This is a mock-up of a page from a document. The page contains information about a document titled "The number of rational points of certain hyperelliptic curves of genus 2" by Washio, Tadashi and Kodama, Tetsuo. The document is from Nagasaki University's Academic Output SITE and is available at the URL http://naosite.lb.nagasaki-u.ac.jp.
The number of rational points of certain hyperelliptic curves of genus 2

Tadashi WASHIO and Tetsuo KODAMA*

Department of Mathematics, Faculty of Education, Nagasaki University, Nagasaki 852, Japan
(Received October 29, 2004)

Abstract

This note is devoted to studying a certain hyperelliptic curve of genus two defined over a finite prime field of characteristic $p$ which has $p + 1$ rational points, where the number of rational points of an algebraic curve means the number of degree one prime divisors of its function field.

1. Introduction

Let $p$ be an odd prime number and $\mathbb{Z}_p$ a prime finite field of characteristic $p$. For an elliptic curve $C$ defined over $\mathbb{Z}_p$ we denote by $N$ the number of rational points of $C$ over $\mathbb{Z}_p$. In this note the number of rational points of an algebraic curve over a finite field $F$ means the number of degree one prime divisors of its function field defined over $F$. For the general theory of algebraic function fields of one variable, refer to Deuring[1].

If $N = p + 1$ then the curve $C$ is said to be supersingular. For instance, if the curve $C$ is defined by $Y^2 = X^3 + D (D \neq 0)$ and $p \equiv 2 \pmod{3}$ then $N = p + 1$ and if the curve $C$ is defined by $Y^2 = X^3 - DX (D \neq 0)$ and $p \equiv 3 \pmod{4}$ then $N = p + 1$, (see Ireland and Rosen[3]). If the curve $C$ is defined by $Y^2 = X(X^2 + X + 1/8)$ and $p \equiv 2 \pmod{3}$ then $N = p + 1$, (see [4]) and if the curve $C$ is defined by $Y^2 = X(X^2 + X + 1/3)$ and $p \equiv 2 \pmod{3}$ then $N = p + 1$, (see [5]).

In the present note we want to consider a curve with genus two of the form $Y^2 = X(X^2 + X + s)(X^2 + X + t)$ instead of a curve $Y^2 = X(X^2 + X + r)$ with genus one and to get a similar result, that is, we will prove the following result.

*Professor emeritus, Kyushu University, Fukuoka 812, Japan.
Assume that \( p \) is a prime number satisfying \( p \equiv 9 \pmod{16} \) and denote by \( r \) the element in \( \mathbb{Z}_p \) satisfying \( 8r = 1 \). Moreover denote by \( s \) and \( t \) two distinct solutions in \( \mathbb{Z}_p \) of the equation \( X^2 - 2rX + r^2/2 = 0 \), where we have known that two polynomials \( X^2 + X + s \) and \( X^2 + X + t \) are irreducible over \( \mathbb{Z}_p \), (see [6]). Then the hyperelliptic curve \( Y^2 = X(X^2 + X + s)(X^2 + X + t) \) has \( p + 1 \) rational points over \( \mathbb{Z}_p \).

2. Roots of biquadratic equations

In order to calculate the number of rational points, we prepare some notation and some lemmas as follows. Let \( p \) be an odd prime number and denote a prime field \( \mathbb{Z}_p \) of characteristic \( p \) by \( F \). Furthermore we denote by \( \chi \) a multiplicative quadratic character of \( F \), namely, \( \chi \) means the Legendre symbol \( (\bullet/p) \).

Throughout this section we assume \( p \equiv 9 \pmod{16} \) and denote by \( r \) the element in \( F \) satisfying \( 8r = 1 \). According to the second complementary law, we have \( \chi(r) = 1 \). Moreover denote by \( s \) and \( t \) two distinct solutions in \( F \) of the equation

\[
X^2 - 2rX + r^2/2 = 0.
\]

Then we know that two polynomials \( X^2 + X + s \) and \( X^2 + X + t \) are irreducible over \( F \) and that \( \chi(s) = \chi(t) = -1 \), (see [6]). Now we put

\[
f(X) = (X^2 + X + s)(X^2 + X + t)
\]

and discuss properties of the roots of the biquadratic equation \( f(X) = \alpha \) for an element \( \alpha \in F \).

To do so, we define

\[
M = \{ [x, x'] ; x \in F, x' = -1 - x, \chi(xx') = 1 \},
\]

\[
M^+ = \{ [x, x'] ; x \in F, x' = -1 - x, \chi(x) = \chi(x') = 1 \},
\]

\[
M^- = \{ [x, x'] ; x \in F, x' = -1 - x, \chi(x) = \chi(x') = -1 \},
\]

\[
M^\pm = \{ [x, x'] ; x \in F, x' = -1 - x, \chi(x) = -\chi(x') \},
\]

where we assume \([x, x'] = [x', x]\). Notice that \( f(x) = f(x') \) for \( x \in F \) if \( x' = -1 - x \).
The number of rational points of certain hyperelliptic curves of genus 2

**Lemma 1.** (1) The roots of the equation $f(X) = 4r^3$ are given by $X = 0, -1$ and $-4r$ and then $[-4r, -4r] \in M^+$. 

(2) The roots of the equation $f(X) = -4r^3$ are given by $X = -4s$ and $-4t$ and then $[-4s, -4t] \in M^-$. 

**Proof.** The assertions follow at once from

\[ f(X) - 4r^3 = f(X) - f(0) = X(X + 1)(X + 4r)^2, \]
\[ f(X) + 4r^3 = (X^2 + X + r)^2 = \{(X + 4s)(X + 4t)\}^2, \]
\[ \chi(-1) = \chi(r) = 1, \]
\[ \chi(s) = \chi(t) = -1. \]

**Lemma 2.** Let $a \in F$ and assume that $[a, a'] \in M$. Moreover set

\[ b = \frac{-1 + 2\sqrt{aa'}}{2}, \quad b' = -1 - b = \frac{-1 - 2\sqrt{aa'}}{2}. \]

If $f(a) \neq 0, \pm 4r^3$ then the equation $f(X) = f(a)$ has four distinct roots $a, a', b$ and $b'$ in $F$. In this case, if $[a, a'] \in M^+$ then $[b, b'] \in M^+$ and if $[a, a'] \in M^-$ then $[b, b'] \in M^-$. 

**Proof.** Since $\chi(aa') = 1$ we have $b, b' \in F$, and further we can get the following factorization

\[ f(X) - f(a) = (X^2 + X - a^2 - a)(X^2 + X + a^2 + a + 2r) \]
\[ = (X - a)(X - a')(X - b)(X - b'). \]

Here, because of

\[ b^2 + b + a^2 + a + 2r = 0, \]
\[ b'^2 + b' + a'^2 + a' + 2r = 0, \]

we obtain

\[ (b + a + 4r)^2 = 2ab, \quad (b' + a' + 4r)^2 = 2a'b'. \]
These lead that \( \chi(a) = \chi(b) \) and \( \chi(a') = \chi(b') \). Therefore we get \( \chi(a) = \chi(a') = \chi(b) = \chi(b') \), and this completes the proof.

**Lemma 3.** Let \( a \in F \) and assume that \([a, a'] \in M\). Moreover set

\[
\begin{align*}
  c &= \frac{-1 + \sqrt{2}(\sqrt{aa'} + a + 4r)}{2}, & c' &= -1 - c = \frac{-1 - \sqrt{2}(\sqrt{aa'} + a + 4r)}{2}, \\
  d &= \frac{-1 + 2\sqrt{cc'}}{2}, & d' &= -1 - d = \frac{-1 - 2\sqrt{cc'}}{2}.
\end{align*}
\]

If \( f(a) \neq 0, \pm 4r^3 \) then the equation \( f(X) = -f(a) \) has four distinct roots \( c, c', d \) and \( d' \) in \( F \). In this case, if \([a, a'] \in M^+ \) then \([c, c'], [d, d'] \in M^- \) and if \([a, a'] \in M^- \) then \([c, c'], [d, d'] \in M^+ \).

**Proof.** From \( \chi(aa') = 1 \) and \( \chi(2) = 1 \) we obtain \( c, c' \in F \), and we have also the factorization

\[
f(X) + f(a) = \{X^2 + X + r - \sqrt{aa'}(a + 4r)\}\{X^2 + X + r + \sqrt{aa'}(a + 4r)\}.
\]

It is clear that \( c \) and \( c' \) are the roots of the quadratic equation

\[
X^2 + X + r - \sqrt{aa'}(a + 4r) = 0,
\]

and hence \( c \) and \( c' \) satisfy that \( f(c) = f(c') = -f(a) \). Moreover it is easy to check

\[
4ac = (2 - \sqrt{2})\{\sqrt{aa'} + (1 + \sqrt{2})a\}^2,
\]

\[
4a'c' = (2 + \sqrt{2})\{a' + (1 - \sqrt{2})\sqrt{aa'}\}^2.
\]

Here, By making use of \( \{2 + \sqrt{2}, 2 - \sqrt{2}\} = \{16s, 16t\} \) and of \( \chi(s) = \chi(t) = -1 \) we get \( \chi(2 + \sqrt{2}) = \chi(2 - \sqrt{2}) = -1 \). These yield that \( \chi(c) = -\chi(a) \) and \( \chi(c') = -\chi(a') \).

Therefore we see that if \([a, a'] \in M^+ \) then \([c, c'] \in M^- \) and if \([a, a'] \in M^- \) then \([c, c'] \in M^+ \). As \( f(X) + f(a) = f(X) - f(c) \), the required result for \( d \) and \( d' \) follows immediately from Lemma 2.
3. The number of rational points

Our main result is stated as follows.

**Theorem.** Let \( p \) be a prime number satisfying \( p \equiv 9 \pmod{16} \) and denote by \( r \) the element in \( \mathbb{Z}_p \) satisfying \( 8r = 1 \). Moreover denote by \( s \) and \( t \) two distinct solutions in \( \mathbb{Z}_p \) of the equation \( X^2 - 2rX + r^2/2 = 0 \). Then the number of rational points of the hyperelliptic curve \( Y^2 = X(X^2 + X + s)(X^2 + X + t) \) defined over \( \mathbb{Z}_p \) is equal to \( p + 1 \).

**Proof.** Denote \( \mathbb{Z}_p \) by \( F \). Let \( N \) be the number of rational points of the hyperelliptic curve \( Y^2 = X(X^2 + X + s)(X^2 + X + t) \) defined over \( F \). Then it is well-known that \( N \) is written \( N = p + 1 + S \) with

\[
S = \sum_{x \in F} \chi(x(x^2 + x + s)(x^2 + x + t)),
\]

where \( \chi \) means the quadratic character of \( F \), (see Hasse[2]). Put

\[
f(X) = (X^2 + X + s)(X^2 + X + t).
\]

Then, using Lemma 1, we have

\[
S = \chi(-f(-1)) + \chi(-4rf(-4r)) + \chi(-4sf(-4s)) + \chi(-4tf(-4t))
+ \sum_{[x,x'] \in M \setminus \{[-4r,-4r],[-4s,-4t]\}} \left( \chi(x) + \chi(x') \right) \chi(f(x))
+ \sum_{[x,x'] \in M^{\pm}} \left( \chi(x) + \chi(x') \right) \chi(f(x))
= 2\left\{ \sum_{[x,x'] \in M^{\pm} \setminus \{[-4r,-4r]\}} \chi(f(x)) - \sum_{[y,y'] \in M^{\pm} \setminus \{[-4s,-4t]\}} \chi(f(y)) \right\}.
\]

In order to prove \( S = 0 \) we consider the pair \( [x,x'] \in M \setminus \{[-4r,-4r],[-4s,-4t]\} \). If we put \( \alpha = f(x) \) then \( \alpha \neq 0, \pm 4r^3 \) and so, applying Lemmas 2 and 3, we can get four roots \( a, a', b \) and \( b' \) in \( F \) of the equation \( f(X) = \alpha \) and four roots \( c, c', d \) and \( d' \) in \( F \) of the equation \( f(X) = -\alpha \). In this case it is obvious that \( \chi(\alpha) = \chi(-\alpha) \) and that

\[
\chi(a) = \chi(a') = \chi(b) = \chi(b') = -\chi(c) = -\chi(c') = -\chi(d) = -\chi(d').
\]
Therefore we see that, for each pair \([x, x'] \in M^+ \setminus \{[-4r, -4r]\}\), there exists some pair \([y, y'] \in M^- \setminus \{[-4s, -4t]\}\) satisfying \(f(y) = -f(x)\) and that its converse is true. Thus we have \(S = 0\) and so \(N = p + 1\) which is the requested assertion.

References


