On the Jacobian Variety of the Fermat Curve

NORIKO YUI*

Department of Mathematics, University of Ottawa, Ottawa, Ontario, KIN 6N5, Canada

Communicated by J. Dieudonné

Received May 5, 1979

The structure of the $p$-divisible groups arising from Fermat curves over finite fields of characteristic $p > 0$ is completely determined, up to isogeny, by purely arithmetic means. In certain cases, the "global" structure of the Jacobian varieties of Fermat curves, up to isogeny, is also determined.

1. INTRODUCTION

Let $p$ be a rational prime.

Let $C$ be the Fermat curve defined by the equation

$$C : X^m + Y^m = 1, \quad m \geq 3, \quad (m, p) = 1$$

over a finite field $k = GF(q)$ of $q = p^f$ elements, where $f$ is the smallest integer such that $p^f \equiv 1 \pmod{m}$. $C$ has genus $g = (m - 1)(m - 2)/2$. Denote by $J$ the Jacobian variety of $C$. We may assume that $J$ as well as the canonical embedding $C \hookrightarrow J$ are defined over $k$. Let $J_n$ be the kernel of multiplication by $n \in \mathbb{N}$ on $J$ onto itself. It is well known that for $n = p^r$, $J_{p^r}$ is a group-scheme and the inductive system $(J_{p^r}, i_r)$ with the obvious inclusion $i_r$, forms the $p$-divisible group $J(p)$ of dimension $g$ and of height $2g$ (Tate [12]). There is a contravariant functor $V_p$ associating to each $p$-divisible group its Dieudonné module; $V_p$ defines an antiequivalence of categories. Let $\bar{k}$ be the algebraic closure of $k$. Let $W$ (resp. $\bar{W}$) be the ring of infinite Witt vectors over $k$ (resp. $\bar{k}$) and let $L$ (resp. $\bar{L}$) be the field of quotients of $W$ (resp. $\bar{W}$). (So $W$ is the ring of integers in the absolutely unramified complete extension field $L$ of $Q_p$.) Let $W[F, V]$ be the noncommutative ring with the indeterminates $F$ (the Frobenius morphism) and $V$ (the Verschiebung morphism) subject to the relations

$$FV = VF = p, \quad F\lambda = \lambda F, \quad \lambda V = V\lambda^p \quad \text{for} \quad \lambda \in W,$$

* Current address: Sonderforschungsbereich, Theoretische Mathematik, Universität Bonn, Beringstrasse 4, D-5300 Bonn, West Germany.
where $\sigma$ is the automorphism of $W$ induced by the map $x \rightarrow x^p$ of $k$. First we put

$$T_p(J(p)) = \lim_{\nu} T_p(J(p)^\nu)$$

with

$$T_p(J(p)^\nu) = \lim_{n} \text{Hom}_{k-\sigma}(J(p)^\nu, W_n) \oplus [W \otimes \mathbb{Z} \text{Hom}_{k-\sigma}(J(p)^\nu, G_m, k)]^\sigma$$

where $W_n$ denotes the $n$th Witt group-scheme, $G_{m, k}$ the multiplicative group scheme over $k$, and $\mathcal{G} = \text{Gal}(\overline{k}/k)$ the Galois group of $\overline{k}$ over $k$. $T_p(J(p))$ is a left $W[F, V]$-module, $W$-free of rank $2g$ (see Demazure [2], Manin [6], and Oda [8]). Put

$$V_p(J(p)) = T_p(J(p)) \otimes W L.$$ 

Then $V_p(J(p))$ captures a structure of a left $L[F]$-module of rank $2g$; it is the Dieudonné module of $J(p)$. Over the algebraic closure $\overline{k}$, $V_p(J(p))$ ($= T_p(J(p)) \otimes_{W} L$) can be expressed as a direct sum:

$$V_p(J(p))(= T_p(J(p)) \otimes W L) = \bigoplus_{i=1}^{t} M_{r_i, s_i},$$

where

$$M_{r_i, s_i} \cong \left( \frac{L[F]}{L[F](F^{r_i} - p^{s_i})} \right)$$

with a unique choice of integers $r_i, s_i$ such that $r_i \geq 0$, $s_i \geq 1$, and $0 \leq r_1/s_1 < r_2/s_2 < \cdots < r_t/s_t \leq 1$. If $(r_i, s_i) = d_i > 1$, then $M_{r_i, s_i} \cong d_iM_{r_i/d_i, s_i/d_i}$.

Here $M_{r_i, s_i} = V_p(G_{r_i, s_i})$ is the Dieudonné module of the $p$-divisible group $G_{r_i, s_i}$ of dimension $r_i$ and of height $s_i$. (See Artin and Mazur [1] and Manin [6].)

In this paper, we shall first determine completely the structure of the isogeny class of the $p$-divisible group $J(p)$, equivalently, the structure of the Dieudonné module $V_p(J(p))$ (over $\overline{k}$) up to isomorphism, and then we shall discuss how much of the global (algebraic) structure of the Jacobian variety $J$ of $C$, up to isogeny, can be recovered from the local (formal) one, namely, $J(p)$.

Weil [16, 17] has computed the zeta function of $C$. The eigenvalues of the Frobenius endomorphism of $J$ are expressed in terms of the Jacobi sums. The theoretical basis of the work is collected in Section 2, where we illustrate the main ideas and develop the techniques to determine the structure of the isogeny class of $J(p)$, and also the algebraic (global) structure of $J$, up to isogeny. The theory is then applied in Sections 3, 4, and 5. We shall summarize the main results here. Let $f$ be the decomposition degree of $p$ in $K_m$. Then the local structure of the Jacobian variety $J$ of $C$, i.e., the isogeny type of $J(p)$, is essentially de-
Jacobian Variety of the Fermat Curve

terminated by \( f \) (Section 2). The structure of the isogeny class of \( J(p) \) sharply differs according to whether \( f \) is even or odd. If \( f \) is even and \( p^{f/2} + 1 \equiv 0 \) (mod \( m \)), then \( J(p) \) is isogenous to \( gG_{1,1} \) (Section 3, Case 1), and moreover, this is the necessary and sufficient conditions for \( J \) to be supersingular (\( J \) is isogenous to \( g \) copies of a supersingular elliptic curve) (Theorem 3.3). If \( f \) is even, but \( p^{f/2} + 1 \not\equiv 0 \) (mod \( m \)), then \( J(p) \) is no longer isogenous to \( gG_{1,1} \); however, it always contains the component \( G_{1,1} \) and in fact \( J(p) \) has the isogeny type

\[
J(p) \sim r_0(G_{1,0} + G_{0,1}) + \sum_{0 < c < f/2} \frac{r_c}{f} (G_{c,f-c} + G_{f-c,c}) + \frac{1}{2}r_{f/2}G_{1,1}
\]

with \( 0 < r_{f/2} < 2g \) and not all \( r_c \neq 0 \) for \( 0 \leq c < f/2 \) (Theorem 3.10). If \( f \) is odd, in particular, if \( f = 1 \), then \( J(p) \) is isogenous to \( g(G_{1,0} + G_{0,1}) \) and \( J \) is an ordinary abelian variety (Section 4, Case 1). If \( f \) is odd and \( f > 1 \), then \( J(p) \) contains no component \( G_{1,1} \) and is indeed isogenous to a formal group of the form

\[
J(p) \sim r_0(G_{1,0} + G_{0,1}) + \sum_{0 < c < [f/2]} \frac{r_c}{f} (G_{c,f-c} + G_{f-c,c}) \quad \text{with} \quad r_0 < g
\]

(Section 4, Case 2). We also prove that there exists no Fermat curve \( C \) whose Jacobian \( J \) has the formal completion \( J(p) \) isogenous to the symmetric formal group of dimension \( g \) (Theorem (4.13)). In Section 5, we determine the isogeny type of \( J(p) \) arising from the Fermat curve \( X^m + Y^m = 1 \), for \( p \geq 2 \) and \( 3 \leq m \leq 25 \). It appears that there are quite a few supersingular Fermat curves. Indeed, the density of the set of Fermat curves with supersingular Jacobians in the set of all Fermat curves, seems greater than or equal to \( \frac{1}{3} \). Finally in Section 6, we give some applications, namely, we consider certain algebraic curves which are dominated by the Fermat curves and study the structure of the associated \( p \)-divisible groups in the connection with the \( p \)-divisible groups of the dominating Fermat curves.

Some of the results of this paper have been announced in Yui [20].

Notations and Terminology

1. The symbols \( \mathbb{N} \), \( \mathbb{Z} \), \( \mathbb{Q} \), \( \mathbb{R} \), and \( \mathbb{C} \) denote, respectively, the set of natural numbers, the ring of rational integers, the field of rational numbers, the field of real numbers, and the field of complex numbers. For a rational prime \( p \), \( \mathbb{Z}_p \) and \( \mathbb{Q}_p \) denote the ring of \( p \)-adic integers and the field of \( p \)-adic numbers, respectively, and we let \( \mathbb{Z}_p \) denote the integral closure of \( \mathbb{Z}_p \) in the algebraic closure \( \overline{\mathbb{Q}_p} \) of \( \mathbb{Q}_p \). All valuations used in this paper are additively written.

2. An abelian variety is said to be elementary or simple if it has no nontrivial abelian subvariety.
3. By a Newton polygon of a polynomial $\sum_{i=0}^{m} c_i U^i \in \mathbb{Z}[U]$, we mean a lower convex envelope of the set of points $\{(i, \text{ord}_U(c_i))\} \subset \mathbb{R} \times \mathbb{R}$.

4. The Hasse–Witt = Cartier–Manin matrix $A$ of the Fermat curve $C : X^m + Y^m = 1$ over $k = GF(q)$ is a $(g \times g)$ matrix with elements in $k$, which is the matrix representation of the Cartier operator with respect to the first-kind differential 1-forms on $C$ over $k$ (Manin [7], cf. Hasse and Witt [3]). Any differential 1-form $\omega$ of the first kind on $C$ over $k$ is expressed as

$$\omega = R(X, Y) \frac{dX}{Y^{m-1}},$$

where $R(X, Y)$ is a polynomial over $k$ of degree at most $m - 3$ and is a linear combination of $1, X, Y, X^2, XY, Y^2, ..., Y^{m-3}$. The canonical basis for the first-kind differential 1-forms on $C$ over $k$ is given by the set

$$\mathcal{B} = \left\{ \omega_1 = \frac{dX}{Y^{m-1}}, \omega_2 = \frac{X dX}{Y^{m-1}}, ..., \omega_g = \frac{Y^{m-3} dX}{Y^{m-1}} \right\}.$$

We rewrite $\omega$ in the form

$$\omega = Y^{-(m-1)p} Y^{(m-1)p-(m-1)} R(X, Y) dX = Y^{-(m-1)p} Q(X, Y) dX.$$

Then the Hasse–Witt = Cartier–Manin matrix $A$ is obtained by applying the Cartier operator to the canonical basis $\mathcal{B}$. In fact, to get $A$, it suffices to compute the coefficients of $R(X, Y)^p X^{p-1}$ in $Q(X, Y)$ (because all other terms are exact differentials and hence are annihilated by the Cartier operator).

5. We employ the notations and definitions of Manin [6] for the formal groups $G_{1,0}$, $G_{1,1}$, and $G_{m,n} + G_{n,m}$. $G_{0,1}$ denotes the constant $p$-divisible group $(\mathbb{Q}_p/\mathbb{Z}_p)^{\times}$.

2. Jacobi Sums and the $p$-Divisible Groups $J(p)$ Arising from Fermat Curves

For any rational integer $m \geq 3$, let $\zeta_m = e^{2\pi i / m}$ be a primitive $m$th root of unity and put $K_m = \mathbb{Q}(\zeta_m)$. Then $K_m$ is the $m$th cyclotomic field over $\mathbb{Q}$ of degree $\phi(m)$, where $\phi$ is the Euler function. If $t$ is any rational integer prime to $m$, $\zeta_m \rightarrow \zeta_m^t$ determines an automorphism $\sigma_t$ of $K_m$ over $\mathbb{Q}$ and the Galois group $G$ of $K_m$ over $\mathbb{Q}$ consists of all $\sigma_t$:

$$G = \{ \sigma_t : \zeta_m \rightarrow \zeta_m^t \mid (t, m) = 1, t \text{ mod } m \}.$$

Therefore $G$ is isomorphic to the multiplicative group $(\mathbb{Z}/m\mathbb{Z})^{\times}$ of rational integers prime to $m$ modulo $m$.  

Let \( p \) be a prime ideal in \( K_m \), prime to \( m \). Put \( q = Np \). Then \( q \equiv 1 \pmod{m} \). We may assume that \( q = p^f \), where \( f \) is the smallest positive integer such that \( p^f \equiv 1 \pmod{m} \). So \( f \) is the decomposition degree of \( p \) in \( K_m \). We denote by \( k \) a finite field \( GF(q) \) with \( q = p^f \) elements.

Now we shall study the Jacobi sums for the field \( k = GF(q) \). We recall some facts on the Jacobi sums for \( k \) from the papers of Weil [16, 17]. Let \( k^* \) denote the multiplicative group of \( k \). Let \( \sigma \) be a generating element of \( k^* \), which may be any \((q - 1)\)th root of unity such that

\[ \sigma \equiv \frac{w^{(q-1)/m}}{m}. \]

We choose such an element \( \sigma \) once and for all and let \( \chi \) be the character of \( k^* \) determined by

\[ \chi(\sigma) = \sigma^{(q-1)/m} = e^{2\pi i/m}. \]

Then \( \chi \) is a multiplicative character of order \( m \) of \( k^* \).

Let \( U_m \) denote the set of all vectors defined as follows:

\[ U_m = \left\{ a = (a_0, a_1, a_2) \mid a_i \in \mathbb{Z}/m\mathbb{Z}, a_i \neq 0 \pmod{m}, a_0 + a_1 + a_2 \equiv 0 \pmod{m} \right\}. \]

It is easy to compute the number of elements in \( U_m \), and in fact, the cardinality of \( U_m = (m - 1)(m - 2) = 2g \).

(2.1) DEFINITION (Weil [17]). For any \( a \in U_m \), the Jacobi sum \( j(a) \) for \( k \) is defined by

\[ j(a) = -\sum_{\substack{1+u_1+u_2=0 \\ u_i \in \mathbb{Z}}} \chi(u_1)^{a_1} \chi(u_2)^{a_2}. \]

The Jacobi sum is an algebraic integer in \( K_m \) with the absolute value

\[ |j(a)| = q^{1/2}. \]

Now we shall be concerned with the prime ideal decomposition of the Jacobi sums. This problem was first considered by Stickelberger in [11]. Let \( p \) be a prime ideal in \( K_m \) such that \( Np = q = p^f \). Then the prime ideal decomposition of the Jacobi sum \( j(a) \) is given as

\[ (j(a)) = p^{\omega(a)}, \]

where \( \omega(a) \) is the element of the group-ring of \( G \) defined by

\[ \omega(a) = \sum_{(t,m)=1}^{\phi(m)} \left[ \sum_{i=1}^{m} \frac{t^a_i}{m} \right] \sigma_t^{-1}. \]

(2.3)
with \( \sigma_t \in G \) such that \( \sigma_t(\zeta_m) = \zeta_m^t \) and \( \langle \lambda \rangle \) denotes the "fractional part" of the real number \( \lambda \in \mathbb{R} \), defined as \( \langle \lambda \rangle = \lambda - [\lambda] \), where \([\lambda]\) is the "integral part" of \( \lambda \) (see Weil [16, 17]).

We can reformulate the prime ideal decomposition of the Jacobi sum \( j(a) \) by introducing the subgroup \( H \) of \( G \). Put

\[
H = \{ p^\mu \mod m \mid 0 \leq \mu < f \}.
\]

Then \( H \) is a subgroup of \( G \) of order \( f \) and moreover it is the decomposition group of \( p \) over \( \bar{p} \). For any \( a \in \mathcal{U}_m \), we put

\[
A_H(a) = \sum_{t \in H} \left( \sum_{i=1}^{g} \left\langle \frac{ta_i}{m} \right\rangle \right).
\] (2.4)

Then we have

(2.5) **Lemma.** \( A_H(a) \) is a rational integer and, moreover, \( 0 \leq A_H(a) \leq f \) for any \( a \in \mathcal{U}_m \).

**Proof.** By (2.4), \( A_H(a) \) is easily seen to be a nonnegative rational integer. Note that for each \( t \in H \) and for \( a = (a_0, a_1, a_2) \in \mathcal{U}_m \),

\[
\left[ \sum_{i=1}^{g} \left\langle \frac{ta_i}{m} \right\rangle \right] \leq \left[ 2 \left\langle \frac{m-1}{m} \right\rangle \right] = 1.
\]

Hence it follows that \( A_H(a) \leq |H| = f \). \( \blacksquare \)

Choose a set \( \{ t_1 = 1, t_2, \ldots, t_r \} \) of representatives of the left coset decomposition \( G \mod H: G = Ht_1 + Ht_2 + \cdots + Ht_r \), so \( \phi(m) = f \cdot r \).

(2.6) **Lemma** (Shioda and Katsura [10]). With the notations as above, the prime ideal decomposition of the Jacobi sum \( j(a) \) is given by

\[
(j(a)) = \prod_{l=1}^{r} p_{l}^{A_H(t_la)},
\]

where \( p_l =: p^{\sigma_l} \) with \( \sigma_l = \sigma_{-t_l}^{-1} \) and \( t_l a = (t_la_0, t_la_1, t_la_2) \in \mathcal{U}_m \).

**Proof.** We can rewrite \( \omega(a) \) in (2.3) as

\[
\omega(a) = \sum_{l=1}^{r} \left( \sum_{t \in H} \left[ \sum_{i=1}^{g} \left\langle \frac{tl_ia_i}{m} \right\rangle \right] \sigma_{-t_l}^{-1} \right).
\]

By noting that \( H \) is the decomposition group of \( p \) over \( \bar{p} \), we have \( p^{\sigma_l} = p \) for any \( t \in H \). So we obtain the expression

\[
(j(a)) = \prod_{l=1}^{r} p_{l}^{A_H(t_la)} = \prod_{l=1}^{r} p_{l}^{A_H(t_la)}. \] \( \blacksquare \)
(2.7) **Lemma.** Let \( \{t_1 = 1, t_2, \ldots, t_r\} \) be a left coset representatives of \( G \) mod \( H \). Then for any \( a \in \mathcal{U}_m \), there exists a unique vector \( a' = t_ia \in \mathcal{U}_m \) such that

\[
A_H(a) + A_H(a') = f.
\]

**Proof.** Note first that the set \( \mathcal{U}_m \) is closed under multiplication by any element \( t_i \in G \) mod \( H \). We know that the Jacobi sum \( j(a) \) is an algebraic integer in \( K_m \) such that \( |j(a)|^2 = j(a)\overline{j(a)} = p' \), where \( \overline{j(a)} \) denotes the complex conjugate of \( j(a) \). Now the prime ideal decomposition of \( j(a) = p'/j(a) \) can be deduced from Lemma (2.6):

\[
(j(a)) = (p'/j(a)) = \prod_{i=1}^{r} p_i^{f-A_H(t_ia)}
\]

with \( 0 \leq f - A_H(t_ia) \leq f \) for every \( 1 \leq l \leq r \). The complex conjugation induces a nontrivial automorphism of \( K_m \), which is an element of \( G \). So there exists a coset \( Ht_s \) which contains the element of \( G \) induced by the complex conjugation. In particular, we get

\[
f - A_H(a) = A_H(t_s a) = A_H(a')
\]

which proves the assertion. \( \square \)

Now we consider the Fermat curve

\[
C: X^m + Y^m = 1, \quad m \geq 3
\]

defined over a finite field \( k = GF(p') \), where \((p, m) = 1\) and \( p' \) is the least power of \( p \) such that \( p' = 1 \) (mod \( m \)). Weil [17] has determined the zeta function of \( C \). The eigenvalues of the Frobenius endomorphism of the Jacobian variety \( J \) of \( C \) relative to \( k \) are expressed explicitly in terms of the Jacobi sums of \( k \). Here we shall determine the structure of the \( p \)-divisible group \( J(p) \) associated to the Jacobian variety \( J \) of \( C \), by investigating the \( p \)-adic decomposition of the Jacobi sums and their \( p \)-adic orders.

(2.8) **Theorem.** Let \( C : X^m + Y^m = 1, m \geq 3 \) be the Fermat curve of genus \( g = (m - 1)(m - 2)/2 \) defined over a finite field \( k = GF(q) \) with \( q = p^f \) elements, where \( f \) is the smallest power of \( p \) such that \( q = p' = 1 \) (mod \( m \)). Let \( J \) be the Jacobian variety of \( C \) defined over \( k \) and \( J(p) \) the associated \( p \)-divisible group of dimension \( g \) and of height \( 2g \). The notations \( \mathcal{U}_m \), \( H \), and \( A_H(a) \) being as above, for any rational integer \( 0 \leq c \leq f \), let \( r_c \) denote the number of the vectors \( a \in \mathcal{U}_m \) such that \( A_H(a) = c \). Then \( J(p) \) is isogenous to a formal group of the form

\[
J(p) \sim r_0(G_{1,0} + G_{0,1}) + \sum_{0 < c < f/2} \frac{r_c}{f} (G_{c,f-c} + G_{f-c,c}) + \frac{1}{2} \frac{r_{f/2}}{f} G_{1,1}
\]
with 
\[ r_c = r_{f-c} \quad \text{for} \quad 0 \leq c \leq f/2 \]
and 
\[ \sum_{0 < c < f/2} r_c = \sum_{0 < c < f/2} r_{f-c} = g - r_0 \quad \text{if} \quad f \text{ is odd,} \]
\[ = g - r_0 - \frac{1}{2} r_{f/2} \quad \text{if} \quad f \text{ is even.} \]

Here the numbers \( c, f - c \) are not necessarily relatively prime. If \( (c, f - c) = d > 1 \), then we identify the formal group \( G_{c, f-c} \) with \( d G_{c, (f-c)/d} \).

**Proof.** By Weil [16, 17], the zeta function \( Z(U) \) of \( C \) is expressed in terms of the Jacobi sums for \( k \):
\[ Z(U) = \frac{\prod_{a} (1 - j(a)U)}{(1 - U)(1 - qU)}. \]

Let \( \pi(=F') \) be the Frobenius endomorphism of \( J \) and \( J(p) \) relative to \( k \) and let \( P(U) \) be the characteristic polynomial of the \( p \)-adic representation of \( \pi \) in the Dieudonné module \( V_{p}(J(p)) \). \( P(U) \) has the Jacobi sums as its roots:
\[ P(U) = \prod_{a \in \mathfrak{M}} (U - j(a)) = \sum_{i=0}^{2g} c_i U^i \in \mathbb{Z}[U] \]
with \( c_{2g} = 1 \) and \( c_0 = q^0 = p^{f_0} \).

Manin has shown in [6, Theorem 4.1] that the structure of the isogeny class of \( J(p) \) parallels the local \( (p \text{-adic}) \) factorization of \( P(U) \). In other words, the \( p \)-adic roots of \( P(U) = 0 \) in the integral closure \( \overline{\mathbb{Z}_p} \) of \( \mathbb{Z}_p \) determines the structure of \( J(p) \), up to isogeny. Let us denote by \( \nu \) the unique valuation in \( \overline{\mathbb{Z}_p} \) which extends the \( p \)-adic valuation \( \text{ord}_p \) in \( \mathbb{Q}_p \), normalized so that \( \nu(p) = 1 \). Now for any rational integer \( 0 \leq c \leq f \), let \( r_c \) be the number of the vectors \( a \in \mathfrak{M} \) such that \( A_H(a) \equiv c \). Then \( P(U) \) has a factor \( P_c(U) \) in \( \mathbb{Z}_p[U] \) such that
\[ P_c(U) = \sum_{\nu(\tau_i) = c} (U - \tau_i) \quad \text{with} \quad \nu(\tau_i) = c. \]

Since \( P(U) \) also has, together with any \( p \)-adic root \( \tau \), a \( p \)-adic root \( q/\tau \), the number of the \( p \)-adic roots with \( \nu(\tau) = c \) is the same as the number of those with \( \nu(\tau) = f - c \) (cf. Lemma (2.7)), so \( r_c = r_{f-c} \). Hence \( P(U) \) can be factored in \( \mathbb{Z}_p[U] \) as
\[ P(U) = \prod_{0 < c < f/2} P_{d}(U) P_{f-c}(U) \cdot P_{f/2}(U). \]

Hence the Dieudonné module \( V_{p}(J(p)) (=T_p(J(p)) \otimes \mathbb{F} \overline{L}) \) is isomorphic to the module of the form
\[ V_{p}(J(p)) \cong \bigoplus_{0 < c < f/2} \left( \overline{L[F]} / \overline{L[F]}(F' - p^e) \right)^{r_{c/f}}. \]
Therefore the $p$-divisible group $J(p)$ is isogenous to a formal group of the form

$$J(p) \sim r_0(G_{1,0} + G_{0,1}) + \sum_{0 < c < f/2} \frac{r_c}{f} (G_{c,f-c} + G_{f-c,c}) + \frac{1}{2} r_{f/2} G_{1,1}.$$  

Now we investigate the algebraic (global) structure of the Jacobian variety $J$ of $C$ up to isogeny.

(2.9) **Theorem.** With the notations and the hypothesis as in Theorem (2.8), let $\mathcal{A}$ denote the endomorphism algebra of $J$: $\mathcal{A} = \text{End}(J) \otimes \mathbb{Q}$. Then $\mathcal{A}$ is a semi-simple algebra with the center $\Phi = \mathbb{Q}[\pi]$. If $J$ is an elementary abelian variety, the local invariants of $\mathcal{A}$ at the primes $v$ in $\Phi$ over $p$ are given by

\begin{align*}
i v(v)(\mathcal{A}) &= \frac{c}{f} \pmod{\mathbb{Z}} \quad \text{if } v \text{ is nonarchimedean and nonreal}, \\
&= \frac{1}{2} \pmod{\mathbb{Z}} \quad \text{if } v \text{ is real}, \\
&= 0 \pmod{\mathbb{Z}} \quad \text{otherwise}.
\end{align*}

**Proof** (cf. Tate [13] or Waterhouse and Milne [15]). Suppose that $P(U) = Q(U)^e$ with $Q$ irreducible over $\mathbb{Q}$, so $\mathcal{A}$ is a division algebra of dimension $e^2$ over its center $\Phi$. Corresponding to the $p$-adic factorization of $Q(U)$:

$$Q(U) = \prod_{0 < c < f/2} Q_{c}(U) Q_{f-c}(U) Q_{f/2}(U),$$

we get the primes $v (= v_v$ or $v_{f/2}$) in $\Phi$ over $p$ with which we have

$$\Phi \otimes \mathbb{Q}_p = \bigoplus_v \Phi_v.$$  

Now the Dieudonné module $V_p(J(p))$ is $2g$-dimensional over $L$ and in it $\pi$ acts by the endomorphism $F'$. Note that $F'$ lies in the center of the ring $L[F]$. As a $L[F]$-module, $V_p(J(p))$ is isomorphic to a direct sum $\bigoplus_v V_v$ with

$$V_v \cong \left( \frac{L[F]}{L[F](Q_v(F'))} \right),$$

where $Q_v(U) = Q_v(U) = Q_v(U)$ for $0 \leq c < f/2$ or $c = f/2$ (cf. Manin [6, Chap. 2, sect. 3]).
Here each component
\[ V_v \cong \left( \frac{L[F]}{L[F](Q_v(F'))} \right) \]
is a central simple algebra of dimension \( f^2 \) over the field \( \Phi_v \), and its Hasse invariant \( h_v \) is derived from the equalities
\[ ||\pi||_v = p^{-c} = q^{-h_v} = p^{-f h_v}, \]
where \( ||\pi||_v \) denotes the normed absolute value of \( \pi \) at \( v \). So we have
\[ h_v = \frac{c}{f} \pmod{\mathbb{Z}} \quad \text{if} \ v \text{ is nonarchimedean and nonreal}, \]
\[ = \frac{1}{2} \pmod{\mathbb{Z}} \quad \text{if} \ v \text{ is real}, \]
\[ = 0 \pmod{\mathbb{Z}} \quad \text{otherwise}. \]

Let \( \text{Br}(\Phi) \) be the Brauer group of \( \Phi \). The class of \( \mathcal{A} \) in \( \text{Br}(\Phi) \) is determined explicitly. In fact, by the theorem of Tate in [13] (for a proof, see Waterhouse and Milne [15]),
\[ \mathcal{A} \otimes \mathbb{Q}_p \to \text{End}_{L[F]}(V_p(J(p))) \]
is an anti-isomorphism. So it follows from this fact that \( \text{Br}(\Phi) \) and the central simple algebra \( V_v \) have the same invariant. Whence the result. □

3. THE STRUCTURE OF \( J(p) \) UP TO ISOGENY: THE CASES OF \( f \) EVEN

In this section, we treat the cases where the decomposition degree \( f \) of \( p \) in \( K_m \) is even. Our discussion is divided into the following two cases:

Case 1. Rational primes \( p \) such that \( p^{f/2} + 1 \equiv 0 \pmod{m} \).

Case 2. Rational primes \( p \) such that \( p^{f/2} + 1 \not\equiv 0 \pmod{m} \).

Case 1

(3.1) Theorem. The notations being as in Section 2, the following conditions are equivalent.

(i) The decomposition degree \( f \) of \( p \) in \( K_m \) is even, and \( p^{f/2} + 1 \equiv 0 \pmod{m} \).

(ii) There exists a positive integer \( \mu \) such that \( \mu \mid f \) and \( p^\mu \equiv -1 \pmod{m} \).

(iii) The subgroup \( H \) of \( G \) contains \(-1 \) mod \( m \).

(iv) \( A_H(a) = f/2 \) for all \( a \in \mathfrak{A}_m \).
Proof. (i) ⇒ (ii). If (i) holds true, then we may take \( \mu = f/2 \), to get (ii). Conversely, assume (ii) and put \( \mu = f/d \in \mathbb{Z} \) with some positive integer \( d > 1 \). Then

\[
p^\mu - 1 = p^{f - (2/d)} - 1 \equiv 0 \pmod{m}.
\]

Since \( f \) is the smallest positive integer satisfying \( p^f \equiv 1 \pmod{m} \), \( f | 2\mu = f \cdot (2/d) \). Hence \( 2/d \in \mathbb{Z} \) and, moreover, from the condition \( 0 \leq 2\mu = f \cdot (2/d) < 2f \) we obtain \( 1 \leq 2/d < 2 \). Hence \( d = 2 \) and \( f = 2\mu \) is even and \( p^{f/2} + 1 \equiv 0 \pmod{m} \).

(ii) ⇔ (iii). Obvious from the definition of \( H \): \( H = \{ p^\mu \pmod{m} \mid 0 \leq \mu < f \} \).

(iii) ⇒ (iv) (Shioda and Katsura [10]). First note that for any \( \lambda \in \mathbb{Q}, \lambda \notin \mathbb{Z}, \langle \lambda \rangle + \langle -\lambda \rangle = 1 \) and \( [\lambda] + [\lambda] = -1 \). If \( H \equiv -1 \pmod{m} \), then it follows from (2.4) that

\[
A_H(a) = A_H(-a) \quad \text{for every } a \in \mathfrak{U}_m
\]

and

\[
A_H(-a) = \sum_{t \in H} \left[ \sum_{i=1}^{2} \frac{\langle -ta_i \rangle}{m} \right] = \sum_{t \in H} \left[ \sum_{i=1}^{2} \left( 1 - \frac{\langle ta_i \rangle}{m} \right) \right] = 2 |H| + \sum_{t \in H} \left( -1 - \left[ \sum_{i=1}^{2} \frac{\langle ta_i \rangle}{m} \right] \right) = 2 |H| - |H| - A_H(a) \quad \text{for every } a \in \mathfrak{U}_m.
\]

Here \( |H| \) means the cardinality of \( H \). Hence we obtain the equality

\[
A_H(a) + A_H(-a) = |H| = f \quad \text{for every } a \in \mathfrak{U}_m.
\]

Therefore one gets

\[
A_H(a) = f/2 \quad \text{for every } a \in \mathfrak{U}_m.
\]

(iv) ⇒ (ii). For \( m \geq 4 \), this is the special case \( (r = 1) \) of Proposition 3.5 of Shioda and Katsura [10]. For \( m = 3, \phi(3) = 2 \) and there are two kinds of primes: \( p \equiv 1 \pmod{3} \) \( (f = 1) \) and \( p \equiv 2 \pmod{3} \) \( (f = 2 \text{ and } p + 1 \equiv 0 \pmod{3}) \). If \( p \equiv 1 \pmod{3} \), \( H = \{1\} \) and \( A_H(a) \neq 1 \) for \( a = (1, 1, 1) \). Hence if \( A_H(a) = 1 \) for all \( a \in \mathfrak{U}_3 \), then \( p \) must be \( \equiv 2 \pmod{3} \). So take \( \mu = 1 \).
(3.2) **Theorem.** Suppose that Theorem (3.1) holds true. Then we have the following equivalent assertions.

(i) Every Jacobi sum \( j(a) \) has the \( p \)-adic order

\[ \nu(j(a)) = f/2. \]

(ii) The Newton polygon \( \mathfrak{N}(P) \) of the characteristic polynomial \( P(U) \) (of the Frobenius endomorphism \( \pi \) of \( J \) and \( J(p) \), relative to \( k \)) has the shape illustrated below:

![Newton polygon](image)

(iii) \( J(p) \) is isogenous to the formal group \( gG_{1,1} \).

(iv) The Dieudonné module \( V_p(J(p)) \) \( (=T_p(J(p)) \otimes_{W} L) \) is isomorphic to the module

\[ V_p(J(p)) \cong \left( \frac{L[F]}{L[F](F^f - p)} \right)^g. \]

**Proof.** Theorem (3.1) (iv) \( \Rightarrow \) Theorem (3.2) (i). By Lemma (2.6), we get

\[ (j(a)) = (p_1 \cdots p_r)^{f/2} = (p^{f/2}) \]

for every \( a \in \mathfrak{U}_m \), and hence

\[ \nu(j(a)) = f/2 \quad \text{for every} \quad a \in \mathfrak{U}_m. \]

(i) \( \iff \) (ii). Assume (i). Then \( P(U) \) has the \( p \)-adic factorization in \( \mathbb{Z}_p[U] \) as

\[ P(U) = \prod_{i=1}^{2g} (U - p^{f/2}x_i) = \sum_{i=0}^{2g} c_i U^i, \]

where \( x_i \) are \( p \)-adic units. So \( \text{ord}_p(c_i) \geq \langle f/2 \rangle (2g - i) \) for every \( 0 \leq i \leq 2g \). Hence the Newton polygon \( \mathfrak{N}(P) \) has only one nonvertical segment with slope \(-f/2\). The converse is trivial.
(ii) $\iff$ (iii). This is a reformulation of Theorem 4.1 of Manin [6] in terms of the Newton polygon $\mathcal{N}(P)$ of $P(U)$.

(iii) $\iff$ (iv). By the definition of $G_{1,1}$ (cf. Manin [6]), the Dieudonné module of $G_{1,1}$ is isomorphic to the module

$$\left( \frac{L[F]}{L[F](F^2 - p)} \right).$$

(iv) $\Rightarrow$ (i). As the Frobenius morphism $F$ and the Verschiebung morphism $V$ have the same $p$-adic order

$$\nu(F) = \nu(V) = \frac{1}{2},$$

the Frobenius endomorphism $\pi(F)$ of $J(p)$ and its $p$-adic dual $q/\pi = p'/\pi$ have the $p$-adic order

$$\nu(\pi) = \nu(q/\pi) = f/2.$$

Since the Jacobi sums are the eigenvalues of $\pi$, it follows that

$$\nu(j(a)) = f/2$$

for every $a \in \mathfrak{U}_m$. 

The converse of Theorem (3.2) also holds true.

(3.3) THEOREM. Suppose that $J(p)$ is isogenous to the formal group $gG_{1,1}$; then $f$ must be even and $p^{f/2} + 1 \equiv 0 \pmod{m}$.

Proof. By Theorem (3.2), for any $a \in \mathfrak{U}_m$, we have

$$\nu(j(a)) = f/2.$$

Then we can write

$$j(a) = -p^{f/2} \sum_{h}^m h$$

with some $h \in \mathbb{Z}$

(see Wil [17]). Hence for some $s \in \mathbb{N}$, we have

$$j(a) = p^{fs/2}.$$

Now by Lemma (2.6) and by the decomposition of $p$ in $K_m$, $(p) = p_1 \cdots p_r$, we get

$$p^{fs/2} = (p_1 \cdots p_r)^{fs/2} = \prod_{i=1}^{r} p_i^{A_H(t_i a)s}. \quad (3.4)$$

So it follows that

$$A_H(t_i a) = f/2$$

for all $l = 1, \ldots, r$. 

and hence

$$A_H(a) = f/2 \quad \text{for all } a \in \mathbb{N}_m.$$  

Therefore, by Theorem (3.2)(i), \(f\) must be even and \(p^{f/2} + 1 \equiv 0 \pmod{m}\).  

Putting together Theorems (3.1), (3.2), and (3.3), we obtain the following arithmetic characterization.

(3.5) Theorem (cf. Shioda and Katsura [10, Proposition 3.10]). The necessary and sufficient condition for \(J(p)\) to be isogenous to the formal group \(gG_{1,1}\) is that \([2 \mid f\) and \(p^{f/2} + 1 \equiv 0 \pmod{m}\).  

When \(J(p) \sim gG_{1,1}\), \(J\) is said to be supersingular.

The algebraic (global) structure of a supersingular Jacobian variety \(J\) of \(C\) up to isogeny is determined completely from its formal structure, i.e., \(J(p)\).

(3.6) Theorem. The following assertions are equivalent.

(i) \(J(p) \sim gG_{1,1}\).

(ii) For some \(s \in \mathbb{N}\), let \(k_s\) denote the finite extension of \(k\) of degree \(s\). Then the local invariant of the endomorphism algebra \(\mathcal{A}_s\) of \(J \times_k k_s\) is given by

$$\text{inv}_v(\mathcal{A}_s) \equiv \frac{1}{2} \pmod{\mathbb{Z}}$$

for all primes \(v\) in the center of \(\mathcal{A}_s\).

(iii) \(J\) is isogenous to the direct product of \(g\) copies of a supersingular elliptic curve \(E\) over some finite extension \(k_s\) of \(k\).

Proof. (i) \(\Rightarrow\) (ii). For every \(a \in \mathbb{N}_m\), the Jacobi sum \(J(a)\) is an algebraic integer (which is the eigenvalue of the Frobenius endomorphism \(\pi\) of \(J\) and \(J(p)\) relative to \(k\)) with \(v(J(a)) = f/2 \in \mathbb{Z}\). So some power of \(J(a)\) becomes rational. Let \(s \in \mathbb{N}\) be the smallest integer such that for every \(J(a)\), its \(s\)th power becomes rational: \(J(a) = -p^{f/2}\). We make a base change and look at the structure of \(J\) over the finite extension \(k_s\) of \(k\) of degree \(s\). Then by Theorem (2.9), the local invariant of the endomorphism algebra \(\mathcal{A}_s = \text{End}(J \times_k k_s) \otimes \mathbb{Q}\) can be computed; in fact, we have

$$\|\pi^s\|_v = p^{fs/2} = q^{s - \text{inv}_v(\mathcal{A}_s)} = p^{-fs(\text{inv}_v(\mathcal{A}_s))}.$$

Therefore

$$\text{inv}_v(\mathcal{A}_s) = -\frac{1}{2} \equiv \frac{1}{2} \pmod{\mathbb{Z}}$$

for all primes \(v\) in the center of \(\mathcal{A}_s\).

(ii) \(\Rightarrow\) (iii) (cf. Tate [13] and Waterhouse [14]). As the least common denominator of all the \(\text{inv}_v(\mathcal{A}_s)\) is 2, there exists a supersingular elliptic curve \(E\)
over $k$, such that the characteristic polynomial of $\pi^s$ of $E$ is $(U - p^{s/2})^2$. And $\mathfrak{A}$ is isomorphic to the full matrix algebra of degree $g$ over the quaternion algebra $\text{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$. Hence $J$ is isogenous to $g$ copies of a supersingular elliptic curve $E$ over $k$.

(iii) $\Rightarrow$ (i). Clear from the fact that a supersingular elliptic curve yields the formal group $G_{1,1}$.

(3.7) Example. We consider the Fermat curve $C : X^4 + Y^4 = 1$ over a finite field $k$ of characteristic $p \in \{3, 7, 11\}$. $C$ has genus $g = 3$. The cyclotomic field $K_4$ has degree $\phi(4) = 2$ and the decomposition degree of $p$ in $K_4$ is $f = 2$ for each $p$. We consider $C$ over $k = GF(p^2)$. The Galois group $G$ of $K_4$ coincides with its subgroup $H = \{1, p\}$. $\mathfrak{U}_4$ consists of six vectors. We can compute easily $A_H(a)$ for every $a \in \mathfrak{U}_4$. In fact, we obtain for every $a \in \mathfrak{U}_4$,

$$A_H(a) = \sum_{t \in \{1, p\}} \sum_{i=1}^{2} \left( \frac{t}{4} \right) = 1.$$  

(3.8) This implies that for every $a \in \mathfrak{U}_4$, $(j(a)) = p$, and hence $\nu(j(a)) = 1$. So $J(p) \sim 3G_{1,1}$. There are only four roots of unity in $K_4$, namely, $\pm 1, \pm i$, so it follows that $j(a) = \pm p$ or $\pm pi$ for any $a \in \mathfrak{U}_4$. Hence the characteristic polynomial of $\pi^s$, for $s \in \{1, 2, 4\}$ is explicitly given by $P_{\pi^s}(U) = (U \pm p^s)^6$, and $J$ is isogenous to three copies of a supersingular elliptic curve over $k$.

Here we remark that the Hasse–Witt = Cartier–Manin matrix $A$ of $C$ is given by

$$A = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

for each $p$.

(3.9) Example. Let us consider the Fermat curve $C : X^5 + Y^5 = 1$ defined over a finite field of characteristic $p \in \{2, 3\}$. $C$ has genus $g = 6$. The cyclotomic field $K_5$ has degree $\phi(5) = 4$ over $\mathbb{Q}$. The decomposition degree $f$ of $p \in \{2, 3\}$ is $f = 4$. We consider $C$ over $k = GF(p^4)$. For each $p$, $p^2 + 1 \equiv 0 \pmod{5}$. The Galois group $G$ of $K_5$ coincides with its subgroup $H = \{1, 2, 3, 4\}$. $\mathfrak{U}_5$ consists of 12 vectors. We now compute $A_H(a)$ for every $a \in \mathfrak{U}_5$. We get

$$A_H(a) = \sum_{t \in H} \sum_{i=1}^{2} \left( \frac{t}{5} \right) = f/2 = 2 \quad \text{for all } a \in \mathfrak{U}_5.$$ 

Hence $J(p)$ is isogenous to $6G_{1,1}$. Each Jacobi sum $j(a)$ is an algebraic integer of the form $j(a) = \pm p^{\frac{s}{2}} \zeta_5^a$, where $\zeta_5^a$ is some root of unity in $K_5$. Therefore, $J$ becomes isogenous to six copies of a supersingular elliptic curve.

We compute the Hasse–Witt = Cartier–Manin matrix $A$ of $C$ for each $p$.

481/65/1-2
Now we confine our attention to the rational primes $p$ such that the decomposition degree $f$ of $p$ in $K_m$ is still even, but $p^{f/2} + 1 \equiv 0 \pmod{m}$.

(3.10) Theorem. With the notations as in Theorem (2.8), let $p$ be the rational primes such that $[2 | f$, but $p^{f/2} + 1 \equiv 0 \pmod{m}]$. Then $J(p)$ is isogenous to a formal group of the form

$$J(p) \sim r_0(G_{1,0} + G_{0,1}) + \sum_{0 < c < f/2} \frac{r_c}{f} (G_{c,f-c} + G_{f-c,c}) + \frac{1}{2} r_{f/2} G_{1,1}$$

with $r_{f/2} \neq 0$ and not all $r_0 \neq 0$ for $0 < c < f/2$.

In particular, if $f = 2$,

$$J(p) \sim r_0(G_{1,0} + G_{0,1}) + \frac{1}{2} r_{f/2} G_{1,1}.$$ 

Proof. First of all, $J(p)$ can be isogenous neither to $gG_{1,1}$ (see Theorem (3.5)), nor to $g(G_{1,0} + G_{0,1})$ (see Theorem (4.2) below). Since $f$ is even, one of the conjugates of some power of the Frobenius endomorphism $\pi^f$, say, of $J(p)$ is nothing but the rational number $\pm \pi^{f/2}$. Hence by Theorem (2.8), $J(p)$ contains the factor $G_{1,1}$, so we have $0 < r_{f/2} < 2g$. Hence $J(p)$ has the isogeny type as claimed. In particular, if $f = 2$, $J(p)$ can contain only $G_{1,0} + G_{0,1}$ and $G_{1,1}$ as its factors and hence the assertion follows immediately.

(3.11) Example. The first case of such primes occurs if we take the Fermat curve $C : X^{21} + Y^{21} = 1$ over a field of characteristic $p = 2$. We have $2^6 \equiv 1 \pmod{21}$, but $2^{6/2} + 1 \not\equiv 0 \pmod{21}$. The 21st cyclotomic field $K_{21} = \Q(e^{2\pi i/21})$ has degree $\phi(21) = 12$ over $\Q$ with the Galois group $G \cong \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$. The decomposition group $H$ of 2 is given by $H = \{2^\mu \pmod{21} \mid 0 \leq \mu < 6\} = \{1, 2, 4, 8, 11, 16\}$ and $G \mod H = H_{t_1} + H_{t_2}$ with $t_1 = 1$ and $t_2 = 5$. $C$ has genus $g = 190$ and the set $\mathfrak{U}_{21}$ consists of 380 vectors. We must compute the value of

$$A_H(a) = \sum_{\mu \in \{1, 2, 4, 8, 11, 16\}} \left[ \sum_{t=1}^{2} \left\langle \frac{ta_t}{21} \right\rangle \right]$$
for all 380 vectors \( a \in \mathcal{A}_{21} \). The results are summarized as follows:

\[
\begin{align*}
A_H(a) &= 0 \quad \text{for 36 vectors} \quad a \in \mathcal{A}_{21}, \\
A_H(a) &= 1 \quad \text{for 36 vectors} \quad a \in \mathcal{A}_{21}, \\
A_H(a) &= 2 \quad \text{for 99 vectors} \quad a \in \mathcal{A}_{21}, \\
A_H(a) &= 3 \quad \text{for 38 vectors} \quad a \in \mathcal{A}_{21},
\end{align*}
\]

and by applying Lemma (2.7),

\[
A_H(a) = 4 \quad \text{for 99 vectors of the form } 5a,
\]

where \( a \) moves all the vectors such that \( A_H(a) = 2 \),

\[
A_H(a) = 5 \quad \text{for 36 vectors of the form } 5a,
\]

where \( a \) moves all the vectors such that \( A_H(a) = 1 \), and finally

\[
A_H(a) = 6 \quad \text{for 36 vectors of the form } 5a,
\]

where \( a \) moves all the vectors such that \( A_H(a) = 0 \).

Hence \( J(2) \) has the isogeny type as

\[
J(2) \sim 36(G_{1,0} + G_{0,1}) + 6(G_{1,5} + G_{5,1}) + (99/6)(G_{2,4} + G_{4,2}) + 19G_{1,1}
\]

\[
= 36(G_{1,0} + G_{0,1}) + 6(G_{1,5} + G_{5,1}) + 33(G_{1,2} + G_{2,1}) + 19G_{1,1}.
\]
and by applying Lemma (2.7),
\[ A_N(a) = 3 \quad \text{for 48 vectors of the form } 5a, \]
where \( a \) moves all the vectors such that \( A_N(a) = 1 \), and finally
\[ A_N(a) = 4 \quad \text{for 24 vectors of the form } 5a, \]
where \( a \) moves all the vectors such that \( A_N(a) = 0 \).

Hence by Theorem (2.8), \( J(p) \) is isogenous to a formal group of the form
\[ J(p) \sim 24(G_{1,0} + G_{0,1}) + 12(G_{1,3} + G_{3,1}) + 33G_{1,1}. \]

(3.13) Problem. It is plausible that there exists a Fermat curve \( C \) over a finite field \( k \) whose Jacobian variety \( J \) has the formal completion \( J(p) \) of the form
\[ r_0(G_{1,0} + G_{0,1}) + \frac{1}{2} r_{f/2} G_{1,1}, \]
but \( J \) itself is \( k \)-simple.

Such a situation may occur if we take the Fermat curve \( C: X^m + Y^m = 1 \) over a finite field \( k = GF(p^2) \) (as above, \( p^2 \) is the least power of \( p \) satisfying the congruence \( p^2 \equiv 1 \pmod{m} \)), where \( m \) is chosen in such a way that \( \phi(m) \geq 4 \), \( \phi(m) \equiv 0 \pmod{4} \) and \( K_m \) has exactly one real quadratic subfield in which \( p \) splits: \( (p) = p_1p_2 \) or \( p_1 \) real prime.

At the moment, I am unable to construct a Fermat curve with \( J(p) \) of the prescribed form, but \( J \) \( k \)-simple.

4. The Structure of \( J(p) \) up to Isogeny: The Cases of \( f \) Odd

In this section, we shall investigate the cases when the decomposition degree \( f \) of \( p \) in \( K_m \) is odd. We again divide the discussion into the following two cases.

Case 1. Rational primes \( p \) such that \( f = 1 \).

Case 2. Rational primes \( p \) such that \( f \geq 1 \).

Case 1

(4.1) Proposition. With the notations as in Section 2, the following conditions are equivalent.

(i) \( p \) splits completely in \( K_m \).

(ii) \( H = \{1\} \).

(iii) \( f = 1 \), i.e., \( p \equiv 1 \pmod{m} \).

(iv) \( A_N(a) = 0 \) for \( g \) vectors \( a \in \mathfrak{A}_m \),
     \[ = 1 \quad \text{for the other } g \text{ vectors } a \in \mathfrak{A}_m. \]
Proof. (i) $\iff$ (ii) $\iff$ (iii). Obvious.

(iii) $\iff$ (iv). By Lemma (2.5), (iii) implies that $A_H(a) = 0$ or 1 for any $a \in \mathbb{A}_m$. If there exist $r_0$ vectors $a \in \mathbb{A}_m$ such that $A_H(a) = 0$, then there are $r_0$ $p$-adic roots $\tau$ of $P(U) = 0$ in $\mathbb{Z}_p$ with $v(\tau) = 0$. But $P(U)$ has the $p$-adic roots $p/\tau$ together with $\tau$, so we get $r_0$ $p$-adic roots $\tau$ of $P(U) = 0$ with $v(\tau) = 1$. Hence we have $2r_0 = 2g$ and hence $r_0 = g$. The converse is clear again by Lemma (2.5).

(4.2) Theorem. With the notations as in Proposition (4.1), the following assertions are equivalent.

(i) Proposition (4.1) holds true.

(ii) The Hasse–Witt = Cartier–Manin matrix $A$ of $C$ has rank $g$.

(iii) The Newton polygon $\mathcal{N}(P)$ of the characteristic polynomial $P(U)$ has the shape illustrated below:

(iv) $J(p)$ is isogenous to a formal group of the form $J(p) \sim g(G_{1,0} + G_{0,1})$.

(v) The Dieudonné module $V_p(J(p)) = T_p(J(p)) \otimes \mathbb{F}$ is isomorphic to the module $V_p(J(p)) \cong \left( L[F]/L[F](F - p) \right)^g \oplus \left( L[F]/L[F](F - 1) \right)^g$.

When this holds true, we say that $J$ is ordinary.

Proof. (i) $\Rightarrow$ (ii). Put $t = (m - 1)(p - 1)/m$. Then $t \in \mathbb{Z}$ if and only if $p \equiv 1 \pmod{m}$. Now suppose that $f = 1$. So $t \in \mathbb{Z}$ and the Hasse–Witt = Cartier–Manin matrix $A$ of $C$ is given by a $(g \times g)$ diagonal matrix $A = (a_{ij})$, where

$$a_{11} = (-1)^{(p-1)/m} \left( t - (p - 1)/m \right), \quad a_{22} = (-1)^{(p-1)/m} \left( t - 2(p - 1)/m \right), \ldots,$$

$$a_{22} = (-1)^{(p-1)/m} \left( t - (m - 3)(p - 1)/m \right),$$
Here \( (\cdot) \) denotes the binomial coefficient. We see that \( a_{ii} \equiv 0 \pmod{p} \) for all \( i \). So \( \det A \equiv 0 \pmod{p} \). Hence \( A \) is nondegenerate and hence has rank \( g \).

(ii) \( \Rightarrow \) (iii). By Manin [7], we have

\[
P(U) \equiv (-1)^g U^g \mid A - \lambda I_g \mid \pmod{p},
\]

where \( I_g \) denotes the \((g \times g)\) identity matrix. Now (ii) asserts that the coefficient of \( U^g \) of \( P(U) \) is a \( p \)-adic unit. Hence \( A \) has the shape illustrated in Theorem (4.2(iii)).

(iii) \( \Rightarrow \) (iv). This follows immediately from Theorem 4.1 of Manin [6].

(iv) \( \Rightarrow \) (v). By the definition, \( G_{1,0} = G_m(p) \) (resp. \( G_{0,1} = (\mathbb{Q}_p/\mathbb{Z}_p) \)) where \( G_m(p) \) (resp. \( (\mathbb{Q}_p/\mathbb{Z}_p) \)) denotes the multiplicative \( p \)-divisible group of dimension 1 and of height 1 (resp. the étale \( p \)-divisible group of dimension 0 and of height 1). The corresponding Dieudonné module \( V_p(G_{1,0} + G_{0,1}) \) is isomorphic to

\[
\left( \frac{L[F]}{L[F](F - p)} \right) \oplus \left( \frac{L[F]}{L[F](F - 1)} \right).
\]

Hence it follows that the Dieudonné module \( V_p(J(p)) \) of \( J(p) \) is isomorphic to the module described in (v).

(v) \( \Rightarrow \) (i). \( P(U) \) is the characteristic polynomial of the representation of \( \pi \) \((=F^f = F)\) with respect to \( V_p(J(p)) \). Hence \( P(U) \) has \( g \) \( p \)-adic unit roots and the other \( g \) \( p \)-adic roots with order 1. This gives condition (iii) of Proposition (4.1) and hence (i).

The algebraic (global) structure of an ordinary Jacobian variety \( J \) of \( C \) up to isogeny can also be determined completely from its formal completion \( J(p) \).

(4.3) \textbf{Theorem.} With the notations as in Theorem (2.9), the following conditions are equivalent.

(i) \( J(p) \sim g(G_{1,0} + G_{0,1}) \).

(ii) \( J \) has \( p^g \) rational points of order \( p \) in \( k \).

(iii) At every prime \( v \) in \( \Phi \) over \( p \), the local invariant is given by

\[
\text{inv}_v(A) = 0 \quad \text{or} \quad 1 \equiv 0 \pmod{2}.
\]

\textbf{Proof.} (i) \( \iff \) (ii). By Satz 10 of Hasse and Witt [3] (see also Serre [9]), the number of the rational points of order \( p \) on \( J \) defined over \( k \) is equal to \( p^g \). Here \( \rho \) is the rank of the matrix \( AA^{(p)}A^{(p^2)} \cdots A^{(p^{g-1})} \), where \( A \) is the Hasse–Witt = Cartier–Manin matrix of \( C \) and \( A^{(p^h)} \) is the matrix with entries of \( p^h \)-power of those of \( A \). Now assume (i). Then by Theorem (4.2), \( A \) has rank \( g \), and hence so does the matrix \( AA^{(p)}A^{(p^2)} \cdots A^{(p^{g-1})} \). Conversely, if (ii) holds true, then \( J(p)_{et} \) (the étale part of \( J(p) \)) has height \( g \). Hence \( J(p) \) contains the factor \((\mathbb{Q}_p/\mathbb{Z}_p)^g \) and hence its dual \((G_m(p))^g \). Hence \( J(p) \sim g(G_{1,0} + G_{0,1}) \).
(i) ⇔ (iii). Assume (i). Then we see easily that there is no real prime in $\Phi$ and that

$$\text{ord}_p(\alpha) = 0 \quad \text{at half the places } v,$$

$$= 1 \quad \text{at the other half the places } v.$$

Hence we get assertion (iii). Conversely if (iii) holds true, then the characteristic polynomial $P(U)$ has $g$ $p$-adic roots with order 0 and also $g$ $p$-adic roots with order 1. Hence by Theorem (4.2) we obtain assertion (i).

(4.4) Example. There are no Fermat curves over finite fields of characteristic $p = 2$ whose Jacobian varieties are ordinary, because $2 \not\equiv 1 \pmod{m}$ for any $m \geq 3$.

(4.5) Example. Consider the Fermat curve $C : X^5 + Y^5 = 1$ over a field of characteristic $p = 11$. Since $11 \equiv 1 \pmod{5}$, 11 splits in $K_5 = \mathbb{Q}(e^{2\pi i/5})$, so that $f = 1$, i.e., $H = \{1\}$. $C$ has genus $g = 6$ and the set $\mathcal{U}_5$ has 12 vectors. Let us compute

$$A_H(a) = \left[ \sum_{i=1}^{2} \langle a_i/5 \rangle \right] \quad \text{for all } a \in \mathcal{U}_5.$$

We get

$$A_H(a) = 0 \quad \text{for 6 vectors } a \in \mathcal{U}_5,$$

$$A_H(a) = 1 \quad \text{for the other 6 vectors } a \in \mathcal{U}_5.$$

Hence $J(11)$ is isogenous to the formal group $6(G_{1,0} + G_{0,1})$ and $J$ is ordinary.

The Hasse–Witt = Cartier–Manin matrix $A$ of $C$ is given in modulo 11 by

$$A = \begin{pmatrix} 6 & 0 & 0 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 & 0 & 0 \\ 0 & 0 & 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 6 \end{pmatrix} \pmod{11}. $$

Hence $\det A = 9 \equiv 0 \pmod{11}$.

(4.6) Example. Consider the Fermat curve $C : X^9 + Y^9 = 1$ over a field of characteristic $p = 19$. Then $19 \equiv 1 \pmod{9}$, so that 19 splits completely in $K_9 = \mathbb{Q}(\zeta_9)$. $K_9$ has degree $\phi(9) = 6$ over $\mathbb{Q}$ with the Galois group $G \simeq \{1, 2, 4, 5, 7, 8\}$. $H = \{1\}$. $C$ has genus $g = 28$ and the set $\mathcal{U}_9$ consists of 56 vectors. Let us compute

$$A_H(a) = \left[ \sum_{i=1}^{9} \langle a_i/9 \rangle \right] \quad \text{for all } a \in \mathcal{U}_9.$$
We obtain the following results:

\[ A_H(a) = 0 \quad \text{for 28 vectors} \quad a \in \mathcal{H}_9 \]

\[ A_H(a) = 1 \quad \text{for the other 28 vectors} \quad a \in \mathcal{H}_9. \]

Hence \( J(19) \) is isogenous to the formal group \( 28(G_{1,0} + G_{0,1}) \) and \( J \) is an ordinary abelian variety.

Case 2

Now we are going to discuss the cases in which \( f \) is odd and \( f > 1 \).

Since \( |G| = \phi(m) = 2 \cdot N \) and since \( H = \{p^\mu \mod m | 0 \leq \mu < f\} \) with \( f > 1 \) odd, \( H \) has order at least 3.

(4.7) Theorem. With the notations as in Section 2, let \( p \) be the rational prime such that the decomposition degree \( f \) is odd and \( f > 1 \). For any rational integer \( 0 \leq c \leq \lfloor f/2 \rfloor \), let \( r_0 \) be the number of the vectors \( a \in \mathcal{H}_m \) such that \( A_H(a) = c \).

Then \( J(p) \) is isogenous to a formal group of the form

\[ J(p) \sim r_0(G_{1,0} + G_{0,1}) + \sum_{0 < c < \lfloor f/2 \rfloor} \frac{r_c}{f} (G_{c,1-c} + G_{f-c,c}). \]

In particular, \( J(p) \) contains no factor \( G_{1,1} \).

Proof. Since \( f/2 \notin \mathbb{Z} \), we see immediately from Lemma (2.5) that there exists no vector \( a \in \mathcal{H}_m \) such that \( A_H(a) = f/2 \). So \( G_{1,1} \) is not a component of \( J(p) \). Moreover, from Theorem (4.2), we can deduce that \( r_0 \neq 0 \) for at least one \( c \), where \( 0 < c < \lfloor f/2 \rfloor \). Hence \( J(p) \) has the isogeny type as described. \( \square \)

The algebraic (global) structure of the isogeny class of \( J \) is described in the following theorem.

(4.8) Theorem (cf. Tate [13]). Under the conditions of Theorem (4.7), suppose that \( P(U) = Q(U)^e \) with \( Q \) irreducible over \( \mathbb{Q} \). Then \( e \) coincides with the greatest common divisor of all the numerators of the local invariants \( \text{inv}_v(\mathcal{A}) \), and \( \mathcal{A} \) has index \( f/e \) and \( J \) becomes isogenous to the direct product of \( e \) copies of a \( k \)-simple abelian variety of dimension \( g/e \). In particular, if the numerators of \( \text{inv}_v(\mathcal{A}) \) are relatively prime, then \( J \) is \( k \)-simple.

Proof. Since there is no real prime in \( \Phi \), the numerators of the local invariants are paired off as \((c, f - c)\) for \( 0 \leq c < \lfloor f/2 \rfloor \). If \( f \) is a prime number, the greatest common divisor of all the numerators of \( \text{inv}_v(\mathcal{A}) \) is obviously equal to 1, while if \( f \) is a composite odd number, it is possible that the greatest common divisor of all the numerators of \( \text{inv}_v(\mathcal{A}) \) becomes greater than 1. In any event, by the theorem of Tate in [13], the greatest common divisor of all the numerators of
inv_v(\mathcal{A}) gives the period of \mathcal{A} in the Brauer group Br(\Phi) of \Phi, whence it coincides with e. Thus J becomes isogenous to e copies of a k-simple abelian variety, and in particular, if e = 1, J is k-simple.

(4.9) Example. Consider the Fermat curve \( C : X^7 + Y^7 = 1 \) over a field of characteristic \( p \in \{2, 3, 11\} \). \( K_7 = \mathbb{Q}(e^{2\pi i/7}) \) has degree \( \phi(7) = 6 \) over \( \mathbb{Q} \) and for each \( p, p^3 \equiv 1 \pmod{7} \). So \( f = 3 \). The Galois group \( G \) of \( K_7 \) is isomorphic to \{1, 2, 3, 4, 5, 6\} and its subgroup \( H \) is the set \{1, 2, 4\} and \( G \mod H = H_{t_1} + H_{t_2} \) with \( t_1 = 1 \) and \( t_2 = 3 \). \( C \) has genus \( g = 15 \) and the set \( \mathfrak{V}_7 \) consists of 30 vectors. Now we shall compute the value of

\[
A_H(a) = \sum_{i=1}^{3} \left[ \sum_{l=1}^{2} \left\langle \frac{lt_1}{7} \right\rangle \right]
\]

for every \( a \in \mathfrak{V}_7 \).

The results are the following:

- \( A_H(a) = 0 \) for 6 vectors \( a \in \mathfrak{V}_7 \),
- \( A_H(a) = 1 \) for 9 vectors \( a \in \mathfrak{V}_7 \),

and by applying Lemma (2.7),

\[
A_H(a) = 2 \quad \text{for 9 vectors of the form } 3a,
\]

where \( a \) moves all the vectors such that \( A_H(a) = 1 \), and finally

\[
A_H(a) = 3 \quad \text{for 6 vectors of the form } 3a,
\]

where \( a \) moves all the vectors such that \( A_H(a) = 0 \).

Hence the isogeny type of \( J(p) \) for \( p \in \{2, 3, 11\} \) is determined by applying Theorem (4.7): Indeed,

\[
J(p) \sim 6(G_{1,0} + G_{0,1}) + 3(G_{1,2} + G_{2,1}).
\]

Moreover, \( J \) is k-simple (\( k = GF(p^3) \)), by Theorem (4.8).

(4.10) Example. We consider the Fermat curve \( C : X^{23} + Y^{23} = 1 \) over a finite field of characteristic \( p \in \{2, 3, 13, 29, 31\} \). \( K_{23} = \mathbb{Q}(e^{2\pi i/23}) \) has degree \( \phi(23) = 22 \) over \( \mathbb{Q} \) and its Galois group \( G \) over \( \mathbb{Q} \) is isomorphic to \((\mathbb{Z}/23\mathbb{Z})^\times\). As \( p^{11} \equiv 1 \pmod{23} \) for each \( p \), we have \( f = 11 \). So \( H = \{p^\mu \mod{23} | 0 \leq \mu < 11\} = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\} \) and \( G = H_{t_1} + H_{t_2} \) with \( t_1 = 1 \) and \( t_2 = 5 \). \( C \) has genus \( g = 231 \) and the set \( \mathfrak{V}_{23} \) consists of 462 vectors. Let us compute the value of

\[
A_H(a) = \sum_{i=1}^{5} \left[ \sum_{l=1}^{2} \left\langle \frac{lt_1}{23} \right\rangle \right]
\]

for every \( a \in \mathfrak{V}_{23} \).
We obtain the following results:

\[ A_H(a) = 1 \quad \text{for 66 vectors} \quad a \in \mathbb{A}_{23}, \]
\[ A_H(a) = 4 \quad \text{for 165 vectors} \quad a \in \mathbb{A}_{23}, \]

and by applying Lemma (2.7),

\[ A_H(a) = 7 \quad \text{for 165 vectors of the form} \quad 5a, \]

where \( a \) moves all the vectors such that \( A_H(a) = 4 \), and finally

\[ A_H(a) = 10 \quad \text{for 66 vectors of the form} \quad 5a, \]

where \( a \) moves all the vectors such that \( A_H(a) = 1 \).

Hence \( J(p) \) for \( p \in \{2, 3, 13, 29, 31\} \) is isogenous to a formal group of the form

\[ J(p) \sim 6(G_{1.10} + G_{10.1}) + 15(G_{4.7} + G_{7.4}). \]

Moreover, as \( \text{GCD}(1, 4, 7, 10) = 1 \), by Theorem (4.8), \( J \) is a simple abelian variety over \( k = GF(p^{11}) \).

(4.11) PROPOSITION. With the notations as in Section 2, suppose that \( f \) is odd and that \( f > 1 \). Then the following conditions are equivalent.

(i) There exists a pair of rational integers \( 0 < c_1, c_2 < g \) such that \( c_1 < c_2 \), \((c_1, c_2) = 1, c_1 + c_2 = g \) and that

\[ A_H(a) = c_1 \quad \text{for} \quad g \text{ vectors} \quad a \in \mathbb{A}_m, \]
\[ c_2 \quad \text{for the other} \quad g \text{ vectors} \quad a \in \mathbb{A}_m. \]

(ii) The characteristic polynomial \( P(U) \) has the \( p \)-adic factorization

\[ P(U) = \prod_{i=1}^{g} (U - p^{c_1}x_i) \prod_{i=1}^{g} (U - p^{c_2}y_i) \]

in \( \overline{\mathbb{Z}}_p[U] \), where \( c_1, c_2 \) are as in (i) and \( x_i, y_i \) are \( p \)-adic units.

(iii) \( J(p) \) is isogenous to the symmetric formal group of dimension \( g \):

\[ J(p) \sim G_{c_1, c_2} + G_{c_2, c_1}, \quad (c_1, c_2) = 1, c_1 + c_2 = g. \]

(iv) The Dieudonné module \( V_p(J(p)) = T_p(J(p)) \otimes_{\mathbb{Z}} \mathbb{L} \) is isomorphic to the module

\[ V_p(J(p)) \cong \left( \frac{\mathbb{L}[F]}{\mathbb{L}[F](F^a - p^{c_1})} \right) \otimes \left( \frac{\mathbb{L}[F]}{\mathbb{L}[F](F^a - p^{c_2})} \right). \]
(v) There exists the imaginary quadratic subfield in $\Phi$, where $(p) = p_1p_2$, in which $(p_1, p_2) = 1$ and $p_i$ are complex conjugates of each other. The ideal $(j(a))$ is primitive and

$$(j(a)) = p_1^{c_1}p_2^{c_2} \quad \text{or} \quad p_1^{c_1}p_2^{c_2}.$$ 

When one of the above conditions holds true, $J$ is $k$-simple.

Proof. We shall show (i) $\Rightarrow$ (ii) $\iff$ (iii) $\Rightarrow$ (iv) $\Rightarrow$ (v) $\Rightarrow$ (i).

(i) $\Rightarrow$ (ii). See the proof of Theorem (2.8).

(ii) $\Rightarrow$ (iii). This is Theorem 4.1' of Manin [6].

(iii) $\iff$ (iv). By the definition of the symmetric formal group of dimension $g$ (see Manin [6]), the corresponding Dieudonné module $V_p(J(p))$ is isomorphic to the module described in (iv) and vice versa.

(iv) $\Rightarrow$ (v) (cf. Honda [5]). Since the Frobenius morphism $F$ and the Verschliebung morphism $V$ have the $p$-adic orders $v(F) = c_1, v(V) = c_2$ (or $v(F) = c_2$ and $v(V) = c_1$), there are two imaginary primes $p_1, p_2$ over $p$ in $\Phi$ such that $(p_1, p_2) = 1$ and that $(p) = p_1p_2$. So the Frobenius endomorphism $\pi = F^g = F^g$ has the $p$-adic order $v(\pi) = c_1$ and its $p$-adic dual $g/\pi = p^g/\pi$ has $v(g/\pi) = c_2$ (or $v(\pi) = c_2$ and $v(q/\pi) = c_1$.) As seen in Section 2, the Jacobi sum $j(a)$ is a Weil number of order $f = g$; we obtain the prime ideal decomposition for $(j(a))$ as (v).

(v) $\Rightarrow$ (i). There are two prime ideals in $\Phi$ over $p$ such that $(p) = p_1p_2$. So we have $r = 2$ and $f = \phi(m)/2$. The group $H = \{ p^\mu \mod m \mid 0 \leq \mu < f \}$ has order $\phi(m)/2$. The fixed field of $H$ is of degree 2 over $\mathbb{Q}$ and it is imaginary. (Because, if it is real, there are real primes in $\Phi$ over $p$. But this is impossible, since $f/2 \notin \mathbb{Z}$.) Hence $G \mod H = H_1 + H_2$ and by Lemma (2.6),

$$(j(a)) = p_1^{A_H(a)}p_2^{A_H(a)},$$

which implies that

$$A_H(a) = c_1 \quad \text{for } g \text{ vectors } a \in \mathfrak{U}_m,$$

$$= c_2 \quad \text{for the other } g \text{ vectors } a \in \mathfrak{U}_m.$$ 

The last assertion follows from Theorem 4.1' of Manin [6].

(4.12) Remark. In Proposition (4.11)(i), if $(c_1, c_2) = d > 1$, replace $g$ by $g/d$, and $c_i$ by $c_i/d$ for $i = 1, 2$, while (ii), (iii), (iv), and (v) are, respectively, replaced by

(ii') $P(U) = \left( \prod_{i=1}^{g/d} (U - p^{c_i/d}x_i) \cdot \prod_{i=1}^{g/d} (U - p^{c_2/d}y_i) \right)^d$.

(iii') $J(p) \sim d(G_{c_1/d, c_2/d} + G_{c_2/d, c_1/d})$. 

(iv) \( V_d(J(p)) \cong \left( \frac{L[F]}{L[F](F^{g/d} - p^{e_1/d})^d} \right)^\oplus \left( \frac{L[F]}{L[F](F^{g/d} - p^{e_2/d})^d} \right). \)

(v') \( p_1 \) and \( p_2 \) are as in (v); the Jacobi sum has the prime ideal decomposition

\[ (j(a)) = (j(a'))^d, \]

where

\[ (j(a')) = p_1^{e_1/d}p_2^{e_2/d} \quad \text{or} \quad p_1^{e_2/d}p_2^{e_1/d}. \]

When one of these assertions holds true, then \( J \) is isogenous to \( d \) copies of a \( k \)-simple abelian variety of dimension \( g/d \) whose Jacobian variety has the symmetric formal group of dimension \( g/d \).

\[ (4.13) \text{ THEOREM. There exists no Fermat curve} \ C \text{ over a finite field of characteristic} \ p \text{ whose Jacobian variety} \ J \text{ has the} \ p \text{-divisible group} \ J(p) \text{ of the symmetric formal group of dimension} \ g. \]

Proof. By Proposition (4.12), for \( J(p) \) to be isogenous to \( G_{c,g-c} + G_{g-c,c} \), \((c, g - c) = 1\), we must have \( r = 2 \) and \( f = g \). But \( f = \phi(m)/2 \), and we always have the inequality

\[ (m - 1)(m - 2) = 2g > m > \phi(m) \quad \text{for any} \quad m \geq 3. \]

This implies that there exists no Fermat curve whose Jacobian has the symmetric formal group of dimension \( g \).

5. THE ISOGENY TYPE OF \( J(p) \) FOR ALL \( p \geq 2 \) (WITH \( 3 \leq m \leq 25 \))

In this section, we carry out the computations\(^1\) and determine for every \( p \) the isogeny type of the \( p \)-divisible group \( J(p) \) of the Jacobian variety \( J \) of the Fermat curve \( C: \ X^m + Y^m = 1, \ m \geq 3, \) defined over finite fields of characteristic \( p \). We move \( m \) in the range \( 3 \leq m \leq 25 \).

Summarizing the points resulting from the computations and applying the theories developed in the previous sections, we obtain with the previous notations in force the following theorem.

\(^1\) All the numerical results and the tables collecting the computational results are not included here, but are available on microfilm from the University of Ottawa, the Vanier Library.
(5.1) Theorem. Let $C : X^m + Y^m = 1$, $m \geq 3$, be the Fermat curve defined over a finite field $k = \text{GF}(p^f)$, where $p$ is a rational prime such that $(p, m) = 1$ and $f$ is the smallest integer satisfying $p^f = 1 \pmod{m}$. Then we have the following assertions.

(a) For $m = 3$, $J$ is ordinary $\iff p \equiv 1 \pmod{3}$, and $J$ is supersingular $\iff p \equiv 1 \pmod{3}$.

(b) For $m = 4$, $J$ is ordinary $\iff p \equiv 1 \pmod{4}$, and $J$ is supersingular $\iff p \equiv 1 \pmod{4}$.

(c) For $m = 5$, $J$ is ordinary $\iff p \equiv 1 \pmod{5}$, and $J$ is supersingular $\iff p \equiv 1 \pmod{5}$.

(d) For $m = 6$, $J$ is ordinary $\iff p \equiv 1 \pmod{6}$, and $J$ is supersingular $\iff p \equiv 1 \pmod{6}$.

(e) For $m = 7$, $J$ is ordinary $\iff p \equiv 1 \pmod{7}$, and $J$ is supersingular $\iff p \equiv 3, 5, 6 \pmod{7}$. For $p = 2, 4 \pmod{7}$, $f = 3$ and $J(p) \sim r_0(G_{1,0} + G_{0,1}) + \left( \frac{r_1}{3} \right) (G_{1,2} + G_{2,1})$ with $r_0 + r_1 = 15$.

(f) For $m = 8$, $J$ is ordinary $\iff p \equiv 1 \pmod{8}$, and $J$ is supersingular $\iff p \equiv 2, 5, 8 \pmod{8}$. For $p = 3, 5 \pmod{8}$, $f = 2$ and $J(p) \sim r_0(G_{1,0} + G_{0,1}) + \frac{1}{2} r_1 G_{1,1}$ with $r_0 + \frac{1}{2} r_1 = 21$.

(g) For $m = 9$, $J$ is ordinary $\iff p \equiv 1 \pmod{9}$, $J$ is supersingular $\iff p \equiv 2, 5, 8 \pmod{9}$. For $p = 4, 7 \pmod{9}$, $f = 3$ and $J(p) \sim r_0(G_{1,0} + G_{0,1}) + \left( \frac{r_1}{3} \right) (G_{1,2} + G_{2,1}) + \left( \frac{r_2}{5} \right) (G_{2,2} + G_{3,2})$ with $r_0 + r_1 + r_2 = 45$.

(h) For $m = 10$, $J$ is ordinary $\iff p \equiv 1 \pmod{10}$, and $J$ is supersingular $\iff p \equiv 1 \pmod{10}$.

(i) For $m = 11$, $J$ is ordinary $\iff p \equiv 1 \pmod{11}$, $J$ is supersingular $\iff p \equiv 2, 6, 7, 8, 10 \pmod{11}$. For $p = 3, 4, 5, 9 \pmod{11}$, $f = 5$ and $J(p) \sim r_0(G_{1,0} + G_{0,1}) + \left( \frac{r_1}{5} \right) (G_{1,4} + G_{4,1}) + \left( \frac{r_2}{5} \right) (G_{2,3} + G_{3,2})$ with $r_0 + r_1 + r_2 = 55$.

(j) For $m = 12$, $J$ is ordinary $\iff p \equiv 1 \pmod{12}$, and $J$ is supersingular $\iff p \equiv 11 \pmod{12}$. For $p = 5, 7 \pmod{12}$, $f = 2$ and $J(p) \sim r_0(G_{1,0} + G_{0,1}) + \frac{1}{2} r_1 G_{1,1}$ with $r_0 + \frac{1}{2} r_1 = 28$.

(k) For $m = 13$, $J$ is ordinary $\iff p \equiv 1 \pmod{13}$, and $J$ is supersingular $\iff p \equiv 1, 3, 9 \pmod{13}$. For $p = 3, 9 \pmod{13}$, $f = 3$ and $J(p) \sim r_0(G_{1,0} + G_{0,1}) + \left( \frac{r_1}{3} \right) (G_{1,2} + G_{2,1})$ with $r_0 + r_1 = 66$.

(l) For $m = 14$, $J$ is ordinary $\iff p \equiv 1 \pmod{14}$, and $J$ is supersingular $\iff p = 3, 5, 13 \pmod{14}$. For $p = 9, 11 \pmod{14}$, $f = 3$ and $J(p) \sim r_0(G_{1,0} + G_{0,1}) + \left( \frac{r_1}{3} \right) (G_{1,2} + G_{2,1})$ with $r_0 + r_1 = 78$.

(m) For $m = 15$, $J$ is ordinary $\iff p \equiv 1 \pmod{15}$, and $J$ is supersingular $\iff p = 7, 14 \pmod{15}$. For $p = 2, 8, 13 \pmod{15}$, $f = 4$ and $J(p) \sim$
For $m = 16$, $J$ is ordinary $\iff p \equiv 1 \pmod{16}$, and $J$ is supersingular $\iff p \equiv 15 \pmod{16}$. For $p = 3, 5, 11, 13 \pmod{16}$, $f = 4$ and $J(p) \sim r_0(G_{1,0} + G_{0,1}) + (r_1/4)(G_{1,3} + G_{3,1}) + \frac{1}{2}r_2G_{1,1}$ with $r_0 + r_1 + \frac{1}{2}r_2 = 105$. For $p \equiv 7, 9 \pmod{16}$, $f = 2$ and $J(p) \sim r_0(G_{1,0} + G_{0,1}) + \frac{1}{2}r_1G_{1,1}$ with $r_0 + \frac{1}{2}r_1 = 105$.

For $m = 17$, $J$ is ordinary $\iff p \equiv 1 \pmod{17}$, and $J$ is supersingular $\iff p \equiv 16 \pmod{17}$. For $p = 2, 3, 5, 8, 10, 12, 13, 14, 15, 17 \pmod{18}$, $f = 9$ and $J(p) \sim r_0(G_{1,0} + G_{0,1}) + \sum_e (r_e/9)(G_{e,9-e} + G_{9-e,e})$ with $r_0 + \sum_e r_e = 153$. For $p = 7, 11 \pmod{19}$, $f = 3$ and $J(p) \sim r_0(G_{1,0} + G_{0,1}) + (r_1/3)(G_{1,2} + G_{2,1})$ with $r_0 + r_1 = 153$.

For $m = 18$, $J$ is ordinary $\iff p \equiv 1 \pmod{18}$, and $J$ is supersingular $\iff p \equiv 17 \pmod{18}$. For $p = 3, 7 \pmod{19}$, $f = 4$ and $J(p) \sim r_0(G_{1,0} + G_{0,1}) + (r_1/4)(G_{1,3} + G_{3,1}) + \frac{1}{2}r_2G_{1,1}$ with $r_0 + r_1 + \frac{1}{2}r_2 = 171$. For $p = 9, 11 \pmod{20}$, $f = 2$ and $J(p) \sim r_0(G_{1,0} + G_{0,1}) + \frac{1}{2}r_1G_{1,1}$ with $r_0 + \frac{1}{2}r_1 = 171$.

For $m = 19$, $J$ is ordinary $\iff p \equiv 1 \pmod{19}$, and $J$ is supersingular $\iff p \equiv 18 \pmod{19}$. For $p = 2, 3, 5, 9, 15 \pmod{20}$, $f = 5$ and $J(p) \sim r_0(G_{1,0} + G_{0,1}) + (r_1/5)(G_{1,4} + G_{4,1}) + (r_2/5)(G_{2,3} + G_{3,2})$ with $r_0 + r_1 + r_2 = 210$.

For $m = 20$, $J$ is ordinary $\iff p \equiv 1 \pmod{21}$, and $J$ is supersingular $\iff p \equiv 20 \pmod{21}$. For $p = 2, 10, 11, 19 \pmod{20}$, $f = 6$ and $J(p) \sim r_0(G_{1,0} + G_{0,1}) + \sum_e (r_e/6)(G_{e,6-e} + G_{6-e,e}) + \frac{1}{2}r_3G_{1,1}$ with $r_0 + \sum_e r_e + \frac{1}{2}r_3 = 190$. For $p = 4, 16 \pmod{21}$, $f = 3$ and $J(p) \sim r_0(G_{1,0} + G_{0,1}) + (r_1/3)(G_{1,2} + G_{2,1})$ with $r_0 + r_1 = 190$. For $p = 8, 13 \pmod{22}$, $f = 2$ and $J(p) \sim r_0(G_{1,0} + G_{0,1}) + \frac{1}{2}r_1G_{1,1}$ with $r_0 + \frac{1}{2}r_1 = 190$.

For $m = 21$, $J$ is ordinary $\iff p \equiv 1 \pmod{22}$, and $J$ is supersingular $\iff p \equiv 21 \pmod{22}$. For $p = 2, 10, 11, 19 \pmod{20}$, $f = 6$ and $J(p) \sim r_0(G_{1,0} + G_{0,1}) + \sum_e (r_e/6)(G_{e,6-e} + G_{6-e,e}) + \frac{1}{2}r_3G_{1,1}$ with $r_0 + \sum_e r_e + \frac{1}{2}r_3 = 190$. For $p = 4, 16 \pmod{21}$, $f = 3$ and $J(p) \sim r_0(G_{1,0} + G_{0,1}) + (r_1/3)(G_{1,2} + G_{2,1})$ with $r_0 + r_1 = 190$. For $p = 8, 13 \pmod{22}$, $f = 2$ and $J(p) \sim r_0(G_{1,0} + G_{0,1}) + \frac{1}{2}r_1G_{1,1}$ with $r_0 + \frac{1}{2}r_1 = 190$.

For $m = 22$, $J$ is ordinary $\iff p \equiv 1 \pmod{23}$, and $J$ is supersingular $\iff p \equiv 22 \pmod{23}$. For $p = 2, 3, 4, 6, 9, 12, 13, 16, 18 \pmod{23}$, $f = 11$ and $J(p) \sim r_0(G_{1,0} + G_{0,1}) + \sum_e (r_e/11)(G_{e,11-e} + G_{11-e,e})$ with $r_0 + \sum_e r_e = 231$.

For $m = 23$, $J$ is ordinary $\iff p \equiv 1 \pmod{24}$, and $J$ is supersingular $\iff p \equiv 23 \pmod{24}$. For $p = 2, 3, 4, 6, 9, 12, 13, 16, 18 \pmod{23}$, $f = 11$ and $J(p) \sim r_0(G_{1,0} + G_{0,1}) + \sum_e (r_e/11)(G_{e,11-e} + G_{11-e,e})$ with $r_0 + \sum_e r_e = 231$.

For $m = 24$, $J$ is ordinary $\iff p \equiv 1 \pmod{24}$, and $J$ is supersingular $\iff p \equiv 23 \pmod{24}$. For $p = 2, 3, 4, 6, 9, 12, 13, 16, 18 \pmod{23}$, $f = 11$ and $J(p) \sim r_0(G_{1,0} + G_{0,1}) + \frac{1}{2}r_1G_{1,1}$ with $r_0 + \frac{1}{2}r_1 = 253$. 

Subtracting $NORIKO YUI$ from the image.
For $m = 25$, $J$ is ordinary $\iff p \equiv 1 \pmod{25}$, and $J$ is supersingular $\iff p \not\equiv 1 \pmod{6, 11, 16, 21} \pmod{25}$. For $p = 6, 11, 16, 21 \pmod{25}$, $f = 5$ and $J(p) \sim r_0(G_{1,0} + G_{0,1}) + (r_1/5)(G_{1,4} + G_{4,1}) + (r_2/5)(G_{2,3} + G_{3,2})$ with $r_0 + r_1 + r_2 = 276$.

(5.2) Observation. Let $C : X^m + Y^m = 1$ be the Fermat curve defined over a finite field of characteristic $p > 0$ and let $J(p)$ be the $p$-divisible group of the Jacobian variety $J$ of $C$. We consider the set of Fermat curves with supersingular Jacobian varieties:

$$\{X^m + Y^m = 1 \text{ over } GF(p^f)(p^f \equiv 1 \pmod{m}) | J(p) \sim gG_{1,1}\}.$$

Then the numerical examples of Theorem (5.1) seem to indicate that this set has density greater than or equal to $\frac{1}{2}$ in the set of all Fermat curves over finite fields.

$$\lim_{p \to \infty \atop m \to \infty} \frac{\{X^m + Y^m = 1 \text{ over } GF(p^f)(p^f \equiv 1 \pmod{m}) | J(p) \sim gG_{1,1}\}}{\{X^m + Y^m = 1 \text{ over } GF(p^f)(p^f \equiv 1 \pmod{m})\}} \geq \frac{1}{2}.$$ 

6. Applications and Problems

In this section, we shall consider the algebraic curve $C_0$ of genus $g_0$ defined by the equation

$$C_0 : Y^e = \gamma X^s + 1, \quad 2 \leq e \leq s, \quad \gamma = \pm 1,$$

over a field of characteristic prime to $e \cdot s$. Such a curve is dominated by a Fermat curve

$$C : X^m + Y^m = 1, \quad m = \text{LCM}(e, s),$$
as there exists a dominant rational map $f_0 : C \to C_0$. In fact, put $Z = Y^{s'}$ with $s' = m/s$ and $\delta = \pm 1$ and $Z = Y^{e'}$ with $e' = m/e$. Then $C$ gives rise to the curve

$$(\delta U)^s + Z^e = 1.$$

By changing the variables, we obtain the algebraic curve $C_0$.

It is easy to see that the genus $g_0$ of $C_0$ is a divisor of the genus $g$ of $C$.

We shall investigate the relationships of the $p$-divisible groups arising from $C_0$ and $C$.

(6.1) Theorem. Let $C : X^m + Y^m = 1$, $m \geq 3$, be the Fermat curve of genus $g$ defined over a finite field $k = GF(p^f)$ of characteristic $p$, where $(p, m) = 1$ and $f$ is the smallest integer satisfying $p^f \equiv 1 \pmod{m}$. Let $C_0$ be the algebraic curve over $k = GF(p^f)$ defined by the equation

$$C_0 : Y^e = \gamma X^s + 1 \quad (\gamma = \pm 1)$$
with \((p, e \cdot s) = 1, LCM(e, s) = m\). We denote by \(J\) (resp. \(J_0\)) the Jacobian variety of \(C\) (resp. \(C_0\)) defined over \(k\) and by \(J(p)\) (resp. \(J_0(p)\)) the \(p\)-divisible group of \(J\) (resp. \(J_0\)). Then \(J_0(p)\) inherits the structure of \(J(p)\), up to isogeny, in the following cases:

(a) \(2 | f\) and \(p^{f/2} + 1 \equiv 0 \pmod{m}\), i.e., \(J\) is supersingular.

(b) \(f = 1\), i.e. \(J\) is ordinary.

(c) \(f\) is odd and \(f > 1\) and \(J(p) \sim d(G_{e,f-c} + G_{f-c,e})\) with \(d > 1\), \((e, f-c) = 1\) and \(d \cdot f = g\).

Proof. As remarked above, there is a rational map

\[
\begin{array}{ccc}
C & \longrightarrow & C_0 \\
(X, Y) & \longrightarrow & (X^{m/e}, Y^{m/e}).
\end{array}
\]

We see easily that this map \(f_0\) is onto. The function field \(k(X, Y)\) of \(C\) contains the function field \(k(X^{m/e}, Y^{m/e})\) of \(C_0\) as a subfield and

\[
\deg f_0 = [k(X, Y) : k(X^{m/e}, Y^{m/e})].
\]

This map \(f_0\) induces a homomorphism \(f_0^*\) of the Jacobian varieties and we get the commutative diagram

\[
\begin{array}{ccc}
J_0 & \xrightarrow{f_0^*} & J \\
\downarrow \pi & & \downarrow \pi \\
J_0 & \xrightarrow{f_0^*} & J
\end{array}
\]

where \(\pi\) denotes the Frobenius endomorphism of \(J_0\) and \(J\) relative to \(k\). Hence the roots of the characteristic polynomial \(P_0(U) = 0\) of \(J_0\) occur among the roots of the characteristic polynomial \(P(U) = 0\) of \(J\). Now we know the characteristic polynomial \(P(U)\) of \(J\) explicitly in cases (a), (b), and (c), namely,

\[
P(U) = \prod_{i=1}^{2g} (U - \tau_i) \quad \text{in case (a)},
\]

\[
P(U) = \prod_{i=1}^{g} (U - \tau_i)(U - q/\tau_i) \quad \text{in case (b)},
\]

\[
\left[ \prod_{i=1}^{g/d} (U - \tau_i)(U - q/\tau_i) \right]^d \quad \text{in case (c)}.
\]
As \( P_0(U) \), always together with a root \( \tau \), has the root \( q/\tau \), the assertion follows from Theorems (3.2) and (4.2) and Remark (4.12).

(6.2) Example (cf. Honda [4]). Consider the hyperelliptic curve \( C_0 \) defined by the equation

\[
C_0 : Y^2 = 1 - X^l, \quad l \text{ odd prime},
\]

over a finite field \( k \) of characteristic \( p > 2 \) and \( p \neq l \). \( C_0 \) has genus \( g_0 = (l - 1)/2 \).

We take \( k \) to be the finite field \( GF(p^l) \), where \( pl \) is the least power of \( p \) such that \( p^l \equiv 1 \pmod{l} \). Now there exists a Fermat curve \( C \) over \( k \) which dominates \( C_0 \).

For example, take the Fermat curve

\[
C : X^{2l} + Y^{2l} = 1 \quad \text{over} \quad k = GF(p^l).
\]

\( C \) has genus \( g = (2l - 1)(2l - 2)/2 = (4l - 2)g_0 \).

Let \( K_{2l} = \mathbb{Q}(\zeta_{2l}) \) be the 2lth cyclotomic field of degree \( \phi(2l) \) over \( \mathbb{Q} \). As \( p > 2 \), it follows that \( p^l \equiv 1 \pmod{2l} \), if and only if \( p^l \equiv 1 \pmod{l} \).

If \( 2 \mid f \) and \( p^l/2 + 1 \equiv 0 \pmod{2l} \) (so \( p^{l/2} + 1 \equiv 0 \pmod{l} \)), then \( J_0(p) \sim gG_{1,1} \) by Theorem (3.6) and \( J_0(p) \sim g_0G_{1,1} \) by Theorem 1 of Honda [4]. So \( J_0(p) \) inherits the structure of \( J_0(p) \).

If \( f \) is even, then by Theorem 2 of Honda [4], we can deduce that \( J_0(p) \) has the isogeny type

\[
J_0(p) \sim r_0(G_{1,0} + G_{0,1}) + \sum_{0 < c < \lfloor f/2 \rfloor} r_c (G_{c,f-c} + G_{f-c,c})
\]

with

\[
r_0 + \sum_{0 < c < \lfloor f/2 \rfloor} r_c = g_0.
\]

In particular, if \( f = 1 \), then \( J_0(p) \sim g_0(G_{1,0} + G_{0,1}) \), while \( J(p) \sim g(G_{1,0} + G_{0,1}) \) by Theorem (4.2). So \( J_0(p) \) inherits the structure of \( J(p) \) in this case also. If \( f \) is odd and \( f > 1 \) and if \( J(p) \) is isogenous to \( d > 1 \) copies of the symmetric formal group of dimension \( f \) (with \( f \cdot d = g \)), then again by Honda's theorem 2 in [4] and by Theorem (6.1), \( J_0(p) \) inherits the structure of \( J(p) \).

(6.3) Remark. The restrictions on \( f \) imposed in Theorem (6.1) are rather crucial ones. Consider the hyperelliptic curves

\[
C_0 : Y^2 = 1 \pm X^7
\]

over a finite field of characteristic \( p \in \{11, 23\} \). \( C_0 \) has genus \( g_0 = 3 \). We can deduce from Example (6.3) in Yui [18] and also from the main theorem in Yui.
that the isogeny class of the $p$-divisible group $J_0(p)$ of the Jacobian variety $J_0$ of $C_0$ is of the form

$$J_0(p) \sim (G_{1,2} + G_{2,1}).$$

Now we can find a Fermat curve $C$, over a finite field of characteristic $p \in \{11, 23\}$, which dominates $C_0$. For example, take the Fermat curve

$$C : X^{14} + Y^{14} = 1.$$  

$C$ has genus $g = 78$. We have $p^3 \equiv 1 \pmod{14}$ for both $p = 11$ and $23$. So $f = 3$. We consider $C$ over $k = GF(p^3)$. By applying Theorems (2.8) and (4.7), we can determine the isogeny type of $J(p)$. In fact, we get

$$J(p) \sim 6(G_{1,0} + G_{0,1}) + 24(G_{1,2} + G_{2,1}).$$

This example shows that $J_0(p)$ does not inherit the isogeny type of $J(p)$, even if $C$ dominates $C_0$, if we ease the restrictions imposed in Theorem (6.1).

(6.4) Observation. Let $l$ be an odd prime. We consider the Fermat curves

$$C' : X^l + Y^l = 1 \quad \text{of genus } g_0 = (l - 1)(l - 2)/2,$$

$$C : X^{2l} + Y^{2l} = 1 \quad \text{of genus } g = (2l - 1)(2l - 2)/2$$

over a finite field $k = GF(p^l)$ of characteristic $p > 2$ and $p \neq l$. We take $f$ to be the smallest integer satisfying $p^f \equiv 1 \pmod{2l}$ ($\not\equiv p^f \equiv 1 \pmod{l}$). Let $J'(p)$ (resp. $J(p)$) denote the $p$-divisible group arising from $C'$ (resp. $C$). The relationship between the isogeny classes of $J'(p)$ and $J(p)$ are illuminated from Theorem 5.1. First of all, we can see easily that if $f = 1$, or $[2 | f$ and $p^{f/2} + 1 \equiv 0 \pmod{2l}]$, then $J'(p)$ inherits the isogeny type of $J(p)$. In other cases, it is plausible that there exist some kinds of relations between the structures of the isogeny classes of $J'(p)$ and $J(p)$ as the following illustrations suggest.

(a) $p = 3, l = 11, \text{so } 2l = 22$. Then $f = 5$ and

$$J'(3) \sim 3(G_{1,4} + G_{4,1}) + 6(G_{2,3} + G_{3,2}),$$

while

$$J(3) \sim 30(G_{1,0} + G_{0,1}) + 18(G_{1,4} + G_{4,1}) + 18(G_{2,3} + G_{3,2}).$$

(b) $p = 11, l = 7, \text{so } 2l = 14$. Then $f = 3$ and

$$J'(11) \sim 6(G_{1,0} + G_{0,1}) + 3(G_{1,2} + G_{2,1}),$$

while

$$J(11) \sim 6(G_{1,0} + G_{0,1}) + 24(G_{1,2} + G_{2,1}).$$
(6.5) Observation. Let $C_0$ be the hyperelliptic curve

$$C_0 : Y^2 = 1 - X^{29}$$

of genus $g_0 = 14$

defined over a finite field $k$ of characteristic $p = 7$. $7^7 = 1 \pmod{29}$, and we may take $k = GF(7^7)$. Honda [4] has determined the isogeny type of the 7-divisible group $J_0(7)$ arising from $C_0$:

$$J_0(7) \sim (G_{2,5} + G_{5,2}) + (G_{3,4} + G_{4,3}),$$

and moreover, as $(2, 3, 4, 5) = 1$, the Jacobian variety $J_0$ of $C_0$ is $k$-simple.

Now we shall consider the Fermat curve

$$C : X^{29} + Y^{29} = 1$$

of genus $g = 378$

over $k = GF(7^7)$. The 29th cyclotomic field $K_{29} = \mathbb{Q}(\zeta_{29})$ has degree $\phi(29) = 28$ over $\mathbb{Q}$ and the Galois group $G$ of $K_{29}$ is isomorphic to $(\mathbb{Z}/29\mathbb{Z})^\times$. The decomposition degree of 7 is $f = 7$. So we get the subgroup $H = \{1, 7, 16, 20, 23, 24, 25\}$. We compute

$$A_H(a) = \sum_{t \in H} \left( \frac{t a_i}{29} \right)$$

for all $a \in \mathbb{F}_{29}$.

We get

$$A_H(a) = 2 \quad \text{for 105 vectors} \quad a \in \mathbb{F}_{29},$$

$$A_H(a) = 3 \quad \text{for 273 vectors} \quad a \in \mathbb{F}_{29},$$

$$A_H(a) = 4 \quad \text{for 273 vectors} \quad a \in \mathbb{F}_{29},$$

$$A_H(a) = 5 \quad \text{for 105 vectors} \quad a \in \mathbb{F}_{29}.$$

Hence by Theorem (2.8), we get

$$J(7) \sim 15(G_{2,5} + G_{5,2}) + 39(G_{3,4} + G_{4,3}).$$

Again, since $(2, 3, 4, 5) = 1$, the Jacobian variety $J$ of $C$ is $k$-simple.

(6.6) Problems. There remain some problems and generalizations of the results we have obtained above. We formulate some of them here.

(1) Generalize the method of this paper to determine the structure of the isogeny class of the $p$-divisible groups arising from more general type of algebraic curves over fields of finite characteristic.
(2) Investigate the possibilities to define and then to determine the $p$-divisible (formal) groups associated to the hypersurfaces (Fermat varieties)

$$X_0^m + X_1^m + \cdots + X_r^m = 0$$

over fields of finite characteristic. For $r = 3$, see Yui [21].

(3) Once (b) is settled, consider the hypersurfaces

$$a_0X_0^m + a_1X_1^m + \cdots + a_rX_r^m = 0$$

defined over fields of finite characteristic. Study the $p$-divisible groups arising from them and investigate the relations with Fermat varieties.

ACKNOWLEDGMENTS

This paper has grown out of correspondence and conversations with Professor T. Shioda. I thank him heartily for his suggestions and encouraging criticism. I am also indebted to Professor S. Takahashi (Montreal) for his assistance in machine computation and to Professor J. Dieudonné for reading through the earlier version and for his advice on the presentation of this article.

REFERENCES


