equiv p_2 \pmod{q_0}$ or $p_1\equiv p_2^* \pmod{q_0}$. From this, as we have seen as before, we see either $p_1\equiv p_2 \pmod{q}$ or $p_1\equiv p_2^* \pmod{q}$, which proves Main Theorem in this case (8.3). Thus we have proved Main Theorem for $q=2l^\nu$. q.e.d.

9. Proof of Main Theorem for $q=2^\nu$ ($\nu\geqq 1$)

By Lemma 6.1, we may assume $\nu\geqq 4$. Since $q=2^\nu$, either p_1+1 or p_1-1 is divisible by 2^2. So that, by the same reason as in the preceding sections, we may assume

$$\text{(9.1)}\qquad \begin{cases}(p_1+1, q)=(p_2+1, q)=2^\mu\\ (p_1-1, q)=(p_2-1, q)=2\,,\end{cases}$$

where $\mu\geqq 2$.

First, assume $\nu-\mu=1$. Then it is easy to see that

$$p_1+1\equiv p_2+1\equiv 2^{\nu-1} \pmod{q_0}$$

which proves our assertion.

Next, assume $\nu-\mu\geqq 2$. Substituting $k=1$ and $k=2^{\nu-\mu}-1$ (which satisfy (4.13) and (4.14)) in (4.18) and taking their sum, we obtain;

$$\text{(9.2)}\qquad \begin{aligned}&-\cot\frac{\pi}{q_0}\frac{p_1-1}{2}-\cot\frac{\pi}{q_0}\frac{p_1-1}{2}k-\cot\frac{\pi}{q_0}\frac{p_1^*-1}{2}-\cot\frac{\pi}{q_0}\frac{p_1^*-1}{2}k\\ &+\cot\frac{\pi}{q_0}\frac{p_2-1}{2}+\cot\frac{\pi}{q_0}\frac{p_2-1}{2}k+\cot\frac{\pi}{q_0}\frac{p_2^*-1}{2}+\cot\frac{\pi}{q_0}\frac{p_2^*-1}{2}k=0\,,\end{aligned}$$

where $k=2^{\nu-\mu}-1$ and $q_0=2^{\nu-1}$.

Lemma 9.1. (i) *If* $p_1^2\equiv 1$ *(mod* q_0*), then* $p_1^*\equiv p_1+2^{\nu-1}$ *(mod* q*).* (ii) *If* $p_1\equiv p_2$ *(mod* q_0*) and* $p_1^2\equiv 1$ *(mod* q_0*), then* $p_1\equiv p_2$ *(mod* q*) or* $p_1\equiv p_2^*$ *(mod* q*).*

Proof. (i) Suppose $p_1^2\equiv 1 \pmod{q}$. Then we have $(p_1-1)(p_1+1)\equiv 0 \pmod{q}$. Since $(p_1-1)(p_1+1)\equiv 2^{\mu+1} \pmod{2^{\mu+2}}$ and $\nu>\mu+1>0$, we have a contradiction. Thus we have $p_1^2\equiv 1+2^{\nu-1} \pmod{q}$. Since $p_1(p_1+2^{\nu-1})\equiv p_1^2+2^{\nu-1}\equiv 1 \pmod{q}$, we have $p_1^*\equiv p_1+2^{\nu-1} \pmod{q}$. (ii) Assume $p_1\equiv p_2 \pmod{q_0}$ and $p_1^2\equiv 1 \pmod{q_0}$. Then we have $p_1\equiv p_2 \pmod{q}$ or $p_1\equiv p_2+2^{\nu-1} \pmod{q}$, and $p_1^*\equiv p_1+2^{\nu-1} \pmod{q}$. Hence, we have $p_1\equiv p_2 \pmod{q}$ or $p_1\equiv p_2^* \pmod{q}$. q.e.d.

Lemma 9.2. *We have*

$$\frac{p_i-1}{2} \not\equiv -\frac{p_i-1}{2} k \quad (mod\ q_0) \tag{9.3}$$

and

$$\frac{p_i-1}{2} \not\equiv -\frac{p_i^*-1}{2} \quad (mod\ q_0)\,, \tag{9.4}$$

for $i=1,2$.

Proof. It sufficies to show Lemma 9.2 for $i=1$. Assume

$$\frac{p_1-1}{2} \equiv -\frac{p_1-1}{2} k \quad (\mathrm{mod}\ q_0)\,. \tag{9.5}$$

Then we obtain

$$(p_1-1)\,(k+1) \equiv 0 \quad (\mathrm{mod}\ q)\,. \tag{9.6}$$

Since $(p_1-1,\ q)=2$ and $k+1 \equiv 2^{\nu-\mu}$ (mod q), we have

$$(p_1-1)\,(k+1) \equiv 2^{\nu-\mu+1} \quad (\mathrm{mod}\ 2^{\nu-\mu+2})\,. \tag{9.7}$$

Since $\nu-\mu \geqq 2$ and $\mu \geqq 2$, we have

$$\nu > \nu-\mu+1 > 0\,. \tag{9.8}$$

So that the (9.6) contradicts (9.7).

Next, assume

$$\frac{p_1-1}{2} \equiv -\frac{p_1^*-1}{2} \quad (\mathrm{mod}\ q_0)\,. \tag{9.9}$$

Then we get

$$(p_1-1)^2 \equiv 0 \quad (\mathrm{mod}\ q)\,, \tag{9.10}$$

which is a contradiction because $(p_1-1)^2 \equiv 2^2$ (mod 2^3) and $\nu \geqq 4$. q.e.d

We assume $p_1 \not\equiv p_2$ (mod q) and $p_1 \not\equiv p_2^*$ (mod q). Applying Lemma 5.3 and Lemma 9.2 to (9.2), we see easily that only the following cases are possible; Case A,

$$\begin{cases} \dfrac{p_1-1}{2} \equiv -\dfrac{p_1^*-1}{2} k & (\mathrm{mod}\ q_0) \quad (9.11) \\ \dfrac{p_1-1}{2} k \equiv -\dfrac{p_1^*-1}{2} & (\mathrm{mod}\ q_0)\,, \quad (9.12) \end{cases}$$

Case B,

$$\begin{cases} \dfrac{p_1-1}{2} \equiv -\dfrac{p_1^*-1}{2} k & (\mathrm{mod}\ q_0) \quad (9.13) \\ \dfrac{p_1-1}{2} k \equiv \dfrac{p_2^*-1}{2} & (\mathrm{mod}\ q_0)\,, \quad (9.14) \end{cases}$$

Case C,

$$\begin{cases} \dfrac{p_1-1}{2} \equiv \dfrac{p_2-1}{2} k & \pmod{q_0} \quad (9.15) \\ \dfrac{p_2-1}{2} \equiv \dfrac{p_1-1}{2} k & \pmod{q_0}, \quad (9.16) \end{cases}$$

Case D,

$$\begin{cases} \dfrac{p_1-1}{2} \equiv \dfrac{p_2-1}{2} k & \pmod{q_0} \quad (9.17) \\ \dfrac{p_1-1}{2} k \equiv \dfrac{p_2^*-1}{2} & \pmod{q_0}, \quad (9.18) \end{cases}$$

and the cases where we interchange p_2 and p_2^* with each other in the cases B,C and D.

Here, we shall prove that, under our assumptions $p_1 \not\equiv p_2 \pmod{q}$ and $p_1 \not\equiv p_2^* \pmod{q}$, the cases A, B, C and D do not occure. The other cases can be treated in the same way as in cases B, C and D.

Case A.

In this case we have also

$$\frac{p_2-1}{2} \equiv -\frac{p_2^*-1}{2} k \pmod{q_0}. \quad (9.19)$$

From (9.11), (9.12) and (9.19), we obtain

$$p_1 \equiv p_1^* \equiv p_2 \equiv k \pmod{q_0}. \quad (9.20)$$

Since (9.20) shows the conditions in (ii) of Lemma 9.1, we have a contradiction. q.e.d.

Case B.

In this case we have also

$$\frac{p_2-1}{2} \equiv -\frac{p_2^*-1}{2} k \pmod{q_0}, \quad (9.21)$$

From (9.14) we obtain

$$p_2(p_1-1)k \equiv -(p_2-1) \pmod{q}. \quad (9.22)$$

By (9.13) and (9.21), we have in the same way as before

$$p_1 \equiv p_2 \equiv k \pmod{q_0}. \quad (9.23)$$

From this we have

$$(k-1)p_2 \equiv k(k-1) \pmod{q} \tag{9.24}$$

and

$$p_1 p_2 \equiv k^2 + 2^{\nu-1} \pmod{q}, \tag{9.25}$$

because $(k-1)$ is even and $p_1 \not\equiv p_2 \pmod{q}$.
Substituting (9.24) and (9.25) to (9.22), we obtain

$$(k^2+1)(k-1) \equiv 2^{\nu-1} \pmod{q}. \tag{9.26}$$

Since $\nu-\mu \geqq 1$, we have $k^2+1 \equiv 2 \pmod{2^2}$ and $k-1 \equiv 2 \pmod{2^2}$. Thus, we have a contradiction because $\nu-1 \geqq 3$. q.e.d.

Case C.

In this case we have also

$$\frac{p_1^*-1}{2} \equiv \frac{p_2^*-1}{2} k \pmod{q_0}. \tag{9.27}$$

Substituting (9.15) to (9.16), we obtain

$$(k+1)(k-1) \equiv 0 \pmod{q_0}. \tag{9.28}$$

Since $k+1=2^{\nu-\mu}$, $k-1=2^{\nu-\mu}-2$ and $\mu \geqq 2$, we see

$$\mu = 2. \tag{9.29}$$

Sustituting (9.29) to (9.15) and (9.27), we obtain

$$p_1 \equiv -p_2 + 2^{\nu-1} + 2 \pmod{q} \tag{9.30}$$

and

$$p_1^* \equiv -p_2^* + 2^{\nu-1} + 2 \pmod{q}. \tag{9.31}$$

Multiplying (9.30) by (9.31) both sides separately, we have

$$1 \equiv 1 - (2^{\nu-1}+2)(p_2+p_2^*) + (2^{\nu-1}+2)^2 \pmod{q}. \tag{9.32}$$

From this we have

$$p_2 + p_2^* \equiv 2 \pmod{q_0}. \tag{9.33}$$

First, suppose

$$p_2 + p_2^* \equiv 2 \pmod{q}. \tag{9.34}$$

Then, multiplying by p_2 in (9.34), we obtain

$$(p_2-1)^2 \equiv 0 \pmod{q}, \tag{9.35}$$

which contradicts $\nu \geqq 4$.

Next, suppose

$$p_2+p_2^* \equiv 2^{\nu-1}+2 \pmod{q}. \tag{9.36}$$

Then, by (9.30) and (9.36), we have

$$p_1 \equiv p_2^* \pmod{q}, \tag{9.37}$$

wih which contradicts our assumption. q.e.d.

Case D.

In this case we have also

$$\frac{p_1^*-1}{2} \equiv \frac{p_2^*-1}{2} k \pmod{q_0}, \tag{9.38}$$

$$\frac{p_1^*-1}{2} k \equiv \frac{p_2-1}{2} \pmod{q_0}. \tag{9.39}$$

Substituting (9.17) to (9.18), (9.18) to (9.38) and (9.38) to (9.39), we have

$$p_2^* \equiv p_1^* \equiv p_2 \equiv -k^2 \pmod{q_0}. \tag{9.40}$$

Since (9.40) shows the conditions in (ii) of Lemma 9.1, we have a contradiction. q.e.d.

OSAKA UNIVERSITY

References

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

[2] M. Berger, P. Gaudachon and E. Mazet: Le spectre d'une variété riemannienne, Lecture notes in Mathematics 194. Springer-Verlag, Berlin-Heidelberg-New York, 1971.

[3] Z.I. Borevich and I.R. Shafarevich: Number theory, Academic Press, New York and London, 1966.

[4] S. Chowla: *The nonexistence of nontrivial linear relations between the roots of a certain irreducible equation,* J. Number Theory **2** (1970), 120–123.

[5] M.M. Cohen: A course in simple-homotopy theory, Graduate Texts in Mathematics 10. Springer-Verlag, New York-Heidelberg-Berlin, 1970.

[6] Colin de Verdière: *Spectre du Laplacian et longueurs des géodésiques périodiques* II, Compositio Math. **27** (1973), 159–184.

[7] J.J. Duistermaat and V.W. Guillemin: *The spectrum of positive elliptic operators and periodic bicharacteristics,* Invent. Math. **29** (1975), 39–79.

[8] H.P. McKean, Jr. and I.M. Singer: *Curvature and eigenvalues of the Laplacian,* J. Differential Geometry **1** (1967), 43–69.

[9] T. Sakai: *On eigenvalues of Laplacian and curvature of Riemannian manifold,*

Tôhoku Math. J. **23** (1971), 589–603.

[10] M. Tanaka: *Compact riemannian manifolds which are isospectral to three dimenensional lens spaces* I, in Minimal Submanifolds and Geodesics, Kaigai Publication, Tokyo, 1978, 273–282.

[11] S. Tanno: *Eigenvalues of the Laplacian of Riemannian manifold,* Tôhoku Math. J. **25** (1973), 391–403.

[12] E.T. Wittaker and G.N. Watson: A course of modern analysis, 4-th edition, Cambridge University Press, 1927.

[13] J.A. Wolf: Spaces of constant curvature, McGraw-Hill, 1967.

[14] Y. Yomamoto: *On the number of lattice points in the square* $|x|+|y| \leqq u$ *with a certain congruence condition,* to appear.

[15] A. Ikeda: *On the spectrum of a riemannian manifold of positive constant curvature,* to appear.

[16] M. Tanaka: *Compact riemannian manifolds which are isospectral to three dimensional lens spaces* II, Proc. Fac. Sci. Tokai Univ. vol. **XIV** (1978), 11–34.