<table>
<thead>
<tr>
<th>Title</th>
<th>A Note on Class Numbers of Elliptic Function Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Washio, Tadashi</td>
</tr>
<tr>
<td>Citation</td>
<td>長崎大学教育学部自然科学研究報告, vol.26, p.1-4; 1975</td>
</tr>
<tr>
<td>Issue Date</td>
<td>1975-02-28</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/10069/32848">http://hdl.handle.net/10069/32848</a></td>
</tr>
<tr>
<td>NAOSITE</td>
<td><a href="http://naosite.lb.nagasaki-u.ac.jp">http://naosite.lb.nagasaki-u.ac.jp</a></td>
</tr>
</tbody>
</table>
A Note on Class Numbers of Elliptic Function Fields

Tadashi Washio

The Department of Mathematics, Faculty of Education,
Nagasaki University, Nagasaki

(Received October 31, 1974)

Abstract

Let \( m \) be an arbitrary fixed positive integer. It is shown that there exist infinitely many prime numbers \( p \) for which we formally get an elliptic function field over \( \text{GF}(p) \) with the class number \( p+1 \) divisible by \( m \).

\[ \text{§1. Theorems} \]

Let \( p \) be a prime number larger than three. Let \( k \) be the prime field \( \text{GF}(p) \) of characteristic \( p \) and let \( K \) be an elliptic function field over \( k \). Then it is well known that the generating equation of \( K=k(x, y) \) is expressible as the Weierstrass' normal form

\[ y^{2} = 4x^{3} - g_{2}x - g_{3} \]

where \( g_{2}, g_{3} \in k \) and \( g_{2}^{3} - 27g_{3}^{2} \neq 0 \). (See M. Eichler [2; p. 200]).

In this note we shall consider the class number of \( K \) under the restriction \( g_{2}g_{3} = 0 \). Then, by the properties of the Hasse invariant, we can concisely prove the following theorem which we proved in [4] in a disorderly manner on the basis of the elementary number theory.

**Theorem 1.** Let \( p \) be a prime number satisfying \( p \geq 3 \). Let \( K \) be an elliptic function field over \( k=\text{GF}(p) \). Denote by \( h \) the class number of \( K \).

(1) If the generating equation of \( K \) is

\[ y^{2} = 4x^{3} - a, \quad (a \in k, a \neq 0), \]

then a necessary and sufficient condition for the equality \( h = p + 1 \) is the congruence \( p \equiv 2 \mod 3 \).

(2) If the generating equation of \( K \) is

\[ y^{2} = 4x^{3} - ax, \quad (a \in k, a \neq 0), \]

then a necessary and sufficient condition for the equality \( h = p + 1 \) is the congruence \( p \equiv 3 \mod 4 \).

This theorem is useful in giving many examples of algebraic function fields with the class numbers divisible by a fixed integer. As an application of Theorem 1 we
can actually get the following theorem.

**Theorem 2.** Let \( m \) be an arbitrary fixed positive integer. Then there exist infinitely many prime numbers \( p \) for which we can formally get an elliptic function field over \( GF(p) \) with the class number \( p+1 \) divisible by \( m \).

Furthermore, we can extend Theorem 2 as follows.

**Theorem 3.** Let \( m \) and \( n \) be arbitrary fixed positive integers. Then there exist infinitely many prime numbers \( p \) for which we can formally get an elliptic function field over \( GF(p) \) whose class number is divisible by \( m \) and can be put in the form \( p^n+1-(\sqrt[-n]{p})^n(1+(-1)^n) \).

§ 2. **Proof of Theorem 1**

We shall prove Theorem 1 in this section. Let \( p \) be a prime number larger than three. Let \( K \) be an elliptic function field over \( k=GF(p) \). We shall indicate the class number of \( K \) by \( h \) and the Hasse invariant by \( A \). Then the relation between \( h \) and \( A \) is given by the following lemma.

**Lemma 1.** A necessary and sufficient condition for \( h=p+1 \) is \( A=0 \).

**Proof.** We shall denote by \( N \) the number of prime divisors of degree one in \( K \). Since \( K \) is elliptic, it is well known that

\[ h=N \quad \text{and} \quad |p+1-N| \leq 2\sqrt{p} \]

hold. (See M. Eichler[2 ; pp. 303-306]). This inequality means, because of \( p>3 \), that \( N=p+1 \) holds if and only if \( N \equiv 1 \mod p \) holds.

Moreover, we proved in [3] that \( N \equiv 1 \mod p \) holds if and only if \( A=0 \) holds. Therefore a necessary and sufficient condition for \( N=p+1 \) is \( A=0 \). Thus, by making use of \( h=N \), we get lemma 1.

In order to prove Theorem 1, we shall also need the following lemma.

**Lemma 2.** (i) If the generating equation of \( K \) is

\[ y^2=4x^3-a, \quad (a \in k, \ a \neq 0), \]

then \( A=0 \) holds if and only if \( p \equiv 2 \mod 3 \) holds.

(ii) If the generating equation of \( K \) is

\[ y^2=4x^3-ax, \quad (a \in k, \ a \neq 0), \]

then \( A=0 \) holds if and only if \( p \equiv 3 \mod 4 \) holds.

**Proof.** Let the generating equation of \( K \) be generally

\[ y^2=4x^3-g_2x-g_3. \]

Then, by a well-known result of M. Deuring[1 ; p. 255], \( A \) is equal to the coefficient of \( x^{-\frac{p-1}{2}} \) in the following polynomial in \( x^{-1} \).

\[ (-g_2x^{-3}-g_2x^{-2}+4)^{\frac{p-1}{2}}. \]

Thus, in case (i) we easily obtain
A Note on Class Numbers of Elliptic Function Fields

\[ A = \begin{cases} \frac{p-1}{2} & (-4^a) \neq 0 \text{ if } p \equiv 1 \mod 3, \\
\frac{p-1}{6} & \neq 0 \text{ if } p \equiv 1 \mod 3, \text{ and} \\
0 & \text{if } p \equiv 2 \mod 3. \\
\end{cases} \]

Similarly, in case (ii) we get

\[ A = \begin{cases} \frac{p-1}{2} & (-4^a) \neq 0 \text{ if } p \equiv 1 \mod 4, \\
\frac{p-1}{4} & \neq 0 \text{ if } p \equiv 3 \mod 4, \text{ and} \\
0 & \text{if } p \equiv 3 \mod 4. \\
\end{cases} \]

Therefore Lemma 2 is completely proved.

Theorem 1 now follows immediately from Lemma 1 and Lemma 2.

§ 3. Proofs of Theorems 2 and 3

We shall prove Theorem 2 and Theorem 3 in this section.

Proof of Theorem 2. Let \( m \) be an arbitrary fixed positive integer. We shall assume that \( t=3 \) or \( t=4 \). Then, since \( tm \) and \( tm-1 \) are coprime, there exist infinitely many prime numbers \( p \) satisfying the congruence \( p \equiv tm-1 \mod tm \) by making use of the Dirichlet's theorem.

If we choose such a prime \( p \), it is obvious that \( p \equiv t-1 \mod t \) and \( m \mid p+1 \) where the notation \( c \mid d \) means that \( d \) is divisible by \( c \). So we shall put \( k=GF(p), \ K=k(x,y) \) and \( y^2=4x^3-ax \) or \( y^2=4x^3-ax^4 \), where \( a \) means an arbitrary non-zero element in \( k \), according as \( p \equiv 2 \mod 3 \) or \( p \equiv 3 \mod 4 \). Then the desired properties of \( K \) follow at once from Theorem 1; the class number \( h \) of \( K \) satisfies \( h=p+1 \) and \( m \mid h \). Theorem 2 is thereby proved.

Proof of Theorem 3. Proceeding as in the proof of Theorem 2, we shall denote by \( K^n \) the constant field extension of \( K \) of degree \( n \). Since \( k \) is finite, it is clear that \( K^n \) is an elliptic function field with \( GF(p^n) \) as its field of constants.

The class number \( h_n \) of \( K^n \) is divisible by \( h \). This is due to the fact that there is a degree preserving natural isomorphism of the divisor class group of \( K \) into the divisor class group of \( K^n \). Hence we get \( m \mid h_n \) because of \( m \mid h \). In order to compute \( h_n \), we shall consider the following polynomial in \( U \).

\[ L(U)=1+(N-p)U+pu^2 \]

where \( N \) means the number of prime divisors of degree one in \( K \).

As is well known in M. Eichler [2; p. 305], if we put

\[ L(U)=(1-w_1U)(1-w_2U) \]

then \( h_n \) is expressed by

\[ h_n=p^n+1-(w_{1}^n+w_{2}^n). \]

Since \( N=h \) and \( h=p+1 \) hold in our case, we have
Therefore we get

\[ h_n = \frac{p^* + 1 - (\sqrt{-p})^*}{1 + (-1)^n}. \]

This completes the proof of Theorem 3.

References