Natural Science Report, Ochanomizu University, Vol. 44, No. 1, 1993 17
お茶の水女子大学 自然科学報告 第44巻 第1号

Unirationality of Surfaces Obtained from Products of Curves

Mari Ohhira

Department of Mathematics, Faculty of science,
Ochanomizu University, Tokyo

(Received April 8, 1993)

Let k be an algebraically closed field of positive characteristic p. A non-singular complete surface defined over k is called supersingular if its second Betti number equals its Picard number. An Abelian variety over k is called supersingular if it is isogenous to a products of supersingular elliptic curves. A non-singular complete curve over k is called supersingular if its Jacobian variety is supersingular. A non-singular complete variety is called unirational if there exists dominant rational map from a projective space to it.

Now, consider the hyperelliptic curves over k

$$C_N : Y^2 = X^N - 1 ,$$

where N is a positive integer such that

$$N \not\equiv 0 (\mathrm{mod}\, p) \quad \text{and} \quad N \geqq 3 ,$$

and

$$C'_n : y^2 = x^n - x ,$$

where n is a positive odd integer such that

$$n-1 \not\equiv 0 (\mathrm{mod}\, p) \quad \text{and} \quad n \geqq 3 .$$

We always denote the involution map of any hyperelliptic curves by ι:

$$\iota : (x, y) \longrightarrow (x, -y) .$$

Consider also surfaces which are products of above curves and quotient surfaces by the involution:

$$T_N := C_N \times C_N , \qquad S_N = \widetilde{T_N / \iota \times \iota} ,$$
$$T'_n ;= C'_n \times C'_n \quad \text{and} \quad S'_n = \widetilde{T'_n / \iota \times \iota} .$$

There are some facts on the unirationality or supersingularity of C_N, C'_n, S_N, or of S'_n already clarified:

PROPOSITION 0.1. ([1, 5]) (1) *If there exists a natural number such* *that* $p^{\nu}\equiv -1 \pmod N$, *then* S_N *is unirational.*

(2) C_5 *is supersingular if and only if* $p\not\equiv 1 \pmod 5$.

(3) C_6 *is supersingular if and only if* $p\equiv 5 \pmod 6$.

(4) C_5' *is supersingular if and only if* $p\equiv 5, 7 \pmod 8$.

It seems that C_N or S_N are easier to handle than C_n' or S_n' because the zeta funtion of C_N has a simple formula introduced by Weil ([9, 10]). But since C_{2n-2} is a double covering of C_n', we can calculate the zeta function of C_n', too. This calculation is the first part of this note, and we deduce some facts on unirationality and supersingularity of S_n' in the following parts. The results are summarized in Theorem 2.7 in § 2.

§ 1. Calculation of zeta functions

Let $k=\boldsymbol{F}_q$ be a finite field with q elements in characteristic p. We denote the congruence zeta function of a proper smooth variety V over k by $Z(T, V/k)$, or simply by $Z(T, V)$ or by $Z(T)$ if there are no ambiguities.

In this section we recall the calculation of $Z(T, C_N/k)$ by Weil ([10]) and calculate $Z(T, C_n'/k)$. At first, fix the notations as follows:

$n\geqq 3$: a positive odd integer,

$N:=2n-2$,

q: the smallest integer such that $q=p^f\equiv 1 \pmod N$,

ω: a generator of the multiplicative group $\boldsymbol{F}_q^*$,

$\tilde{C}_N/k$: $\tilde{Y}^2=\omega^{n-1}\tilde{X}^N-\omega^{-1}$: a hyperelliptic curve over k,

$N_\mu :=\text{Card}.\, C_N(\boldsymbol{F}_{q^\mu})$,

$N_\mu' :=\text{Card}.\, C_n'(\boldsymbol{F}_{q^\mu})$,

$\tilde{N}_\mu :=\text{Card}.\, \tilde{C}_N(\boldsymbol{F}_{q^\mu})$,

The formula of zeta function by Weil is described by Jacobi sums.

DEFITITION 1.1. Let $a\neq n-1$ be a positive integer such that $1\leqq a\leqq 2n-2$, and let N' be the greatest common devisor of a and N. Let a' (resp. N'') be the devisor of a (resp. N) such that $a=a'N'$ (resp. $N=N'N''$.) When N'' is even, we set $a_0=a'$, $b_0=N''/2$, and let χ be a character of k^* such that

$$\chi : k^* \longrightarrow \boldsymbol{C}^*;\ \omega \longmapsto \exp(2\pi i/N'').$$

When N'' is odd, we set $a_0=2a'$, $b_0=N''$, and let χ be a character of k^* such that

$$\chi : k^* \longrightarrow \boldsymbol{C}^*;\ \omega \longmapsto \exp(2\pi i/2N'').$$

We define the Jacobi sum j_a as follows:

$$j_a = \sum_{x,y\in k^*,\, x+y+1=0} \chi(x)^{a_0}\chi(y)^{b_0}.$$

LEMMA 1.2. ([10]) *The zeta functions of C_N and $\tilde{C}_N$ are given by the following formulae:*

$$Z(T, C_N/k) = (1-T)^{-1}(1-qT)^{-1} \prod_{1<a<N,\, a\neq N-1} (1+\chi((-1)^{a_0})j_a T),$$

$$Z(T, \tilde{C}_N/k) = (1-T)^{-1}(1-qT)^{-1} \prod_{1<a<N,\, a\neq N-1} (1+\chi((-\omega^{-n+1})^{a_0}\omega^{-b_0})j_a T).$$

Since C_N is a double covering of C'_n, we can calculate $Z(T, C'_n/k)$ from the above formulae.

LEMMA 1.3. *The numbers of rational points of C'_n, C_N and $\tilde{C}_N$ over k are related as the following formula:*

$$N'_1 = (N_1 + \tilde{N}_1)/2. \tag{1.1}$$

PROOF. Any rational point (x_0, y_0) over $k = \boldsymbol{F}_q$ of C'_n corresponds to a pair of rational points $(\pm\sqrt{x_0}, \pm y_0/\sqrt{x_0})$ over $\boldsymbol{F}_{q^2}$ of C_N. Conversely, if a rational point $(X_0, Y_0) \in C_N(\boldsymbol{F}_{q^2})$ corresponds to a rational point $(X_0^2, X_0 Y_0) \in C'_n(\boldsymbol{F}_q)$, one of the following two conditions must hold:

$$X_0,\ Y_0 \in k, \tag{1.2}$$

or

$$\sqrt{\omega}\, X_0,\ \sqrt{\omega}\, Y_0 \in k. \tag{1.3}$$

The condition (1.2) is equivalent to $(X_0, Y_0) \in C_N(k)$, and the condition (1.3) is equivalent to $(X_0, Y_0) \in \tilde{C}_N(k)$. So, we have the formula (1.1). □

PROPOSITION 1.4. *The zeta functions of C'_n is given by the following formula:*

$$Z(T, C'_n/k) = (1-T)^{-1}(1-qT)^{-1} \prod_{1\leq a<N,\, a\neq N-1,\, a:\text{odd}} (1-(\pm j_a)T). \tag{1.4}$$

PROOF. From the definition of zeta functions it suffices to show the following formula:

$$N'_1 = 1 + q + \sum_{a:\text{odd}} \chi(-1)^{a_0} j_a. \tag{1.5}$$

From Lemma 1.2, we can calculate N_1 and $\tilde{N}_1$ as the following:

$$N_1 = 1 + q + \sum_a \chi(-1)^{a_0} j_a, \tag{1.6}$$

and

$$\tilde{N}_1 = 1 + q + \sum_a \chi(-1)^{a_0}\chi(\omega)^{-(N/2)a_0 - b_0} j_a, \tag{1.7}$$

so, the proof is completed. □

§ 2. Unirationality and supersingularity

In this section, we use the same notations as in § 1 unless otherwise mentioned.

PROPOSITION 2.1. *Assume that there exists a positive integer* ν *such that*

$$p^{\nu}\equiv -1, n(\mathrm{mod}\, N)\,. \tag{2.1}$$

Then, the surface S_n' *is unirational.*

PROOF. If $p^{\nu}\equiv -1(\mathrm{mod}\, N)$, then S_N is unirational ([5]). So, S_n' is unirational, too. Assume that $p^{\nu}\equiv n(\mathrm{mod}\, N)$. S_n' is birationally equivalent to a hypersurface H_0 in $\boldsymbol{A}^3$ whose defining equation is as follows:

$$H_0: t^2=(u^n-u)(x^n-x)\,.$$

H_0 is birationally equivalent to a hypersurface H_1 in $\boldsymbol{A}^3$ whose defining equation is as follows:

$$H_1: t^2z^{2n-2}=(u^n-uz^{n-1})(1-z^{n-1})\,. \tag{2.2}$$

From (2.2), we have

$$u=\frac{t^2z^{n-1}}{z^{n-1}-1}+u^n/z^{n-1}\,. \tag{2.3}$$

Since $p^{\nu}\equiv n(\mathrm{mod}\, N)$, there exists an integer such that $p^{\nu}=2(n-1)l+n=(n-1)(2l+1)+1$. Putting $s^{2l+1}=u$, we have

$$s=\frac{t^2z^{n-1}}{z^{n-1}-1}s^{-2l}+s^{p^{\nu}}/z^{n-1}\,. \tag{2.4}$$

Putting $\beta=(z^{n-1}s^{-l}/z^{n-1}-1)t$, we have

$$s-\beta^2=(s^{p^{\nu}}-\beta^2)/z^{n-1}\,. \tag{2.5}$$

Putting $\beta=\gamma^{p^{\nu}}$, we have

$$s-\gamma^{2p^{\nu}}=(s-\gamma^2)^{p^{\nu}}/z^{n-1}\,. \tag{2.6}$$

Putting $\delta=(s-\gamma^2)^{2l+1}/z$ finally, we have

$$s-\gamma^{2p^{\nu}}=(s-\gamma^2)\delta^{n-1}\,. \tag{2.7}$$

Since the equation (2.7) shows that the function field $k(S_n')=k(H_1)$ is contained in the function field $k(\gamma, \delta)=k(\boldsymbol{P}^2)$, the proof is completed. □

REMARK 2.2. Since it is known that any unirational surface is supersingular ([3]), we know from Proposition 2.1 that if we assume that there exists a positive integer ν such that $p^{\nu}\equiv -1,\ n(\mathrm{mod}\ N)$, then, the surface S'_n is supersingular.

It is known that supersingularity of T'_n is equivalent to that all the eigenvalues of the second ℓ-adic étale cohomology group are equal to q^{-1} ([8]). Since these eigenvalues can be calculated from $Z(T, C'_n)$, we have the following lemma.

LEMMA 2.3. *The following two conditions are equivalent.*

(1) S'_n *is supersingular.*

(2) *For suitable even power q of p and all the odd integer a such that $1\leqq a<N$, it holds that $j_a=q^{1/2}$.*

PROOF. Consider another condition

(3) T'_n is supersingular.

Since the equivalence of (2) and (3) is shown from the formula of $Z(T, C'_n)$ proved in Propoition 1.4, it suffices to show the equivalence of (1) and (3). Since ι acts as -1 in $H^1(\boldsymbol{Q}_\iota, C'_n)$, by Künneth formula, ι acts as identity in $H^2(\boldsymbol{Q}_\iota, T'_n)$. This shows the equivalence of (1) and (3). □

Now, we have the following problem.

PROBLEM 2.4. Assume that S'_n is supersingular. Then, does the conditional equation (2.1) hold?

We prepare more notations to handle this problem.

$K=\boldsymbol{Q}(\zeta_N)$: the N-th cyclotomic field,

$G=\mathrm{Gal}(K/\boldsymbol{Q})$,

$H\subset G$: the decomposition group of p over K. (Card. $H=f$.)

We identify the elements of H and integers t_i such that $1\leqq t_i\leqq N-3$:

$$H=\{t_0=1, \cdots, t_{f-1}\}.$$

For a integer a such that $1\leqq a\leqq N-1$ and $a\neq n-1$, we set

$$A_H(a)=\sum_{i=0}^{f-1}[1/2+\langle t_i a/N\rangle],$$

where $\langle\ \rangle$ denotes the fractional part.

$s\in H$: the unique elements in H such that $s^2=1$ and $s\neq 1$. (s exists only when f is even.)

With an odd integer N' and an integer $e\geqq 2$, we decompose N as follows:

$$N=2^e N'$$

$\phi:(\boldsymbol{Z}/N)\to(\boldsymbol{Z}/2^e)$: the canonical projection.

$H' := \phi(H)$, $f' :=\mathrm{Card}.\, H'$, $s' := \phi(s)$.

By Stickelberger's relation, we can calculate j_a with $A_H(a)$.

LEMMA 2.5. *The following two conditions on a are equivalent:*

(1) $(j(a)^{\nu}) \neq (p^{\nu f/2})$ *for all positive integers* ν.

(2) $A_H(a) \neq f/2$.

PROOF. This can be proved similarly to the Lemma 3.1 in [6]. □

PROPOSITION 2.6. *Assume the following conditions* A_0 *and* B_0.

A_0: *There exists no integers* ν *which suffices the condition* (2.1).

B_0: *The characteristic* p *suffices one of the following conditions* $B_1, \cdots,$ *or* B_4.

B_1: $f=2$.

B_2: $N=2^e$.

B_3: f *or* f' *is odd.*

B_4: $f'=2$ *and* $H' \not\ni 2^e-1, 2^{e-1}+1$.

Then, there exists an odd integer a *such that* $1 \leqq a \leqq N-1$ *and* $A_H(a) \neq f/2$.

PROOF. **Case (1)** the case where the condition B_1 is satisfied.

In this case, it suffices that $N \geqq 8$ and $H=\{1, s\}$.

At first, we devide reductively the interval $L_{\infty}=[0, N)$, where s is in:

$I_0 := L_0 = [0, N/2]$,

$I_1 := (4N/6, 5N/6)$, $L_1 := L_0 + I_1 = [0, N/2] \cup (4N/6, 5N/6)$,

$I_2 := (6N/10, 7N/10) \cup (8N/10, 9N/10)$,

$L_2 := L_1 \cup I_2 := [0, N/2] \cup (6N/10, 9N/10)$,

$I_k := \left(\frac{(2k+2)N}{4k+2}, \frac{(2k+3)N}{4k+2}\right) \cup \left(\frac{4kN}{4k+2}, \frac{(4k+1)N}{4k+2}\right)$,

$\vdots$

$L_k := L_{k-1} \cup I_k = [0, N/2] \cup \left(\frac{(2k+2)N}{4k+2}, \frac{(4k+1)N}{4k+2}\right)$,

If $s \in L_0$, then,

$$A_H(1) = [1/2 + \langle 1/N \rangle] + [1/2 + \langle s/N \rangle] = 0\,.$$

If $s \in I_1$, then,

$$A_H(3) = [1/2 + \langle 3/N \rangle] + [1/2 + \langle 3s/N \rangle] = 0\,.$$

For $k \geqq 1$, assume that $s \notin L_k$. Since s is a square-root of 1, it must hold that $\sqrt{N} \geqq N/4k+2$. Especially, it holds that $N > 4k+6$.

If $s \in I_{k+1}$, then, it holds that

$$A_H(2k+3) = [1/2 + \langle (2k+3)/N \rangle] + [1/2 + \langle (2k+3)s/N \rangle] = 0\,.$$

Since the inductive limit of L_K's is L_{∞}, the proof in this case is completed.

Case (**2**) the case where the condition B_2 is satisfied.

It may assume that $f \geqq 4$, i.e., H has an element c of order 4. Then, a simple calculation shows that $c^2 = n \in H$. It conflicts to the assumption A_0.

Case (**3**) the case where the condition B_3 or B_4 is satisfied.

If f is odd, this proposition is trivial.

It may assume that $N' \geqq 3$. Then, for an odd integer a, it holds that

$$A_H(N'a) = \sum_{t \in H} [1/2 + \langle N'at/2^e N' \rangle] = \text{Card.}(H/H')A'_H(a).$$

So, this case is reduced to the case (2). □

Finally, we summarize our results as in the following.

THEOREM 2.7. *For the characteristic p, assume that the condition* B_0 *in Proposition* 2.6 *is satisfied. Then, the following three conditions are equivalent.*

(1) S'_n *is unirational.*

(2) S'_n *is supersingular.*

(3) *There exists a positive integer* ν *such that*

$$p^\nu \equiv -1, n (\text{mod } N).$$

References

[1] T. Ibukiyama, T. Katsura and F. Oort: *Supersingular curves of genus two and class numbers*, Compositio Math. **57** (1986), 127-152.

[2] T. Katsura: *Generalized Kummer Surfaces and their unirationality in charcteristic p*, J. Fac. Sci. Univ. Tokyo, Sec. IA **34** (1987), 1-41.

[3] T. Shioda: *An example of unirational surfaces in characteristic p*, Math. Ann. **211** (1974), 233-236.

[4] T. Shioda: *On unirationality of supersingular surfaces*, Math. Ann. **225** (1977), 155-159.

[5] T. Shioda: *Some results on unirationality of algebraic surfaces*, Math. Ann. **230** (1977), 153-168.

[6] T. Shioda and T. Katsura: *On Fermat varieties*, Tôhoku Math. J. **31** (1979), 97-115.

[7] J. Tate: *Algebraic cycles and poles of zeta functions*, in Arithmetic Algebraic Geometry (1965), Harper and Row, New York, 93-110.

[8] J. Tate: *Endmorphism of abelian varieties over fields*, Inventiones Math. **2** (1966), 134-144.

[9] A. Weil: *Number of solutions of equations in finite fields*, Bull. A. M. S. **55** (1949), 497-508.

[10] A. Weil: *Jacobi sums as "Grössencharactere"*, Trans. A. M. S. **73** (1952), 487-495.