Bulletin of Faculty of Education, Nagasaki University: Natural Science No. 66, 1 ~ 3 (2002. 3)

On a certain supersingular elliptic curve

Tadashi WASHIO and Tetsuo KODAMA*

Department of Mathematics, Faculty of Education,

Nagasaki University, Nagasaki 852, Japan

(Received Oct. 31, 2001)

Abstract

In this note, by means of determination of the number of rational points, it is shown that if F is a finite prime field of characteristic p satisfying $p \equiv 5 \pmod 8$ then the elliptic curve $Y^2 = X(X^2+X+r)$ defined over F is supersingular where $r = 1/8 \in F$. As an application, it is also shown that the following equality

$$\sum_{k=0}^{n} \begin{pmatrix} 2n \\ k \end{pmatrix} \begin{pmatrix} 2n-k \\ k \end{pmatrix} r^k = 0$$

holds where $n = (p-1)/4$.

1. Introduction

The purpose of this note is to study supersingular elliptic curves defined over finite prime fields and to obtain information related to binomial coefficients. Generally, for the cases of normal form $Y^2 = X^3+aX+b$ and $Y^2 = X(X-1)(X-a)$, Deuring [1] has already studied circumstantially and for special cases of the form $Y^2 = X^3+aX$ and $Y^2 = X^3+a$, Olson [3] also has studied in detail.

In this note, we will consider a curve of the form $Y^2 = X(X^2+X+a)$. Let p be a prime such that $p \equiv 5 \pmod 8$ and let F be a finite prime field of characteristic p. If we put $r = 1/8 \in F$ then the polynomial X^2+X+r is irreducible over F and so we see that the curve defined by $Y^2 = X(X^2+X+r)$ over F is elliptic. We want to prove that this elliptic curve is supersingular and that the following equality

$$\sum_{k=0}^{n} \begin{pmatrix} 2n \\ k \end{pmatrix} \begin{pmatrix} 2n-k \\ k \end{pmatrix} r^k = 0$$

holds where $n = (p-1)/4$.

---

* Professor emeritus, Kyushu University, Fukuoka 812, Japan

2. The number of ratinal points

We denote by p a prime. Let F be a finite prime field of characteristic p. Moreover we put

$$f(X) = X^2 + X + r \in F[X]$$

where $r = 1/8 \in F$.

Then we can get the following result.

THEOREM 1. *Assume that* $p \equiv 5 \pmod 8$ *and denote by N the number of rational points of the elliptic curve* $Y^2 = Xf(X)$ *defined over* $F = GF(p)$. *Then* $N = p + 1$.

PROOF. We denote by χ the multiplicative quadratic character of F. Then N is given by

$$N = p + 1 + \sum_{x \in F} \chi(h(x))$$

where $h(x) = x(x^2 + x + r)$.

Since $\chi(h(0)) + \chi(h(-1)) + \chi(h(-4r)) = 0 - 1 + 1 = 0$, we have

$$\begin{aligned} N &= p + 1 + \sum_{x \in S} \chi(h(x)) \\ &= p + 1 + \frac{1}{2} \sum_{x \in S} \{\chi(x) + \chi(x')\} \chi(f(x)), \end{aligned}$$

where $S = F \setminus \{0, -1, -4r\}$ and $x' = -1 - x$.

For any $x \in S$ satisfying $\chi(x) = \chi(x')$, we can easily show that the quadratic equation

$$X^2 + X + r = -f(x)$$

has the solutions y and $y' = -1 - y$ in F and that $y \in S$ and $\chi(y) = \chi(y') = -\chi(x)$ as $(x + y + 4r)^2 = 2xy$ and $\chi(2) = -1$.

Then $\chi(-1) = 1$ leads to

$$\{\chi(x) + \chi(x')\} \chi(f(x)) + \{\chi(y) + \chi(y')\} \chi(f(y)) = 0.$$

Therefore we obtain

$$\sum_{x \in F} \chi(h(x)) = 0$$

and so $N = p + 1$.

3. Hasse invariant and binomial coefficients

We will now give a certain family of supersingular elliptic curves over finite prime fields and certain congruences for binomial coefficients associated to these curves.

THEOREM 2. *Let F be a finite prime field of characteristic p. If* $p \equiv 5 \pmod 8$ *then the elliptic curve* $Y^2 = X(X^2 + X + r)$ *defined over F is supersingular where* $r = 1/8 \in F$.

PROOF. Using Theorem 1, we obtain that our elliptic curve has $p + 1$ rational points over F and so the Hasse invariant is equal to zero (cf. Manin [2]). Therefore we see that this

curve is supersingular.

This result is restated by means of binomial coefficients as follows.

THEOREM 3. *Let p be a prime satisfying $p \equiv 5 \pmod 8$ and put $n = (p-1)/4$. Moreover put $r = 1/8$ in the finite field $F = GF(p)$. Then*

$$\sum_{k=0}^{n} \binom{2n}{k} \binom{2n-k}{k} r^k = 0,$$

i.e., in the ring $\mathbf{Z}$ of rational integers,

$$\sum_{k=0}^{n} \binom{2n}{k} \binom{2n-k}{k} 8^{n-k} \equiv 0 \pmod p.$$

PROOF. The Hasse invariant A of the elliptic curve $Y^2 = X(X^2+X+r)$ defined over F is given by

$$A = \sum_{\substack{i+j+k=2n \\ 2i+j=2n \\ 0 \leqq i,\ j,\ k \leqq 2n}} \frac{(2n)!}{i!\ j!\ k!} r^k,$$

because A is the coefficient of X^{2n} in $(X^2+X+r)^{2n}$ (cf. Deuring [1]).

By use of binomial coefficients, it is rewritten as

$$A = \sum_{k=0}^{n} \binom{2n}{k} \binom{2n-k}{k} r^k.$$

So the desired assertions follow immediately from Theorem 2.

References

[1] M. DEURING, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hamburg Univ., **14** (1941), 197-272

[2] JU. I. MANIN, *The Hasse-Witt matrix of an algebraic curve*, Trans. Amer. Math. Soc., **45** (1965), 245-264.

[3] L. D. OLSON, *Hasse invariants and anomalous primes for elliptic curves with complex multiplication*, J. Number Theory **8** (1976), 397-414