<table>
<thead>
<tr>
<th>Title</th>
<th>On elliptic function fields with the class number p+1 over finite prime fields of characteristic p≠2,3</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.24, p.7-11; 1973</td>
</tr>
<tr>
<td>Issue Date</td>
<td>1973-02-28</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/10069/32974">http://hdl.handle.net/10069/32974</a></td>
</tr>
</tbody>
</table>

NAOSITE: Nagasaki University’s Academic Output SITE
http://naosite.lb.nagasaki-u.ac.jp
On Elliptic Function Fields with the Class Number $p+1$ over Finite Prime Fields of Characteristic $p \neq 2, 3$

Tadashi WASHIO

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

(Received Oct. 31, 1972)

Abstract

Let $k$ be a finite prime field of characteristic $p$ which differs from 2 and 3. Let $K$ be an elliptic function field over $k$ and denote by $h$ the class number of $K$. It is shown that, in the case where $K$ is defined by the equation $y^2 = x^3 - a$, $(a \neq 0, a \in k)$, a necessary and sufficient condition of the equality $h = p + 1$ is the congruence $p \equiv 2 \mod 3$, and that, in the case where $K$ is defined by the equation $y^2 = x^3 - ax$, $(a \neq 0, a \in k)$, a necessary and sufficient condition of the equality $h = p + 1$ is the congruence $p \equiv 3 \mod 4$.

§ 1. Introduction

Let $k$ be a finite prime field of characteristic $p$ which differs from 2 and 3, and let $K$ be an elliptic function field over $k$. Then we know that $K = k(x, y)$ can be defined by the equation of the Weierstrass' normal form $y^2 = 4x^3 - g_2x - g_3$, where $g_2, g_3 \in k$ and $g_2^3 - 27g_3^2 \neq 0$. We want to study of the class number $h$ of $K$ under the assumption that $g_3 = 0$ or $g_2 = 0$.

As $p$ differs from 2, we may suppose, with no loss in generality, that $K = k(x, y)$ is defined by $y^2 = x^3 - a$ or $y^2 = x^3 - ax$, $(a \neq 0, a \in k)$. The result of this note is:

Theorem

Let $k$ be a finite prime field $GF(p)$ of characteristic $p$ which differs from 2 and 3. Then, (i) in the case where $K$ is defined by the equation $y^2 = x^3 - a$, $(a \neq 0, a \in k)$, a necessary and sufficient condition of the equality $h = p + 1$ is the congruence $p \equiv 2 \mod 3$; and
(ii) In the case where $K$ is defined by the equation $y^2 = x^3 - ax$, $(a \neq 0, a \in \mathbb{k})$, a necessary and sufficient condition of the equality $h = p + 1$ is the congruence $p \equiv 3 \mod 4$.

In order to prepare for the proof of the theorem, we shall find out formulas which are useful to estimate $h$. Let $N_1$ be the number of prime divisors of degree one of $K$. As is well known, $h$ equals to $N_1$ in our case. (See Eichler[1], p.303). Denote by the symbol $N[F(x, y) \equiv 0 \mod p]$ the number of solutions of the congruence $F(x, y) \equiv 0 \mod p$ in two variables $x, y \mod p$, where $F(x, y)$ means a polynomial with integral coefficients.

Then it is well known that the following equality holds. $N_1 = 1 + N[f(x) \equiv y^2 \mod p]$ where $f(x) = x^3 - a$ or $x^3 - ax$. (See Hasse[2], p.154). So we get the formula

\[ h = 1 + N[f(x) \equiv y^2 \mod p]. \]

Moreover, let $m$ be the number of solutions of the congruence $f(x) \equiv 0 \mod p$ in one variable $x \mod p$ and let $m'$ be the number of elements $z$ in $k$ such that $f(z) \neq 0$ and $f(z)$ are square in $k$. Then it is clear that the formula (1) can be transformed into the formula

\[ h = 1 + m + 2m'. \]

We shall prove Part (i) and (ii) in the theorem separately in Section 2 and Section 3 with the help of the formulas (1) and (2).

\section{2. The case in which $K = \mathbb{k}(x, y)$ is defined by $y^2 = x^3 - a$, $(a \neq 0, a \in \mathbb{k})$}

We shall identify $k$ with the set $\{0, 1, \ldots, p-1\}$ which means a complete residue system of $p$ and we shall denote by $\bar{n}$ the residue of $n \mod p$ in $\{0, 1, \ldots, p-1\}$ as far as $n$ is a rational number whose denominator and $p$ are coprime. Now we shall prove Part (i) in the theorem.

Under the assumption $p \equiv 2 \mod 3$, we can get $h = p + 1$ as follows. The set $\{0, 1, \ldots, p-1\}$ is a complete system of the third power residue classes of $p$ because of $p \equiv 2 \mod 3$. So a set $\{x^3 \equiv a \mod p \}$ coincides with the set $\{0, 1, \ldots, p-1\}$ for all $a \in \mathbb{k}$. Judging from the fact that the number of quadratic residues of $p$ in $\{1, 2, \ldots, p-1\}$ equals to $\frac{p-1}{2}$, we have $m=1$ and $m' = \frac{p-1}{2}$. Hence, by means of the formula (2), $h = p + 1$ holds.

Suppose, on the other hand, that $p \equiv 1 \mod 3$. For the sake of convenience, we shall define the symbol $\varepsilon(n)$ for every integer $n$ to mean 1 if $n$ is a third power residue of $p$, and -1 if $n$ is a third power nonresidue of $p$. Then, since the same values appear three times in the series $\{-a, \frac{1}{3}(a-a), \ldots, \frac{p-1}{3}(a-a)\}$ except for $-a$ which appears once for all in it, we can easily show that
On Elliptic Function Fields with the Class Number \( p+1 \) over Finite Prime Fields of Characteristic \( p \neq 2, 5 \)

\[
m = \begin{cases} 
3 & \text{if } \varepsilon(a) = 1 \\
0 & \text{if } \varepsilon(a) = -1 \text{ and }
\end{cases}

\]

\[
m' = \begin{cases} 
1 \mod 3 & \text{if } \left( \frac{-a}{p} \right) = 1 \\
0 \mod 3 & \text{if } \left( \frac{-a}{p} \right) = -1,
\end{cases}
\]

where the notation \( \left( \frac{-a}{p} \right) \) means the Kronecker's symbol.

Hence the formula (2) leads to

\[
h = \begin{cases} 
0 \mod 6 & \text{if } \varepsilon(a) = 1 \text{ and } \left( \frac{-a}{p} \right) = 1 \\
4 \mod 6 & \text{if } \varepsilon(a) = 1 \text{ and } \left( \frac{-a}{p} \right) = -1 \\
3 \mod 6 & \text{if } \varepsilon(a) = -1 \text{ and } \left( \frac{-a}{p} \right) = 1 \\
1 \mod 6 & \text{if } \varepsilon(a) = -1 \text{ and } \left( \frac{-a}{p} \right) = -1,
\end{cases}
\]

so that we get the inequality \( h \neq p+1 \) because of \( p+1 \equiv 2 \mod 6 \). Thus Part (i) in the theorem is completely proved.

§ 3. The case in which \( K = k(x, y) \) is defined by \( y^2 = x^3 - ax \), \( a \neq 0, a \in k \)

We shall prove Part (ii) in the theorem. In the case \( p \equiv 3 \mod 4 \), we can obtain \( h = p+1 \) as is shown below. It is clear that

\[
m = \begin{cases} 
3 & \text{if } \left( \frac{a}{p} \right) = 1 \\
1 & \text{if } \left( \frac{a}{p} \right) = -1.
\end{cases}
\]

Define the symbol \( r_i \) to mean \( \frac{i}{a} \) as long as an integer \( i \) is not a root of \( x^3 - ax \equiv 0 \mod p \). Then, since \( \left( \frac{i^3 - ai}{p} \right) = \left( \frac{i^3}{p} \right) = \left( \frac{r_i}{p} \right) \) holds, \( m' \) equals to the number of quadratic residues of \( p \) in the series \( \{ r_i ; 1 \leq i \leq p-1 \text{ and } i \text{ is not a root of } x^3 - ax \equiv 0 \mod p \} \). So we get

\[
m' = \frac{1}{2} \sum_i \left( \frac{r_i}{p} \right) + 1 \]

\[
= \begin{cases} 
\frac{p-3}{2} + \frac{1}{2} \sum_i \left( \frac{r_i}{p} \right) & \text{if } \left( \frac{a}{p} \right) = 1 \\
\frac{p-1}{2} + \frac{1}{2} \sum_i \left( \frac{r_i}{p} \right) & \text{if } \left( \frac{a}{p} \right) = -1.
\end{cases}
\]

But \( \sum_i \left( \frac{r_i}{p} \right) = 0 \) follows from \( \left( \frac{p-r_i}{p} \right) = -\left( \frac{r_i}{p} \right) \) and \( r_{p-i} = p-r_i \) for every integer \( i \) which is not a root of \( x^3 - ax \equiv 0 \mod p \). Hence we have
L. Tadashi WASHIO

\[ m' = \begin{cases} 
\frac{p-3}{2} & \text{if } \left( \frac{a}{p} \right) = 1 \\
\frac{p-1}{2} & \text{if } \left( \frac{a}{p} \right) = -1.
\end{cases} \]

Therefore the formula (2) lets \( h = p + 1 \) hold.

Finally, under the assumption of the congruence \( p \equiv 1 \mod 4 \), we want to get the inequality \( h \neq p + 1 \). In order to calculate \( h \), we shall modify the process described by Hasse [2], pp. 161-165, in which he dealt only in the case \( a = 1 \). As is well known,

\[ N[{x^3 - ax \equiv y^2} \mod p] = \sum_{x \mod p} \left\{ 1 + \left( \frac{x^2 - ax}{p} \right) \right\} \]

\[ = p + \sum_{x \mod p} \left( \frac{x^2 - ax}{p} \right). \]

But judging from \( \sum_{x \mod p} \left( \frac{x^2 - ax}{p} \right) = -1 \), we get

\[ \sum_{x \mod p} \left( \frac{x^2 - ax}{p} \right) = \sum_{x \mod p} \left( \frac{x}{p} \right) \left( \frac{x^2 - ax}{p} \right) \]

\[ = \sum_{x \mod p} \left( 1 + \left( \frac{x}{p} \right) \right) \left( \frac{x^2 - ax}{p} \right) = \sum_{x \mod p} \left( \frac{x^2 - ax}{p} \right) + 1 \]

\[ = \sum_{x \mod p} \left( 1 + \left( \frac{x^2 - ax}{p} \right) \right) = p + 1 \]

\[ = N[{x^2 - ax \equiv y^2} \mod p] - 1. \]

so that we obtain the following formula

(3) \[ N[{x^3 - ax \equiv y^2} \mod p] = N[{x^4 - ax \equiv y^2} \mod p] + 1. \]

Thus it will be sufficient to compute \( N[{x^4 - ax \equiv y^2} \mod p] \) instead of \( N[{x^3 - ax \equiv y^2} \mod p] \). We shall now estimate \( N[{x^4 - ax \equiv y^2} \mod p] \). Denote by the symbol \( N_u[G(z) \equiv w \mod p] \), for every integer \( w \) and every polynomial \( G(z) \) having the integral coefficients, the number of solutions of the congruence \( G(z) \equiv w \mod p \) in one variable \( z \mod p \). Then we can easily show

\[ N[{x^4 - ax \equiv y^2} \mod p] = \sum_{u \equiv w \mod p} N_u[{x^4 \equiv u} \mod p] N_u[{y^2 \equiv v} \mod p] \]

\[ = \sum_{u \equiv w \mod p} N_u[{x^4 \equiv u} \mod p] \left( 1 + \left( \frac{v}{p} \right) \right). \]

\( N_u[{x^4 \equiv u} \mod p] \) can be calculated as follows. If \( g \) is a primitive root of \( p \) and \( t \) is the exponent of a power of \( g \) which is congruent to \( b \mod p \) for an integer \( b \) such that \( b \equiv 0 \mod p \), then we put \( X_p(b) = \sqrt{-1} \). If \( b \equiv 0 \mod p \), put \( X_p(b) = 0 \). Then we clearly get

\[ N_u[{x^4 \equiv u} \mod p] = 1 + X_p(u) + \left( \frac{u}{p} \right) + \overline{X}_p(u), \]

where \( \overline{X}_p(u) \) means the complex conjugate of \( X_p(u) \).

Hence we have

\[ N[{x^4 - ax \equiv y^2} \mod p] = \sum_{u \equiv w \mod p} \left( 1 + X_p(u) + \left( \frac{u}{p} \right) + \overline{X}_p(u) \right) \left( 1 + \left( \frac{v}{p} \right) \right) \]
On Elliptic Function Fields with the Class Number $p + 1$ over
Finite Prime Fields of Characteristic $p \neq 2$, 3

\[ p = \sum_{u \mod p} \left( \frac{u-a}{p} \right) \lambda_p(u) + \sum_{u \mod p} X_p(u) \left( \frac{u-a}{p} \right) + \sum_{u \mod p} \overline{X}_p(u) \left( \frac{u-a}{p} \right). \]

Put \( \pi = \sum_{u \mod p} X_p(u) \left( \frac{u-a}{p} \right) \) and \( \overline{\pi} = \sum_{u \mod p} \overline{X}_p(u) \left( \frac{u-a}{p} \right) \).

Then \( \overline{\pi} \) is the complex conjugate of \( \pi \) and we obtain \( N[x^4 - a = y^2 \mod p] = p - 1 + \pi + \overline{\pi}, \) because of \( \sum_{u \mod p} \left( \frac{u-a}{p} \right) = -1. \) Hence the formulas (1) and (3) lead to \( h = p + 1 + \pi + \overline{\pi}. \)

On the other hand, we can easily get \( |\pi|^2 = p \) by means of the slight modification of the proof in Hasse [2], p. 164, where he dealt only in the case \( a = 1. \) This implies that \( \pi + \overline{\pi} \neq 0 \) holds, judging from the fact that \( \pi \) is of the form \( c + d\sqrt{-1} \) with rational integers \( c \) and \( d \) and \( p \) is an odd prime. Thus we have \( h = p + 1 \) in the case \( p \equiv 1 \mod 4. \) Hence the proof of Part (ii) in the theorem is complete.

Bibliography
