Tôhoku Math. Journ.
31 (1979), 97-115.

ON FERMAT VARIETIES

TETSUJI SHIODA AND TOSHIYUKI KATSURA

(Received March 17, 1978)

0. Introduction. By the Fermat variety of dimension r and of degree m we mean the non-singular hypersurface in the projective space $\boldsymbol{P}^{r+1}$ defined by the equation

$$x_0^m + x_1^m + \cdots + x_{r+1}^m = 0 . \tag{0.1}$$

Throughout this paper, we denote it by X_m^r, or by $X_m^r(p)$, when we need to specify the characteristic p of the base field k; we always assume that $m \not\equiv 0 \pmod{p}$.

The purpose of this paper is to clarify the "inductive structure" of Fermat varieties of a common degree and of various dimensions, and apply it to the questions concerning the unirationality and algebraic cycles of a Fermat variety. The main results are stated as follows:

THEOREM I. *For any positive integers r and s, X_m^{r+s} is obtained from the product $X_m^r \times X_m^s$ by* 1) *blowing up a subvariety isomorphic to $X_m^{r-1} \times X_m^{s-1}$,* 2) *taking the quotient of the blown up variety with respect to an action of the cyclic group of order m, and* 3) *blowing down from the quotient two subvarieties isomorphic to $\boldsymbol{P}^r \times X_m^{s-1}$ and $X_m^{r-1} \times \boldsymbol{P}^s$.*

THEOREM II. *Suppose that r is even and $m \geqq 4$. Then the l-adic cohomology ring of $X_m^r(p)$ is spanned by algebraic cycles if and only if*

$$p^\nu \equiv -1 \pmod{m} \quad \textit{for some integer } \nu . \tag{0.2}$$

THEOREM III. *Suppose that r is even. If the condition* (0.2) *is satisfied, then $X_m^r(p)$ is a unirational variety, and the converse is also true if $r = 2$ and $m \geqq 4$.*

COROLLARY. *A Fermat surface $X_m^2(p)$ is unirational if and only if it is supersingular* (*cf.* [8]).

This paper is organized as follows. In §1, we study the relationship between X_m^{r+s} and $X_m^r \times X_m^s$, and obtain Theorem I (for a more precise statement, see Theorem 1.7). As a consequence, it will be seen, in §2, that the cohomology of X_m^r is described in terms of that of $X_m^{r'}$ with $r' < r$. Then we prove the if part of Theorem II in a slightly generalized form (Theorem 2.10) by induction on r, the first step of which is based

on some results of Weil [11], [12] and of Tate [10]. In §3, we first recall Weil's results on the zeta function of $X_m^r(p)$ over a finite field and then prove the only if part of Theorem II, by making use of a result due to I. Miyawaki (Theorem 3.4). In §4, we prove Theorem III by reducing it to the case of surfaces (Theorem 4.1).

It should be remarked that the if part of Theorem II was first discovered by Tate [9] whose proof is based on the representation theory of finite unitary groups (compare the recent article [4] of Hotta and Matsui). In case $r = 2$, Shioda [6] deduced it from the unirationality. The only if part of Theorem II was observed in some special cases by Shioda [7], [8] and applied to the unirationality question of certain algebraic surfaces. Theorem III for p odd was proved before in [6]. We shall improve it here by clarifying the higher dimensional case by means of Theorem I and supplying a proof for the case $p = 2$.

Finally we wish to thank I. Miyawaki who has kindly communicated to us the proof of Proposition 3.5 of §3.

1. Inductive structure of Fermat varieties. We study in this section the relationship among Fermat varieties of a common degree and of various dimensions. Let m, r and s be positive integers, and let us consider Fermat varieties X_m^r, X_m^s, and X_m^{r+s}:

$$\text{(1.1)} \qquad \begin{cases} X_m^r\colon x_0^m + x_1^m + \cdots + x_{r+1}^m = 0 \\ X_m^s\colon y_0^m + y_1^m + \cdots + y_{s+1}^m = 0 \\ X_m^{r+s}\colon z_0^m + z_1^m + \cdots + z_{r+s+1}^m = 0\,. \end{cases}$$

The characteristic of the base field k is arbitrary provided that it does not divide the degree m.

LEMMA 1.1. *There exists a rational map of degree* m

$$\text{(1.2)} \qquad \varphi\colon X_m^r \times X_m^s \to X_m^{r+s}$$

defined by

$$\text{(1.3)} \qquad \begin{cases} z_i = x_i y_{s+1} & (i = 0, 1, \cdots, r) \\ z_{r+1+j} = \varepsilon x_{r+1} y_j & (j = 0, 1, \cdots, s)\,, \end{cases}$$

ε being a fixed $2m$-th root of unity such that $\varepsilon^m = -1$.

PROOF. Immediate.

Let Y denote the locus of points of $X_m^r \times X_m^s$ where the rational map φ is not defined. Then Y is the subvariety of $X_m^r \times X_m^s$ defined by $x_{r+1} = y_{s+1} = 0$, which can be naturally identified with $X_m^{r-1} \times X_m^{s-1}$. Let

$$\text{(1.4)} \qquad \beta\colon Z_m^{r,s} \to X_m^r \times X_m^s$$

denote the blowing up of $X_m^r \times X_m^s$ along the non-singular center Y. More explicitly, $Z_m^{r,s}$ is given as follows. We denote by U_i (or V_j) the affine open subset of X_m^r (or X_m^s) defined by $x_i \neq 0$ (or $y_j \neq 0$). Then $\{U_i \times V_j | 0 \leqq i \leqq r, 0 \leqq j \leqq s\}$ forms an affine open covering of $X_m^r \times X_m^s$. In the product $U_i \times V_j \times \boldsymbol{P}^1$, we consider the subset

$$(1.5) \qquad Z_{ij} = \left\{((x_0: \cdots: x_{r+1}), (y_0: \cdots: y_{s+1}), (t_0: t_1)) \mid t_1 \frac{x_{r+1}}{x_i} = t_0 \frac{y_{s+1}}{y_j}\right\}$$

and the natural projections

$$(1.6) \qquad \beta_{ij}: Z_{ij} \to U_i \times V_j\ , \quad \gamma_{ij}: Z_{ij} \to \boldsymbol{P}^1\ .$$

We form the union

$$(1.7) \qquad Z_m^{r,s} = \bigcup_{i,j} Z_{ij}$$

by identifying a point $(x, y, t_0: t_1)$ of Z_{ij} with a point $(x, y, t_0': t_1')$ of $Z_{i'j'}$ if and only if

$$(1.8) \qquad \frac{y_{j'}}{x_{i'}} \frac{t_1'}{t_0'} = \frac{y_j}{x_i} \frac{t_1}{t_0}\ .$$

Then we have a unique morphism (1.4) such that its restriction to Z_{ij} coincides with β_{ij}. Obviously β induces an isomorphism of $Z_m^{r,s} - \beta^{-1}(Y)$ onto $X_m^r \times X_m^s - Y$, while the exceptional set $\beta^{-1}(Y)$ is a $\boldsymbol{P}^1$-bundle over Y.

LEMMA 1.2. *The composed map*

$$(1.9) \qquad \psi = \varphi \circ \beta: Z_m^{r,s} \to X_m^{r+s}$$

is a morphism.

PROOF. We look at the map

$$\psi_{ij} = \varphi \circ \beta_{ij}: Z_{ij} \to X_m^{r+s} \quad (i \leqq r, j \leqq s)\ .$$

By (1.3), (1.5) and (1.6), we have

$$(1.10) \qquad \psi_{ij}((x_0: \cdots: x_{r+1}), (y_0: \cdots: y_{s+1}), (t_0: t_1)) = \left(t_1 \frac{x_0}{x_i}: \cdots: t_1 \frac{x_r}{x_i}: \varepsilon t_0 \frac{y_0}{y_j}: \cdots: \varepsilon t_0 \frac{y_s}{y_j}\right).$$

This shows that all ψ_{ij}, and hence ψ, are morphisms. q.e.d.

We put

$$(1.11) \qquad S_0 = \bigcup_{i,j} \gamma_{ij}^{-1}(1: 0)\ , \quad S_\infty = \bigcup_{i,j} \gamma_{ij}^{-1}(0: 1)\ .$$

By (1.8), S_0 and S_∞ are subvarieties of codimension 1 in $Z_m^{r,s}$, and β

induces isomorphisms:

$$S_0 \simeq X_m^r \times X_m^{s-1}, \quad S_\infty \simeq X_m^{r-1} \times X_m^s . \tag{1.12}$$

On the other hand, we fix the following embeddings of X_m^{r-1} and X_m^{s-1} into X_m^{r+s}:

$$\begin{cases} X_m^{r-1} \simeq \{(x_0 \colon \cdots \colon x_r \colon 0 \colon \cdots \colon 0) \in X_m^{r+s}\} \subset X_m^{r+s} \\ X_m^{s-1} \simeq \{(0 \colon \cdots \colon 0 \colon y_0 \colon \cdots \colon y_s) \in X_m^{r+s}\} \subset X_m^{r+s} . \end{cases} \tag{1.13}$$

Note that X_m^{r-1} and X_m^{s-1} are disjoint from each other in X_m^{r+s}.

LEMMA 1.3. *With the above notation, the restrictions of the morphism ψ to S_0 and S_∞ are the projections:*

$$\begin{cases} S_0 \simeq X_m^r \times X_m^{s-1} \to X_m^{s-1} \subset X_m^{r+s} \\ S_\infty \simeq X_m^{r-1} \times X_m^s \to X_m^{r-1} \subset X_m^{r+s} . \end{cases} \tag{1.14}$$

The induced map

$$\psi \colon Z_m^{r,s} - S_0 \cup S_\infty \to X_m^{r+s} - X_m^{s-1} \cup X_m^{r-1} \tag{1.15}$$

is a finite morphism. Moreover, if B is the divisor of X_m^{r+s} defined by $z_0^m + \cdots + z_r^m = 0$, then

$$\psi \colon Z_m^{r,s} - \psi^{-1}(B) \to X_m^{r+s} - B \tag{1.16}$$

is an étale morphism of degree m.

PROOF. This is easily verified by using (1.10). q.e.d.

Now we introduce an action of the group μ_m of m-th roots of unity on $X_m^r \times X_m^s$:

$$\begin{aligned} &((x_0 \colon \cdots \colon x_r \colon x_{r+1}), (y_0 \colon \cdots \colon y_s \colon y_{s+1})) \\ &\quad \mapsto ((x_0 \colon \cdots \colon x_r \colon \zeta x_{r+1}), (y_0 \colon \cdots \colon y_s \colon \zeta y_{s+1})) \quad (\zeta \in \mu_m) . \end{aligned} \tag{1.17}$$

The fixed point set of this action is the subvariety Y defined before, and this μ_m-action naturally extends to one on the blown up variety $Z_m^{r,s}$.

LEMMA 1.4. *The quotient $Z_m^{r,s}/\mu_m$ is non-singular.*

PROOF. By (1.5) and (1.7), $\{Z_{ij}\}$ forms a μ_m-invariant open covering of $Z_m^{r,s}$. Each Z_{ij} is covered by the two affine open subsets Z_{ijk} defined by $t_k \neq 0 (k = 0, 1)$. The coordinate ring of Z_{ij0} is

$$\begin{aligned} &k\left[\frac{x_0}{x_i}, \cdots, \frac{x_{r+1}}{x_i}, \frac{y_0}{y_j}, \cdots, \frac{y_{s+1}}{y_j}, \frac{t_1}{t_0}\right] \\ &\quad = k\left[\frac{x_0}{x_i}, \cdots, \frac{x_{r+1}}{x_i}, \frac{y_0}{y_j}, \cdots, \frac{y_s}{y_j}, \frac{t_1}{t_0}\right] . \end{aligned} \tag{1.18}$$

The subring of invariants with respect to the μ_m-action is given by

$$k\left[\frac{x_0}{x_i}, \cdots, \frac{x_r}{x_i}, \left(\frac{x_{r+1}}{x_i}\right)^m, \frac{y_0}{y_j}, \cdots, \frac{y_s}{y_j}, \frac{t_1}{t_0}\right]. \tag{1.19}$$

Hence the quotient Z_{ij0}/μ_m is isomorphic to the hypersurface in $A^r \times A^s \times A^1$ defined by

$$(1 + \xi_1^m + \cdots + \xi_r^m)t^m - (1 + \eta_1^m + \cdots + \eta_s^m) = 0\,, \tag{1.20}$$

and so it is non-singular. In the same way, we can see that Z_{ijl}/μ_m is non-singular. q.e.d.

LEMMA 1.5. *Let π denote the quotient morphism of $Z_m^{r,s}$ to $Z_m^{r,s}/\mu_m$. Then*

$$\begin{cases}\pi(S_0) \simeq \boldsymbol{P}^r \times X_m^{s-1} \\ \pi(S_\infty) \simeq X_m^{r-1} \times \boldsymbol{P}^s\,. \end{cases} \tag{1.21}$$

PROOF. With the notation of the previous proof, $\pi(S_0)$ is contained in the union of $\pi(Z_{ij0})$ for $i \leqq r$ and $j \leqq s$. Hence the first assertion immediately follows from the equation (1.20) for all i and j. The second one is similarly shown. q.e.d.

LEMMA 1.6. *The morphism ψ of $Z_m^{r,s}$ to X_m^{r+s} induces a birational morphism*

$$\bar{\psi}\colon Z_m^{r,s}/\mu_m \to X_m^{r+s}\,, \tag{1.22}$$

and it blows down $\pi(S_0)$ and $\pi(S_\infty)$ to X_m^{s-1} and X_m^{r-1} respectively.

PROOF. Since ψ is compatible with the μ_m-action on $Z_m^{r,s}$ (cf. (1.10) and (1.17)), we obtain the morphism $\bar{\psi}$. By (1.14) and (1.21), $\bar{\psi}$ induces the maps

$$\begin{cases}\pi(S_0) \simeq \boldsymbol{P}^r \times X_m^{s-1} \to X_m^{s-1} \subset X_m^{r+s} \\ \pi(S_\infty) \simeq X_m^{r-1} \times \boldsymbol{P}^s \to X_m^{r-1} \subset X_m^{r+s}\,, \end{cases} \tag{1.14}$$

which are nothing but the projections. Then (1.15) implies that the restriction of $\bar{\psi}$

$$Z_m^{r,s}/\mu_m - \pi(S_0) \cup \pi(S_\infty) \to X_m^{r+s} - X_m^{s-1} \cup X_m^{r-1} \tag{1.24}$$

is a finite birational morphism and hence an isomorphism since X_m^{r+s} is non-singular. q.e.d.

Summarizing the above, we obtain the following result which was stated as Theorem I in the Introduction.

THEOREM 1.7. *There exists a commutative diagram:*

$$
\begin{array}{ccccccc}
 & & Z_m^{r,s} & \xrightarrow{\pi} & Z_m^{r,s}/\mu_m & \hookleftarrow & \boldsymbol{P}^r \times X_m^{s-1}\,, \quad X_m^{r-1} \times \boldsymbol{P}^s \\
 & & \beta\downarrow & \searrow^{\psi} & \downarrow\bar{\psi} & & \downarrow \qquad\qquad \downarrow \\
Y = X_m^{r-1} \times X_m^{s-1} & \subset & X_m^r \times X_m^s & \overset{\varphi}{\dashrightarrow} & X_m^{r+s} & \hookleftarrow & X_m^{s-1}\,, \qquad X_m^{r-1}
\end{array} \tag{1.25}
$$

where 1) β *is the blowing up of* $X_m^r \times X_m^s$ *along the center* Y, 2) π *is the quotient morphism, and* 3) $\bar{\psi}$ *is a birational morphism blowing down the two subvarieties from the quotient to the disjoint subvarieties* X_m^{s-1} *and* X_m^{r-1} *of* X_m^{r+s}.

REMARK 1.8. As is seen from the above consideration, all varieties and morphisms appearing in the diagram (1.25) are defined over arbitrary field containing a primitive $2m$-th root of unity. Furthermore, Theorem 1.7 can be proven in the category of schemes, smooth and projective over $\boldsymbol{Z}[1/m, e^{\pi i/m}]$, without any essential alteration.

REMARK 1.9. The Fermat variety X_m^{r-1} is reducible if and only if $r = 1$, and in this case X_m^0 consists of m distinct points. Thus, for the case $r = s = 1$, $Z_m^{1,1}$ is obtained from the self-product $X_m^1 \times X_m^1$ of the Fermat curve by blowing up m^2 points, and the Fermat surface X_m^2 is obtained from the quotient $Z_m^{1,1}/\mu_m$ by blowing down $2m$ non-singular rational curves (cf. Sasakura [5]).

REMARK 1.10. The proof given above for Theorem 1.7 can be applied to a slightly more general situation. Namely, let X_m^{r-1} (or X_m^{s-1}) denote for a moment arbitrary non-singular hypersurface of degree m defined by

$$f(x_0, \cdots, x_r) = 0 \quad (\text{or } g(y_0, \cdots, y_s) = 0)\,,$$

and let X_m^r, X_m^s and X_m^{r+s} respectively denote the hypersurfaces:

$$
\begin{cases}
f(x_0, \cdots, x_r) + x_{r+1}^m = 0 \\
g(y_0, \cdots, y_s) + y_{s+1} = 0 \\
f(z_0, \cdots, z_r) + g(z_{r+1}, \cdots, z_{r+s+1}) = 0\,.
\end{cases} \tag{1.1}'
$$

Then X_m^{r+s} is obtained from the product $X_m^r \times X_m^s$ by exactly the same steps as those described in Theorem 1.7 for the case of Fermat varieties.

COROLLARY 1.11. *For any* $r \geqq 1$, *there exist rational maps of finite degree*:

$$\underbrace{X_m^1 \times \cdots \times X_m^1}_{r\text{-times}} \to X_m^r \tag{1.26}$$

and

$$\underbrace{X_m^2 \times \cdots \times X_m^2}_{r\text{-times}} \to X_m^{2r} . \tag{1.27}$$

PROOF. This is an immediate consequence of Theorem 1.7, or more simply, of Lemma 1.1. q.e.d.

2. Algebraic cycles on Fermat varieties. It follows from Theorem 1.7 that the cohomological structure of a Fermat variety can be described in terms of that of lower dimensional ones. To see it, let us first recall the following general facts.

Let X be a non-singular projective variety over an algebraically closed field k. Fixing a prime number l different from the characteristic of k, we denote by $H^i(X)$ the l-adic étale cohomology group of X. Moreover, we denotes by $H^i(X)(j)$ the j-fold twisting of $H^i(X)$, i.e., $H^i(X) \otimes_{Q_l} W^{\otimes j}$, where $W = H^2(\boldsymbol{P}^1)$ is a one-dimensional vector space over $\boldsymbol{Q}_l$.

LEMMA 2.1. *Let $\beta: Z \times X$ be the blowing up of X along a non-singular subvariety Y of codimension d in X. Then there is a natural isomorphism:*

$$H^i(Z) \simeq H^i(X) \oplus \sum_{j=1}^{d-1} H^{i-2j}(Y)(j) . \tag{2.1}$$

LEMMA 2.2. *Suppose that G is a finite group of automorphisms of X such that the quotient X/G is non-singular. Then $H^i(X/G)$ is isomorphic to the subspace $H^i(X)^G$ of G-invariants in $H^i(X)$:*

$$H^i(X/G) \simeq H^i(X)^G . \tag{2.2}$$

LEMMA 2.3. *Assume that X is a non-singular hypersurface in $\boldsymbol{P}^{r+1}$. Then, for any $i \neq r$, $0 \leqq i \leqq 2r$, we have*

$$H^i(X) = 0 \quad \textit{for} \quad i \textit{ odd} , \tag{2.3}$$

and

$$H^i(X) : 1\textit{-dimensional for} \quad i \textit{ even} . \tag{2.4}$$

In the latter case, $H^i(X)$ is generated by algebraic cycles.

For the proofs, see [4], [3] Exp. VII and [2] Ch. V.
Now we go back to the case of Fermat varieties.

PROPOSITION 2.4. *With the notation used in §1, we have*

$$\begin{aligned} H^{r+s}(X_m^{r+s}) \oplus \sum_{j=1}^{s} H^{r+s-2j}(X_m^{r-1})(j) \oplus \sum_{k=1}^{r} H^{r+s-2k}(X_m^{s-1})(k) \\ \simeq H^{r+s}(X_m^r \times X_m^s)^{\mu_m} \oplus H^{r+s-2}(X_m^{r-1} \times X_m^{s-1})(1) . \end{aligned} \tag{2.5}$$

PROOF. Applying Lemma 2.1 to the blowing up (1.4) of $X_m^r \times X_m^s$ along $Y = X_m^{r-1} \times X_m^{s-1}$, we have

$$H^{r+s}(Z_m^{r,s}) \simeq H^{r+s}(X_m^r \times X_m^s) \oplus H^{r+s-2}(X_m^{r-1} \times X_m^{s-1})(1) . \tag{2.6}$$

Then, considering the μ_m-action (1.17), we have by Lemma 2.2

$$H^{r+s}(Z_m^{r,s}/\mu_m) \simeq H^{r+s}(X_m^r \times X_m^s)^{\mu_m} \oplus H^{r+s-2}(Y)(1) , \tag{2.7}$$

since μ_m acts trivially on Y. On the other hand, Lemma 2.1, applied to the birational morphism (1.22), gives

$$\begin{aligned} H^{r+s}(Z_m^{r,s}/\mu_m) \simeq H^{r+s}(X_m^{r+s}) \oplus \sum_{j=1}^{s} H^{r+s-2j}(X_m^{r-1})(j) \\ \oplus \sum_{k=1}^{r} H^{r+s-2k}(X_m^{s-1})(k) . \end{aligned} \tag{2.8}$$

Hence (2.5) follows at once from (2.7) and (2.8). q.e.d.

COROLLARY 2.5. *We have*

$$\begin{aligned} H^r(X_m^r) \oplus H^{r-2}(X_m^{r-2})(1) \oplus \begin{cases} mW^{\otimes r/2} & (r\text{: even}) \\ 0 & (r\text{: odd}) \end{cases} \\ \simeq H^r(X_m^{r-1} \times X_m^1)^{\mu_m} \oplus mH^{r-2}(X_m^{r-2})(1) . \end{aligned} \tag{2.9}$$

Here mV denotes the direct sum of m copies of a vector space V.

PROOF. We replace r and s in (2.5) by $r-1$ and 1 respectively. Since X_m^0 consists of m distinct points, we obtain (2.9) by Lemma 2.3. q.e.d.

Now we shall consider questions concerning algebraic cycles on a Fermat variety (cf. Tate [9]). In general, let $\mathfrak{A}^i(X)$ denote the subspace of $H^{2i}(X)(-i)$ generated by algebraic cycles of codimension i in X. If X is defined over a finite field k_0 and k is its algebraic closure, then the Galois group $G = \mathrm{Gal}(k/k_0)$ acts on the space $H^{2i}(X)$ in a natural way and one has the inclusion

$$\mathfrak{A}^i(X) \subset [H^{2i}(X)(-i)]^G \quad (0 \leqq i \leqq \dim X) \tag{2.10}$$

by replacing k_0 by a suitable finite extension. Tate [9] has conjectured that the equality should hold in (2.10) in place of the inclusion, and verified it for a Fermat variety $X_m^r(p)$ (r: even) in the following two cases:

(I) $p^\nu \equiv -1 (\mathrm{mod}\, m)$ for some integer ν

(II) $r = 2$ and $p \equiv 1 (\mathrm{mod}\, m)$.

Also he has proved in [10] the equality

$$\mathfrak{A}^1(X) = [H^2(X)(-1)]^G \tag{2.11}$$

in case X is an abelian variety or a product of curves, defined over a finite field.

By making use of this latter result, we first see that Tate's conjecture holds for any Fermat surface $X_m^2(p)$, thus improving (II). We shall then give a new proof in case (I) which is perhaps more geometric than the original proof in [9].

THEOREM 2.6. *For a Fermat surface* $X = X_m^2(p)$, *the space* $[H^2(X)(-1)]^G$ *is generated by algebraic cycles.*

PROOF. Setting $r = 2$ in (2.9), we have

$$H^2(X_m^2) \xleftarrow{(\bar{\psi})^*} H^2(X_m^1 \times X_m^1)^{\mu_m} \oplus mH^0(X_m^0)(1) . \tag{2.12}$$

The action of $G = \mathrm{Gal}\,(k/k_0)$ on the space $H^2(X_m^1 \times X_m^1)(-1)$ commutes with the μ_m-action, provided that k_0 is sufficiently large. Hence it follows from (2.12) that

$$[H^2(X_m^2)(-1)]^G \subset [H^2(X_m^1 \times X_m^1)(-1)^G]^{\mu_m} \oplus (m^2\boldsymbol{Q}_l) . \tag{2.13}$$

In view of (2.11) quoted above, the first term on the right is spanned by algebraic cycles, and the second term is obviously algebraic. This proves the assertion. q.e.d.

REMARK 2.7. The above theorem holds for any surface in $\boldsymbol{P}^3$ defined by the equation $f(x_0, x_1) + g(x_2, x_3) = 0$, where f and g are binary forms without multiple factors and with coefficients in a finite field. The proof is completely parallel to the above (cf. Remark 1.10).

Now we make the following definition:

DEFINITION 2.8. A non-singular variety X of an *even* dimension will be called *supersingular* if the cohomology groups $H^{2i}(X)$ are spanned by algebraic cycles for all i, $0 \leqq i \leqq \dim X$.

For instance, a non-singular hypersurface X of an even dimension r is supersingular if and only if $H^r(X^r)$ is spanned by algebraic cycles (cf. Lemma 2.3).

LEMMA 2.9. *Assume that*

$$p^\nu \equiv -1 \pmod{m} \quad \textit{for some integer } \nu . \tag{2.14}$$

Then the product of Fermat curves $X_m^1(p) \times X_m^1(p)$ *is supersingular.*

PROOF. Under the assumption (2.14), the zeta function of the curve $X_m^1(p)$ over $k_0 = \boldsymbol{F}_q$ (q: sufficiently large even power of p) is given by

$$(1 - q^{1/2}T)^{(m-1)(m-2)}/(1 - T)(1 - qT) ; \tag{2.15}$$

this follows from Weil [11], [12] and will be explained in the next section (see Lemma 3.3). Therefore the zeta function of the product $X = X_m^1(p) \times X_m^1(p)$ over k_0 has a pole at $T = 1/q$ of order

$$2 + \{(m-1)(m-2)\}^2 = \dim H^2(X) . \tag{2.16}$$

Then, by Theorem 4 of Tate [10] (which is equivalent to (2.11)), the subspace $\mathfrak{A}^1(X)$ of algebraic cycles has the same dimension (2.16) as $H^2(X)$, which proves that $X = X_m^1(p) \times X_m^1(p)$ is supersingular. q.e.d.

THEOREM 2.10. *Assume that* (2.14) *holds. Then* (i) *for r even, the Fermat variety $X_m^r(p)$ is supersingular, and* (ii) *for r odd, the product of $X_m^r(p)$ with the curve $X_m^1(p)$ is supersingular.*

PROOF. We prove this by induction on r, the first step $r = 1$ being true by Lemma 2.9. Assume that the statement is true up to $r-1$ and $r \geqq 2$. By Corollary 2.5, we have

$$H^r(X_m^r) \hookrightarrow H^r(X_m^{r-1} \times X_m^1)^{\mu_m} \oplus mH^{r-2}(X_m^{r-2})(1) . \tag{2.17}$$

(Recall that this inclusion is induced by the birational morphism $\bar{\psi}: Z_m^{r-1,1}/\mu_m \to X_m^r$, (1.22).) (i) In case r is even, both $X_m^{r-1} \times X_m^1$ and X_m^{r-2} are supersingular by the induction assumption, and the right side of (2.17) is spanned by algebraic cycles. Hence X_m^r is also supersingular. (ii) In case r is odd, we consider the following diagram:

$$\begin{array}{ccc} Z_m^{r-1,1} \times X_m^1 & \xrightarrow{\psi \times \mathrm{id}} & X_m^r \times X_m^1 \\ \downarrow{\scriptstyle \beta \times \mathrm{id}} & & \\ (X_m^{r-1} \times X_m^1) \times X_m^1 & & \end{array} \tag{2.18}$$

which is deduced from (1.25). The surjective morphism $\psi \times \mathrm{id}$ induces the inclusion:

$$H^{r+1}(X_m^r \times X_m^1) \hookrightarrow H^{r+1}(Z_m^{r-1,1} \times X_m^1) . \tag{2.19}$$

Since $\beta \times \mathrm{id}$ is the blowing up of $X_m^{r-1} \times X_m^1 \times X_m^1$ along the subvariety $X_m^{r-2} \times X_m^0 \times X_m^1$, we have by Lemma 2.1

$$\begin{aligned} H^{r+1}(Z_m^{r-1,1} \times X_m^1) \simeq\ & H^{r+1}(X_m^{r-1} \times X_m^1 \times X_m^1) \\ & \oplus H^{r-1}(X_m^{r-2} \times X_m^0 \times X_m^1)(1) . \end{aligned} \tag{2.20}$$

By Künneth formula and Lemma 2.3, the right side is isomorphic to

$$\begin{aligned} & H^{r+1}(X_m^{r-1}) \oplus [H^{r-1}(X_m^{r-1}) \otimes H^2(X_m^1 \times X_m^1)] \\ & \oplus [H^{r-3}(X_m^{r-1}) \otimes H^4(X_m^1 \times X_m^1)] \oplus mH^{r-1}(X_m^{r-2} \times X_m^1)(1) . \end{aligned} \tag{2.21}$$

All the terms in (2.21) are spanned by algebraic cycles by the induction assumption, and by Lemma 2.3. It follows from (2.19) that $X_m^r \times X_m^1$ is supersingular (of course under the assumption (2.14)). This completes the proof of Theorem 2.10. q.e.d.

REMARK 2.11. It is still unknown whether Tate's conjecture holds for a Fermat variety $X_m^r(p)$ if r is even >2 and the condition (2.14) is not satisfied. By the same arguments as above, we can reduce it to the corresponding conjecture for the self-products of the Fermat curve $X_m^1(p)$ of dimensions up to r.

3. Zeta functions and Jacobi sums. In this section, we shall prove the second part of Theorem II in the Introduction, the first part of which is contained in Theorem 2.10 of the previous section.

For this purpose, we first recall Weil's results expressing the zeta function of a Fermat variety in terms of Jacobi sums (cf. [11], [12]). For the sake of simplicity, we consider the Fermat variety $X_m^r(p)$ over the finite field $\boldsymbol{F}_q$ with q elements, where $q = p^f$ is the least power of p such that $q \equiv 1 \pmod{m}$. The zeta function of $X_m^r(p)$ over $\boldsymbol{F}_q$ is given by

$$P(T)^{(-1)^{r-1}}/(1-T)(1-qT)\cdots(1-q^rT) \tag{3.1}$$

where

$$P(T) = \prod_{\alpha}(1 - j(\alpha)T)\,. \tag{3.2}$$

In the above, $\alpha = (a_0, a_1, \cdots, a_{r+1})$ runs over the set

$$\mathfrak{A}_{m,r} = \left\{(a_0, a_1, \cdots, a_{r+1}) \,\middle|\, \begin{array}{l} a_i \in \boldsymbol{Z}/m\boldsymbol{Z},\ a_i \not\equiv 0 \\ a_0 + a_1 + \cdots + a_{r+1} \equiv 0 \end{array}\right\}, \tag{3.3}$$

and $j(\alpha)$ denotes the Jacobi sum:

$$j(\alpha) = (-1)^r \sum_{\substack{1+v_1+\cdots+v_{r+1}=0 \\ v_i \in \boldsymbol{F}_q}} \chi(v_1)^{a_1}\cdots\chi(v_{r+1})^{a_{r+1}}\,, \tag{3.4}$$

χ being a fixed character of order m of the multiplicative group of $\boldsymbol{F}_q$.

At this point, we can give a geometric explanation to the following fact, observed by Weil ([12] p. 488 and p. 492): for any $r \geqq 2$ and any $\alpha \in \mathfrak{A}_{m,r}$, the Jacobi sum $j(\alpha)$ can be expressed as a suitable product of $j(\beta)$'s with $\beta \in \mathfrak{A}_{m,1}$. Indeed, by the general theory of zeta functions, the quantities $j(\alpha)$ defined by (3.1) and (3.2) are the eigenvalues of the endomorphism of $H^r(X_m^r(p))$ induced by the Frobenius morphism of $X_m^r(p)$ relative to $\boldsymbol{F}_q$. But the vector space $H^r(X_m^r(p))$ can be naturally considered as a subspace of a direct sum of spaces of the form $H^1(X_m^1(p))^{\otimes r'}$ with

$r' < r$, as is easily seen from Corollary 2.5 by induction on r. The above mentioned fact follows immediately from this.

Now each $j(\alpha)$ is an algebraic integer of absolute value $q^{r/2}$ in the m-th cyclotomic field $K = \boldsymbol{Q}(e^{2\pi i/m})$, and its prime ideal decomposition is described by Stickelberger's theorem ([12] p. 490):

$$(j(\alpha)) = \mathfrak{p}^{\omega(\alpha)} \tag{3.5}$$

where $\mathfrak{p}$ is a prime ideal in K with $N\mathfrak{p} = p^f = q$ and where $\omega(\alpha)$ is an element of the group ring of the Galois group G of K over $\boldsymbol{Q}$ defined by

$$\begin{aligned}\omega(\alpha) &= \sum_{\substack{(t,m)=1 \\ t \bmod m}} \left\{\sum_{\rho=1}^{r+1} \left\langle \frac{ta_\rho}{m} \right\rangle - \left\langle \frac{-ta_0}{m} \right\rangle\right\} \sigma_{-t}^{-1} \\ &= \sum_{\substack{(t,m)=1 \\ t \bmod m}} \left[\sum_{\rho=1}^{r+1} \left\langle \frac{ta_\rho}{m} \right\rangle\right] \sigma_{-t}^{-1} .\end{aligned} \tag{3.6}$$

(Here σ_t is the automorphism of K over $\boldsymbol{Q}$ mapping $e^{2\pi i/m}$ to $e^{2\pi it/m}$, and $\langle\lambda\rangle = \lambda - [\lambda]$ denotes the fractional part of the real number λ.) Identifying G with $(\boldsymbol{Z}/m\boldsymbol{Z})^\times$, we denote by H the subgroup of G generated by p mod m:

$$H = \{p^\nu \bmod m \mid 0 \leqq \nu < f\} ; \tag{3.8}$$

it is the decomposition group of $\mathfrak{p}$ over p. We put

$$A_H(\alpha) = \sum_{t \in H} \left[\sum_{\rho=1}^{r+1} \left\langle \frac{ta_\rho}{m} \right\rangle\right] . \tag{3.9}$$

Taking a set of representatives $\{t_1 = 1, t_2, \cdots, t_g\}$ of G mod H and letting $\mathfrak{p}_i = \mathfrak{p}^{\sigma_i}$ $(\sigma_i = \sigma_{-t_i}^{-1})$, we can rewrite (3.5) as follows:

$$(j(\alpha)) = \prod_{i=1}^{g} \mathfrak{p}_i^{A_H(t_i\alpha)} , \tag{3.10}$$

in which $t_i\alpha$ denotes the element $(t_ia_0, t_ia_1, \cdots, t_ia_{r+1})$ of $\mathfrak{A}_{m,r}$.

LEMMA 3.1. *With the above notation, the following conditions on $\alpha \in \mathfrak{A}_{m,r}$ are equivalent:*

(i) *some power of $j(\alpha)$ is a power of p:*

$$j(\alpha)^\nu = p^{\nu fr/2} \quad \textit{for some } \nu . \tag{3.11}$$

(ii) *the integers $A_H(t_i\alpha)$ are independent of i, and equal to $fr/2$.*

PROOF. Since $(p) = \mathfrak{p}_1 \cdots \mathfrak{p}_g$, (i) implies (ii) by (3.10). Conversely, (ii) implies that the ideal $(j(\alpha))$ is equal to (p^μ), μ being the common value of $A_H(t_i\alpha)$. If we set $j(\alpha) = \varepsilon(\alpha)p^\mu$, $\varepsilon(\alpha)$ is a unit in K and $\varepsilon(\alpha)^{\sigma_t} =$

$\varepsilon(t\alpha)$ for all t with $(t, m) = 1$. It follows that $\mu = fr/2$ and that all the conjugates of $\varepsilon(\alpha)$ are of absolute value 1. Hence $\varepsilon(\alpha)$ is a root of unity by Kronecker's theorem, and we can find some ν satisfying (3.11).

q.e.d.

Now the condition that $p^\nu \equiv -1 \pmod m$ for some ν is obviously equivalent to the condition:

$$H \ni -1 \mod m . \tag{3.12}$$

LEMMA 3.2. *If* (3.12) *holds, then* $A_H(\alpha) = fr/2$ *for all* $\alpha \in \mathfrak{A}_{m,r}$.

PROOF. This is easily verified by the definition (3.9) of $A_H(\alpha)$.

q.e.d.

LEMMA 3.3. *If* $p^\nu \equiv -1 \pmod m$ *for some* ν, *then the zeta function of the Fermat variety* $X^r_m(p)$ *over* $\boldsymbol{F}_{q_1}$ *for a suitable* p-*power* q_1 *is of the form*

$$(1 - q_1^{r/2}T)^{(-1)^{r-1}b}/(1 - T) \cdots (1 - q_1^r T) , \tag{3.13}$$

where b *is the cardinality of* $\mathfrak{A}_{m,r}$.

PROOF. By Lemmas 3.1 and 3.2, we can find a positive integer ν such that (3.11) holds for all $\alpha \in \mathfrak{A}_{m,r}$. Then the assertion follows from (3.1) and (3.2) by taking $q_1 = q^\nu$. q.e.d.

THEOREM 3.4. *Suppose that* $X^r_m(p)$ (r: *even*, $r \geqq 2$) *is supersingular. If* $m \geqq 4$, *then there exists an integer* ν *such that* $p^\nu \equiv -1 \pmod m$.

PROOF. By assumption, $H^r(X^r_m(p))$ is spanned by algebraic cycles. Choosing a suitable finite field $k_0 = \boldsymbol{F}_{q_1}$ (q_1: p-power), we may assume that $H^r(X^r_m(p))$ has a basis consisting of elements which are represented by k_0-rational algebraic cycles on $X^r_m(p)$. Then the Frobenius morphism of $X^r_m(p)$ over k_0 acts on $H^r(X^r_m(p))$ by multiplication by $q_1^{r/2}$, so that the zeta function of $X^r_m(p)$ over k_0 takes the form (3.13). By comparing it with (3.1) and (3.2), we see that some power of each Jacobi sum $j(\alpha)$ is a power of p for all $\alpha \in \mathfrak{A}_{m,r}$. Therefore, by Lemma 3.1, we have

$$A_H(\alpha) = fr/2 \quad \text{for all} \quad \alpha \in \mathfrak{A}_{m,r} . \tag{3.14}$$

Thus Theorem 3.4 will follow from the following

PROPOSITION 3.5. *For any* $r \geqq 1$ *and* $m \geqq 4$, *the condition* (3.14) *implies the condition* (3.12).

The proof of this proposition given below is essentially due to I. Miyawaki. We need some lemmas. First, setting

$$S_H(a) = \sum_{t \in H} \left\langle \frac{ta}{m} \right\rangle \tag{3.15}$$

for any integer a such that $a \not\equiv 0 \pmod{m}$, we have

$$A_H(\alpha) = \sum_{i=1}^{r+1} S_H(a_i) - S_H(-a_0) \tag{3.16}$$

for $\alpha = (a_0, a_1, \cdots, a_{r+1}) \in \mathfrak{A}_{m,r}$ (cf. (3.6)).

LEMMA 3.6. *If* (3.14) *holds, then* $S_H(a)$ *is independent of* a.

PROOF. Assume (3.14). First we claim that, if $0 < i < m - 2$, then

$$S_H(i+1) - S_H(i) = S_H(i+2) - S_H(i+1)\,. \tag{3.17}$$

In fact, given such an i, we can easily find an element $\alpha_1 = (a_0, i+1, i+1, a_3, \cdots, a_{r+1})$ of $\mathfrak{A}_{m,r}$ unless $r = 1$ and $2i + 2 \equiv 0 \pmod{m}$. Aside from the latter case, $\alpha_2 = (a_0, i, i+2, a_3, \cdots, a_{r+1})$ belongs also to $\mathfrak{A}_{m,r}$. By (3.14), $A_H(\alpha_1)$ is equal to $A_H(\alpha_2)$, and hence, using (3.16), we have (3.17). When $r = 1$ and $2i + 2 \equiv 0\ (m)$, (3.17) follows from the definition (3.15) of S_H.

It follows from (3.17) that

$$S_H(a) = S_H(1) + (a-1)\{S_H(2) - S_H(1)\} \quad (1 \leqq a \leqq m-1)\,. \tag{3.18}$$

Now we note that $H \neq \{1\}$. Indeed, setting

$$\alpha = \begin{cases} (-3, 1, 1, 1, 1, -1, \cdots, 1, -1) & r\text{: even} \\ (-2, 1, 1, 1, -1, \cdots, 1, -1) & r\text{: odd}\,, \end{cases} \tag{3.19}$$

we easily see that $A_{\{1\}}(\alpha) \neq A_{\{1\}}(-\alpha)$ for $m \geqq 4$. Since we are assuming (3.14), we have $H \neq \{1\}$. Therefore there exists an integer a such that $1 < a < m$ and $a \bmod m \in H$. Obviously we have then $S_H(a) = S_H(1)$, which implies by (3.18) that $S_H(2) = S_H(1)$. Using (3.17), we conclude that $S_H(i)$ is independent of i. q.e.d.

LEMMA 3.7. *Let* m_0 *be a divisor of* m, *and let* H_0 *denote the image of* H *under the natural homomorphism*

$$\varphi\colon (\boldsymbol{Z}/m\boldsymbol{Z})^\times \to (\boldsymbol{Z}/m_0\boldsymbol{Z})^\times\,. \tag{3.20}$$

Define $S_{H_0}(a)$ *in the same way as* (3.15). *Then, if* (3.14) *holds,* $S_{H_0}(a)$ *is independent of* a *with* $a \not\equiv 0 \pmod{m_0}$.

PROOF. For any integer a with $a \not\equiv 0 \pmod{m_0}$, we have

$$S_H(am/m_0) = \sum_{t \in H} \left\langle \frac{tam/m_0}{m} \right\rangle = |H \cap \operatorname{Ker} \varphi|\, S_{H_0}(a)\,. \tag{3.21}$$

Hence the assertion follows from Lemma 3.6. q.e.d.

PROOF OF PROPOSITION 3.5. Assume (3.14). We shall derive a contradiction assuming that $H \not\ni -1 \bmod m$. Let H' be the subgroup of $G = (\boldsymbol{Z}/m\boldsymbol{Z})^\times$ generated by H and $-1 \bmod m$; we have $[H' : H] = 2$. Then there exists a character of G, say χ, which is trivial on H but non-trivial on H'. Hence $\chi(-1) = -1$. Let χ_0 be the primitive character inducing χ and let m_0 be the conductor of χ_0. Obviously we have $\chi_0(-1) = -1$ and χ_0 is trivial on $H_0 = \varphi(H)$, φ being as in (3.20).

Extending χ_0 to a function on $\boldsymbol{Z}$ by setting $\chi_0(a) = 0$ for $(a, m_0) \neq 1$, we define the Dirichlet L-series $L(s, \chi_0)$. Since $\chi(-1) = -1$, we have

$$0 \neq L(1, \chi_0) = \sum_{n=1}^{\infty} \chi_0(n)/n = (\pi\sqrt{-1}\,\tau(\chi_0)/m_0^2) \sum_{x=1}^{m_0} \bar{\chi}_0(x)x \tag{3.22}$$

where $\tau(\chi_0)$ denotes the Gauss sum (see e.g., [1] Ch. 5, §2).

On the other hand, we have

$$S_{H_0}(a) = \sum_{t \in H_0} \left\langle \frac{ta}{m_0} \right\rangle = \sum_{x \in aH_0} \left\langle \frac{x}{m_0} \right\rangle = \sum_{\substack{x \in aH_0 \\ 0 < x < m_0}} \frac{x}{m_0} . \tag{3.23}$$

Since χ_0 is trivial on H_0, we have

$$\frac{1}{m_0} \sum_{x=1}^{m_0} \bar{\chi}_0(x)x = \sum_a \bar{\chi}_0(a) \Big(\sum_{\substack{x \in aH_0 \\ 0 < x < m_0}} \frac{x}{m_0} \Big) = \sum_a \bar{\chi}_0(a) S_{H_0}(a) , \tag{3.24}$$

where a runs over the coset representatives of the group $(\boldsymbol{Z}/m_0\boldsymbol{Z})^\times$ modulo H_0. By Lemma 3.7, the right hand side of (3.24) is equal to

$$(\sum_a \bar{\chi}_0(a)) \cdot S_{H_0}(1) ,$$

which vanishes because $\bar{\chi}_0$ can be considered as a non-trivial character of the factor group of $(\boldsymbol{Z}/m\boldsymbol{Z})^\times$ by H_0. This contradicts (3.22), and proves the proposition. q.e.d.

REMARK 3.8. Proposition 3.5 also holds for $m = 3$ except for the case $r = 2$. The verification is straightforward. In the exceptional case $r = 2$, X_3^2 is a rational surface (as a cubic surface) and hence supersingular in the sense of §2 in any characteristic $p \neq 3$.

REMARK 3.9. The above proof of Proposition 3.5 is not so elementary since it depends on the fact (3.22). We have a more elementary proof for it in case m is a power of a prime number, but it will be omitted.

Finally we state an application of the case $r = 1$ of Proposition 3.5:

PROPOSITION 3.10. *The Jacobian variety of the Fermat curve $X_m^1(p)$ is isogenous to a product of supersingular elliptic curves if and only if $p^\nu \equiv -1 \pmod m$ for some integer ν.*

PROOF. In view of Theorem 2 of Tate [10], the if part follows from Lemma 3.3, while the only if part follows from Lemma 3.1 and Proposition 3.5. q.e.d.

In [8] §1, a similar result for the curve $y^2 = 1 - x^m$ was applied to the proof of the unirationality of arbitrary supersingular Kummer surfaces.

4. **Unirationality.** An irreducible variety X is called *unirational* if there exists a rational map of finite degree from a projective space to X. Equivalently, X is unirational if the function field $k(X)$ of X is contained in a purely transcendental extension of the base field k.

THEOREM 4.1. *If* $p^\nu \equiv -1 \pmod{m}$ *for some integer* ν, *then the Fermat variety* $X_m^r(p)$ *of an even dimension* r *is unirational.*

PROOF. By Corollary 1.11, the unirationality of $X_m^r(p)$ (r: even) will follow from that of $X_m^2(p)$. Also, for any positive integer d, the map $(x_i) \to (x_i^d)$ defines a surjective morphism of X_{md}^r to X_m^r. Therefore the proof of the theorem is reduced to the case where $r = 2$ and $m = q + 1$, q being a power of p. In this case, we further distinguish the case $p > 2$ and the case $p = 2$.

In case $p > 2$, the proof can be found is Shioda [6], but it will be reproduced here for the reader's convenience. We write the equation of $X_{q+1}^2(p)$ in the form:

$$x_1^{q+1} - x_2^{q+1} = x_3^{q+1} - x_0^{q+1} \tag{4.1}$$

by replacing x_2 and x_3 by εx_2 and εx_3 ($\varepsilon^{q+1} = -1$). By the coordinate transformation

$$\begin{cases} x_1 = y_1 + y_2 \\ x_2 = y_1 - y_2 \end{cases}, \quad \begin{cases} x_3 = y_3 + y_0 \\ x_0 = y_3 - y_0 \end{cases},$$

the equation (4.1) becomes

$$y_1^q y_2 + y_1 y_2^q = y_3^q y_0 + y_3 y_0^q . \tag{4.2}$$

If we set $y_0 = 1$, $y_2 = y_1 u$ and $y_3 = uv$, the function field of $X_{q+1}^2(p)$ over k is isomorphic to the field $k(y_1, u, v)$ with the relation

$$u^{q-1}(y_1^{q+1} - v^q) = v - y_1^{q+1} . \tag{4.3}$$

Hence, putting

$$t = y_1^{1/q} , \quad s = u(t^{q+1} - v) , \tag{4.4}$$

we have

$$s^{q-1}(t^{q+1} - v) = v - t^{q(q+1)} \tag{4.5}$$

which shows that the field $k(y_1, u, v)$ is contained in the field $k(s, t)$.

In case $p = 2$, we modify the above as follows. Letting ρ be a primitive cube root of unity, we put

$$\begin{cases} x_1 = y_1 + y_2 \\ x_2 = \rho y_1 + y_2 , \end{cases} \quad \begin{cases} x_3 = y_3 + y_0 \\ x_0 = \rho y_3 + y_0 . \end{cases} \tag{4.6}$$

Then the equation (4.1) becomes

$$\begin{aligned} (1 + \rho^{q+1})y_1^{q+1} + (1 + \rho^q)y_1^q y_2 + \rho^2 y_1 y_2^q \\ = (1 + \rho^{q+1})y_3^{q+1} + (1 + \rho^q)y_3^q y_0 + \rho^2 y_3 y_0^q . \end{aligned} \tag{4.7}$$

Since $q = 2^\nu$ is congruent to 1 or 2 (mod 3) according to the parity of ν, we have

$$1 + \rho^{q+1} = \begin{cases} 0 \\ \rho , \end{cases} \qquad 1 + \rho^q = \begin{cases} \rho & (\nu\text{: odd}) \\ \rho^2 & (\nu\text{: even}) . \end{cases}$$

First, suppose that ν is odd. Then the equation (4.7) reads

$$y_1^q y_2 + \rho y_1 y_2^q = y_3^q y_0 + \rho y_3 y_0^q . \tag{4.8}$$

Comparing this with (4.2), we can prove its unirationality exactly in the same way as before.

Next, suppose that ν is even. Then we have

$$y_1^{q+1} + \rho y_1^q y_2 + \rho y_1 y_2^q = y_3^{q+1} + \rho y_3^q y_0 + \rho y_3 y_0^q . \tag{4.9}$$

Set here

$$y_1 = y_3 + 1 , \quad y_0 = y_2 + \rho^2 u + \rho^2 . \tag{4.10}$$

Then the function field of $X^2_{q+1}(p)$ is isomorphic to the field $k(y_2, y_3, u)$ with the relation

$$y_3^q u + y_3 u^q + \rho y_2^q + \rho y_2 + 1 = 0 . \tag{4.11}$$

Putting

$$t = y_3^{1/q} , \quad s = tu + \rho y_2 , \tag{4.12}$$

we have

$$t^{q^2-1}(s + \rho y_2) + s^q + \rho y_2 + 1 = 0 , \tag{4.13}$$

which shows that $k(y_2, y_3, u)$ is contained in $k(s, t)$. This completes the proof of Theorem 4.1. q.e.d.

REMARK 4.2. Let $k_0 = \boldsymbol{F}_{p^2}$ for $p = 2$ and $k_0 = \boldsymbol{F}_p(\varepsilon)$ for $p > 2$, ε being a root of unity such that $\varepsilon^{p^\nu+1} = -1$. Then the above proof shows that the Fermat variety $X^r_m(p)$ of an even dimension r and of degree m

dividing $p^\nu + 1$ is k_0-unirational, i.e., there exists a rational map of finite degree *defined over* k_0 from $\boldsymbol{P}^r$ to $X_m^r(p)$.

THEOREM 4.3. *For the Fermat surface* $X_m^2(p)$ *of order* $m \geqq 4$, *the following conditions are equivalent to each other*:

(i) $X_m^2(p)$ *is unirational*,

(ii) $X_m^2(p)$ *is supersingular*,

(iii) $p^\nu \equiv -1 \pmod{m}$ *for some integer* ν.

PROOF. Since every unirational surface is supersingular, (i) implies (ii) (cf. Shioda [6] §2). By Theorem 3.4, (ii) implies (iii). Finally (iii) $\Rightarrow$ (i) follows from Theorem 4.1. q.e.d.

REMARK 4.4. We expect that Theorem 4.3 should hold also for higher dimensional cases. The only unproven part is the implication (i) $\Rightarrow$ (ii). We stated before in [6] p. 236 that this would follow from the resolution of singularities for higher dimensional varieties in characteristic p, but it was a wrong observation. In fact, it should be noticed that *there are unirational* (or *even rational*) *varieties which are not supersingular*. For instance, let Y be a non-singular surface in $\boldsymbol{P}^4$ and let X be the rational variety of dimension 4 which is obtained by blowing up $\boldsymbol{P}^4$ along Y. Then X is supersingular (i.e., $H^4(X)$ is spanned by algebraic cycles) if and only if Y is supersingular. (This follows easily from Lemma 2.1.) Since there certainly exist Y's which are not supersingular, we thus obtain examples of rational varieties which are not supersingular.

REMARK 4.5. Going back to the case of surfaces, the part (ii) $\Rightarrow$ (i) of Theorem 4.4 lends some support to a rather optimistic conjecture that any supersingular surface in $\boldsymbol{P}^3$ might be unirational (cf. Shioda [8], p. 167).

REFERENCES

[1] Z. I. BOREVICH AND I. R. SHAFAREVICH, Number Theory, Academic Press, New York and London, 1966.

[2] A. GROTHENDIECK, Sur quelques points d'algèbre homologique, Tôhoku Math. J., 9 (1957), 119-221.

[3] A. GROTHENDIECK, Cohomologie l-adique et Fonctions L (SGA 5), Lecture Notes in Math., 589 (1977), Springer, Berlin-Heidelberg-New York.

[4] R. HOTTA AND K. MATSUI, On a lemma of Tate-Thompson, Hiroshima Math. J., 8 (1978), 255-268.

[5] N. SASAKURA, On some results on the Picard numbers of certain algebraic surfaces, J. Math. Soc. Japan, 20 (1968), 297-321.

[6] T. SHIODA, An example of unirational surfaces in characteristic p, Math. Ann., 211 (1974), 233-236.

[7] T. SHIODA, On unirationality of supersingular surfaces, Math. Ann., 225 (1977), 155-159.
[8] T. SHIODA, Some results on unirationality of algebraic surfaces, Math. Ann., 230 (1977), 153-168.
[9] J. TATE, Algebraic cycles and poles of zeta functions, in *Arithmetical Algebraic Geometry*, Harper and Row, New York, 1965, 93-110.
[10] J. TATE, Endomorphisms of abelian varieties over finite fields, Inventiones Math., 2 (1966), 134-144.
[11] A. WEIL, Number of solutions of equations in finite fields, Bull. Amer. Math. Soc., 55 (1949), 497-508.
[12] A. WEIL, Jacobi sums as "Grössencharaktere", Trans. Amer. Math. Soc., 73 (1952), 487-495.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF TOKYO
TOKYO, 113 JAPAN
AND
MATHEMATICAL INSTITUTE
TÔHOKU UNIVERSITY
SENDAI, 980 JAPAN

Added in proof.

(1) The rational map φ of Lemma 1.1 (p. 98) has been independently introduced by P. Deligne in his hand-written note: "Cycles de Hodge sur les variétés abéliennes", in order to define the embedding of $H^*(X_m^r)$ into $H^*(\prod X_m^1)$. Also Professor Šafarevič has told one of the authors that Sermenev (unpublished) studied the motif of X_m^r using such an embedding.

(2) For the results in §3, compare the paper of N. Koblitz in Compositio Math., 31 (1975). In particular, the proof of Proposition 3.5 proves his Conjectures (I), (II), (III) in p. 199-200.