Bull. Fac. Educ., Nagasaki Univ. : Natural Science No .73, 1 ~ 7 (2005. 6)

The number of rational points of certain hyperelliptic curves of genus 3

To the Memory of Professor Katsumi Shiratani

Tadashi WASHIO and Tetsuo KODAMA*

Department of Mathematics, Faculty of Education,
Nagasaki University, Nagasaki 852, Japan
(Received March 15, 2005)

Abstract

This note is devoted to studying a certain hyperelliptic curve of genus three 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 $\mathbf{Z}_p$ a prime finite field of characteristic p. For an elliptic curve C defined over $\mathbf{Z}_p$ we denote by N the number of rational points of C over $\mathbf{Z}_p$. 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 $p \equiv 5 \pmod 8$ then $N = p+1$,(see [4]) and if the curve C is defined by $Y^2 = X(X^2+X+1/3)$ and $p \equiv 2$ (mod 3) then $N = p+1$, (see [5]).

Moreover let $p \equiv 9 \pmod{16}$ and denote by s and t two distinct solutions in $\mathbf{Z}_p$ of the equation $X^2 - 2rX + r^2/2 = 0$, where r means the element in $\mathbf{Z}_p$ satisfying $8r = 1$. Then the hyperelliptic curve

$$Y^2 = X(X^2 + X + s)(X^2 + X + t)$$

*Professor emeritus, Kyushu University, Fukuoka 812, Japan.

has $p+1$ rational points over $\mathbf{Z}_p$, (see [7]).

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

Assume that p is a prime number satisfying $p \equiv 13 \pmod{24}$ and denote by r the element in $\mathbf{Z}_p$ satisfying $8r = 1$. Furthermore denote by s and t two distinct solutions in $\mathbf{Z}_p$ of the equation $X^2 - 2rX + r^2/4 = 0$. Then three polynomials X^2+X+r, X^2+X+s and X^2+X+t are irreducible over $\mathbf{Z}_p$ and the hyperelliptic curve

$$Y^2 = X(X^2+X+r)(X^2+X+s)(X^2+X+t)$$

has $p+1$ rational points over $\mathbf{Z}_p$.

2. Roots of sextic eqations

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 $\mathbf{Z}_p$ of characteristic p by F. Furthermore we denote by χ a multiplicative quadratic character of F, namely, χ means the Legendre symbol $(\bullet/p)$.

Throughout this section we assume $p \equiv 13 \pmod{24}$ and denote by r the element in F satisfying $8r = 1$. It is clear that the assumption $p \equiv 13 \pmod{24}$ leads to $\chi(-1) = \chi(3) = 1$ and $\chi(2) = \chi(r) = -1$. The polynomial X^2+X+r is irreducible over F because its discriminant is equal to $4r$.

Moreover denote by s and t two distinct solutions in F of the equation

$$X^2 - 2rX + r^2/4 = 0.$$

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

$$g(X) = (X^2+X+r)(X^2+X+s)(X^2+X+t)$$

and discuss properties of the roots of the sextic equation $g(X) = \alpha$ for an element $\alpha \in F$.

To do so, we define

$$\begin{aligned}
M &= \{\,[x,x']\,;\,x \in F,\ x' = -1-x,\ \chi(xx') = 1\,\},\\
M^{+} &= \{\,[x,x']\,;\,x \in F,\ x' = -1-x,\ \chi(x) = \chi(x') = 1\,\},\\
M^{-} &= \{\,[x,x']\,;\,x \in F,\ x' = -1-x,\ \chi(x) = \chi(x') = -1\,\},\\
M^{\pm} &= \{\,[x,x']\,;\,x \in F,\ x' = -1-x,\ \chi(x) = -\chi(x')\,\},
\end{aligned}$$

where we assume $[x,x'] = [x',x]$. Notice that $g(x) = g(x')$ for $x \in F$ if $x' = -1-x$.

LEMMA 1. (1) *The roots of the equation* $g(X) = 2r^4$ *are given by* $X = 0, -1, -2r$ *and* $-6r$ *and then* $[-2r, -6r] \in M^{+}$.

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

PROOF. The assertion (1) follows from $\chi(-1) = \chi(3) = 1$ and

$$g(X) - 2r^4 = X(X+1)\{(X+2r)(X+6r)\}^2.$$

Similarly the assertion (2) follows from $\chi(s) = \chi(t) = -1$ and

$$g(X) + 2r^4 = \{(X+4r)(X+4s)(X+4t)\}^2.$$

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

$$\begin{aligned}
b &= \frac{-1+a+4r+\sqrt{3aa'}}{2}, \quad b' = -1-b = \frac{-1-a-4r-\sqrt{3aa'}}{2},\\
c &= \frac{-1+a+4r-\sqrt{3aa'}}{2}, \quad c' = -1-c = \frac{-1-a-4r+\sqrt{3aa'}}{2}.
\end{aligned}$$

If $g(a) \neq 0, \pm 2r^4$ *then the equation* $g(X) = g(a)$ *has six distinct roots* a, a', b, b', c *and* c' *in* F. *In this case, if* $[a,a'] \in M^{+}$ *then* $[b,b']$, $[c,c'] \in M^{+}$ *and if* $[a,a'] \in M^{-}$ *then* $[b,b']$, $[c,c'] \in M^{-}$.

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

$$g(X) - g(a) = (X^2+X+r)^3 - 6r^3(X^2+X+r) - (r-aa')^3 + 6r^3(r-aa')$$

$$
\begin{aligned}
&= (X^2+X+aa')\{(X^2+X+r)^2+(r-aa')(X^2+X+r) \\
&\quad +(r-aa')^2-6r^3\} \\
&= (X-a)(X-a')(X^2+X+r+\frac{r-aa'+(a+4r)\sqrt{3aa'}}{2}) \\
&\quad \cdot(X^2+X+r+\frac{r-aa'-(a+4r)\sqrt{3aa'}}{2}) \\
&= (X-a)(X-a')(X-b)(X-b')(X-c)(X-c').
\end{aligned}
$$

Here, we can easily obtain

$$
\begin{aligned}
&4ab=(\sqrt{3}a+\sqrt{aa'})^2, \quad 4a'b'=(\sqrt{3}a'-\sqrt{aa'})^2, \\
&4ac=(\sqrt{3}a-\sqrt{aa'})^2, \quad 4a'c'=(\sqrt{3}a'+\sqrt{aa'})^2.
\end{aligned}
$$

These show that $\chi(a)=\chi(b)$, $\chi(a')=\chi(b')$, $\chi(a)=\chi(c)$ and $\chi(a')=\chi(c')$. So we have $\chi(a)=\chi(a')=\chi(b)=\chi(b')=\chi(c)=\chi(c')$, and this completes the proof.

LEMMA 3. *Let $a\in F$ and assume that $[a,a']\in M$. Moreover set*

$$
\begin{aligned}
&d=\frac{-1+2\sqrt{aa'}}{2}, \quad d'=-1-d=\frac{-1-2\sqrt{aa'}}{2}, \\
&e=\frac{-1+a+4r+\sqrt{3dd'}}{2}, \quad e'=-1-e=\frac{-1-a-4r-\sqrt{3dd'}}{2}, \\
&f=\frac{-1+a+4r-\sqrt{3dd'}}{2}, \quad f'=-1-f=\frac{-1-a-4r+\sqrt{3dd'}}{2}.
\end{aligned}
$$

If $g(a)\neq 0, \pm 2r^4$ then the equation $g(X)=-g(a)$ has six distinct roots d, d', e, e', f and f' in F. In this case, if $[a,a']\in M^+$ then $[d,d']$, $[e,e']$, $[f,f']\in M^-$ and if $[a,a']\in M^-$ then $[d,d']$, $[e,e']$, $[f,f']\in M^+$.

PROOF. It is trivial that the quadratic equation $X^2+X+2r-aa'=0$ has two solutions d and d' and, because of

$$g(X)+g(a)=(X^2+X+r)^3-6r^3(X^2+X+r)+(r-aa')^3-6r^3(r-aa'),$$

we see that the polynomial $g(X)+g(a)$ has the factor $X^2+X+2r-aa'$. Thus d and d' are two solutions of the equation $g(X)=-g(a)$.

Here, from $\chi(aa') = 1$, we have d, $d' \in F$. Furthermore it is easy to check

$$2ad = (a + d + \frac{1}{2})^2,$$

$$2a'd' = (a' + d' + \frac{1}{2})^2.$$

These mean that $\chi(a) = -\chi(d)$ and $\chi(a') = -\chi(d')$. Hence we get that if $[a, a'] \in M^+$ then $[d, d'] \in M^-$ and if $[a, a'] \in M^-$ then $[d, d'] \in M^+$. As $g(X) + g(a) = g(X) - g(d)$, the desired result for e, e', f and f' follows at once from Lemma 2.

3. The number of rational points

Our main result is stated as follows.

THEOREM 1. *Let p be a prime number satisfying $p \equiv 13 \pmod{24}$ and denote by r the element in $\mathbf{Z}_p$ satisfying $8r = 1$. Moreover denote by s and t two distinct solutions in $\mathbf{Z}_p$ of the equation $X^2 - 2rX + r^2/4 = 0$. Then the number of rational points of the hyperelliptic curve $Y^2 = X(X^2+X+r)(X^2+X+s)(X^2+X+t)$ defined over $\mathbf{Z}_p$ is equal to $p+1$.*

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

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

where χ denotes the quadratic character of F, (see Hasse[2]). Put

$$g(X) = (X^2 + X + r)(X^2 + X + s)(X^2 + X + t).$$

Then, applying Lemma 1, we have

$$\begin{aligned} S = {} & \chi(-g(-1)) + \chi(-2rg(-2r)) + \chi(-6rg(-6r)) \\ & +\chi(-4rg(-4r)) + \chi(-4sg(-4s)) + \chi(-4tg(-4t)) \\ & + \sum_{[x,x'] \in M \setminus \{[-2r,-6r],[-4r,-4r],[-4s,-4t]\}} (\chi(x) + \chi(x'))\chi(g(x)) \end{aligned}$$

$$
\begin{aligned}
&+\sum_{[x,x']\in M^{\pm}}(\chi(x)+\chi(x'))\chi(g(x))\\
&=2\{\sum_{[x,x']\in M^{+}\backslash\{[-2r,-6r]\}}\chi(g(x))-\sum_{[y,y']\in M^{-}\backslash\{[-4r,-4r],[-4s,-4t]\}}\chi(g(y))\}.
\end{aligned}
$$

In order to prove $S=0$ we consider the pair

$$[x,x']\in M\backslash\{[-2r,-6r],[-4r,-4r],[-4s,-4t]\}.$$

If we put $\alpha=g(x)$ then $\alpha\neq 0,\pm 2r^4$ and so, by making use of Lemmas 2 and 3, we can get six roots a, a', b, b', c and c' in F of the equation $g(X)=\alpha$ and six roots d, d', e, e', f and f' in F of the equation $g(X)=-\alpha$. In this case it is clear that $\chi(\alpha)=\chi(-\alpha)$ and that

$$
\begin{aligned}
&\chi(a)=\chi(a')=\chi(b)=\chi(b')=\chi(c)=\chi(c')\\
&\quad=-\chi(d)=-\chi(d')=-\chi(e)=-\chi(e')=-\chi(f)=-\chi(f').
\end{aligned}
$$

Thus we obtain that, for each pair $[x,x']\in M^{+}\backslash\{[-2r,-6r]\}$, there exists some pair $[y,y']\in M^{-}\backslash\{[-4r,-4r],[-4s,-4t]\}$ satisfying $g(y)=-g(x)$ and that its converse is true. Therefore we get $S=0$ and so $N=p+1$ which is the desired assertion.

Finally we discuss our curve $Y^2=X(X^2+X+r)(X^2+X+s)(X^2+X+t)$ in Theorem 1 as a curve over $GF(p^3)$. In this case we put $F=GF(p^3)$ and take χ as the multiplicative quadratic character of F. Then, in an entirely same manner as above, we can get the similar result to Theorem 1, namely the extended result is stated as follows.

THEOREM 2. *Let p be a prime number satisfying $p\equiv 13 \pmod{24}$ and denote by r the element in $\mathbf{Z}_p$ satisfying $8r=1$. Moreover denote by s and t two distinct solutions in $\mathbf{Z}_p$ of the equation $X^2-2rX+r^2/4=0$. Then the number of rational points of the hyperelliptic curve $Y^2=X(X^2+X+r)(X^2+X+s)(X^2+X+t)$ defined over $GF(p^3)$ is equal to p^3+1.*

References

[1] M.DEURING, *Lectures on the theory of algebraic functions of one variable*, Tata Institute of Fundamental Research Bombay, 1959

[2] H.HASSE, *The Riemann hypothesis in algebraic function fields over a finite constants field*, The Pennsylvania State University, 1968

[3] K.IRELAND and M.ROSEN, *A classical introduction to modern number theory*, Springer-Verlag, 1982

[4] T.WASHIO and T.KODAMA, *On a certain supersingular elliptic curve*, Bull. Fac. Educ., Nagasaki Univ.:Natural Science, No.66 (2002), 1-3.

[5] T.WASHIO and T.KODAMA, *Note on a certain supersingular elliptic curve*, Bull. Fac. Educ., Nagasaki Univ.:Natural Science, No.67 (2002), 1-2.

[6] T.WASHIO and T.KODAMA, *Note on certain quadratic nonrsidues*, Bull. Fac. Educ., Nagasaki Univ.:Natural Science, No.72 (2005), 1-4.

[7] T.WASHIO and T.KODAMA, *The number of rational points of certain hyperelliptic curves of genus 2*, Bull. Fac. Educ., Nagasaki Univ.:Natural Science, No.72 (2005), 5-10.