<table>
<thead>
<tr>
<th>Title</th>
<th>Note on a certain supersingular elliptic curve</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Washio, Tadashi; Kodama, Tetsuo</td>
</tr>
<tr>
<td>Citation</td>
<td>長崎大学教育学部紀要 [自然科学 47(2002)1-2]</td>
</tr>
<tr>
<td>Issue Date</td>
<td>2002-06-28</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/10069/6110">http://hdl.handle.net/10069/6110</a></td>
</tr>
</tbody>
</table>

NAOSITE: Nagasaki University’s Academic Output SITE
http://naosite.lb.nagasaki-u.ac.jp
Note on a certain supersingular elliptic curve

Tadashi WASHIO and Tetsuo KODAMA∗
Department of Mathematics, Faculty of Education,
Nagasaki University, Nagasaki 852, Japan
(Received Mar. 15, 2002)

Abstract

Let \( p \) be an odd prime number such that \( p \equiv 2 \pmod{3} \) and denote by \( F \) a finite prime field of characteristic \( p \). Then it is shown that an elliptic curve \( y^2 = X(X^2 + X + s) \) defined over \( F \) is supersingular and so that the following equality
\[
\sum_{k=0}^{n} \binom{t}{k} \binom{t-k}{k} s^k = 0
\]
holds in \( F \) where \( t = (p-1)/2 \), \( n = \lceil t/2 \rceil \) and \( s = 1/3 \in F \).

1. Introduction

We denote by \( p \) an odd prime number and by \( F \) a finite prime field of characteristic \( p \). In the previous note [1], we proved that if \( p \equiv 5 \pmod{8} \) then the elliptic curve \( y^2 = X(X^2 + X + r) \) defined over \( F \) is supersingular and so the following equality
\[
\sum_{k=0}^{n} \binom{2n}{k} \binom{2n-k}{k} r^k = 0
\]
holds in \( F \) where \( n = (p-1)/4 \) and \( r = 1/8 \in F \).

In this note, we want to prove, after the manner of [1], that if \( p \equiv 2 \pmod{3} \) then the following equality
\[
\sum_{k=0}^{n} \binom{t}{k} \binom{t-k}{k} s^k = 0
\]
holds where \( t = (p-1)/2 \), \( n = \lceil t/2 \rceil \) and \( s = 1/3 \in F \).

2. The number of rational points

Let \( p \) be an odd prime number such that \( p \equiv 2 \pmod{3} \) and denote by \( F \) a finite prime field of characteristic \( p \). Moreover we put \( s = 1/3 \in F \). Then it is clear that the polynomial \( X^2 + X + s \) is irreducible over \( F \) and so the curve defined by \( Y^2 = X(X^2 + X + s) \) over \( F \) is elliptic.

THEOREM 1. Denote by \( N \) the number of rational points of elliptic curve \( Y^2 = f(X) \) over \( F \) where \( f(X) = X(X^2 + X + s) \). Then \( N = p + 1 \) holds.

PROOF. We denote by \( \chi \) the multiplicative quadratic character of \( F \). Then \( N \) is

∗Professor emeritus, Kyushu University, Fukuoka 812, Japan
given by

\[ N = p + 1 + \sum_{x \in F} \chi(f(x)). \]

Using our assumptions of \( p \equiv 2 \mod 3 \) and \( s = 1/3 \), we can easily show that, for any \( x, y \in F \), if \( x \neq y \) then \( f(x) \neq f(y) \). This means that \( \{ f(x) ; x \in F \} = F \).

Therefore we get

\[ \sum_{x \in F} \chi(f(x)) = \sum_{x \in F} \chi(x) = 0 \]

and so we obtain \( N = p + 1 \).

3. Hasse invariant and binomial coefficients

We will now show that our curves are supersingular and give the congruence relations for binomial coefficients associated to these curves.

**Theorem 2.** If \( p \equiv 2 \mod 3 \) and \( s = 1/3 \in F = GF(p) \) then the elliptic curve \( Y^2 = X(X^2 + X + s) \) defined over \( F \) is supersingular.

**Proof.** According to Theorem 1, we see that our curve has \( p + 1 \) rational points over \( F \). This means that the Hasse invariant of our curve is zero and so our curve is supersingular.

Rewriting the Hasse invariant of curve \( Y^2 = X(X^2 + X + s) \) in terms of binomial coefficients, it is clear that Theorem 2 leads to the following result.

**Theorem 3.** If \( p \equiv 2 \mod 3 \) and \( s = 1/3 \in F = GF(p) \) then

\[ \sum_{k=0}^{n} \binom{t}{k} \binom{t-k}{k} s^k = 0 \]

where \( t = (p-1)/2 \) and \( n = \lfloor t/2 \rfloor \). i.e., in the ring \( \mathbb{Z} \) of rational integers,

\[ \sum_{k=0}^{n} \binom{t}{k} \binom{t-k}{k} 3^{n-k} \equiv 0 \pmod{p}. \]

**References**