Supersingularity of Motives with Complex Multiplication and a Twisted Polarization

ASVIN G*†

Let \( X \) be a smooth, projective variety over a finite field \( \mathbb{F}_q \). We say that its crystalline cohomology \( H^i_{\text{cris}}(X)/W(\mathbb{F}_q) \) is supersingular if all the eigenvalues for the action of the Frobenius \( \sigma_q \) on it are of the form \( q^{i/2} \zeta \) for \( \zeta \) a root of unity. In this note, we prove a criteria for supersingularity when the variety has a large automorphism group and a perfect bilinear pairing. This criteria unifies and extends many known results on the supersingularity of curves and varieties and in particular, applies to a large family of Artin-Schreier curves.

1 introduction

Informally, a smooth projective variety \( X/\mathbb{F}_q \) is said to be supersingular if for each \( i \), the Newton slopes of the motive \( H^i(X) \) are all equal to \( i/2 \). There are many (equivalent) ways of making this definition precise and in the case of Abelian varieties (and K3 surfaces), it is a well studied notion. For the purposes of this article, we will use the slightly non standard definition:

**Definition 1.** A smooth, projective variety \( X/\mathbb{F}_q \) is said to be supersingular in degree \( i \) if the eigenvalues of the Frobenius \( \sigma_q \) on the crystalline cohomology \( H^i_{\text{cris}}(X)/W(\mathbb{F}_q) \) are of the form \( q^{i/2} \zeta \) for \( \zeta \) a root of unity. We say \( X \) is supersingular if it is supersingular in every degree \( i \).

In this paper, we consider varieties \( X \) with a large automorphism group \( G \) so that \( H^i_{\text{ét}}(X, \mathbb{Q}_\ell) \) is a quotient of \( \mathbb{Q}_\ell[G] \) as \( G \) modules compatible with the Frobenius action ("complex multiplication") and an equivariant inner product

\[
H^i_{\text{ét}}(X, \mathbb{Q}_\ell) \otimes H^i_{\text{ét}}(X, \mathbb{Q}_\ell) \to \mathbb{Q}_\ell(-d).
\]

**Theorem 1.** If \( H^i_{\text{ét}}(X, \mathbb{Q}_\ell) \) is self-dual, i.e., for any character \( \chi \) of \( G \), the \( \chi^{-1} \)-isotypic eigenspace of \( H^i_{\text{ét}}(X, \mathbb{Q}_\ell) \) is in the Frobenius orbit of the \( \chi \)-isotypic eigenspace, then \( X \) is supersingular in degree \( i \). The converse is also true if \( d = 1 \).

The proof is elementary and it generalizes and unifies many old results proven by disparate methods. Some examples of this theorem are as follows. In each case \( n \) is a positive integer co-prime to the characteristic \( p \). An interesting feature of the proof is that while supersingularity is invariant under extending the base field, our necessity criterion is not. Therefore, the minimal field of definition of \( X \) becomes important for this direction.

* Department of Mathematics, University of Wisconsin, Madison.
† Email: gasvinseeker94@gmail.com
1. **Fermat varieties:** Hypersurfaces of dimension $d$ defined by

$$F_{n,d} : X_0^n + \cdots + X_{d+1}^n = 0.$$  

In this case, much is known by the results of Shioda [SK79] and our methods offer an alternate proof of some of their results. For Fermat Curves in particular ($d = 1$), we prove that $F_{n,1}$ is supersingular in characteristic $p$ if and only if there exists some $s \geq 1$ such that $p^s \equiv -1 \pmod{n}$. In higher dimensions, we prove that the condition is sufficient while [SK79] also proves necessity. This also implies the supersingularity of quotients such as the Hurwitz curves [DFL+19] and superelliptic curves since they are quotients of Fermat curves.

2. **Abelian varieties with CM by a cyclotomic field:** Let $A_n / \mathbb{F}_q$ be an abelian variety with $\mu_n \subset \text{End}_{\mathbb{F}_q}(A_n)$ and $\dim A_n \leq n$. For instance $A$ could be the reduction of an abelian variety in characteristic zero with CM by $\mathbb{Q}(\mu_n)$. In this case, we prove that $A_n$ is supersingular if there exists a $s \geq 1$ such that $q^s \equiv -1 \pmod{n}$. If moreover $q$ is a prime, i.e., the field of moduli is a prime field then the converse is also true. This is a special case of a known fact (Remark 1) although the method of proof is completely different.

3. **Artin-Schreier curves:** Let $C_{q,n}$ be the (smooth, projective models corresponding to the) degree $n$ cyclic covers of $\mathbb{P}^1$ defined by the equation

$$y^q - y = x^n \text{ over } \mathbb{F}_p.$$  

We prove that $C_{q,n}$ is supersingular if there exists $s \geq 1$ such that $p^s \equiv -1 \pmod{n}$. We suspect that the converse is also true but cannot prove it. This result in this generality is new to our knowledge although much is known about this question. Most notably, [Bla12] characterizes completely the $f(x)$ such that $y^p - y = f(x)$ is supersingular and our result (with $q = p$) is Corollary 3.7, (iii) of that paper. This proof is by an explicit examination of the $p$-adic valuations of the Gauss sums that appear as eigenvalues of the Frobenius in this case. By different methods, [VdGVdV92, Theorem 13.7] proves that $y^p - y = xR(x)$ is supersingular if $R(x)$ is an additive polynomial. This recovers the case $q = p, n = p + 1$ of our theorem. Notably, the proofs in both these preceding results are significantly more complicated than ours.

This result should also be contrasted with the main theorem of [IS91]. They show that the Jacobian of the smooth projective curve corresponding to the equation

$$y^p - y = f(x)$$

is superspecial, i.e., isomorphic to a product of supersingular elliptic curves exactly when $f(x) = x^n$ with $n|p + 1$. This is a strictly stronger condition than being supersingular, i.e., isogenous to a product of supersingular elliptic curves and the two results together produce a large family of Jacobian varieties that are supersingular but not superspecial.

As some motivation for considering supersingularity:

- Suppose $q$ is a square. Then, supersingular curves are exactly the maximizers/minimizers of $|C(\mathbb{F}_q)|$ as $C$ ranges over all smooth, projective curves of genus $g$ by [GT07, Theorem 2.1].
- Supersingular abelian varieties are isogenous to a product of supersingular elliptic curves (over $\mathbb{F}_q$) by Honda-Tate theory.

---

1 Over a finite field, the field of moduli coincides with the field of definition.
• If the cycle class map is surjective, then $X$ is supersingular in degree $2i$ and the converse is true if the Tate conjecture is true for the degree $2i$ cohomology.

• The Tate conjecture is known for supersingular $K3$ surfaces over a finite field (and indeed, the supersingular case is the hardest among all $K3$ surfaces) due to a series of papers by Charles, Kim, Madapusi Pera, and Maulik ([Cha13], [KP15], [MP15], [Mau14]). For a nice survey, see [Tot17]. In particular, supersingular $K3$ surfaces have Picard rank $22$, the maximal possible.

• A conjecture due to Artin, Rudakov, Shafarevich and Shioda asserts that a $K3$ surface is supersingular if and only if it is unirational. Little is known about this conjecture [BL19, Section 1.2] except for Fermat surfaces and $K3$ surfaces with low Artin height.

• Fermat varieties

$$X^n_0 + \cdots + X^n_{2r+1} = 0$$

of even dimension $2r$ are unirational if they are supersingular and the converse is true for $r = 1$ and $m \geq 4$ by [SK79].

Acknowledgments. I would like to thank Rachel Pries for discussions about the paper and references in the literature.

2 Preliminary Definitions

We establish notation and definitions first. We will fix two distinct primes $p, \ell$ throughout and a prime power $q = p^r$ for some $r \geq 1$. We also fix a finite abelian group $G$ (of size $n$) throughout. All objects considered in this paper come equipped with a “Frobenius” action $\sigma_q$. For varieties over $\mathbb{F}_q$, $\sigma_q$ is the usual geometric Frobenius. For the group $G$, we denote the action by $g \to g^q$.

We will let $R$ be either an extension of $\mathbb{Q}_l$ or the Witt vectors $\mathbb{Z}_q$ of a finite field $\mathbb{F}_q$. In the first case, $\sigma_q$ acts trivially while in the second case, $\sigma_q$ is the functorial lift of the Frobenius.

For us $M$ will denote a finite free $R$-moduleootnote{When $R$ is an extension of $\mathbb{Z}_p$, we will sometimes use $W$ instead of $M$.} with an action of $G$ and a semilinear action of $\sigma_q$, i.e.,

$$\sigma_q(rm) = \sigma_q(r)\sigma_q(m) \text{ for any } r \in R[G].$$

We define $\overline{M} = M \otimes_R \overline{R}$ and denote the eigenspace corresponding to the character $\chi$ by

$$M(\chi) := \{m \in M : g(m) = \chi(g)m\}.$$

The action of $\sigma_q$ permutes the characters $\chi : G \to R(\mu_n)$ by

$$\chi \to \chi^{\sigma_q} := \chi \circ \sigma_q^{-1} : G \to R(\mu_n).$$

We will abuse notation and also denote by $\chi$ the linear extension

$$\chi : R[G] \to \overline{R},$$

$$\sum_{h \in H} a_h[h] \to \sum_{h \in H} a_h \chi(h).$$

When $R$ is an extension of $\mathbb{Z}_p$, we assume further that $n$ is co-prime to $p$ and in either case, define the isotypic projections

$$\pi_\chi = \frac{1}{n} \sum_{h \in G} \chi^{-1}(h)h \in R(\mu_n)[G].$$

Note that $\sigma_q \circ \pi_\chi = \pi_\chi \sigma_q$. Finally, we denote by $R(-d)$ the one dimensional free module over $R$ with $G$ acting trivially and the action of $\sigma_q$ twisted by $q^d$, i.e., $\sigma_q(m) = q^d$ for $m$ some generator of $R(-d)$.

In this paper, we consider finite free modules $M$ as above with the following three additional structures associated to it.
• The group $G$ acts on it so that there exists a $G$-equivariant surjection $R[G] \to M$. Equivalently, every character of $G$ appears at most once in $M$. We fix such a surjection and let $m$ be the image of $1 \in R[G]$ and further define $m_\chi = \pi_\chi(m).

• By the above assumption, we can pick $a \in R[G]$ such that $\sigma_\chi(m) = am$. We observe here that $\sigma_\chi$ maps $M(\chi) \to M(\chi^d)$:

$$g \sigma_\chi(m_\chi) = \sigma_\chi \circ g_\sigma^{-1}(m_\chi) = \chi(g_\sigma^{-1})\sigma_\chi(m) = \chi^{\sigma_\chi}(g)\sigma_\chi(m_\chi).$$

Moreover,

$$\sigma_\chi(m_\chi) = \sigma_\chi \circ \pi_\chi(m) = \pi_{\chi^d} \circ \sigma_\chi(m) = \chi^{\sigma_\chi}(a)m_{\chi^d}. \quad (1)$$

• There is a $G, \sigma_\chi$ equivariant perfect pairing

$$\langle -,-\rangle : M \otimes_R M \to R(-d).$$

For two characters $\eta, \rho$ of $G$ and $g \in G$, we see that

$$g(m_\eta, m_\rho) = (gm_\eta, gm_\rho) = \eta(g)\rho(g)(m_\eta, m_\rho).$$

Since $G$ acts trivially on $R(-d)$, $\langle m_\eta, m_\rho \rangle = 0$ unless $\rho = \eta^{-1}$. Since the pairing is perfect, this shows that for every character $\chi$ of $G$ appearing in $M$, $\chi^{-1}$ also occurs in $M$ and $\langle m_\chi, m_{\chi^{-1}} \rangle \neq 0$.

**Definition 2.** For $M$ as above, we say that it is supersingular if all the eigenvalues of $\sigma_\chi$ (considered as a vector space over $\mathbb{Z}_p$ or $\mathbb{Q}_l$) are of the form $q^e\zeta$ for $e \in \mathbb{Z}_{\geq 0}$ and $\zeta$ a root of a unity.

The above definition matches the classical definition of supersingularity in the case where $M$ is a $F$-crystal over $R$, i.e., $\mathbb{Z}_p \subset R$ and $\sigma_\chi : M \to M$ is an injective $\sigma_\chi$-endomorphism. If $X/F_\chi$ is an algebraic variety, then the crystalline cohomology groups $H^i_{\text{cris}}(X)/W(F_\chi)$ is a $F$-crystal over the Witt vectors $R = W(F_\chi)$.

**Definition 3.** We say that $X$ is supersingular if all the crystalline cohomology groups are supersingular and more specifically, we say that $X$ is supersingular in degree $i$ if $H^i_{\text{cris}}(X)/W(F_\chi)$ is supersingular.

By Katz-Messing [KM74, Theorem 1], $X$ is supersingular in degree $i$ if and only if the étale cohomology group $H^i_{\text{ét}}(X, \mathbb{Z}_l)$ is supersingular considered as a module over $R = \mathbb{Z}_l$ with $\sigma_\chi$ induced by the geometric Frobenius.

3 A SUFFICIENT CRITERION FOR SUPER SINGULARITY

**Theorem 2.** Let $M$ be as above, defined over $R \supset \mathbb{Q}_l$. Suppose that for each character $\chi$ of $G$ occurring in $M$, $\chi^{-1}$ is in the $\sigma_\chi$ orbit of $\chi$. Then $M$ is supersingular.

**Proof.** Since our theorem is insensitive to the base change $R \to R(\mu_r)$, we suppose that $\mu_r \subset R$. Let $\chi_1, \ldots, \chi_r$ be an orbit of characters under the Frobenius action so that $\chi_{i+1} = \chi_i^{\sigma_\chi}$ for $1 \leq i < r$ and $\chi_1 = \chi_r^{\sigma_\chi}$. Then, $\sigma_\chi^{\sigma_\chi}$ acts as an endomorphism of $M(\chi_i)$ for each $i$ and we will prove that its eigenvalue $\mu$ is given by $q^{r/2}$ so that the eigenvalues of $\sigma_\chi$ are given by $q^{r/2} \zeta^k$ for some $k$:

In terms of the $a \in R[G]$ defining the action of $\sigma_\chi$, we see that $\langle a \rangle \sigma_\chi(m) = \sigma_\chi^{\sigma_\chi}(a) \ldots \sigma_\chi(a)am$ so that for $\chi \in \{\chi_1, \ldots, \chi_r\}$,

$$\sigma_\chi^{\sigma_\chi}(m_\chi) = \sigma_\chi^{\sigma_\chi} \pi_\chi(m) = \pi_\chi \sigma_\chi^{\sigma_\chi}(m) = \prod_{i=1}^r \chi_i(a)m \implies \mu = \prod_{i=1}^r \chi_i(a). \quad (2)$$
Moreover, using equation 1,
\[ q^d \langle m_{X_i}, m_{X_i}^{-1} \rangle = \langle \tau_q m_{X_i}, \sigma_q m_{X_i}^{-1} \rangle = \left( \chi_{i+1}(a) m_{X_{i+1}}, \chi_{i+1}^{-1}(a) m_{X_{i+1}}^{-1} \right). \]
Rearranging, we obtain
\[ \chi_{i+1}(a) \chi_{i+1}^{-1}(a) = q^d \frac{\langle m_{X_i}, m_{X_i}^{-1} \rangle}{\langle m_{X_{i+1}}, m_{X_{i+1}}^{-1} \rangle}. \] (3)

By our hypothesis, for every \( i \) there exists a \( j \) such that \( \chi_i^{-1} = \chi_j \). Taking a product over \( i = 1, \ldots, r \) of equation 3 yields (together with equation 2):
\[ \mu^2 = \left( \prod_{i=1}^r \chi_i(a) \right)^2 = \frac{\prod_{i=1}^r q^d \langle m_{X_i}, m_{X_i}^{-1} \rangle}{\prod_{i=1}^r \langle m_{X_{i+1}}, m_{X_{i+1}}^{-1} \rangle} = q^{rd} \]
as required.

\[ \square \]

4 A NECESSARY CRITERION FOR SUPERSINGULARITY

In this section, we prove a converse to the criterion of the previous section that will be applicable to curves (and their Jacobians). Note that supersingularity is insensitive to extending the ground field \( \mathbb{F}_q \to \mathbb{F}_q[m] \) but for \( q \) large enough and \( \chi \) any character of \( G \), \( \sigma_q \circ \chi = \chi \). Therefore we will need more stringent hypotheses.

In order to make sense of \( p \)-divisibility, we now switch to working with modules over \( R \) the Witt ring of a finite field. We assume that \( q = p, \gcd(n, p) = 1 \) and that \( d = 1 \) so that we have a perfect pairing (compatible with the \( G, \sigma_p \) action)
\[ W \otimes_R W \to R(-1). \]

**Theorem 3.** If there exists a character \( \chi \) of \( G \) such that it appears in \( G \) but \( \chi^{-1} \) does not lie in the \( \sigma_p \) orbit of \( \chi \), then \( W \) is not supersingular.

**Proof.** Since the theorem is insensitive to the base change \( W \to W \otimes \mathbb{Z}_p[\mu_n] \), we can suppose that \( \mu_n \subset \mathbb{Z}_p \). We continue with the same notation as in Theorem 2 (with \( W \) replacing \( M \) throughout to emphasize the \( p \)-adic nature of it). Let \( \chi_1, \ldots, \chi_r \) be a Frobenius orbit of characters for \( G \). By our assumption, we can suppose that \( \chi_i \neq \chi_i^{-1} \) for any \( 1 \leq i, j \leq r \).

Exactly as in Theorem 2, we see that
\[ \chi_{i+1}(a) \chi_{i+1}^{-1}(a) = p \frac{\langle w_{X_i}, w_{X_i}^{-1} \rangle}{\langle w_{X_{i+1}}, w_{X_{i+1}}^{-1} \rangle} \]
and taking a product over \( i = 1, \ldots, r \), we have
\[ \prod_{i=1}^r \chi_i(a) \prod_{i=1}^r \chi_i^{-1}(a) = p^r. \] (4)

Note that both the products on the left are eigenvalues of \( \sigma_p \) on \( W(\chi_i), W(\chi_i^{-1}) \) respectively. Since \( \sigma_p \) is an automorphism of \( G \), we have \( \sigma_p(g) = g^{m_g} \) for some \( m_g \) coprime to \( n \). Therefore, \( \chi_i(g) = \chi_i^{m_g^{-1}}(g) \) is Galois conjugate over \( \mathbb{Z}_p \) to \( \chi_1(g) \) (since \( \chi_1(g) \in \mu_n \)) and the \( \chi_i(a) \) are all Galois conjugates of \( \chi_1(a) \) (and similarly for \( \chi_i^{-1}(a) \) with respect to \( \chi_1^{-1}(a) \)) in the ring \( R \), and hence have the same \( p \)-adic valuation.
Let $p^a$ be the highest power of $p$ dividing $\chi_1(a)$ (and hence $\chi_i(a)$ for $i = 1, \ldots, r$) and $p^\beta$ be the highest power dividing the $\chi_{i}^{-1}(a)$. Both $\alpha, \beta \geq 0$ since $a$ is an integral element and are integers since $\mathbb{Z}_q$ is unramified.

Comparing the $p$-adic valuation of the two sides of equation 4 then shows that $p^r = p^r(\alpha + \beta)$ and hence $\alpha + \beta = 1$ which implies that one of them is 1 and the other is 0. That is, the eigenvalues of $\sigma_p^r$ come in pairs, exactly one of which is a $p$-adic unit. This implies that $W$ is not supersingular.

5 EXAMPLES

We demonstrate several applications of the above theorems to the cohomology of varieties. We note that for every character $\sigma$ this case $\mu$ is an injection: If $\chi$ supersingular. $\mu_\chi$ and $\chi^{-1}$ are in the same $\sigma_q$ orbit if and only if $q^s \equiv -1 \pmod{n}$ for some $s \geq 1$. Moreover, in this case $\sigma_q : \mu_\chi \to \mu_\chi$ is given by $g \mapsto g^q$.

**Theorem 4.** Let $X/\mathbb{F}_q$ be a $d$ dimensional variety with an abelian subgroup $G \subset \text{End}_{\mathbb{F}_q}(X)$ such that $H^d_{\text{et}}(X, \mathbb{Q}_\ell)$ is a quotient of $\mathbb{Q}_\ell[G]$. Suppose that for every character $\chi$ of $G$ appearing in $H^d_{\text{et}}(X, \mathbb{Q}_\ell)$, $\chi^{-1}$ is in the Frobenius orbit of $\chi$. Then, $H^d_{\text{et}}(X, \mathbb{Q}_\ell)$ is supersingular.

**Proof.** We apply Theorem 2 using the intersection pairing

$$H^d_{\text{et}}(X, \mathbb{Q}_\ell) \otimes H^d_{\text{et}}(X, \mathbb{Q}_\ell) \to H^{2d}_{\text{et}}(X, \mathbb{Q}_\ell) \cong \mathbb{Q}_\ell(-d).$$

**Example 1.** Examples of varieties satisfying the hypothesis are given by the Fermat varieties [And87]

$$X_0^n + \cdots + X_{d+1}^n = 0 \subset \mathbb{P}^{d+1}.$$ Our criterion is equivalent to the existence of an $i \in \mathbb{Z}$ such that $q^i \equiv -1 \pmod{n}$. [SK79, Theorem 2.1] proves a stronger result using an inductive argument and an explicit computation with Jacobi sums.

**Theorem 5.** Let $A/\mathbb{F}_q$ be an abelian variety with an abelian subgroup $G \subset \text{End}_{\mathbb{F}_q}(A)$ such that $2 \dim A \leq |G|$. Suppose that for every character $\chi$ of $G$ appearing in $H^1_{\text{et}}(A, \mathbb{Q}_\ell)$, $\chi^{-1}$ is in the Frobenius orbit of $\chi$. Then, $A$ is supersingular.

If moreover $p \nmid |G|$ and $A$ is defined over $\mathbb{F}_p$, then $A$ is supersingular only if $\chi^{-1}$ is in the $\sigma_p$ orbit of $\chi$ for every character $\chi$ appearing in $H^1_{\text{et}}(A, \mathbb{Q}_\ell)$.

**Proof.** Since $H^1_{\text{et}}(A, \mathbb{Q}_\ell) = \wedge^1 H^1_{\text{et}}(A, \mathbb{Q}_\ell)$, supersingularity of $A$ is equivalent to the supersingularity of $H^1_{\text{et}}(A, \mathbb{Q}_\ell)$. For $v \in H^1_{\text{et}}(A, \mathbb{Q}_\ell)$, note that the map

$$\mathbb{Q}_\ell[G] \to H^1_{\text{et}}(A, \mathbb{Q}_\ell)$$

$$f \to fv$$

is an injection: If $f \in \mathbb{Q}_\ell[G] \subset \text{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}_\ell$ maps to 0, then $k\deg(f)$ for $k$ arbitrarily large and consequently $f = 0$. Since $\dim_{\mathbb{Q}_\ell} H^1_{\text{et}}(A, \mathbb{Q}_\ell) = 2 \dim A \leq \dim_{\mathbb{Q}_\ell} \mathbb{Q}_\ell[G]$, $H^1_{\text{et}}(A, \mathbb{Q}_\ell)$ is a quotient of $\mathbb{Q}_\ell[G]$ and each character of $G$ appears at most once.

For the forward implication, we apply Theorem 2 using the Weil pairing

$$H^1_{\text{et}}(A, \mathbb{Q}_\ell) \otimes H^1_{\text{et}}(A, \mathbb{Q}_\ell) \to \mathbb{Q}_\ell(-1).$$
To prove the necessity of the criterion, we apply Theorem 3 with $W = \tcrys^1(A/F_q)$ and the Cartier pairing ([Oda89, Theorem 1.1])

$$\tcrys^1(A) \otimes \tcrys^1(A) \to \mathbb{Z}_q(-1).$$

Note that since $A$ is assumed to be defined over $\mathbb{F}_p$, in this case, $\sigma_p : W \to W$ is well defined.

\[\square\]

**Example 2.** Let $A_n$ be the CM Abelian variety with CM by the cyclotomic field $\mathbb{Q}(\mu_n)$. Then our criterion applies to the reduction of $A_n$ at any place of $\mathbb{Q}(\mu_n)$. We can take $G = \mu_n$ in the above theorem so that $2 \dim A = \phi(n) < n = |G|$. The above theorem then implies that the reduction $A_n/F_q$ is supersingular if there exists some $r$ such that $q^r \equiv -1 \pmod{n}$. If moreover the place splits completely, i.e., $q = p$ then the converse is also true.

**Remark 1.** The above example is also a special case of the fact that if $A$ is a CM Abelian variety with endomorphism algebra $K$ and totally real subfield $K^+$, and if every prime in $K^+$ over some $p$ is inert in $K$, then $A$ is supersingular over the reductions of these primes. In the case where $K = \mathbb{Q}(\mu_n)$, this criterion is exactly equivalent to there existing some $r$ such that $p^r \equiv -1 \pmod{n}$.

**Example 3.** We note that the above theorem also applies for curves $C$ with the same hypothesis since $\tcrys^1(A, K)$ can be canonically identified with $\tcrys^1(A, \mathbb{Q}_l)$. A family of examples is given by the Fermat curves and their quotients. An alternate characterization of these curves is as abelian covers of $\mathbb{P}^1$ ramified over three points.

Theorem 2 does not apply to the Artin-Schreier curves $C_{q,n}$:

$$y^q - y = x^n \text{ over } \mathbb{F}_p$$

even though $G = \mathbb{F}_q \times \mu_n$ acts on $C_{q,n}$ so that its cohomology $\tcrys^1(C, \mathbb{Q}_l)$ is a quotient of $\mathbb{Q}_l[G]$. Since $\sigma_q$ fixes the first factor $\mathbb{F}_q \subset G$, it is never the case that the inverse of every character $\chi$ of $G$ appearing in $\tcrys^1(C, \mathbb{Q}_l)$ is in the Frobenius orbit of $\chi$. Nevertheless, we can modify the above proof.

**Theorem 6.** The curves $C_{q,n}/\mathbb{F}_p$ (with $\gcd(n, p) = 1$) are supersingular if there exists some $s$ such that $p^s \equiv -1 \pmod{n}$.

**Proof.** For any prime $\ell$ (including $\ell = p$), let $K_\ell = \mathbb{Q}_\ell(\zeta_{\ell p}, \zeta_n)$ be the minimal extension over which the characters of $G$ split. As in the proof of Theorem 5, we can use either étale cohomology ($\ell \neq p$) $M_\ell = \tcrys^1(C_{q,n}, \mathbb{Q}_l)$ or crystalline cohomology ($\ell = p$) $M_p = \tcrys^1(C_{q,n})$ to compute the eigenvalues of $\sigma_p$.

As before, we suppose that $\sigma_p$ acts on $M_\ell$ by $a_\ell \in \mathbb{Z}_\ell[G]$ after fixing a generator $m \in M$. Let us fix a character $\theta = (\psi, \chi)$ of $G = \mathbb{F}_q \times \mu_n$ so that $\psi$ is non trivial and $\chi$ is primitive and let $r$ be the size of its orbit $\theta = 1, \ldots, r$ under the Frobenius $\sigma_p$ so that $\sigma_p^r$ fixes the eigenspace of $\theta$ in $M$ and the eigenvalues of $\sigma_p^r$ are given by

$$\mu^r = \prod_{i=1}^r \theta_i(a_\ell) \in K_\ell.$$ (5)

In this case, since the $\sigma_p$ action fixes the $\psi$ component of $\theta$, it is never the case that $\theta^{-1}$ is in the orbit of $\theta$.

As before, we can use the Weil pairing or the Cartier pairing (in the cases $\ell \neq p$ and $\ell = p$ respectively) to show that

$$\mu^r \mu^{-1} = p^r.$$ (6)

The Frobenius acts on $\mu_n$ by $g \to g^q$ for $g \in \mu_n$. Since $\chi(g) \in \mu_N$, it is Galois conjugate to $\chi^{q^r}(g) = \chi^{-p}(g)$. By assumption, $\chi^{-1}$ is in the Frobenius orbit of $\chi$ so that $\theta^{-1}(a_p)$ is Galois conjugate

---

3 The cyclotomic field $\mathbb{Q}(\mu_n)$ has degree $\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$ over $\mathbb{Q}$ and the dimension of the corresponding CM abelian variety is equal to half this degree.
to $\theta(a_p)$ considered as elements of $K_p/Q_p$. Equation 5 then shows that $\mu_\theta$ and $\mu_{\theta-1}$ are conjugate to each other and thus have the same $p$-adic valuation. Equation 6 then implies that $\mu_\theta, \mu_{\theta-1}$ are both divisible by $p^{1/2}$ for each $\theta$ as above.

In particular, $p^{-1/2} \mu_\theta$ is a $p$-adic unit and equation 6 shows also that it is a $\ell$-adic unit for all $\ell$. Therefore, it is an algebraic unit and so are all its Galois conjugates (since these Galois conjugates correspond to other $\theta$ as above). The only such numbers are roots of unity and therefore, $C_{q,n}$ is supersingular.

The theorem also shows the necessity of (at least some of) the hypothesis in Theorem 3.

Remark 2. We do not know of an exact characterization of supersingularity for Artin-Schreier curves. Numerical evidence suggests that the converse of our Theorem is also true.

REFERENCES

[And87] Greg W Anderson. Torsion points on Fermat Jacobians, roots of circular units and relative singular homology. Duke Mathematical Journal, 54(2):501–561, 1987.

[BL19] Daniel Bragg and Max Lieblich. Perfect points on genus one curves and consequences for supersingular $K_3$ surfaces. arXiv preprint arXiv:1904.04803, 2019.

[Bla12] Régis Blache. Valuation of exponential sums and the generic first slope for artin–schreier curves. Journal of Number Theory, 132(10):2336–2352, 2012.

[Cha13] François Charles. The Tate conjecture for $K_3$ surfaces over finite fields. Inventiones mathematicae, 194(1):119–145, 2013.

[DFL+19] Erin Dawson, Henry Frauenhoff, Michael Lynch, Amethyst Price, Seamus Somerstep, Eric Work, Dean Bisogno, and Rachel Pries. The supersingularity of Hurwitz curves. Involve, a Journal of Mathematics, 12(8):1293–1306, Oct 2019.

[GT07] Arnaldo Garcia and Saeed Tafazolian. Certain maximal curves and Cartier operators. Niedersächsische Staats-und Universitätsbibliothek, 2007.

[IS91] Susumu Irokawa and Ryuji Sasaki. A remark on Artin-Schreier curves whose Hasse-Witt maps are the zero maps. Tsukuba journal of mathematics, 15(1):185–192, 1991.

[KM74] Nicholas M Katz and William Messing. Some consequences of the riemann hypothesis for varieties over finite fields. Inventiones mathematicae, 23(1):73–77, 1974.

[KP15] Wansu Kim and Keerthi Madapusi Pera. 2-adic integral canonical models and the Tate conjecture in characteristic 2. arXiv preprint arXiv:1512.02540, 2015.

[Mau14] Davesh Maulik. Supersingular $K_3$ surfaces for large primes. Duke Mathematical Journal, 163(13):2357–2425, 2014.

[MP15] Keerthi Madapusi Pera. The Tate conjecture for $K_3$ surfaces in odd characteristic. Inventiones mathematicae, 201(2):625–668, 2015.

[Oda69] Tadao Oda. The first de rham cohomology group and dieudonné modules. In Annales scientifiques de l’École Normale Supérieure, volume 2, pages 63–135, 1969.

[SK79] Tetsuji Shioda and Toshiyuki Katsura. On Fermat varieties. Tohoku Mathematical Journal, Second Series, 31(1):97–115, 1979.
[Tot17] Burt Totaro. Recent progress on the Tate conjecture. *Bulletin of the American Mathematical Society*, 54(4):575–590, 2017.

[VdGVdV92] Gerard Van der Geer and Marcel Van der Vlugt. Reed-Muller codes and supersingular curves. I. *Compositio Mathematica*, 84(3):333–367, 1992.