PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 150, Number 2, February 2022, Pages 525–537
https://doi.org/10.1090/proc/15681
Article electronically published on November 4, 2021

EVERY BT_1 GROUP SCHEME APPEARS IN A JACOBIAN

RACHEL PRIES AND DOUGLAS ULMER

(Communicated by Matthew A. Papanikolas)

ABSTRACT. Let p be a prime number and let k be an algebraically closed field of characteristic p. A BT_1 group scheme over k is a finite commutative group scheme which arises as the kernel of p on a p-divisible (Barsotti–Tate) group. Our main result is that every BT_1 group scheme over k occurs as a direct factor of the p-torsion group scheme of the Jacobian of an explicit curve defined over $\mathbb{F}_p$. We also treat a variant with polarizations. Our main tools are the Kraft classification of BT_1 group schemes, a theorem of Oda, and a combinatorial description of the de Rham cohomology of Fermat curves.

1. INTRODUCTION

Fix a prime number p and let k be an algebraically closed field of characteristic p. A BT_1 *group scheme* over k is a finite commutative group scheme which is the kernel of p on a p-divisible group. (The term BT_1 stands for Barsotti–Tate truncated at level 1, and Barsotti–Tate is a synonym for p-divisible.) These are the finite commutative group schemes killed by p which also satisfy $\mathrm{Ker}F = \mathrm{Im}V$ and $\mathrm{Ker}V = \mathrm{Im}F$ where F and V are the Frobenius and Verschiebung maps respectively. The simplest BT_1 group schemes are $\mathbb{Z}/p\mathbb{Z}$ and μ_p.

We also consider *polarized BT_1 group schemes* over k, i.e., BT_1 group schemes G with a pairing that induces a non-degenerate, alternating pairing on the Dieudonné module of G, as in [11, §9]. If A is a principally polarized abelian variety of dimension g over k, its p-torsion subscheme $A[p]$ is naturally a polarized BT_1 group scheme of order p^{2g}.

If C is a smooth irreducible projective curve of genus g over k, then its Jacobian $\mathrm{Jac}(C)$ is a principally polarized abelian variety of dimension g, and thus $G = \mathrm{Jac}(C)[p]$ is a polarized BT_1 group scheme of order p^{2g}. By a result of Oda [10], the de Rham cohomology of C over k determines the isomorphism class of G uniquely via its Dieudonné module.

In general, it is not known which polarized BT_1 group schemes occur for Jacobians of curves. In fact, there are very few examples of curves for which the isomorphism class of $\mathrm{Jac}(C)[p]$ has been computed. Our main result is:

Received by the editors January 21, 2021, and, in revised form, May 9, 2021.

2020 *Mathematics Subject Classification.* Primary 11D41, 11G20, 14F40, 14H40, 14L15; Secondary 11G10, 14G17, 14K15, 14H10.

Key words and phrases. Curve, finite field, Jacobian, abelian variety, Fermat curve, Frobenius, Verschiebung, group scheme, de Rham cohomology, Dieudonné module, p-divisible group.

The first author was partially supported by NSF grant DMS-1901819.

The second author was partially supported by Simons Foundation grants 359573 and 713699.

Theorem 1.1.

(1) *Every BT_1 group scheme over k appears as a direct factor of $Jac(C)[p]$ for an explicit curve C defined over $\mathbb{F}_p$.*
(2) *Every polarized BT_1 group scheme over k appears as a direct factor (with pairing) of $Jac(C)[p]$ for an explicit curve C defined over $\mathbb{F}_p$.*
(3) *In particular, if G is an indecomposable BT_1 group scheme of order p^ℓ with $\ell > 1$, or if G is an indecomposable polarized BT_1 group scheme of order p^ℓ with $\ell > 2$, then the curve C in part (1) or part (2) can be chosen to have genus $\leq (p^\ell - 2)/2$.*

We prove this theorem in Section 6. Using a result of Oort (Proposition 2.1), parts (1) and (2) are essentially equivalent. In part (3), a polarized BT_1 group scheme is indecomposable if it is not the orthogonal direct sum of two proper polarized subgroup schemes. The restrictions on ℓ in (3) are not significant, because the omitted groups are known to appear in elliptic curves.

A weaker version of parts (1) and (2) follows from the fact that every abelian variety appears as a subvariety of a Jacobian together with the non-emptiness of each E–O stratum of $\mathcal{A}_g$; see Remark 6.6. Our proof of Theorem 1.1 is more elementary, and it yields a stronger result because: (i) there are no conditions on p; (ii) the curve C is explicit and its field of definition is $\mathbb{F}_p$; (iii) the genus of C is bounded in terms of the order of G; and (iv) the other group schemes that occur in $\mathrm{Jac}(C)[p]$ can be explicitly computed.

In almost all cases the "explicit curve" of the theorem can be taken to be a quotient of a Fermat curve. Fermat curves are a natural class of curves to consider because their de Rham cohomology, with its Frobenius and Verschiebung operators, admits a simple combinatorial description. A result of independent interest in this paper is that we determine the structure of the BT_1 module for the Jacobian of the Fermat curve F_d of degree d, for all positive integers d that are relatively prime to p; see Theorem 5.5. This complements work of Yui, who determined the Newton polygons of Fermat curves [16, Thm. 4.2].

Our arguments use parts of three classifications of BT_1 group schemes largely due to Kraft, Ekedahl, and Oort. In a companion paper [12], we provide a complete translation between these classifications, and we apply them to give a detailed study of the p-torsion subgroups of Jacobians of Fermat curves, including well-known invariants like the p-rank and a-number, as well as two other invariants related to supersingular elliptic curves.

2. Groups and modules

2.1. **Dieudonné modules.** We refer to [5] for background on contravariant Dieudonné theory for finite group schemes of p-power order over k and for p-divisible groups.

Write σ for the absolute Frobenius of k and extend it to the Witt vectors $W(k)$. Define the *Dieudonné ring* $\mathbb{D} = W(k)\{F, V\}$ as the $W(k)$-algebra generated by F and V with relations

$$FV = VF = p, \ F\alpha = \sigma(\alpha)F, \text{ and } \alpha V = V\sigma(\alpha) \text{ for } \alpha \in W(k).$$

Let $\mathbb{D}_k = \mathbb{D}/p\mathbb{D} \cong k\{F, V\}$.

If G is a finite, commutative group scheme over k of p-power order, then its *Dieudonné module* $M(G)$ is the left $\mathbb{D}$-module of homomorphisms of k-group

schemes from G to the co-Witt vectors. The functor $G \rightsquigarrow M(G)$ is contravariant and induces an anti-equivalence between the category of finite group schemes of p-power order over k and the category of left $\mathbb{D}$-modules that are of finite length as $W(k)$ modules [5, III.1.4].

2.2. BT_1 **group schemes and** BT_1 **modules.** By definition, a BT_1 *group scheme* over k is a finite commutative group scheme G that is killed by p and that has the properties

$$\mathrm{Ker}(F : G \to G) = \mathrm{Im}(V : G \to G) \quad \text{and} \quad \mathrm{Im}(F : G \to G) = \mathrm{Ker}(V : G \to G).$$

The notation BT_1 is an abbreviation of "Barsotti–Tate of level 1".

By definition, a BT_1 *module* over k is a $\mathbb{D}_k$-module M of finite dimension over k such that

$$\mathrm{Ker}(F : M \to M) = \mathrm{Im}(V : M \to M) \quad \text{and} \quad \mathrm{Im}(F : M \to M) = \mathrm{Ker}(V : M \to M).$$

A $\mathbb{D}_k$-module M is a BT_1 module if and only if $M = M(G)$ for a BT_1 group scheme G over k.

The group schemes $\mathbb{Z}/p\mathbb{Z}$ and μ_p are BT_1 group schemes. So is $G_{1,1}$, the kernel of p on a supersingular elliptic curve over k. On the other hand, α_p is not.

2.3. **Duality.** If G is a finite, commutative group scheme over k, define its *Cartier dual* G^D as $G^D := \mathrm{Hom}_{k-Gr}(G, \mathbb{G}_m)$ (homomorphisms of k-group schemes), where $\mathbb{G}_m$ is the multiplicative group over k. A BT_1 group scheme G is *self-dual* if $G \cong G^D$.

If M is a left $\mathbb{D}$-module of finite length over $W(k)$, define its *dual module* M^* as follows: If M is killed by p^n, set $M^* = \mathrm{Hom}_{W(k)}(M, W_n(k))$ with $(F\phi)(m) = \sigma(\phi(Vm))$ and $(V\phi)(m) = \sigma^{-1}(\phi(Fm))$ for all $\phi \in M^*$ and $m \in M$. A BT_1 module M is *self-dual* if $M \cong M^*$.

A basic result of Dieudonné theory [5, §III.5.3] is that $M(G^D) \cong M(G)^*$. In particular, G is self-dual if and only if $M(G)$ is self-dual.

2.4. **Polarized** BT_1 **group schemes.** A *polarized* BT_1 *module* is a BT_1 module M equipped with a non-degenerate, alternating pairing $\langle \cdot, \cdot \rangle : M \times M \to k$ of Dieudonné modules (i.e., such that $\langle x, x \rangle = 0$ and $\langle Fx, y \rangle = \langle x, Vy \rangle^p$ for all $x, y \in M$). Clearly, a polarized BT_1 module is self-dual.

A *polarized* BT_1 *group scheme* is a BT_1 group scheme G equipped with a bilinear form with the property that the induced form on $M(G)$ is non-degenerate and alternating. (The reason for this unusual definition is that when $p = 2$, an alternating form on G need not induce an alternating form on $M(G)$. See [11, p. 346].)

Oort proved [11, §§2, 5, 9] (see also [12, Cor. 4.2.3]) that any self-dual BT_1 module can be given a unique polarization:

Proposition 2.1. *Every self-dual* BT_1 *module admits a polarization, i.e., a non-degenerate* alternating *pairing, and this pairing is unique up to* (*non-unique*) *isomorphism.*

3. The Kraft classification of BT_1 modules

In this section, we review a bijection due to Kraft between isomorphism classes of BT_1 modules over k and certain data obtained from words on a two-letter alphabet; see [6].

3.1. **Words.** Let $\mathcal{W}$ be the monoid of words w on the two-letter alphabet $\{f, v\}$ with law of composition given by concatenation, and write 1 for the empty word. The *complement* w^c of w is the word obtained by exchanging f and v at every letter.

If $w \in \mathcal{W}$ is a word of length λ, we write $w = u_{\lambda-1} \cdots u_0$ where $u_i \in \{f, v\}$ for $0 \leq i \leq \lambda - 1$. Equip $\mathcal{W}$ with an action of the group $\mathbb{Z}$ where $1 \in \mathbb{Z}$ maps $w = u_{\lambda-1} \cdots u_0$ to $u_0 u_{\lambda-1} \cdots u_1$. If w and w' are in the same orbit of this action, we say w' is a *rotation* of w. The orbit $\overline{w}$ of w under the action of $\mathbb{Z}$ is called a *cyclic word*.

A word is *primitive* if it is not a power of a shorter word, i.e., not of the form w^e for some integer $e > 1$.

3.2. **Cyclic words to BT_1 modules.** Following Kraft [6], we attach a BT_1 module to a multiset of primitive cyclic words.

Suppose that $w \in \mathcal{W}$ is a word of length λ, say $w = u_{\lambda-1} \cdots u_0$ with $u_j \in \{f, v\}$. Let $M(w)$ be the k-vector space with basis e_j with $j \in \mathbb{Z}/\lambda\mathbb{Z}$ and define a p-linear map $F : M(w) \to M(w)$ and a p^{-1}-linear map $V : M(w) \to M(w)$ by setting

$$F(e_j) = \begin{cases} e_{j+1} & \text{if } u_j = f, \\ 0 & \text{if } u_j = v, \end{cases} \qquad \text{and} \qquad V(e_{j+1}) = \begin{cases} e_j & \text{if } u_j = v, \\ 0 & \text{if } u_j = f. \end{cases}$$

This construction yields a BT_1 module of dimension λ over k which up to isomorphism only depends on the cyclic word $\overline{w}$ associated to w.

Kraft proves that if w is primitive then $M(w)$ is indecomposable, and that every indecomposable BT_1 module is isomorphic to one of the forms $M(w)$ for a unique primitive cyclic word $\overline{w}$. Thus every BT_1 module M is isomorphic to a direct sum $\oplus M(w_i)$ where $\overline{w}_i$ runs through a uniquely determined multiset of primitive cyclic words.

Even if w is not primitive, the formulas above define a BT_1 module. If $w = (w')^e$, Kraft also proves that $M(w) \cong M(w')^e$.

It is clear that $M(f) = M(\mathbb{Z}/p\mathbb{Z})$, $M(v) = M(\mu_p)$, and $M(fv)$ is the Dieudonné module of the kernel of p on a supersingular elliptic curve. More generally, if w has length > 1 and is primitive, then $M(w)$ is the Dieudonné module of a unipotent, connected BT_1 group scheme.

3.3. **Duality.** It is clear from the definitions that duality of modules corresponds to complementation of words, i.e., $M(w)^* \cong M(w^c)$. It follows that an indecomposable, self-dual BT_1 module is either of the form $M(w)$ where w is primitive and induces a self-complementary cyclic word ($\overline{w^c} = \overline{w}$) or of the form $M(w) \oplus M(w^c)$ where w is primitive and $\overline{w^c} \neq \overline{w}$.

4. Permutations and BT_1 modules

In this section, we associate a BT_1 module to certain permutations via the Kraft construction.

4.1. **Permutations.** Consider a finite set S written as the disjoint union $S = S_f \cup S_v$ of two subsets. Let $\pi : S \to S$ be a permutation of S. Two such collections of data $(S = S_f \cup S_v, \pi)$ and $(S' = S'_f \cup S'_v, \pi')$ are isomorphic if there is a bijection $\iota : S \to S'$ such that $\iota(S_f) = S'_f$, $\iota(S_v) = S'_v$, and $\iota\pi = \pi'\iota$.

4.2. **Permutations to words.** Given $S = S_f \cup S_v$ and π as above, we define a multiset of cyclic words as follows: For $a \in S$ with orbit of size λ, define the word $w_a = u_{\lambda-1} \cdots u_0$ where

$$u_j = \begin{cases} f & \text{if } \pi^j(a) \in S_f, \\ v & \text{if } \pi^j(a) \in S_v. \end{cases}$$

Then $\overline{w}_a$ depends only on the orbit of a. This gives a well-defined map from orbits of π to cyclic words. Taking the union over orbits, we can associate to $(S = S_f \cup S_v, \pi)$ a multiset of cyclic words. If S and S' are isomorphic, then they yield the same multiset.

For example, let $S = \{1, \ldots, 9\}$, $S_f = \{2, 3, 5, 6, 9\}$, and $S_v = \{1, 4, 7, 8\}$. Let π be the permutation $(135)(246)(789)$. The orbit through 1 and the orbit through 2 both give rise to the cyclic word $\overline{ffv}$, and the orbit through 7 gives rise to the cyclic word $\overline{fvv}$. The associated multiset is $\{(\overline{ffv})^2, \overline{fvv}\}$ (where $(\overline{ffv})^2$ means the cyclic word $\overline{ffv}$ taken with multiplicity 2).

4.3. **Permutations to BT_1 modules.** Given $S = S_f \cup S_v$ and π as above, we obtain a multiset of words, and thus a BT_1 module of dimension equal to the cardinality of S. This BT_1 module can be described directly in terms of S as follows: Form the k-vector space $M(S)$ with basis elements $\{e_a \mid a \in S\}$ and define a p-linear map $F : M(S) \to M(S)$ and a p^{-1}-linear map $V : M(S) \to M(S)$ by setting

$$F(e_a) = \begin{cases} e_{\pi(a)} & \text{if } a \in S_f, \\ 0 & \text{if } a \in S_v, \end{cases} \qquad \text{and} \qquad V(e_{\pi(a)}) = \begin{cases} e_a & \text{if } a \in S_v, \\ 0 & \text{if } a \in S_f. \end{cases}$$

Note that $M(S)$ decomposes (as a BT_1 module) into submodules indexed by the orbits of π. The submodule corresponding to an orbit of π is indecomposable if and only if the word associated to the orbit is primitive.

4.4. **Duality.** Given $S = S_f \cup S_v$ and π as above, form the BT_1 module $M(S)$. It is clear from the definitions that the dual module $M(S)^*$ is the module associated to data $(S^* = S_f^* \cup S_v^*, \pi^*)$ where $S^* = S$, $S_f^* = S_v$, $S_v^* = S_f$, and $\pi^* = \pi$. It follows that $M(\mathrm{S})$ is self-dual if and only if there exists a bijection $\iota : S \xrightarrow{\sim} S$ which satisfies $\iota(S_f) = S_v$ and $\pi \circ \iota = \iota \circ \pi$.

5. Fermat Jacobians

In this section, we study p-torsion group schemes of Jacobians of Fermat curves.

5.1. **BT_1 modules associated to curves.** Let $\mathcal{C}$ be an irreducible, smooth, projective curve of genus g over k, and let $J = J_{\mathcal{C}}$ be its Jacobian. In [10, §5], Oda gives $H^1_{dR}(\mathcal{C}) = H^1_{dR}(J)$ the structure of a BT_1 module. In particular, writing H for $H^1_{dR}(\mathcal{C})$, we have

$$\mathrm{Im}(V : H \to H) = \mathrm{Ker}(F : H \to H) \cong H^0(\mathcal{C}, \Omega^1_{\mathcal{C}}), \tag{5.1}$$

and

$$\mathrm{Im}(F : H \to H) = \mathrm{Ker}(V : H \to H) \cong H^1(\mathcal{C}, \mathcal{O}_{\mathcal{C}}).$$

Oda proves [10, Cor. 5.11] that there is a canonical isomorphism of $\mathbb{D}_k$-modules

$$H^1_{dR}(\mathcal{C}) \cong M(J[p]). \tag{5.2}$$

5.2. **Fermat curves.** For each positive integer d not divisible by p, let F_d be the Fermat curve of degree d, i.e., the smooth, projective curve over k with affine model $F_d : X^d + Y^d = 1$ and let J_{F_d} be its Jacobian. Let $\mathcal{C}_d$ be the smooth, projective curve over k with affine model

$$\mathcal{C}_d : \qquad y^d = x(1-x), \tag{5.3}$$

and let J_d be its Jacobian.

The curve $\mathcal{C}_d$ is a quotient of F_d. (Substitute X^d for x and XY for y in the equation for $\mathcal{C}_d$.) The map $F_d \to \mathcal{C}_d$ is the quotient of F_d by a subgroup of $(\mu_d)^2 \subset \mathrm{Aut}(F_d)$ of index d. Since the degree of $F_d \to \mathcal{C}_d$ is prime to p, $J_d[p]$ is a direct factor of $J_{F_d}[p]$. Most of our results depend only on the simpler curve $\mathcal{C}_d$, so we use it whenever possible.

5.3. **Cohomology of $\mathcal{C}_d$.** The Riemann-Hurwitz formula shows that the genus of $\mathcal{C}_d$ is

$$g(\mathcal{C}_d) = \lfloor (d-1)/2 \rfloor = \begin{cases} (d-1)/2 & \text{if } d \text{ is odd,} \\ (d-2)/2 & \text{if } d \text{ is even.} \end{cases}$$

Moreover, $\mathcal{C}_d$ admits an action of $\zeta \in \mu_d$ with $\zeta : (x, y) \mapsto (x, \zeta y)$.

We next describe $H^1_{dR}(\mathcal{C}_d)$ in a form conducive to studying it as a $\mathbb{D}_k$-module. First, write

$$H^1_{dR}(\mathcal{C}_d) = \bigoplus_{a \in \mathbb{Z}/d\mathbb{Z}} H_a,$$

where H_a is the subspace of $H^1_{dR}(\mathcal{C}_d)$ where every $\zeta \in \mu_d$ acts by multiplication by ζ^a. Since the action of μ_d on $\mathcal{C}_d$ induces the trivial action on $H^2_{dR}(\mathcal{C}_d)$, the cup product induces a perfect duality between H_a and H_{-a}, and a trivial pairing between H_a and H_b if $b \not\equiv -a \pmod{d}$.

Let

$$S = \begin{cases} \mathbb{Z}/d\mathbb{Z} \setminus \{0\} & \text{if } d \text{ is odd,} \\ \mathbb{Z}/d\mathbb{Z} \setminus \{0, d/2\} & \text{if } d \text{ is even.} \end{cases}$$

Multiplication by p induces a permutation of S. We make sense of any archimedean statement about an element $a \in S$ (e.g., "$0 < a < d/2$") by implicitly lifting a to its least positive residue.

Proposition 5.1.

(1) *If $a \in \mathbb{Z}/d\mathbb{Z}$, then $\dim_k(H_a) = 1$ if $a \in S$ and $H_a = 0$ if $a \notin S$.*
(2) *$H^0(\mathcal{C}_d, \Omega^1_{\mathcal{C}_d}) = \oplus_{0<a<d/2} H_a$.*
(3) *If $0 < a < d/2$, then $FH_a = 0$ and V induces an isomorphism $V : H_{pa} \to H_a$.*
(4) *If $d/2 < a < d$, then $VH_{pa} = 0$ and F induces an isomorphism $F : H_a \to H_{pa}$.*

There are several similar calculations in the literature (e.g., [15], [3, §5], and [14, §6]). For the convenience of the reader, we include the following efficient and transparent proof.

Proof. For $0 < a < d/2$, a simple calculation shows that the 1-form $y^a dx/y^d$ on the affine model (5.3) extends to a global 1-form on $\mathcal{C}_d$, and its class in $H^1_{dR}(\mathcal{C}_d)$ lies in H_a. This shows that $\dim_k(H_a) \geq 1$ for $0 < a < d/2$. Because of the perfect duality between H_a and H_{-a}, we see that $\dim_k(H_a) \geq 1$ for $d/2 < a < d$. Since

$g(\mathcal{C}_d) = \lfloor (d-1)/2 \rfloor$, it follows that $\dim_k(H_a) = 1$ for $a \in S$ and $H_a = 0$ for $a \notin S$. This proves parts (1) and (2).

By definition, $FH_a \subset H_{pa}$ and $VH_{pa} \subset H_a$. By (5.1), F kills $H^0(\mathcal{C}_d, \Omega^1_{\mathcal{C}_d}) = \oplus_{0<a<d/2} H_a$. Since $\dim(\mathrm{Ker}F) = g$, the map $F : H_a \to H_{pa}$ is injective, and thus bijective, for $d/2 < a < d$. Similarly, by (5.1), $\mathrm{Im}V = H^0(\mathcal{C}_d, \Omega^1_{\mathcal{C}_d})$. So $V : H_{pa} \to H_a$ is surjective, and thus bijective, for $0 < a < d/2$ and zero for $d/2 < a < d$. This proves parts (3) and (4). □

Now let $S_f, S_v \subset S$ be given by

$$S_f = \{a \mid d/2 < a < d\} \quad \text{and} \quad S_v = \{a \mid 0 < a < d/2\},$$

and let $\pi : S \to S$ be the permutation induced by multiplication by p.

Theorem 5.2. *The Dieudonné module $M(J_d[p])$ is the BT_1 module associated to the data*

$$S = \begin{cases} \mathbb{Z}/d\mathbb{Z} \setminus \{0, d/2\} & \text{if } d \text{ is even,} \\ \mathbb{Z}/d\mathbb{Z} \setminus \{0\} & \text{if } d \text{ is odd,} \end{cases}$$

$$S_f = \{a \in S \mid d/2 < a < d\}, \quad S_v = \{a \in S \mid 0 < a < d/2\},$$

and the permutation $\pi : S \to S$ given by $\pi(a) = pa$.

Proof. This is immediate from Oda's Theorem (Equation (5.2)), Proposition 5.1, and Section 4.3. □

Remark 5.3. The proof of the theorem shows that $J_d[p]$ decomposes as a direct sum over the orbits of π on S. By Sections 3.2 and 4.3, the summand corresponding to an orbit is indecomposable if and only if the word associated to the orbit is primitive.

Remark 5.4. The data $(S = S_f \cup S_v, \pi)$ also completely determines $J_d[p]$ up to isomorphism as a polarized BT_1 group scheme. Indeed, by Proposition 2.1, given any non-degenerate, alternating form on the BT_1 module defined by $(S = S_f \cup S_v, \pi)$, we may choose the isomorphism in the theorem so that it intertwines the given form with the polarization on $H^1_{dR}(\mathcal{C}_d)$ induced by the cup product.

5.4. **The p-torsion of Fermat curves.** In this section, we determine the BT_1 modules of the Jacobians of Fermat curves. We need this material to complete Theorem 1.1 when $p < 5$.

First, note that μ_d^2 acts on F_d via $(\zeta_1, \zeta_2) : (X, Y) \mapsto (\zeta_1 X, \zeta_2 Y)$. The cohomology $H = H^1_{dR}(F_d)$ decomposes into subspaces $H_{a,b}$ indexed by $(a, b) \in (\mathbb{Z}/d\mathbb{Z})^2$ on which $(\zeta_1, \zeta_2) \in \mu_d^2$ acts by $\zeta_1^a \zeta_2^b$. An argument parallel to Proposition 5.1 shows that $H_{a,b}$ is 1-dimensional if $(a, b) \in T$ and 0 otherwise, where

$$T = \left\{(a, b) \in (\mathbb{Z}/d\mathbb{Z})^2 \mid a \neq 0, b \neq 0, a + b \neq 0\right\}.$$

Moreover, setting

$$T_f = \{(a, b) \in S \mid a + b > d\}, \text{ and } T_v = \{(a, b) \in S \mid a + b < d\},$$

then F induces an isomorphism $F : H_{a,b} \to H_{pa,pb}$ if $(a, b) \in T_f$, and V induces an isomorphism $V : H_{pa,pb} \to H_{a,b}$ if $(a, b) \in T_v$. Consider the permutation $\sigma : T \to T$ given by $\sigma(a, b) = (pa, pb)$. We may associate words to elements of T and cyclic words to orbits of σ. As in Section 4.3, this defines a BT_1 module. Applying Oda's Theorem (5.2) proves that:

Theorem 5.5. *The module $M(J_{F_d}[p])$ is the BT_1 module associated to the data $(T = T_f \cup T_v, \sigma)$.*

5.5. **A Shimura variety perspective.** Another proof of Theorem 5.2 can be extracted from [8] as follows. By [15], J_d is an abelian variety with complex multiplication, and Proposition 5.1(1)–(2) reveals the CM type of J_d. The corresponding Shimura subvariety of $\mathcal{A}_g$ is zero-dimensional, so each point is a component of both the Newton stratification and the E-O stratification of the Shimura subvariety. Using [8, §1], one can compute the isomorphism type of $J_d[p]$ in terms of the CM type.

5.6. **Other related work.** The curve $\mathcal{C}_d$ is hyperelliptic. When $p = 2$, Theorem 5.2 is a special case of [4], where the authors compute the BT_1 module and E–O type for all hyperelliptic curves in characteristic 2. When p is odd, Devalapurkar and Halliday compute the action of F and V on the mod p Dieudonné module for every hyperelliptic curve [2]. However, it appears to be difficult to deduce Theorem 5.2 from their result because it describes the actions of F and V by unwieldy formulas. Our work gives them essentially as permutation matrices.

In [9], the author gives a method for computing the BT_1 module of a smooth complete intersection curve over a field whose characteristic is greater than the largest of the multidegrees. This method can be used to recover a version of Theorem 5.2 for the Fermat curve F_d in characteristic p when $d < p$. However, this is not adequate to prove Theorem 1.1 because most BT_1 modules do not appear in Jacobians of Fermat curves of degrees $d < p$.

6. Proof of Theorem 1.1

We will prove most cases of Theorem 1.1 by considering the Fermat quotient curve $\mathcal{C}_d$ for d of the form $p^\ell - 1$. When $p < 5$, we also need the Fermat curve F_d and an auxiliary fiber product.

6.1. **p-adic digits.** Fix a positive integer ℓ and let $d = p^\ell - 1$. As before, let

$$S = \begin{cases} \mathbb{Z}/d\mathbb{Z} \setminus \{0, d/2\} & \text{if } d \text{ is even,} \\ \mathbb{Z}/d\mathbb{Z} \setminus \{0\} & \text{if } d \text{ is odd,} \end{cases}$$

$$S_f = \{a \in S \mid d/2 < a < d\}, \quad S_v = \{a \in S \mid 0 < a < d/2\},$$

and let the permutation $\pi : S \to S$ be given by $\pi(a) = pa$. Given $a \in S$, consider the p-adic expansion of its least positive residue:

$$a = a_0 + a_1 p + \cdots + a_{\ell-1} p^{\ell-1},$$

where $a_i \in \{0, \ldots, p-1\}$. We exclude: $a = 0$ (all $a_i = 0$); $a = d$ (all $a_i = p-1$); and, if p is odd, $a = d/2$ (all $a_i = (p-1)/2$). Note that

$$pa \equiv a_{\ell-1} + a_0 p + \cdots + a_{\ell-2} p^{\ell-1} \pmod{d},$$

so π corresponds to permuting the digits of a cyclically.

By definition, $a \in S_v$ if and only if $0 < a < d/2$. In terms of digits, this holds if and only if

$$\begin{aligned} &a_{\ell-1} < (p-1)/2, \text{ or} \\ &a_{\ell-1} = (p-1)/2 \quad \text{and} \quad a_{\ell-2} < (p-1)/2, \text{ or} \\ &a_{\ell-1} = a_{\ell-2} = (p-1)/2 \quad \text{and} \quad a_{\ell-3} < (p-1)/2, \text{ or } \ldots. \end{aligned}$$

In other words, the condition is that the first p-adic digit to the left of $a_{\ell-1}$ (inclusive) which is not $(p-1)/2$ is in fact less than $(p-1)/2$.

Similarly $a \in S_f$ if and only if $a > d/2$. This holds if and only if the first p-adic digit to the left of $a_{\ell-1}$ (inclusive) which is not $(p-1)/2$ is in fact greater than $(p-1)/2$.

For $a \in S$, let λ be the size of the orbit of π through a. We say that a is *primitive* if $\lambda = \ell$. It is clear that a is primitive if $gcd(d, a) = 1$. More generally, a fails to be primitive if and only if $d/\gcd(d, a)$ divides $p^\lambda - 1$ for some $\lambda < \ell$. Note that a primitive does not imply that w_a is primitive.

Let $w_a = u_{\lambda-1} \cdots u_0$ be the word attached to a as in Section 4.2. The discussion above shows that $u_j = v$ if and only if the first p-adic digit of a to the left of $a_{\ell-1-j}$ (inclusive) which is not $(p-1)/2$ is in fact less than $(p-1)/2$. (Finding the first such digit may require "wrapping around," i.e., passing from a_0 to $a_{\ell-1}$.)

Using these observations, we may write down elements $a \in S$ with given words:

Proposition 6.1. *Suppose w is a word of length $\ell > 1$.*

(1) *If w is primitive, then there is an element $a \in S$ such that $w_a = w$.*
(2) *If $p > 3$ and w is any word (not necessarily primitive), then there is an element $a \in S$ such that $w_a = w$.*

Proof. (1) Let $w = u_{\ell-1} \cdots u_0$ be a primitive word of length $\ell > 1$. For $0 \le j < \ell$, set

$$a_j = \begin{cases} 0 & \text{if } u_{\ell-1-j} = v, \\ p-1 & \text{if } u_{\ell-1-j} = f. \end{cases}$$

Since w is primitive, and in particular not equal to f^ℓ nor to v^ℓ, the integer $a = a_0 + \cdots + a_{\ell-1}p^{\ell-1}$ defines an element of S, and it is clear that $w_a = w$.

(2) If $w = v^\ell$ (resp. $w = f^\ell$), we may take $a = 1$ (resp. $a = d-1$). (Here we use $p > 2$.) For any other word, the recipe in the preceding paragraph yields an element of S. However, if w is not primitive, say $w = w'^e$, this element is not what we need because its word is w'. Modify a as follows: choose j so that $a_j = 0$ (which exists because $w \neq v^\ell$), and change a_j to 1. Then the new a is primitive (because exactly one of its digits is 1) and satisfies $w_a = w$. (Here we use that $1 < (p-1)/2$, i.e., $p > 3$.) This completes the proof of the proposition. □

Remark 6.2. In [12], we give a more refined analysis and compute the number of $a \in S$ with $w_a = w$ for any w, p, and ℓ. It turns out that the restriction on p in part (2) is essential. If $p = 3$ and $e > 1$, then the word $(fv)^e$ is not the word associated to an element of S, and if $p = 2$, $e > 1$, and w' is non-trivial, then w'^e is also not associated to an element of S.

6.2. **Proof of Theorem 1.1, part (3).** Let G be an indecomposable BT_1 group scheme over k of order p^ℓ with $\ell > 1$. Then there is a primitive word w of length ℓ such that $M(G) \cong M(w)$. According to Proposition 6.1, there is an element $a \in S$ such that $w_a = w$. By Theorem 5.2, G appears as a direct factor of $J_d[p]$. Since $\mathcal{C}_d$ has genus $\lfloor (p^\ell - 2)/2 \rfloor$, this establishes the desired result for an indecomposable BT_1.

Now consider an indecomposable polarized BT_1 group scheme G. If G is indecomposable as a BT_1 group scheme (ignoring the pairing), the proof in the previous paragraph applies with the same bound on the genus. Otherwise, there is a primitive word w of length $\ell/2$ such that $M(G) \cong M(w) \oplus M(w^c)$. Let $d' = p^{\ell/2} - 1$

and let S' be the usual set for d':

$$S' = \begin{cases} \mathbb{Z}/d'\mathbb{Z} \setminus \{0\} & \text{if } d' \text{ is odd,} \\ \mathbb{Z}/d'\mathbb{Z} \setminus \{0, d/2\} & \text{if } d' \text{ is even.} \end{cases}$$

Since $\ell/2 > 1$, by Proposition 6.1, there is an element $a \in S'$ such that $w_a = w$ (and so $w_{-a} = w^c$). By Theorem 5.2, G is a direct factor of $J_{d'}[p]$. To confirm the bound on the genus, we note that $\mathcal{C}_{d'}$ has genus $\lfloor (p^{\ell/2} - 2)/2 \rfloor$.

In the polarized case, if G is a direct factor of $J_d[p]$, we check that the given pairing on G is induced from that of $J_d[p]$ using Oort's result (Proposition 2.1). The same argument applies if G is a direct factor of $J_{d'}[p]$. Write $J_d[p] \cong G \oplus G'$. Since $J_d[p]$ and G are self-dual, so is G'. By the existence part of Proposition 2.1, G and G' both admit polarizations, and by the uniqueness part, we may choose the isomorphism $J_d[p] \cong G \oplus G'$ so that the direct sum polarization on $G \oplus G'$ corresponds to the canonical polarization of $J_d[p]$.

This completes the proof of part (3) of Theorem 1.1.

The following result establishes Theorem 1.1, parts (1) and (2) for $p > 3$. Recall that J_d is the Jacobian of the curve $\mathcal{C}_d$ with affine equation $y^d = x(1-x)$.

Theorem 6.3. *If $p > 3$, then every BT_1 group scheme over k appears as a direct factor of $J_d[p]$ for an integer d of the form $d = p^\ell - 1$. The same holds for polarized BT_1 group schemes.*

Proof. Suppose that $p > 3$ and let G be a BT_1 group scheme over k. Let $\{(\overline{w}_i)^{e_i}\}$ be the multiset of distinct primitive cyclic words corresponding to G in the Kraft classification, and let ℓ_i be the length of $w_i^{e_i}$. Let $d_i = p^{\ell_i} - 1$ and let $S_i = \mathbb{Z}/d_i\mathbb{Z} \setminus \{0, d_i/2\}$ with the usual partition and permutation. According to part (2) of Proposition 6.1, there is an element $a \in S_i$ with $w_a = w_i^{e_i}$, and using Theorem 5.2, we conclude that the group scheme G_i with $M(G_i) \cong M(w_i^{e_i})$ appears as a direct factor of $J_{d_i}[p]$.

If d' divides d, then there is a natural quotient morphism $\pi : \mathcal{C}_d \to \mathcal{C}_{d'}$ of degree d/d', which is prime to p. The induced composition $J_{d'} \xrightarrow{\pi^*} J_d \xrightarrow{\pi_*} J_{d'}$ is multiplication by d/d' and therefore induces an isomorphism on $J_{d'}[p]$. Thus $J_{d'}[p]$ is a direct factor of $J_d[p]$.

Now let ℓ be the least common multiple of the ℓ_i (so that d_i divides $d = p^\ell - 1$ for all i). Using the maps $J_{d_i} \to J_d$ shows that each G_i is a direct factor of $J_d[p]$, and since the G_i have pairwise non-isomorphic indecomposable factors, $G = \oplus G_i$ is a direct factor of $J_d[p]$ as well. This completes the proof for BT_1 group schemes without polarization.

The polarized case follows from the unpolarized case and Proposition 2.1 by the same argument given at the end of the proof of part (3). This completes the proof of the theorem. □

The following result reproves Theorem 1.1, parts (1) and (2) for $p > 3$; it proves those results for $p = 3$, and it handles the main case for $p = 2$. Recall that J_{F_d} is the Jacobian of the Fermat curve with affine equation $X^d + Y^d = 1$.

Theorem 6.4.

(1) *If $p > 2$, then every BT_1 group scheme over k appears as a direct factor of $J_{F_d}[p]$ for an integer d of the form $d = p^\ell - 1$. The same holds for polarized BT_1 group schemes.*

(2) *The same is true if $p = 2$ as long as the group scheme has no factors of $\mathbb{Z}/2\mathbb{Z}$ or μ_2.*

Proof. Since $\mathcal{C}_d$ is a quotient of F_d by a group of order prime to p, the case $p > 3$ follows immediately from Theorem 6.3. Thus we assume $p = 2$ or 3. To handle these cases, we argue as in the proof of Theorem 6.3, where Theorem 5.5 plays the role of Theorem 5.2 and where the set T associated to the Fermat curve F_d plays the role of the set S associated to $\mathcal{C}_d$.

When $p = 3$, to prove (1), the essential point is to show that any word w appears as the word of an element of the set T associated to $d = 3^\ell - 1$ for a suitable ℓ. When $p = 2$, to prove (2), the essential point is to show that any word w which is not a power of f or a power of v appears as the word of an element of the set T associated to $d = 2^\ell - 1$ for a suitable ℓ.

Note that there is an injection $S \hookrightarrow T$ sending a to (a, a) which is compatible with the partitions $S = S_f \cup S_v$ and $T = T_f \cup T_v$ and intertwines the permutations π and σ. Thus, if $a \in S$ has word $w_a = w$, then the word of $(a, a) \in T$ satisfies $w_{(a,a)} = w$.

Consider the case where $p = 3$ and $w = f^\ell$ (resp. v^ℓ). It is no loss of generality to assume that $\ell > 1$, and in this case we may take $d = 3^\ell - 1$ and $a = (-1, -1)$ (resp. $a = (1, 1)$). Consideration of 3-adic digits shows that $w_a = v^\ell$ (resp. $w_a = f^\ell$). Thus we have produced the required elements of T when $p = 3$ and w is a power of f or v.

Finally, consider the case where $p = 2$ or 3 and w is not a power of f or a power of v. If w is primitive, part (1) of Proposition 6.1 gives an $a \in S$ with $w_{(a,a)} = w$. If w is not primitive, write $w = w'^e$ where $e > 1$ and w' is primitive of length λ. Let a' be the element of S associated to w as in the proof of Proposition 6.1, i.e., we use the digit 0 for v and the digit $p-1$ for f. Note that $w_{a'} = w_{(a',a')} = w'$. Since w is a power of w', consideration of digits shows that $a' \neq \pm 1$ and that $a' \neq d/2 \pm 1$. Thus $(a' + 1, a' - 1)$ is an element of T, and it is clear that $w_{(a'+1,a'-1)} = w$. Therefore every word of length ℓ which is not a power of f or a power of v arises as $w_{(a,b)}$ for a suitable $(a, b) \in T$, and this completes the proof of Theorem 6.4. □

6.3. **The case $p = 2$.** To finish the proof of Theorem 1.1, it remains to treat the case where $p = 2$ and G is a BT_1 group scheme over k with factors of $\mathbb{Z}/2\mathbb{Z}$ or μ_2. Write

$$G \cong (\mathbb{Z}/2\mathbb{Z})^{f_1} \oplus (\mu_2)^{f_2} \oplus G',$$

where G' is a BT_1 group scheme with no factors of $\mathbb{Z}/2\mathbb{Z}$ and no factors of μ_2. We have already proven that G' is a direct factor of $J_{F_d}[2]$ for a suitable value of d of the form $2^\ell - 1$. Choose one such value of d.

Let r be an odd positive integer and let X_r be the smooth, projective curve over k defined by

$$X_r : \qquad \left(x^2 - x\right)\left(z^r - 1\right) = 1.$$

One computes that X_r has genus $r - 1$, and by [13, Prop. 3.2], it is ordinary, i.e.,

$$J_{X_r}[2] \cong \left(\mathbb{Z}/2\mathbb{Z} \oplus \mu_2\right)^{r-1}.$$

Choose $r \geq \max\{f_1, f_2\} + 1$ and odd, and let F_1 be the Fermat curve of degree 1 (given by $X + Y = 1$). Consider the degree r projection $X_r \to F_1$ given by

$$(x, z) \mapsto (X = x, Y = 1 - x).$$

Define C as the fiber product of that projection and the degree d^2 projection $F_d \to F_1$. Since d and r are odd, $J_{X_r}[2]$ and $J_{F_d}[2]$ are direct factors of $J_C[2]$. Thus G' and $(\mathbb{Z}/2\mathbb{Z} \oplus \mu_2)^{r-1}$ are direct factors of $J_C[2]$. Since they have no indecomposable factors in common,

$$G \subset (\mathbb{Z}/2\mathbb{Z} \oplus \mu_2)^{r-1} \oplus G'$$

is a direct factor of $J_C[2]$. This completes the proof of the case $p = 2$ of Theorem 1.1.

Remark 6.5. Another approach to adding factors of $\mathbb{Z}/2\mathbb{Z}$ and μ_2 to G' is to use an argument similar to [7, Cor. 4.7]. Using that F_d has CM, so lies in the μ-ordinary locus, one finds curves C whose Newton polygon is that of F_d with additional segments of slopes 0 and 1 of arbitrarily large multiplicity f. Again using μ-ordinarity, one deduces that $G' \oplus (\mathbb{Z}/2\mathbb{Z} \oplus \mu_2)^f$ is a direct factor of $J_C[2]$, thus so is G. This method has the drawbacks that the curve C is no longer explicit and we have no control over its field of definition other than that it is a finite field.

Remark 6.6. A weaker version of parts (1) and (2) of Theorem 1.1 follows from the facts that each E–O stratum of $\mathcal{A}_g$ is non-empty and that every abelian variety A appears as a subvariety of a Jacobian J. However, we need $A[p]$ to be a direct factor of $J[p]$. If A has dimension ℓ, this can be verified when $p > 3$ and $p \geq \ell$, via the theory of Prym–Tyurin varieties [1, Corollary 12.2.4]. As discussed in Section 1, our proof avoids this restriction on p and gives more information about the curve.

Acknowledgment

Both authors thank the anonymous referee for a quick, thorough, and thoughtful review.

References

[1] Christina Birkenhake and Herbert Lange, *Complex abelian varieties*, 2nd ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 302, Springer-Verlag, Berlin, 2004, DOI 10.1007/978-3-662-06307-1. MR2062673

[2] S. Devalaparkur and J. Halliday, *The Dieudonné modules and Ekedahl–Oort types of Jacobians of hyperelliptic curves in odd characteristic*, Preprint, `arXiv:1712.04921`, 2017.

[3] Neil Dummigan, *The determinants of certain Mordell-Weil lattices*, Amer. J. Math. **117** (1995), no. 6, 1409–1429, DOI 10.2307/2375024. MR1363073

[4] Arsen Elkin and Rachel Pries, *Ekedahl-Oort strata of hyperelliptic curves in characteristic 2*, Algebra Number Theory **7** (2013), no. 3, 507–532, DOI 10.2140/ant.2013.7.507. MR3095219

[5] Jean-Marc Fontaine, *Groupes p-divisibles sur les corps locaux* (French), Société Mathématique de France, Paris, 1977. Astérisque, No. 47-48. MR0498610

[6] Hanspeter Kraft, *Kommutative algebraische Gruppen und Ringe* (German), Lecture Notes in Mathematics, Vol. 455, Springer-Verlag, Berlin-New York, 1975. MR0393051

[7] W. Li, E. Mantovan, R. Pries, and Y. Tang, *Newton polygon stratification of the Torelli locus in PEL-type Shimura varieties*, Preprint, to appear in Int. Math. Res. Not. IMRN `arXiv:1811.00604`, 2018.

[8] Ben Moonen, *Serre-Tate theory for moduli spaces of PEL type* (English, with English and French summaries), Ann. Sci. École Norm. Sup. (4) **37** (2004), no. 2, 223–269, DOI 10.1016/j.ansens.2003.04.004. MR2061781

[9] Ben Moonen, *Computing discrete invariants of varieties in positive characteristic I: Ekedahl–Oort types of curves*, Preprint, 2020.

[10] Tadao Oda, *The first de Rham cohomology group and Dieudonné modules*, Ann. Sci. École Norm. Sup. (4) **2** (1969), 63–135. MR241435

[11] Frans Oort, *A stratification of a moduli space of abelian varieties*, Moduli of abelian varieties (Texel Island, 1999), Progr. Math., vol. 195, Birkhäuser, Basel, 2001, pp. 345–416, DOI 10.1007/978-3-0348-8303-0_13. MR1827027

[12] Rachel Pries and Douglas Ulmer, *On BT_1 group schemes and Fermat curves*, New York J. Math. **27** (2021), 705–739. MR4250272
[13] Doré Subrao, *The p-rank of Artin-Schreier curves*, Manuscripta Math. **16** (1975), no. 2, 169–193, DOI 10.1007/BF01181639. MR376693
[14] Douglas Ulmer, *Explicit points on the Legendre curve III*, Algebra Number Theory **8** (2014), no. 10, 2471–2522, DOI 10.2140/ant.2014.8.2471. MR3298546
[15] André Weil, *Sur les périodes des intégrales abéliennes* (French), Comm. Pure Appl. Math. **29** (1976), no. 6, 813–819, DOI 10.1002/cpa.3160290620. MR422164
[16] Noriko Yui, *On the Jacobian variety of the Fermat curve*, J. Algebra **65** (1980), no. 1, 1–35, DOI 10.1016/0021-8693(80)90236-7. MR578793

Department of Mathematics, Colorado State University, Fort Collins, Colorado 80523
Email address: pries@math.colostate.edu

Department of Mathematics, University of Arizona, Tucson, Arizona 85721
Email address: ulmer@math.arizona.edu