Cyclic coverings of an elliptic curve with two branch points and the gap sequences at the ramification points

by

JIRYO KOMEDA (Atsugi)

1. Introduction. Let $C$ be a complete non-singular irreducible algebraic curve of genus $g \geq 2$ defined over an algebraically closed field $k$ of characteristic 0, which is called a curve in this paper. Let $P$ be its point. A positive integer $\gamma$ is called a gap at $P$ if there exists a regular 1-form $\omega$ on $C$ such that $\text{ord}_P(\omega) = \gamma - 1$. We denote by $G(P)$ the set of gaps at $P$. Then the cardinality of $G(P)$ is equal to $g$. Now the sequence $\{\gamma_1, \ldots, \gamma_g\} = G(P)$ with $\gamma_i < \gamma_j$ for $i < j$ is called the gap sequence at $P$.

Let $\pi : C \to C'$ be a cyclic covering of curves of degree $d$ with total ramification points $P$. It is well known that in the case of $C' = \mathbb{P}^1$ and $d = 2$ we have $G(P) = \{1, 3, \ldots, 2g - 1\}$. In the case of $C' = \mathbb{P}^1$ and $d = 3$ (resp. 4) the gap sequences $G(P)$ are known (see [1], [2], [3] (resp. [4], Prop. 4.5)). If $C' = \mathbb{P}^1$ and $d$ is a prime number $\geq 5$, we can also determine the gap sequences $G(P)$ (for example, see [5], Prop. 1). In this paper we shall consider the case $C' = E$ where $E$ is an elliptic curve. If $d = 2$, then $G(P)$ are known ([4], Prop. 2.9, 3.10). However, for $d \geq 3$ there are only a few results on the gap sequences $G(P)$. For example, I. Kuribayashi and K. Komiya ([8], Th. 5) showed the following: If $\pi : C \to E$ is a cyclic covering of an elliptic curve of degree 6 which is branched over three points $P'_i$ ($i = 1, 2, 3$) such that $2\pi^{-1}(P'_i) = i$, then the gap sequence $G(P_1)$ can be determined, where $P_1$ denotes the point of $C$ over $P'_1$. Moreover, the author ([6], Lemma 4.6) showed the following: Let $E$ be an elliptic curve with the origin $Q'$. Let $P'_1$ (resp. $P'_2$) be a point of $E$ such that $P'_1 \neq Q'$ and $2[P'_1] = [Q']$ (resp. $P'_2 \neq Q'$ and $3[P'_2] = [Q']$), where for any positive integer $m$ and any point $P'$ of the elliptic curve $E$ the multiplication of $P'$ by $m$ is denoted by $m[P']$. Then there is an element $z$ of $K(E)$ such

---

1991 Mathematics Subject Classification: Primary 14H55; Secondary 14H30, 14H52, 11A05.
that \( \text{div}(z) = 4P'_1 + 3P'_2 - 7Q' \) where \( \mathbf{K}(E) \) denotes the function field of \( E \). Let \( \pi : C \to E \) be the surjective morphism of curves corresponding to the inclusion \( \mathbf{K}(E) \subset \mathbf{K}(E)(z^{1/7}) = \mathbf{K}(C) \). If \( P_2 \) denotes the point of \( C \) over \( P'_2 \), then the gap sequence \( G(P_2) \) is equal to \( \{1, 2, 3, 4, 5, 7, 13\} \). In this paper we shall prove the generalization of the above statement for the degree of the covering \( \pi : C \to E \), which is the following:

**Main Theorem.** Let \( g \geq 7 \). We can construct cyclic coverings \( \pi : C \to E \) of an elliptic curve \( E \) of degree \( g \) which have only two ramification points \( P_1 \) and \( P_2 \), which are totally ramified, such that

\[
G(P_1) = G(P_2) = \{1, \ldots, g - 2, g, 2g - 1\}.
\]

Now we consider the following situation. Let \( G \) be a finite subset of the set \( \mathbb{N} \) of positive integers such that the complement \( \mathbb{N}_0 \setminus G \) of \( G \) in the additive semigroup \( \mathbb{N}_0 \) of non-negative integers forms its subsemigroup. If the cardinality of \( G \) is \( g \), then \( \{\gamma_1, \ldots, \gamma_g\} = G \) with \( \gamma_i < \gamma_j \) for \( i < j \) is called a gap sequence of genus \( g \). We say that a gap sequence \( G \) is Weierstrass if there exists a pointed curve \( (C, P) \) such that \( G = G(P) \). Let \( a(G) = \min\{h \in \mathbb{N}_0 \setminus G \mid h > 0\} \). Then \( a(G) \leq g + 1 \). If \( a(G) = g + 1 \), then \( G = \{1, \ldots, g\} \).

In this case \( G \) is Weierstrass, because for any point \( P \) of a curve of genus \( g \) except finitely many points we have \( G(P) = \{1, \ldots, g\} \). If \( a(G) = g \), then there is a positive integer \( k \leq g - 1 \) such that \( G = \{1, \ldots, g - 1, g + k\} \). These \( g - 1 \) kinds of gap sequences are Weierstrass (cf. [9], Th. 14.5). If \( l \) is a fixed integer \( \geq 2 \), then for any sufficiently large \( g \) there exists a non-Weierstrass gap sequence \( G \) of genus \( g \) such that \( a(G) = g - l \) (cf. [7], Th. 3.5 and 4.5). Hence we pose the following problem: Is any gap sequence \( G \) of genus \( g \) with \( a(G) = g - 1 \) Weierstrass?

Now we say that \( G \) is primitive if \( 2a(G) > \gamma_g \). Since any gap sequence of genus \( g \leq 7 \) is Weierstrass (cf. [6], Th. 4.7), combining the Main Theorem with Lemma 1 we get the following:

Any non-primitive gap sequence \( G \) of genus \( g \) with \( a(G) = g - 1 \) is Weierstrass.

In Sections 2, 3 and 4 we construct our desired cyclic coverings \( \pi : C \to E \) of an elliptic curve in the cases when \( g \equiv 3, 1 \) and \( 0 \) mod 4 respectively. In Section 5 the case when \( g \equiv 2 \) mod 4 is treated. In this case we need an arithmetic lemma (Key Lemma 4) which is important for the constructions of the coverings \( \pi : C \to E \).

**2. The case** \( g \equiv 3 \) mod 4. First we prove the following:

**Lemma 1.** Let \( G \) be a non-primitive gap sequence of genus \( g \geq 3 \) with \( a(G) = g - 1 \). Then \( G = \{1, \ldots, g - 2, g, 2g - 1\} \).
Proof. Let \( G = \{ \gamma_1, \ldots, \gamma_g \} \) with \( \gamma_i < \gamma_j \) for \( i < j \). In view of \( a(G) = g-1 \) we must have \( \gamma_i = i \) for \( i \leq g-2 \) and \( \gamma_{g-1} \geq g \). Since \( G \) is non-primitive, we have \( \gamma_g > 2a(G) = 2g - 2 \). It is a well-known fact that \( \gamma_g \leq 2g - 1 \) (for example, see [4], Lemma 2.1), which implies that \( \gamma_g = 2g - 1 \). Suppose that \( \gamma_{g-1} \geq g+1 \). Then \( N_0 \setminus G \) contains \( g-1 \) and \( g \). Since \( N_0 \setminus G \) is a subsemigroup of \( N_0 \), we must have \( \gamma_g = 2g - 1 \in N_0 \setminus G \), which is a contradiction. Hence we obtain \( \gamma_{g-1} = g \). □

In the remainder of this section we will prove the Main Theorem in the case \( g \equiv 3 \mod 4 \) with \( g \geq 7 \).

Let \( g = 4h + 3 = 2n + 1 \) with \( h \in \mathbb{N} \) and \( n = 2h + 1 \). Let \( E \) be an elliptic curve over \( k \) with the origin \( Q' \). Let \( P'_1 \) be a point of \( E \) such that \( P'_1 \neq Q' \) and \( 2[P'_1] = [Q'] \). Moreover, \( P'_2 \) denotes a point of \( E \) such that \( n[P'_2] = [Q'] \) and \( m[P'_2] \neq [Q'] \) for any positive integer \( m < n \). Hence in view of \( g \geq 7 \) we have \( P'_2 \neq Q' \). Moreover, \( P'_1 \neq P'_2 \), because \( 2hP'_2 + P'_2 = nP'_2 \sim nQ' = (2h + 1)Q' \sim 2hP'_1 + Q' \). Now we have

\[
(n + 1)P'_1 + nP'_2 \sim 2(h + 1)P'_1 + nQ' \sim 2(h + 1)Q' + nQ' = (2n + 1)Q'.
\]

Hence we may take \( z \in \mathbf{K}(E) \) such that \( \text{div}(z) = (n+1)P'_1 + nP'_2 -(2n+1)Q' \).

Let \( C \) be the curve whose function field \( \mathbf{K}(C) \) is \( \mathbf{K}(E)(z^{1/(2n+1)}) \). Moreover, \( \pi : C \rightarrow E \) denotes the surjective morphism of curves corresponding to the inclusion \( \mathbf{K}(E) \subset \mathbf{K}(C) \). Then we may take \( y \in \mathbf{K}(C) \) and \( \sigma \in \text{Aut}(\mathbf{K}(C)/\mathbf{K}(E)) \) such that

\[
\sigma(y) = \zeta_{2n+1} y \quad \text{and} \quad \text{div}_E(y^{2n+1}) = (n+1)P'_1 + nP'_2 -(2n+1)Q',
\]

where \( \zeta_{2n+1} \) is a primitive \((2n+1)\)th root of unity. Then there are only two branch points \( P'_i \) and \( P'_2 \) of \( \pi \). Moreover, \( \pi^{-1}(P'_i) \) consists of only one point \( P_i \) for \( i = 1, 2 \). Hence the ramification index of \( P_i \) is \( 2n + 1 \) for \( i = 1, 2 \). Therefore

\[
\text{div}(y) = (n+1)P_1 + nP_2 - \pi^*(Q'),
\]

where \( \pi^* \) denotes the pull-back of \( \pi \). If we denote by \( g \) the genus of \( C \), then by the Riemann–Hurwitz formula we have \( g = 2n + 1 \). Hence

\[
\text{div}(dy) = nP_1 + (n-1)P_2 - 2\pi^*(Q') + \sum_{i=1}^{3} \pi^*(R'_i),
\]

where \( R'_i \)'s are points of \( E \) which are distinct from \( P'_1, P'_2 \) and \( Q' \), because \( \text{div}(dy) \) is invariant under \( \text{Aut}(\mathbf{K}(C)/\mathbf{K}(E)) \).

We set

\[
D'_0 = -P'_1 - P'_2 - Q' + \sum_{i=1}^{3} R'_i,
\]
\[ D'_{2l+1} = -(2l + 2)Q' + lP_1' + lP_2' + \sum_{i=1}^{3} R'_i \quad \text{for } 0 \leq l \leq n - 1 \]

and

\[ D'_{2l} = -(2l + 1)Q' + lP_1' + (l - 1)P_2' + \sum_{i=1}^{3} R'_i \quad \text{for } 1 \leq l \leq n. \]

First we show that \( l(D'_0) = 1 \), i.e., \( D'_0 \) is linearly equivalent to 0, where for any divisor \( D' \) on \( E \) the number \( l(D') \) denotes the dimension of the \( k \)-vector space

\[ L(D') = \{ f \in K(E) \mid \text{div}_E(f) \geq -D' \}. \]

Since

\[ \sigma \left( \frac{dy}{y} \right) = \frac{d(\sigma y)}{\sigma y} = \frac{d(\zeta_{2n+1}y)}{\zeta_{2n+1}y} = \frac{dy}{y}, \]

the 1-form \( dy/y \) on \( C \) is regarded as the one on \( E \). Hence there exists an element \( f \) of \( K(E) \) such that \( fdy/y \) is regular. Then

\[ \text{div}_E(f) = P'_1 + P'_2 + Q' - \sum_{i=1}^{3} R'_i \]

because

\[ 0 \leq \text{div}_C \left( \frac{fdy}{y} \right) = \text{div}_C(f) + \text{div}_C \left( \frac{dy}{y} \right) \]

\[ = \text{div}_C(f) - P_1 - P_2 - \pi^*(Q') + \sum_{i=1}^{3} \pi^*(R_i). \]

Hence

\[ D'_0 = -P'_1 - P'_2 - Q' + \sum_{i=1}^{3} R'_i \sim 0. \]

Moreover, \( l(D'_r) = 1 \) for any \( r \) with \( 1 \leq r \leq 2n \), because \( \deg(D'_r) = 1 \).

To compute the numbers \( l(D'_r - P'_1) \) and \( l(D'_r - P'_2) \) we show that \( mP'_1 \not\sim mP'_2 \) for any positive integer \( m \) with \( m \leq n \). In fact, suppose that there exists a positive integer \( m \leq n \) such that \( mP'_1 \sim mP'_2 \). If \( m \) is even, then

\[ mP'_2 \sim \frac{m}{2}2P'_1 \sim \frac{m}{2}2Q' = mQ', \]

which is a contradiction. Let \( m \) be odd. Then \( 2mP'_2 \sim 2mP'_1 \sim 2mQ' \). If \( m < n/2 \), then

\[ (n - 2m)P'_2 = nP'_2 - 2mP'_2 \sim nQ' - 2mQ' = (n - 2m)Q', \]
Cyclic coverings of an elliptic curve

279

a contradiction. If \( n/2 < m < n \), then \((2m - n)P'_2 \sim (2m - n)Q'\), a contradiction. If \( m = n \), then

\[(n-1)Q' + P'_1 \sim (n-1)P'_1 + P'_1 \sim nP'_2 \sim nQ',\]

which implies that \( P'_1 \sim Q' \). This is a contradiction. Hence we have shown that for any \( m \) with \( 0 < m \leq n \), \( mP'_1 \not\sim mP'_2 \).

Now for any \( l \) with \( 0 \leq l \leq n - 2 \) we have \( l(D'_{2l+1} - P'_1) = 0 \). In fact, suppose that \( l(D'_{2l+1} - P'_1) = 1 \). Then

\[0 \sim D'_{2l+1} - P'_1 - D'_0 \sim (n-2l-1)Q' + lP'_1 + (l+1-n)P'_2 \sim (n-l-1)P'_1 - (n-l-1)P'_2,\]

because \( nQ' \sim nP'_2 \) and \( 2P'_1 \sim 2Q' \). Hence

\[1 \leq n-l-1 \leq n-1 \quad \text{and} \quad (n-l-1)P'_1 \sim (n-l-1)P'_2,\]

which is a contradiction.

Now in view of \( 2P'_1 \sim 2Q' \) and \( nP'_2 \sim nQ' \) we have

\[D'_{2n-1} - P'_1 - D'_0 \sim -(2n-1)Q' + (n-1)Q' + nQ' = 0,\]

which implies that \( D'_{2n-1} - P'_1 \sim 0 \). Hence

\[l(D'_{2n-1}) = l(D'_{2n-1} - P'_1) = 1 \quad \text{and} \quad l(D'_{2n-1} - 2P'_1) = 0.\]

Suppose that \( l(D'_{2l} - P'_1) = 1 \). Then in view of \( 2P'_1 \sim 2Q' \) we have

\[0 \sim D'_{2l} - P'_1 - D'_0 \sim -2lP'_1 + lP'_1 + lP'_2 = -lP'_1 + lP'_2,\]

a contradiction. Hence \( l(D'_{2l} - P'_1) = 0 \) for any \( l \) with \( 1 \leq l \leq n \).

Next we show that \( l(D'_1 - P'_2) = 0 \). If \( l(D'_1 - P'_2) = 1 \), then

\[-2Q' + \sum_{i=1}^{3} R'_i - P'_2 = D'_1 - P'_2 \sim 0 \sim D'_0 \sim -P'_1 - P'_2 - Q' + \sum_{i=1}^{3} R'_i,\]

which implies that \( P'_1 \sim Q' \). This is a contradiction. Now in view of \( 2P'_1 \sim 2Q' \) we obtain \( D'_2 - P'_2 \sim D'_0 \sim 0 \), which implies that

\[l(D'_2) = l(D'_2 - P'_2) = 1 \quad \text{and} \quad l(D'_2 - 2P'_2) = 0.\]

Let \( 1 \leq l \leq n - 1 \). Suppose that \( l(D'_{2l+1} - P'_2) = 1 \). Then

\[-(2l+2)Q' + lP'_1 + (l-1)P'_2 + \sum_{i=1}^{3} R'_i \sim D'_0 \sim -P'_1 - P'_2 - Q' + \sum_{i=1}^{3} R'_i,\]

which implies that \(-l+1)P'_1 \sim -(2l+1)Q' + lP'_2 \). Since \( nP'_2 \sim nQ' \) and \( n \) is odd, we have

\[nP'_2 - (l+1)P'_1 \sim (n-(2l+1))Q' + lP'_2 \sim (n-(2l+1))P'_1 + lP'_2,\]

which implies that \((n-l)P'_2 \sim (n-l)P'_1 \). This contradicts \( mP'_1 \not\sim mP'_2 \) for any \( 0 < m < n \). Hence \( l(D'_{2l+1} - P'_2) = 0 \) for any \( 1 \leq l \leq n - 1 \).
Let \(2 \leq l \leq n\). Suppose that \(l(D'_{2l} - P'_2) = 1\). Then
\[
-(2l + 1)Q' + lP'_2 + (l - 2)P'_2 + \sum_{i=1}^{3} R'_i \sim -P'_1 - P'_2 - Q' + \sum_{i=1}^{3} R'_i,
\]
which implies that \((l + 1)P'_1 + (l - 1)P'_2 \sim 2lQ' \sim 2lP'_1\). Hence \((l - 1)P'_2 \sim (l - 1)P'_1\), a contradiction. Therefore \(l(D'_{2l} - P'_2) = 0\) for any \(2 \leq l \leq n\).

Now let \(f\) be an element of \(K(E)\) and set
\[
\text{div}_E(f) = \sum_{P' \in E} m(P') P'.
\]

Then for any non-negative integer \(r\) we obtain
\[
\text{div}_C \left( \frac{f dy}{y^{1-r}} \right) = ((2n + 1)m(P'_1) + n + (n + 1)(r - 1))P_1 \\
+ ((2n + 1)m(P'_2) + n - 1 + n(r - 1))P_2 \\
+ (m(Q') - r - 1)\pi^*(Q') \\
+ \sum_{i=1}^{3} (m(R'_i) + 1)\pi^*(R'_i) + \sum_{P' \in S} m(P') \pi^*(P'),
\]
where we set \(S = E \setminus \{P'_1, P'_2, Q', R'_1, R'_2, R'_3\}\). We note that if \(R'_1 \neq R'_2\) and \(R'_2 = R'_3\) (resp. \(R'_1 = R'_2 = R'_3\)), then
\[
\sum_{i=1}^{3} (m(R'_i) + 1)\pi^*(R'_i)
\]
is replaced by
\[
(m(R'_1) + 1)\pi^*(R'_1) + (m(R'_2) + 2)\pi^*(R'_2) \quad \text{(resp.} \ (m(R'_1) + 3)\pi^*(R'_1))\).

For each \(r = 0, 1, \ldots, 2n\), we take a non-zero element \(f_r \in L(D'_r)\) and set \(\phi_r = f_r dy/y^{1-r}\). Then by the above,
\[
\text{ord}_{P_i}(\phi_0) = 2n + 1 - 1 = g - 1 \quad \text{for } i = 1, 2.
\]

For any \(l\) with \(0 \leq l \leq n - 2\) we have
\[
\text{ord}_{P_1}(\phi_{2l+1}) = n + l + 1 - 1 \quad \text{and} \quad \text{ord}_{P_2}(\phi_{2l+1}) = n - l - 1.
\]

Let \(l = n - 1\), i.e., \(2l + 1 = 2n - 1\). Since \(L(D'_{2n-1}) = L(D'_{2n-1} - P'_1)\) and \(L(D'_{2n-1}) \supset L(D'_{2n-1} - P'_2) = (0)\), we obtain
\[
\text{ord}_{P_1}(\phi_{2n-1}) = 4n + 1 - 1 = 2g - 1 - 1 \quad \text{and} \quad \text{ord}_{P_2}(\phi_{2n-1}) = 1 - 1.
\]

Let \(l = 1\), i.e., \(2l = 2\). Since \(L(D'_2) \supset L(D'_2 - P'_1) = (0)\) and \(L(D'_2) = L(D'_2 - P'_2)\), we obtain
\[
\text{ord}_{P_1}(\phi_2) = 1 - 1 \quad \text{and} \quad \text{ord}_{P_2}(\phi_2) = 2g - 1 - 1.
\]
For any \( l \) with \( 2 \leq l \leq n \) we have
\[
\text{ord}_{P_1}(\phi_{2l}) = l - 1 \quad \text{and} \quad \text{ord}_{P_2}(\phi_{2l}) = 2n - l + 1 - 1.
\]
Hence for each \( r = 0, 1, \ldots, 2n \), \( \phi_r \) is a regular 1-form on \( C \). Therefore \( G(P_1) = G(P_2) = \{1, \ldots, g - 2, g, 2g - 1\} \).

3. The case \( g \equiv 1 \text{ mod } 4 \). In this section we prove the Main Theorem in the case \( g \equiv 1 \text{ mod } 4 \) with \( g \geq 9 \).

Let \( g = 4h + 1 = 2n + 1 \) with \( h \in \mathbb{N}, h \geq 2 \) and \( n = 2h \). Let \( E \) be an elliptic curve over \( k \) with the origin \( Q' \). Let \( P'_1 \) be a point of \( E \) such that \( P'_1 \neq Q' \) and \( 2[P'_1] = [Q'] \). Moreover, \( P'_2 \) denotes a point of \( E \) such that \( n[P'_2] = -[P'_1] \) and \( m[P'_2] \neq -[P'_1] \) for any positive integer \( m < n \), where \(-[P'_1]\) denotes the inverse of \( P'_1 \) under the addition on the elliptic curve \( E \). Then \( P'_2 \neq Q' \) and \( P'_2 \neq P'_1 \). Moreover, \( (n+1)P'_1 + nP'_2 \sim nQ' + P'_1 + (n+1)Q' - P'_1 = (2n+1)Q' \).

Hence we may take \( z \in K(E) \) such that \( \text{div}(z) = (n+1)P'_1 + nP'_2 - (2n+1)Q' \).

Let \( C, \pi : C \to E \), \( y \in K(C) \), \( P_1, P_2, R'_1, D'_0, D'_{2l+1} \) and \( D'_{2l} \) be as in Section 2. Then, in the same way as in Section 2, \( D'_0 \) is linearly equivalent to zero. Moreover, \( l(D'_r) = 1 \) for any \( r \) with \( 1 \leq r \leq 2n \).

To compute the numbers \( l(D'_r - P'_1) \) and \( l(D'_r - P'_2) \) we show that for any positive integer \( m \) with \( m \leq n \), \( mP'_1 \not\sim mP'_2 \). In fact, suppose that there exists a positive integer \( m \leq n \) such that \( mP'_1 \sim mP'_2 \). If \( m \) is odd, then \( mP'_2 + P'_1 \sim (m+1)P'_1 \sim (m+1)Q' \). This contradicts \( m[P'_2] \neq -[P'_1] \) for any positive integer \( m \leq n \). If \( m \) is even, then
\[
(n+1)Q' \sim nP'_2 + P'_1 = (n-m)P'_2 + P'_1 + mP'_2 \\
\sim (n-m)P'_2 + P'_1 + mP'_2 \sim (n-m)P'_2 + P'_1 + mQ',
\]
which implies that \((n-m)P'_2 + P'_1 \sim (n+1-m)Q' \). This is a contradiction.

For any \( l \) with \( 0 \leq l \leq n - 2 \) we have \( l(D'_{2l+1} - P'_1) = 0 \). In fact, suppose that \( l(D'_{2l+1} - P'_1) = 1 \). Then \( 0 \sim D'_{2l+1} - P'_1 - D'_0 = -(2l+1)Q' + lp'_1 + (l+1)P'_2 \). Since \( nP'_2 + P'_1 \sim (n+1)Q' \) and \( n \) is even, we have
\[
nP'_2 - lp'_1 \sim P'_1 + (n+1)Q' - (2l+1)Q' + (l+1)P'_2 \\
= -P'_1 + (l+1)P'_2 + (n-2l)Q' \sim -P'_1 + (l+1)P'_2 + (n-2l)P'_1,
\]
which implies that \((n-l-1)P'_2 \sim (n-l-1)P'_1 \). This contradicts \( mP'_1 \not\sim mP'_2 \) for \( 1 \leq m \leq n \). Since \( nP'_2 + P'_1 \sim (n+1)Q' \) and \( n \) is even, we have
\[
D'_{2n-1} - P'_1 - D'_0 \sim -(2n-1)Q' + (n-1)P'_1 + nP'_2 \\
= -(n-2)Q' + (n-2)P'_1 \sim -(n-2)Q' + (n-2)Q' = 0,
\]
which implies that \( l(D'_{2n-1}) = 1 = l(D'_{2n-1} - P'_1) \). Moreover, in the same way as in Section 2, we obtain \( l(D'_{2l} - P'_1) = 0 \) for any \( l \) with \( 1 \leq l \leq n \).

Next, as in Section 2, we have
\[
l(D'_1 - P'_2) = 0 \quad \text{and} \quad l(D'_2) = l(D'_2 - P'_2) = 1.
\]
Let $1 \leq l \leq n - 1$. Suppose $l(D'_{2l+1} - P'_2) = 1$. Then $D'_{2l+1} - P'_2 \sim 0 \sim D'_0$, which implies that $-(l+1)P' _2 \sim -(2l+1)Q' + lP'_2$. Since $nP'_2 + P'_1 \sim (n+1)Q'$ and $n$ is even, we have $nP'_2 - lP'_1 \sim (2l+1)Q' - (n+1)Q' + lP'_2 \sim (n - 2l)P'_1 + lP'_2$, which implies that $(n - l)P'_2 \sim (n - l)P'_1$. This is a contradiction. Hence $l(D'_{2l+1} - P'_2) = 0$ for any $1 \leq l \leq n - 1$.

As in Section 2 we have $l(D'_{2l} - P'_2) = 0$ for any $2 \leq l \leq n$. Therefore $G(P_1) = G(P_2) = \{1, \ldots, g - 2, g, 2g - 1\}$.

4. The case $g \equiv 0 \pmod{4}$. First we show the following lemma, which is useful to construct the desired coverings of an elliptic curve in the even genus cases.

**Lemma 2.** Let $\pi_0 : C \to C_0$ be a finite morphism of curves of degree 2, Let $P \in C$ be a ramification point of $\pi_0$. Then $n \in \mathbb{N}_0 \setminus G(\pi_0(P))$ if and only if $2n \in \mathbb{N}_0 \setminus G(P)$.

**Proof.** Suppose that $n \in \mathbb{N}_0 \setminus G(\pi_0(P))$, i.e., there exists $f_0 \in \mathbb{K}(C_0)$ such that $(f_0)_\infty = n\pi_0(P)$, where $(f_0)_\infty$ denotes the polar divisor of $f_0$. Since $P$ is a ramification point of $\pi_0$, we have $(\pi_0^* f_0)_\infty = 2nP$, where $\pi_0^*$ denotes the inclusion map $\mathbb{K}(C_0) \subset \mathbb{K}(C)$ corresponding to the surjective morphism $\pi_0 : C \to C_0$. Hence $2n \in \mathbb{N}_0 \setminus G(P)$.

Conversely, suppose that $2n \in \mathbb{N}_0 \setminus G(P)$, i.e., there exists $f \in \mathbb{K}(C)$ such that $(f)_\infty = 2nP$. Let $\sigma$ be an involution of $C$ such that $C/\langle \sigma \rangle \cong C_0$. Then we may take a local parameter $t$ at $P$ such that $\sigma^* t = -t$. Since we can write

$$f = c_{-2n} t^{-2n} + c_{-2n+1} t^{-2n+1} + \ldots$$

where $c_{-2n}$ is a non-zero constant and $c_i$’s ($i \geq -2n + 1$) are constants, we obtain

$$\sigma^* f = c_{-2n} t^{-2n} - c_{-2n+1} t^{-2n+1} + \ldots$$

Hence

$$f + \sigma^* f = 2c_{-2n} t^{-2n} + 2c_{-2n+2} t^{-2n+2} + \ldots,$$

which implies that $(f + \sigma^* f)_\infty = 2nP$. Now

$$\sigma^* (f + \sigma^* f) = \sigma^* f + (\sigma^2)^* f = f + \sigma^* f,$$

which implies that $f + \sigma^* f \in \mathbb{K}(C_0)$. Therefore $(f + \sigma^* f)_\infty = n\pi_0(P)$ on $C_0$, which implies that $n \in \mathbb{N}_0 \setminus G(\pi_0(P))$. \hfill $\blacksquare$

Using the above lemma we get the following:

**Proposition 3.** Let $\pi_0 : C \to C_0$ be a finite morphism of curves of degree 2. Suppose that the genus $g$ of $C$ is even and that the genus of $C_0$ is equal to $g/2$. Let $P \in C$ be a ramification point of $\pi_0$. If $G(P)$ contains $\{2, 4, \ldots, g - 2, g, 2g - 1\}$, then $G(P) = \{1, 2, \ldots, g - 2, g, 2g - 1\}$. 
Proof. Suppose that \( G(P) \supset \{ 2, 4, \ldots, g-2, g, 2g-1 \} \). Then by Lemma 2 we obtain
\[
G(\pi_0(P)) = \{ 1, 2, \ldots, g/2 \}.
\]
If \( h \) is an even integer \( > g \), then by the above we have \( h/2 \in \mathbb{N}_0 \setminus G(\pi_0(P)) \). Hence by Lemma 2 we get \( h \in \mathbb{N}_0 \setminus G(P) \). On the other hand, if \( h \) is an even integer with \( g + 2 \leq h \leq 2g - 2 \), then \( 2g - 1 - h \in G(P) \). In fact, if \( 2g - 1 - h \in \mathbb{N}_0 \setminus G(P) \), then \( 2g - 1 = h + (2g - 1 - h) \in \mathbb{N}_0 \setminus G(P) \), a contradiction. Hence \( G(P) \) contains the set
\[
\{ 2, 4, \ldots, g-2, g, 2g-1 \} \cup \{ 2g - 1 - h \mid h \text{ is even with } g + 2 \leq h \leq 2g - 2 \} = \{ 1, 2, 3, 4, \ldots, g - 3, g - 2, g, 2g - 1 \}.
\]
Since the cardinality of \( G(P) \) is \( g \), we get the desired result. \[ \square \]

Using this result we show the Main Theorem in the case \( g \equiv 0 \mod 4 \) with \( g \geq 8 \).

Let \( g = 4h = 2n \) with \( h \in \mathbb{N}, h \geq 2 \) and \( n = 2h \). Let \( E \) be an elliptic curve over \( k \) with the origin \( Q' \). Let \( P^*_1 \) be a point of \( E \) such that \((2n-1)[P^*_1] = [Q']\) and \( m[P^*_1] \neq [Q'] \) for any positive integer \( m < 2n - 1 \). Moreover, \( P^*_2 \) denotes the point of \( E \) such that \([P^*_2] = 3[P^*_1]\). Then \( P^*_2 \neq Q' \) and \( P^*_1 \neq P^*_2 \) because \( g \geq 8 \). Now we have
\[
(n + 1)P'_{1} + (n - 1)P'_{2} - (n + 1)P'_{1} + (n - 1)(3P'_{1} - 2Q')
\]
\[
\sim 2(2n - 1)P'_{1} - (2n - 2)Q' \sim 2nQ'.
\]
Hence we may take \( z \in \mathbf{K}(E) \) such that \(\text{div}(z) = (n+1)P'_{1} + (n-1)P'_{2} - 2nQ'\).

Let \( C \) be the curve whose function field \( \mathbf{K}(C) \) is \( \mathbf{K}(E)(z^{1/(2n)}) \). Moreover, \( \pi : C \to E \) denotes the surjective morphism of curves corresponding to the inclusion \( \mathbf{K}(E) \subset \mathbf{K}(C) \). Then we may take \( y \in \mathbf{K}(C) \) and \( \sigma \in \text{Aut}(\mathbf{K}(C)/\mathbf{K}(E)) \) such that
\[
\sigma(y) = \zeta_{2n} y \quad \text{and} \quad \text{div}_E(y^{2n}) = (n + 1)P'_{1} + (n - 1)P'_{2} - 2nQ'.
\]
Since \( n \) is even, we get \((2n, n + 1) = (2n, n - 1) = 1\). Therefore the branch points of \( \pi \) are \( P'_{1} \) and \( P'_{2} \) whose ramification indices are \( 2n \). Therefore
\[
\text{div}(y) = (n + 1)P_{1} + (n - 1)P_{2} - \pi^*(Q').
\]
Moreover, by the Riemann–Hurwitz formula we have \( g(C) = 2n = g \). Hence
\[
\text{div}(dy) = nP_{1} + (n - 2)P_{2} - 2\pi^*(Q') + \sum_{i=1}^{3} \pi^*(R'_{i}),
\]
where \( R'_{i} \)'s are points of \( E \) which are distinct from \( P'_{1}, P'_{2} \) and \( Q' \).

Let \( D'_{0} \) and \( D'_{2l} \) \((1 \leq l \leq n - 1)\) be as in Section 2. Moreover, we set
\[
D'_{n-1} = D'_{2(n/2-1)+1} = -nQ' + \left( \frac{n}{2} - 1 \right)P'_{1} + \left( \frac{n}{2} - 1 \right)P'_{2} + \sum_{i=1}^{3} R'_{i}
\]
and

\[ D'_{n+1} = D'_{2n/2+1} = -(n+2)Q' + \left( \frac{n}{2} + 1 \right) P'_1 + \left( \frac{n}{2} - 1 \right) P'_2 + \sum_{i=1}^{3} R'_i. \]

Then \( D'_0 \sim 0 \). Moreover, for any \( l \) with \( 1 \leq l \leq n-1 \) we have \( l(D'_{2l}) = 1 \) and \( l(D'_{2l} - P'_1) = l(D'_{2l} - P'_2) = 0 \). In fact, first assume \( l(D'_{2l} - P'_1) = 1 \). Then \( 0 \sim D'_{2l} - P'_1 \sim 4lP'_1 - 4Q' \), which implies that \( 2n-1 \) divides \( 4l \). In view of \( 1 \leq l \leq n-1 \) we must have \( 4l = 2n-1 \), which is a contradiction. Secondly, assume \( l(D'_{2l} - P'_2) = 1 \). Then \( 0 \sim D'_{2l} - P'_2 - D'_0 \sim -(4l-2)Q' + (4l-2)P'_1 \), which implies that \( 2n-1 \) divides \( 4l-2 \). This is a contradiction. Now we have

\[ D'_{n+1} - P'_1 - D'_0 \sim (2n-1)P'_1 - (2n-1)Q' \sim 0, \]

which implies that \( l(D'_{n+1} - P'_1) = l(D'_{n+1} - 2P'_1) = 0 \). Moreover, \( D'_{n+1} - P'_2 - D'_0 \sim -(2n-1)Q' + (2n-1)P'_1 \sim 0 \), which implies that \( l(D'_{n+1}) = l(D'_{n+1} - P'_2) = 1 \) and \( l(D'_{n+1} - 2P'_2) = 0 \).

Let \( f \in K(E) \) and set

\[ \text{div}_E(f) = \sum_{P' \in E} m(P') P'. \]

Then for any non-negative integer \( r \) we obtain

\[
\text{div}_C\left( \frac{f dy}{y^{1-r}} \right) = (2nm(P'_1) + n + (n+1)(r-1))P_1 + (2nm(P'_2) + n - 2 + (n-1)(r-1))P_2 + (m(Q') - r - 1)\pi^*(Q') + \sum_{i=1}^{3} (m(R'_i) + 1)\pi^*(R'_i) + \sum_{P' \in S} m(P') \pi^*(P'),
\]

where we set \( S = E \setminus \{ P'_1, P'_2, Q', R'_1, R'_2, R'_3 \} \).

For each \( r \in \{0, 2, \ldots, 2n-2\} \cup \{n-1\} \cup \{n+1\} \) we take a non-zero element \( f_r \in L(D'_r) \) and set \( \phi_r = f_r dy/y^{1-r} \). Then, by the above, 

\[
\text{ord}_{P_1}(\phi_{n-1}) = 2n - 1 - 1 = 2g - 1 - 1,
\]

\[
\text{ord}_{P_2}(\phi_{n-1}) \geq -2n\left( \frac{n}{2} - 1 \right) + n - 2 + (n-1)(n-2) = 0,
\]

\[
\text{ord}_{P_1}(\phi_{n+1}) \geq -2n\left( \frac{n+1}{2} + n(n+1)(n+2) = 0 \text{ and } \text{ord}_{P_2}(\phi_{n+1}) = 2g-1-1.
\]

Hence \( \phi_0, \phi_2, \ldots, \phi_{2n-2}, \phi_{n-1}, \phi_{n+1} \) are regular 1-forms on \( C \). Therefore we get \( G(P_i) \supset \{2, 4, \ldots, g - 2, g, 2g - 1\} \) for \( i = 1, 2 \).
Now let $C_0$ be the curve whose function field $K(C_0)$ is $K(E)(z^{1/n})$. Moreover, $\eta : C_0 \to E$ denotes the surjective morphism of curves corresponding to the inclusion $K(E) \subset K(C_0)$. Let $\pi_0 : C \to C_0$ be the double covering corresponding to the inclusion $K(C_0) \subset K(C)$. Since $\pi = \eta \circ \pi_0 : C \to E$ has only two ramification points $P_1$ and $P_2$, which are totally ramified, by the Riemann–Hurwitz formula we get $g(C_0) = g/2$. Moreover, $P_1$ and $P_2$ are ramification points of $\pi_0$. Therefore by Proposition 3 we obtain $G(P_1) = G(P_2) = \{1, 2, \ldots, g - 2, g, 2g - 1\}$.

5. The case $g \equiv 2 \mod 4$. First we show the following arithmetic lemma which is the key to proving the next Proposition 5.

Key Lemma 4. Let $l \geq 2$ be an integer and let $p_1, \ldots, p_l$ be distinct prime numbers. Then there is a partition

$$\{i_1, \ldots, i_t\} \cup \{i_{t+1}, \ldots, i_l\} = \{1, \ldots, l\}$$

with $1 \leq t \leq l - 1$ such that $(4p_{i_1} \ldots p_{i_t} + 1, p_{i_{t+1}} \ldots p_{i_l}) = 1$.

Proof. We may assume that $p_1, \ldots, p_l$ are odd. In fact, if $p_1 = 2$, then $(4p_2 \ldots p_l + 1, p_1) = 1$. We prove the lemma by induction on $l \geq 2$.

Let $l = 2$. We may assume that $p_1 < p_2$. Suppose that

$$(4p_1 + 1, p_2) \neq 1 \quad \text{and} \quad (4p_2 + 1, p_1) \neq 1,$$

which implies that $p_2 | (4p_1 + 1)$ and $p_1 | (4p_2 + 1)$. Let $4p_1 + 1 = mp_2$. Then $m$ must be 1 or 3. Moreover, $p_1$ divides $(4p_2 + 1)m = 16p_1 + 4 + m$, which implies that $p_1 | (4 + m)$. Let $m = 1$. Then $p_1 | 5$, which implies that $p_1 = 5$. Hence $p_2 = 4p_1 + 1 = 21$ is not prime, a contradiction. Let $m = 3$. Then $p_1 | 7$, which implies that $p_1 = 7$. Hence $3p_2 = 4p_1 + 1 = 29$, a contradiction.

Let $l \geq 3$. We may assume that $p_1 > p_j$ for all $j \neq l$. Suppose that

$$(4p_1 \ldots p_{i-1}p_{i+1} \ldots p_l + 1, p_i) \neq 1, \quad \text{i.e.,} \quad p_i | (4p_1 \ldots p_{i-1}p_{i+1} \ldots p_l + 1)$$

for all $i = 1, \ldots, l$. Then $p_i | (4p_1 \ldots p_{i-1}p_{i+1} \ldots p_l - 1)$ for all $i = 1, \ldots, l - 1$. In fact, suppose that $p_i | (4p_1 \ldots p_{i-1}p_{i+1} \ldots p_{l-1} + 1)$ for some $i$. In view of $p_i | (4p_1 \ldots p_{i-1} + 1)$ we get

$$p_i | 4p_1 \ldots p_{i-1}p_{i+1} \ldots p_{l-1}(p_i - 1),$$

which implies that $p_i | (p_i - 1)$. This contradicts $p_i > p_j$ for all $j \neq l$.

Moreover, we may assume that $p_i | (4p_1 \ldots p_{i-1}p_{i+1} \ldots p_l + 1)$ for each $i = 1, \ldots, l - 1$. In fact, suppose that $p_i | (4p_1 \ldots p_{i-1}p_{i+1} \ldots p_{l-1} + 1)$ for some $i$. In view of $p_i | (4p_1 \ldots p_{i-1}p_{i+1} \ldots p_l + 1)$ we obtain a partition

$$\{1, \ldots, i-1, i+1, \ldots, l-1\} \cup \{i, l\} = \{1, \ldots, l\}$$

such that $(p_ip_i, 4p_1 \ldots p_{i-1}p_{i+1} \ldots p_{l-1} + 1) = 1$. Hence

$$p_i | 4p_1 \ldots p_{i-1}p_{i+1} \ldots p_{l-1}(p_i - 1)$$
for each \( i = 1, \ldots, l - 1 \). Therefore \( p_i | (p_i - 1) \) for all \( i = 1, \ldots, l - 1 \), which implies that \( p_i - 1 = mp_1 \cdots p_{i-1} \) for some integer \( m \). If \( m \geq 5 \), then 
\[ p_i \geq 5p_1 \cdots p_{i-1} + 1, \]
which contradicts \( p_i | (4p_1 \cdots p_{i-1} + 1) \). If \( m \leq 3 \), then 
\[ (mp_1 \cdots p_{i-1} + 1) | (4p_1 \cdots p_{i-1} + 1), \]
a contradiction.

Hence \( m = 4 \). By the induction hypothesis there is a partition
\[ \{i_1, \ldots, i_t\} \cup \{i_{t+1}, \ldots, i_{l-1}\} = \{1, \ldots, l - 1\} \]
with \( 1 \leq t \leq l - 2 \) such that \((4p_{i_1} \cdots p_{i_t} + 1, p_{i_{t+1}} \cdots p_{i_{l-1}}) = 1\). In view of
\[ p_i = 4p_1 \cdots p_{i-1} + 1 > 4p_{i_1} \cdots p_{i_t} + 1 \]
we get \( p_i | (4p_{i_1} \cdots p_{i_t} + 1) \). Hence we obtain \((4p_{i_1} \cdots p_{i_t} + 1, p_{i_{t+1}} \cdots p_{i_{l-1}}, p_i) = 1\). □

Using the Key Lemma we show the following proposition, which is crucial to the proof of the remaining case of the Main Theorem.

**Proposition 5.** Let \( n = 10t + 3 \) with an integer \( t \geq 1 \). Then there exists an integer \( s \) with \( 3 \leq s \leq (n-3)/2 \) such that \( s | (2n-1) \) and \((2n-1, n+2s) = 1\).

**Proof.** First, we consider the case \( 2n-1 = p_1^2p_2 \cdots p_r \) with \( e \geq 2 \) if \( p_1 \geq 5 \) or \( e \geq 3 \) if \( p_1 = 3 \), where \( p_2, \ldots, p_r \) may not be distinct. Let \( s = p_1p_2 \cdots p_r \) and \( q = p_1^{e-1} \). Then \( s | (2n-1) \) and
\[
(2n-1, n+2s) = (2n-1, 2n+4s) = (2n-1, 4s+1) = (sq, 4s+1) = (q, 4s+1) = (p_1^{e-1}, 4p_1p_2 \cdots p_r + 1) = 1.
\]
Moreover,
\[
s = p_1p_2 \cdots p_r = \frac{2n-1}{q} \leq \frac{2n-1}{5} \leq \frac{n-3}{2}
\]
because \( q = p_1^{e-1} \geq 5 \) and \( n \geq 13 \).

Secondly, we consider the case \( 2n-1 = p_1^2p_2 \cdots p_r \) with \( p_1 = 3 \) where \( p_1, \ldots, p_r \) are distinct. In view of \( 2n-1 = 5(4t+1) \) we have \( r \geq 2 \). By Lemma 4 we have a partition
\[ \{i_1, \ldots, i_t\} \cup \{i_{t+1}, \ldots, i_r\} = \{1, \ldots, r\} \]
with \( 1 \leq t \leq r-1 \) such that \((4p_{i_1} \cdots p_{i_t} + 1, p_{i_{t+1}} \cdots p_{i_r}) = 1\). Hence we get 
\[ (4p_{i_1} \cdots p_{i_t} + 1, p_{i_{t+1}}p_{i_{t+2}} \cdots p_{i_r}) = 1. \]
Let \( s = p_{i_1} \cdots p_{i_t} \) and \( q = p_{i_{t+1}} \cdots p_{i_r} \). Then \( s | (2n-1) \) and
\[
(2n-1, n+2s) = (q, 4s+1) = (p_{i_1}p_{i_{t+1}} \cdots p_{i_r}, 4p_{i_1} \cdots p_{i_t} + 1) = 1.
\]
Moreover,
\[
s = \frac{2n-1}{q} \leq \frac{2n-1}{9} < \frac{n-3}{2}
\]
because \( q = p_{i_1}p_{i_{t+1}} \cdots p_{i_r} \geq 9 \).
Lastly, we consider the case $2n - 1 = p_1 p_2 \ldots p_r$ where $p_1, \ldots, p_r$ are distinct. By Lemma 4 we have a partition \( \{i_1, \ldots, i_t\} \cup \{i_{t+1}, \ldots, i_r\} = \{1, \ldots, r\} \) with \( 1 \leq t \leq r - 1 \) such that \((4p_{i_1} \cdots p_{i_t} + 1, p_{i_{t+1}} \cdots p_{i_r}) = 1\). Let \( t \leq r - 2 \) or \( p_i > 3 \) for all \( i \). We set \( s = p_{i_1} \cdots p_{i_t} \) and \( q = p_{i_{t+1}} \cdots p_{i_r} \). Then \( s \mid (2n - 1) \) and \( (2n - 1, n + 2s) = 1 \). Moreover,

\[
s = \frac{2n - 1}{q} = \frac{2n - 1}{p_{i_{t+1}} \cdots p_{i_r}} \leq \frac{2n - 1}{5} \leq \frac{n - 3}{2}
\]

because \( n \geq 13 \).

Let \( t = r - 1 \) and \( p_i = 3 \) for some \( i \). In this case \( r \geq 3 \), because \( 2n - 1 = 5(4t + 1) \) with \( 4t + 1 \geq 5 \). Then we may assume that \( p_1 = 3 \). Let \( p_r > p_j \) for all \( j \neq r \). Moreover, we may assume either

(1) \( (p_1, 4p_1 \cdots p_{i-1}p_{i+1} \cdots p_r + 1) = 1 \) for some \( i = 2, \ldots, r \), or

(2) there exists a partition

\[
\{i_1, \ldots, i_t\} \cup \{i_{t+1}, \ldots, i_r-1\} = \{1, \ldots, r - 1\}
\]

with \( 1 \leq t \leq r - 2 \) such that \((p_{i_{t+1}} \cdots p_{i_r} - p_r, 4p_1 \cdots p_{i_t} + 1) = 1\).

In fact, suppose that (1) does not hold, i.e.,

\[
p_i \mid (4p_1 \cdots p_{i-1}p_{i+1} \cdots p_r + 1) \quad \text{for all} \quad i = 2, \ldots, r.
\]

Then

\[
p_r \mid (4p_1 \cdots p_{i-1}p_{i+1} \cdots p_{r-1} + 1) \quad \text{for all} \quad i = 2, \ldots, r - 1.
\]

In fact, suppose that

\[
p_r \mid (4p_1 \cdots p_{i-1}p_{i+1} \cdots p_{r-1} + 1) \quad \text{for some} \quad i = 2, \ldots, r - 1.
\]

In view of \( p_r \mid (4p_1 \cdots p_{r-1} + 1) \) we obtain \( p_r \mid 4p_1 \cdots p_{i-1}p_{i+1} \cdots p_{r-1}(p_i - 1) \), which implies that \( p_r \mid (p_i - 1) \). This contradicts \( p_r > p_i \).

Moreover, we may assume that

\[
p_i \mid (4p_1 \cdots p_{i-1}p_{i+1} \cdots p_{r-1} + 1) \quad \text{for all} \quad i = 2, \ldots, r - 1.
\]

In fact, suppose that

\[
p_i \mid (4p_1 \cdots p_{i-1}p_{i+1} \cdots p_{r-1} + 1) \quad \text{for some} \quad i = 2, \ldots, r - 1.
\]

In view of \( p_i \mid (4p_1 \cdots p_{i-1}p_{i+1} \cdots p_{r-1} + 1) \) we have a partition

\[
\{1, \ldots, i-1, i+1, \ldots, r-1\} \cup \{i, r\} = \{1, \ldots, r\}
\]

such that \((p_ip_{i+1} \cdots p_{i+r-1} + 1) = 1\). This case reduces to the case \( t \leq r - 2 \) in which we have already proven the statement. Hence in view of

\[
p_i \mid (4p_1 \cdots p_{i-1}p_{i+1} \cdots p_r + 1) \quad \text{for all} \quad i = 2, \ldots, r - 1
\]

we have \( p_i \mid 4p_1 \cdots p_{i-1}p_{i+1} \cdots p_{r-1}(p_r - 1) \) for all \( i = 1, \ldots, r - 1 \), which implies \( p_i \mid (p_r - 1) \) for all \( i = 2, \ldots, r - 1 \). Therefore \( p_2 \cdots p_{r-1} \mid (p_r - 1) \).
which in turn implies that \( p_r - 1 = mp_2 \ldots p_{r-1} \) where \( m \) is even. In view of \( p_r \mid (4p_1p_2 \ldots p_{r-1} + 1) \) with \( p_1 = 3 \) we have

\[
12p_2 \ldots p_{r-1} + 1 = m'p_r = m'(mp_2 \ldots p_{r-1} + 1) = m'mp_2 \ldots p_{r-1} + m'
\]

with a positive integer \( m' \). Then we must have \( m' = 1 \), i.e., \( m = 12 \). In fact, suppose that \( m' \geq 2 \). Then \( 12 - m'm > 0 \), which implies that \( 12 > m'm \geq 2m' \). Hence \( m' \leq 5 \), which implies that

\[
4 \geq m' - 1 = (12 - m'm)p_2 \ldots p_{r-1} \geq p_2 \ldots p_{r-1} \geq 5p_3 \ldots p_{r-1}.
\]

This is a contradiction. Hence \( m' = 1 \).

Therefore we obtain

\[
p_r = 12p_2 \ldots p_{r-1} + 1 = 4p_1p_2 \ldots p_{r-1} + 1.
\]

Since \( p_1, p_2, \ldots, p_{r-1} \) are distinct primes and \( r - 1 \geq 2 \), by Lemma 4 there exists a partition \( \{i_1, \ldots, i_t\} \cup \{i_{t+1}, \ldots, i_{r-1}\} = \{1, \ldots, r-1\} \) with \( 1 \leq t \leq r - 2 \) such that \( (4p_{i_1} \ldots p_{i_t} + 1, p_{i_{t+1}} \ldots p_{i_{r-1}}) = 1 \). In view of \( p_r = 4p_1p_2 \ldots p_{r-1} + 1 > 4p_{i_1} \ldots p_{i_t} + 1 \) we have \( p_r \mid (4p_{i_1} \ldots p_{i_t} + 1) \). Hence \( (4p_{i_1} \ldots p_{i_t} + 1, p_{i_{t+1}} \ldots p_{i_{r-1}}p_r) = 1 \). Thus we have proven that if \( t = r - 1 \) and \( p_1 = 3 \), then we may assume that either (1) or (2) holds.

In case (1) (resp. (2)) we set \( s = p_1 \ldots p_{i-1}p_{i+1} \ldots p_r \) (resp. \( s = p_{i_1} \ldots p_{i_t} \)) and \( q = p_i \geq 5 \) (resp. \( q = p_{i+t} \ldots p_{i_{r-1}}p_r \geq 15 \)). Then we have \( s \mid (2n - 1) \) and \( (2n - 1, n + 2s) = (q, 4s + 1) = 1 \). Moreover,

\[
s = \frac{2n - 1}{q} \leq \frac{2n - 1}{5} \leq \frac{n - 3}{2}
\]

because \( n \geq 13 \). \( \blacksquare \)

Now we prove the Main Theorem in the case \( g \equiv 2 \mod 4 \) with \( g \geq 10 \).

Let \( g = 2n \) where \( n \) is an odd integer \( \geq 5 \). First we show that there exists an odd integer \( s \) with \( 1 \leq s \leq (n - 3)/2 \) such that

\[
s \mid (2n - 1) \quad \text{and} \quad (2n - 1, n + 2s) = 1.
\]

In fact, let \( g \equiv 1 \mod 5 \), which implies that \( n + 2 \not\equiv 0 \mod 5 \). Then

\[
(2n - 1, n + 2) = (2n - 1, 2n + 4) = (2n - 1, 5) = 1.
\]

Hence in this case we may take \( s = 1 \). Let \( g \equiv 1 \mod 5 \). Then we can write \( n = 10t + 3 \) with \( t \geq 1 \). By Proposition 5 we may take an integer \( s \) with \( 3 \leq s \leq (n - 3)/2 \) such that \( s \mid (2n - 1) \) and \( (2n - 1, n + 2s) = 1 \).

Now there exists a unique integer \( m \) with \( 0 < m \leq 2n - 3 \) such that

\[
(m + 1)(n + 2s) \equiv 1 \mod 2n - 1.
\]

In fact, in view of \( (2n - 1, n + 2s) = 1 \) there exists a unique integer \( 0 \leq m \leq 2n - 3 \) such that \( (m + 1)(n + 2s) \equiv 1 \mod 2n - 1 \). If \( m = 0 \), then
n + 2s \equiv 1 \text{ mod } 2n - 1. \text{ Since}

n + 2s - 1 \geq n + 1 > 0 \quad \text{and} \quad n + 2s - 1 \leq n + 2 \cdot \frac{n - 3}{2} - 1 = 2n - 4,

this contradicts \((2n - 1) \mid (n + 2s - 1)\).

Let \(E\) be an elliptic curve over \(k\) with the origin \(Q'\). Let \(P_1'\) be a point of \(E\) such that \((2n - 1)[P_1'] = [Q']\) and \(h[P_1'] \neq [Q']\) for any positive integer \(h < 2n - 1\). Moreover, \(P_2'\) denotes the point of \(E\) such that \([P_2'] = -m[P_1']\), i.e., \(P_2' \sim -mP_1' + (m + 1)Q'\). Then \(P_1', P_2'\) and \(Q'\) are distinct because \(0 < m \leq 2n - 3\). Now we obtain

\[(n - 2s)P_1' + (n + 2s)P_2' \sim 2nQ'.\]

In fact,

\[(n - 2s)P_1' + (n + 2s)P_2' \sim (n - 2s)(n + 2s)P_1' + (n + 2s)(n + 1)Q'.\]

Then \(-m(n + 2s)n - 2s \equiv -1 + 2n \equiv 0 \text{ mod } 2n - 1\) because \((m + 1)(n + 2s) \equiv 1 \text{ mod } 2n - 1\). Hence

\[
(n - 2s)P_1' + (n + 2s)P_2' \\
\sim \frac{-m(n + 2s) + n - 2s}{2n - 1}(n - 2s)(n + 1)P_1' + (n + 2s)(n + 1)Q' \sim 2nQ'.
\]

Hence we may take \(z \in K(E)\) such that

\[
\text{div}(z) = (n - 2s)P_1' + (n + 2s)P_2' - 2nQ'.
\]

Let \(C\) be the curve whose function field \(K(C)\) is \(K(E)(z^{1/(2n)})\). Moreover, \(\pi : C \to E\) denotes the surjective morphism of curves corresponding to the inclusion \(K(E) \subset K(C)\). Then we may take \(y \in K(C)\) and \(\sigma \in \text{Aut}(K(C)/K(E))\) such that

\[
\sigma(y) = \zeta_{2n}y \quad \text{and} \quad \text{div}_E(y^{2n}) = (n - 2s)P_1' + (n + 2s)P_2' - 2nQ'.
\]

Now we have \((n, s) = 1\). In fact, \((n, s) \mid (2n - 1, n + 2s)\) because \(s \mid (2n - 1)\), which implies that \((n, s) = 1\). Therefore \((2n, n + 2s) = (s, n) = 1\) and \((2n, n - 2s) = 1\), because \(n\) is odd. Therefore the branch points of \(\pi\) are \(P_1'\) and \(P_2'\) whose ramification indices are \(2n\). Thus

\[
\text{div}(y) = (n - 2s)P_1 + (n + 2s)P_2 - \pi^*(Q').
\]

Moreover, by the Riemann–Hurwitz formula we have \(g(C) = 2n = g\). Hence

\[
\text{div}(dy) = (n - 2s - 1)P_1 + (n + 2s - 1)P_2 - 2\pi^*(Q') + \sum_{i=1}^{3} \pi^*(R_i'),
\]

where \(R_i'\)'s are points of \(E\) which are distinct from \(P_1', P_2'\) and \(Q'\).

We set

\[
D'_0 = -P_1' - P_2' - Q' + \sum_{i=1}^{3} R_i',
\]
which is linearly equivalent to zero. Let \( l \in \{0, 1, \ldots, 2s - 1\} \) be fixed. Then for any even \( r > 0 \) with
\[
\frac{2ln - 1}{2s} < r \leq \frac{2(l + 1)n - 1}{2s}
\]
we set
\[
D'_r = -(r + 1)Q' + \left(\frac{r}{2} - l - 1\right)P'_1 + \left(\frac{r}{2} + l\right)P'_2 + \sum_{i=1}^{3} R'_i.
\]
Next we show that for any \( r, l \), \( l(D'_r - P'_1) = 0 \) and \( l(D'_r - P'_2) = 0 \), i.e., \( D'_r - P'_1 \not\sim 0 \) and \( D'_r - P'_2 \not\sim 0 \). Suppose that \( D'_r - P'_1 \sim 0 \). Then
\[
0 \sim D'_r - P'_1 - D'_0,
\]
which implies that
\[
\left(\frac{r}{2} + l + 1\right)(m + 1) - r \equiv 0 \mod 2n - 1.
\]
In view of \( s | (2n - 1) \), we get
\[
\left(\frac{r}{2} + l + 1\right)(m + 1) - r \equiv 0 \mod s.
\]
Moreover, since \((m+1)(n+2s) \equiv 1 \mod 2n-1\) we have \((m+1)n \equiv 1 \mod s\). Hence
\[
0 \equiv 2\left(\frac{r}{2} + l + 1\right)(m + 1)n - 2rn \equiv 2(l + 1) \mod s,
\]
which implies that \( l + 1 \equiv 0 \mod s \). In view of \( 0 \leq l \leq 2s - 1 \) we have \( l = s - 1 \) or \( 2s - 1 \).

Let \( l = s - 1 \). Then \( r \) satisfies
\[
\frac{2(s - 1)n - 1}{2s} < r \leq \frac{2sn - 1}{2s}.
\]
Moreover,
\[
\left(\frac{r}{2} + s\right)(m + 1) \equiv r \mod 2n - 1.
\]
In view of \((m+1)(n+2s) \equiv 1 \mod 2n-1\) we have
\[
\frac{r}{2} + s \equiv \left(\frac{r}{2} + s\right)(m + 1)(n + 2s) \equiv r(n + 2s)
\]
\[
\equiv \frac{r}{2}(1 + 4s) \mod 2n - 1,
\]
which implies that \( s(2r - 1) \equiv 0 \mod 2n - 1 \). Hence we may set
\[
2r - 1 = \frac{2n - 1}{s} \cdot k \quad \text{with a positive odd integer } k.
\]
Then
\[
\frac{2(s-1)n-1}{2s} < r = \frac{(2n-1)k+s}{2s} \leq \frac{2sn-1}{2s},
\]
which implies that \(2(k-s)n \leq k-s-1 < 2(k-s+1)n\). If \(k > s\), then
\[
2n \leq \frac{k-s-1}{k-s} = 1 - \frac{1}{k-s} < 1,
\]
a contradiction. If \(k = s\), then \(0 \leq -1\), a contradiction. Let \(k-s = -1\). Since \(k\) and \(s\) are odd, this is a contradiction. If \(k-s < -1\), then
\[
2n < \frac{k-s-1}{k-s+1} = 1 + \frac{2}{-k+s-1} \leq 3,
\]
a contradiction.

Let \(l = 2s - 1\). Then \(r\) satisfies
\[
\frac{2(2s-1)n-1}{2s} < r \leq \frac{4sn-1}{2s}.
\]
Moreover,
\[
\left(\frac{r}{2} + 2s\right)(m+1) \equiv r \mod 2n-1.
\]
Hence
\[
\frac{r}{2} + 2s \equiv \left(\frac{r}{2} + 2s\right)(m+1)(n+2s) \equiv r(1+4s) \mod 2n-1,
\]
which implies that \(2s(r-1) \equiv 0 \mod 2n-1\). Therefore we may set
\[
r - 1 = \frac{2n-1}{s} \cdot k \quad \text{with a positive odd integer } k.
\]
Then
\[
\frac{2(2s-1)n-1}{2s} < r = \frac{(4n-2)k+2s}{2s} \leq \frac{4sn-1}{2s},
\]
which implies that \(4(k-s)n \leq 2k-2s-1 < 2(2k-2s+1)n\). This is a contradiction.

Moreover, we prove that \(D'_r - P'_2 \not\sim 0\). Suppose that \(D'_r - P'_2 \sim 0\). Then
\[
0 \sim D'_r - P'_2 - D'_0,
\]
which implies that
\[
\left(\left(\frac{r}{2} + l\right)(m+1) - r\right)Q' \sim \left(\left(\frac{r}{2} + l\right)(m+1) - r\right)P'_1.
\]
Hence
\[
\left(\frac{r}{2} + l\right)(m+1) - r \equiv 0 \mod 2n-1.
\]
In view of \(s \mid (2n-1)\), we get
\[
\left(\frac{r}{2} + l\right)(m+1) - r \equiv 0 \mod s.
Since \((m + 1)n \equiv 1 \mod s\), we obtain

\[
0 \equiv \left( \frac{r}{2} + l \right)(m + 1)n - rn \equiv r/2 + l - nr \mod s,
\]

which implies that \(0 \equiv r + 2l - 2nr \equiv 2l \mod s\). Since \(s\) is odd, we have \(l \equiv 0 \mod s\), which implies that \(l = 0\) or \(l = s\).

Let \(l = 0\). Then \(2 \leq r \leq (2n - 1)/(2s)\). Moreover,

\[
\frac{r}{2}(m + 1) \equiv r \mod 2n - 1.
\]

Hence

\[
\frac{r}{2} \equiv \frac{r}{2}(m + 1)(n + 2s) \equiv 2sr + \frac{r}{2} \mod 2n - 1,
\]

which implies that \(0 \equiv 2sr \mod 2n - 1\). Therefore \(r \equiv 0 \mod (2n - 1)/s\), which contradicts \(2 \leq r \leq (2n - 1)/(2s)\).

Let \(l = s\). Then

\[
\frac{2sn - 1}{2s} < r \leq \frac{2(s + 1)n - 1}{2s}.
\]

Moreover,

\[
\left( \frac{r}{2} + s \right)(m + 1) \equiv r \mod 2n - 1.
\]

Hence

\[
\frac{r}{2} + s \equiv \left( \frac{r}{2} + s \right)(m + 1)(n + 2s) \equiv \frac{r}{2}(4s + 1) \mod 2n - 1,
\]

which implies that \(s \equiv 2sr \mod 2n - 1\). Hence we may set

\[
2r - 1 = \frac{2n - 1}{s} \cdot k,
\]

where \(k\) is an odd positive integer. If \(k \geq s + 2\), then

\[
2r - 1 \geq \frac{2n - 1}{s} (s + 2) > 2n - 1 + \frac{2n - 1}{s} = \frac{2(s + 1)n - 1}{s} - 1 = 2 \cdot \frac{2(s + 1)n - 1}{2s} - 1 \geq 2r - 1,
\]

a contradiction. Now we have

\[
2r - 1 > 2 \cdot \frac{2sn - 1}{2s} - 1 = 2n - \frac{1}{s} - 1,
\]

which implies that \(2r - 1 \geq 2n - 1\). If \(k \leq s - 2\), then

\[
2n - 1 \leq 2r - 1 \leq \frac{2n - 1}{s} (s - 2) = 2n - 1 - \frac{2(2n - 1)}{s} < 2n - 1,
\]
a contradiction. Hence \( k = s \), which implies that
\[
2r - 1 = \frac{2n - 1}{s} \cdot s = 2n - 1.
\]
Therefore \( r = n \). Since \( r \) is even and \( n \) is odd, this is a contradiction. Hence
\( D'_r - P'_2 \neq 0 \). Thus we obtain the following: Let \( l \in \{0, 1, \ldots, 2s - 1\} \) be fixed. Then for any even \( r > 0 \) with \((2l(n - 1)/(2s)) < r \leq (2(l + 1)n - 1)/(2s)\) we get
\[
l(D'_r) = 1 \quad \text{and} \quad l(D'_r - P'_2) = l(D'_r - P'_2) = 0.
\]
Now in view of \((n, s) = 1\) there is a unique non-negative integer \( q \leq 2s - 1 \) such that \((2q + 1)n \equiv 2s + 1 \mod 4s\). Then we define
\[
r_1 = 2 \cdot \frac{2s + 1 - (2q + 1)n + 4s(n - 1)}{4s} + 1 = 2 \cdot \frac{(4s - 2q - 1)n - (2s - 1)}{4s} + 1.
\]
Note that \( r_1 \) is an odd integer \( \geq 3 \). In fact,
\[
4s - 2q - 1 \geq 4s - 2(2s - 1) - 1 = 1.
\]
Hence in view of \( s \leq (n - 3)/2 \) we get
\[
(4s - 2q - 1)n - (2s - 1) \geq n - (2s - 1) \geq 2s + 3 - (2s - 1) = 4 > 0,
\]
which implies that \( r_1 \geq 3 \). Then we define
\[
D'_{r_1} = -(r_1 + 1)Q' + \frac{(4s - 2q - 1)n - (2s - 1) - 4s(2s - q)}{4s} P'_1
+ \frac{(4s - 2q - 1)n - (2s - 1) + 4s(2s - q)}{4s} P'_2 + \sum_{i=1}^{3} R'_i.
\]
Note that \( \deg D'_{r_1} = 1 \). We prove that \( D'_{r_1} - P'_1 \sim 0 \). In fact, in view of
\[
P'_2 \sim (m + 1)Q' - mP'_1,\]
we have
\[
D'_{r_1} - P'_1 - D'_0 \sim \frac{(4s - 2q - 1)n(m - 1) + (4s(2s - q) + 2s + 1)(m + 1) - 2}{4s}(Q' - P'_1).
\]
Then
\[
(4s - 2q - 1)n(m - 1) + (4s(2s - q) + 2s + 1)(m + 1) - 2
= 4s(n(m - 1) + 2s(m + 1))
- ((2q + 1)n(m - 1) - (2s + 1)(m - 1) + 4sq(m + 1) - 4s).
\]
Let
\[
u = \frac{(n + 2s)(m + 1) - 1}{2n - 1},
\]
which is a positive integer because \((m + 1)(n + 2s) \equiv 1 \mod 2n - 1\). We have
\[
(2q + 1)n(m - 1) - (2s + 1)(m - 1) + 4sq(m + 1) - 4s \\
= 2q((n + 2s)(m + 1) - 2n) + (n + 2s)(m + 1) - 2n - 4sm - m + 1 - 4s \\
= 2q((2n - 1)u + 1 - 2n) + (2n - 1)u + 1 - 2n \\
- 2((n + 2s)(m + 1) - n(m + 1)) - m + 1 \\
= (2n - 1)((2q - 1)u - 2q + m).
\]

Now \((2q - 1)n = (2q + 1)n - 2n \equiv 2s + 1 - 2n \equiv 0 \mod s\), which implies that \(s \mid (2q - 1)\) because \((n, s) = 1\). Moreover,
\[
(-2q + m)n = -2qn + mn \equiv n - 2s - 1 + mn \\
= (n + 2s)(m + 1) - 1 - 2s - 2sm - 2s \equiv 0 \mod s
\]
because \(s \mid (2n - 1)\). In view of \((n, s) = 1\) we get \(s \mid (-2q + m)\). Therefore \(4s \mid ((2q - 1)u - 2q + m)\) because \((4, 2n - 1) = 1\), which implies that
\[
(2n - 1)4s \mid ((2q + 1)n(m - 1) - (2s + 1)(m - 1) + 4sq(m + 1) - 4s).
\]

Moreover,
\[
4s(n(m - 1) + 2s(m + 1)) = 4s((m + 1)(n + 2s) - 1 - (2n - 1)),
\]
which implies that \(4s(2n - 1) \mid 4s(n(m - 1) + 2s(m + 1))\). Hence the integer
\[
\frac{(4s - 2q - 1)n(m - 1) + (4s(2s - q) + 2s + 1)(m + 1) - 2}{4s}
\]
is divisible by \(2n - 1\), which implies that \(D_{r_1}^\prime - P^\prime_1 \sim 0\).

Next we set
\[
r_2 = \frac{(2q + 1)n - 1}{2s} = 2 \cdot \frac{(2q + 1)n - (2s + 1)}{4s} + 1,
\]
which is an odd integer because \((2q + 1)n \equiv 2s + 1 \mod 4s\). Moreover,
\[
3 \leq r_2 \leq 2n - 3.
\]
In fact, \(1 \leq 2q + 1 \leq 4s - 1\) because \(0 \leq q \leq 2s - 1\). Hence
\[
\frac{n - 1}{2s} \leq r_2 = \frac{(2q + 1)n - 1}{2s} \leq \frac{(4s - 1)n - 1}{2s} = 2n - \frac{n + 1}{2s}.
\]

In view of \(0 < 1 \leq s \leq (n - 3)/2\) we have
\[
1 < \frac{n - 1}{n - 3} \leq \frac{n - 1}{2s} \quad \text{and} \quad 2n - \frac{n + 1}{2s} \leq 2n - \frac{n + 1}{n - 3} < 2n - 1.
\]

Now we set
\[
D_{r_2}^\prime = -(r_2 + 1)Q' + \frac{(2q + 1)n - (2s + 1) - 4sq}{4s} P_1^\prime \\
+ \frac{(2q + 1)n - (2s + 1) + 4sq}{4s} P_2^\prime + \sum_{i=1}^{3} R_i,
\]
which is of degree 1. We prove that \( D'_{r_2} - P'_2 \sim 0 \). We have
\[
D'_{r_2} - P'_2 - D'_0 \sim \frac{(2q+1)n(m-1) - (2s+1)(m-1) + 4sq(m+1) - 4s}{4s}(Q' - P'_1).
\]
By the argument in the proof of \( D'_{r_1} - P'_1 \sim 0 \) we show that
\[
\frac{(2q+1)n(m-1) - (2s+1)(m-1) + 4sq(m+1) - 4s}{4s}
\]
is divisible by \( 2n - 1 \), which implies that \( D'_{r_2} - P'_2 \sim D'_0 \sim 0 \).

Now we are in a position to prove that \( \{1, \ldots, g-2, g, 2g-1\} \) is the gap sequence at \( P_1 \) and \( P_2 \). Let \( f \in K(E) \) and set
\[
\text{div}_E(f) = \sum_{P' \in E} m(P')P'.
\]
Then for any non-negative integer \( r \) we obtain
\[
\text{div}_C\left( \frac{f \, dy}{y^{1-r}} \right) = (2nm(P'_1) + r(n - 2s) - 1)P_1 + (2nm(P'_2) + r(n + 2s) - 1)P_2 + (m(Q') - r - 1)\pi^*(Q') + \sum_{i=1}^{3} (m(R'_i) + 1)\pi^*(R'_i) + \sum_{P' \in S} m(P')\pi^*(P'),
\]
where we set \( S = E \setminus \{P'_1, P'_2, Q', R'_1, R'_2, R'_3\} \). Fix \( l \in \{0, 1, \ldots, 2s - 1\} \), and let \( r \) be a positive even integer with \( (2ln - 1)/(2s) < r \leq (2(l+1)n-1)/(2s) \).

If \( f_r \in L(D'_r) \), then
\[
\text{ord}_{P_1} \left( \frac{f \, dy}{y^{1-r}} \right) = 2(l + 1)n - 1 - 2sr \geq 0
\]
and
\[
\text{ord}_{P_2} \left( \frac{f \, dy}{y^{1-r}} \right) = 2sr - (2ln - 1) - 2 \geq 0.
\]
In fact, suppose that \( 2sr - (2ln - 1) = 1 \), which implies that \( r = ln/s \). We know that \( (n, s) = 1 \), \( n \) is odd and \( r \) is even. Hence \( l/s \) must be even, which implies that \( l = 2us \) with a non-negative integer \( u \). In view of \( 0 \leq l \leq 2s - 1 \) we must have \( l = 0 \), which implies that \( r = 0 \). This is a contradiction. Hence \( 2sr - (2ln - 1) - 2 \geq 0 \). Therefore \( f_r \, dy/y^{1-r} \) is a regular 1-form on \( C \), which implies that \( 2n - (2sr - 2nl) \) (resp. \( 2sr - 2nl \)) is a gap at \( P_1 \) (resp. \( P_2 \)).

Now we show that
\[
\left\{ \begin{array}{l}
2sr - 2nl \quad l = 0, 1, \ldots, 2s - 1, \quad r \text{ is even} \geq 0 \\
\quad \text{with} \quad \frac{2ln - 1}{2s} < r \leq \frac{2l + 1)n - 1}{2s} \end{array} \right\} = \{2, 4, \ldots, g - 2\}.
\]
First we show that the above elements $2sr - 2nl$ are distinct. Let $l' \in \{0, 1, \ldots, 2s - 1\}$ with $l' \geq l$ and let $r'$ be even with

$$\frac{2l' - 1}{2s} < r' \leq \frac{2(l' + 1)n - 1}{2s}$$

such that $2sr - 2nl = 2sr' - 2nl'$. Then $n(l' - l) = s(r' - r)$. In view of $(n, s) = 1$ we obtain $s \mid (l' - l)$, which implies that $l' = l$ or $l' = l + s$. Hence we may assume that $l' = l + s$, which implies that $r' - r = n$. Since $r' - r$ is even and $n$ is odd, this is a contradiction. Hence the elements $2sr - 2nl$ are distinct.

Next if $l = 0$ (resp. $l = 2s - 1$), then

$$\frac{2ln - 1}{2s} = -1 2s < 0 \quad \text{(resp.} \quad 2n - 1 \leq \frac{2(l + 1)n - 1}{2s} = 2n - \frac{1}{2s} < 2n = g) \quad \text{.}$$

In view of $r > 0$ the cardinality of the set of the elements $2sr - 2nl$ is equal to that of $\{2, 4, \ldots, g - 2\}$. Moreover, $1 \leq 2sr - 2nl$. In view of $r \leq (2(l + 1)n - 1)/(2s)$ we have $2sr - 2nl \leq g - 1$. Hence we obtain the desired result. Therefore $2, 4, \ldots, g - 2$ are gaps at $P_1$ and $P_2$.

Now if $f_0 \in L(D'_{0})$, then

$$\text{ord}_{P_i} \left( \frac{f_0 dy}{y} \right) = 2n - 1 = g - 1 \quad \text{for } i = 1, 2,$$

which implies that $g$ is also a gap at $P_1$ and $P_2$. Let $f_{r_1} \in L(D'_{r_1} - P_1') \neq \{0\}$. Then

$$\text{ord}_{P_1} \left( \frac{f_{r_1} dy}{y^{1-r_1}} \right) = 4n - 2 = (2g - 1) - 1$$

and

$$\text{ord}_{P_2} \left( \frac{f_{r_2} dy}{y^{1-r_2}} \right) \geq -2n \cdot \frac{(4s - 2q - 1)n - (2s - 1) + 4s(2s - q)}{4s} + r_1(n + 2s) - 1 = 0.$$

Therefore $f_{r_1} dy/y^{1-r_1}$ is a regular $1$-form on $C$, which implies that $2g - 1$ is a gap at $P_1$. Moreover, let $f_{r_2} \in L(D'_{r_2} - P_2') \neq \{0\}$. Then

$$\text{ord}_{P_1} \left( \frac{f_{r_2} dy}{y^{1-r_2}} \right) \geq -2n \cdot \frac{(2q + 1)n - (2s + 1) - 4sq}{4s} + r_2(n - 2s) - 1 = 0$$

and

$$\text{ord}_{P_2} \left( \frac{f_{r_2} dy}{y^{1-r_2}} \right) = (2g - 1) - 1.$$

Therefore $2g - 1$ is a gap at $P_2$. In the same way as in Section 4 we get $G(P_1) = G(P_2) = \{1, 2, \ldots, g - 2, g, 2g - 1\}$. 
References


Department of Mathematics
Kanagawa Institute of Technology
Shimo-ogino 1030, Atsugi-shi
Kanagawa 243-02, Japan
E-mail: komeda@gen.kanagawa-it.ac.jp

Received on 26.11.1996