Semistable models for modular curves and power operations for Morava E-theories of height 2

YIFEI ZHU

We construct an integral model for Lubin–Tate curves. These curves arise as moduli of finite subgroups of deformations of formal groups. In particular, they are p-adic completions of the modular curves $X_0(p)$ at a mod-p supersingular point. Our model is semistable in the sense that the only singularities of its special fiber are normal crossings. Given this model, we obtain a uniform presentation for the Dyer–Lashof algebras for Morava E-theories of height 2. These algebras are local moduli of power operations in elliptic cohomology.

Contents

1 Introduction **2**

1.1 Overview 2

1.2 Moduli of elliptic curves and of formal groups, and Theorem A 4

1.3 Moduli of Morava E-theory spectra and Theorem C 8

1.4 Acknowledgments 12

1.5 Outline for the rest of the paper 12

2 Modeling Morava E-theories of height 2 via moduli spaces of elliptic curves **13**

2.1 Models for an E-theory and Lubin–Tate curves of level 1 14

2.2 Models for power operations on E and Lubin–Tate curves of level $\Gamma_0(p)$ 15

Date: April 7, 2019.

2.3 Atkin–Lehner involution on the global moduli 17
2.4 h and α as deformation and norm parameters in the local moduli . . . 17
2.5 The norm parameters α and $\tilde{\alpha}$ near the cusps of $X_0(p)$ 19

3 Proof of Theorem A **25**

4 Proof of Theorems B and C **29**
4.1 The total power operation formula and the Adem relations 29
4.2 The commutation relations 30

References **32**

1 Introduction

1.1 Overview

Understanding various sorts of moduli spaces is central to contemporary mathematics. In algebraic geometry, (elliptic) modular curves parametrize elliptic curves equipped with level structures, which specify features attached to the group structure of an elliptic curve. Each type of level structures corresponds to a specific subgroup of the modular group $\mathrm{SL}_2(\mathbb{Z})$, which acts on the upper half of the complex plane. The complex-analytic model for a modular curve is the quotient of the upper-half plane by the action of such a subgroup, as a Riemann surface.

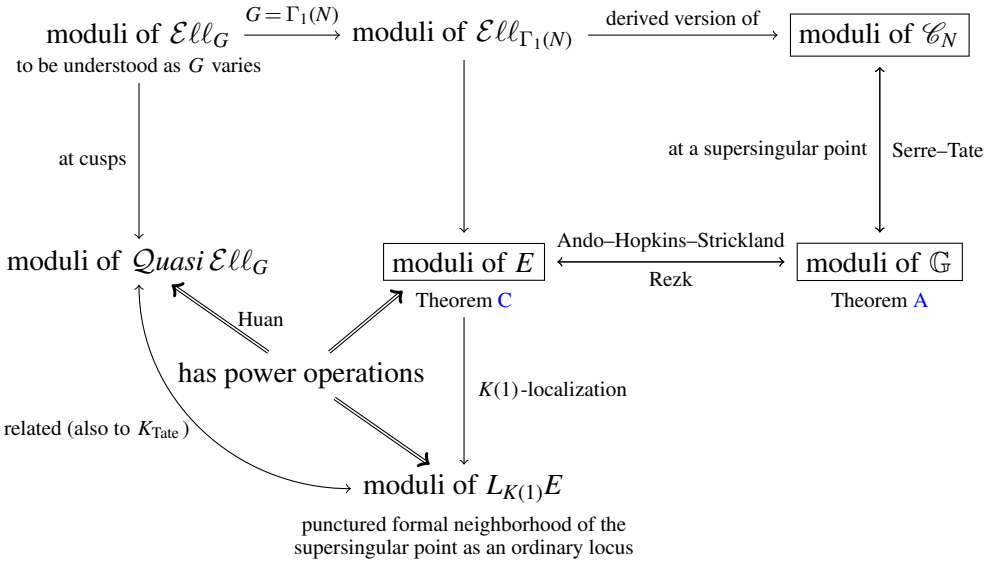
Over $\mathbb{Z}$, Deligne and Rapoport initiated the study of semistable models for the modular curves $X_0(Np)$ [Deligne–Rapoport1973, VI.6]. The affine curve $xy = p$ over $W(\overline{\mathbb{F}}_p)$ appeared in their work as a local model for $X_0(p)$ near a mod-p supersingular point. Recently, Weinstein produced semistable models for Lubin–Tate curves (at height 2) by passing to the infinite p^∞-level, when they each have the structure of a perfectoid space [Weinstein2016]. Such a Lubin–Tate curve is the rigid space attached to the p-adic completion of a modular curve at one of its mod-p supersingular points. Since the supersingular locus is the interesting part of the special fiber of a modular curve, Weinstein's work essentially provides semistable models for $X(Np^m)$. His affine

models include curves with equations $xy^q - x^q y = 1$ and $y^q + y = x^{q+1}$ over $\overline{\mathbb{F}}_q$, where q is a power of $p \neq 2$.

In this paper, with motivation from algebraic topology, we construct a new semistable model over $W(\overline{\mathbb{F}}_p)$ for the modular curve $X_0(p)$ near a mod-p supersingular point. The equation (see (1.3) below) for our integral affine model is more complicated than that of the Deligne–Rapoport model, while it reduces modulo p to $x(y - x^p) = 0$. The integral modular equation is essential to our application that produces an explicit presentation for the Dyer–Lashof algebra of a Morava E-theory at height 2, uniform with all p.

The Dyer–Lashof algebra governs power operations on Morava E-theory as a generalized cohomology theory [Rezk2009]. Since cohomology operations are natural transformations between functors, this algebra is a moduli space. Indeed, over the sphere spectrum $\mathbb{S}$, Morava E-theories are topological realizations of Lubin–Tate curves of level 1. Their operations are thus parametrized by Lubin–Tate curves of higher levels.

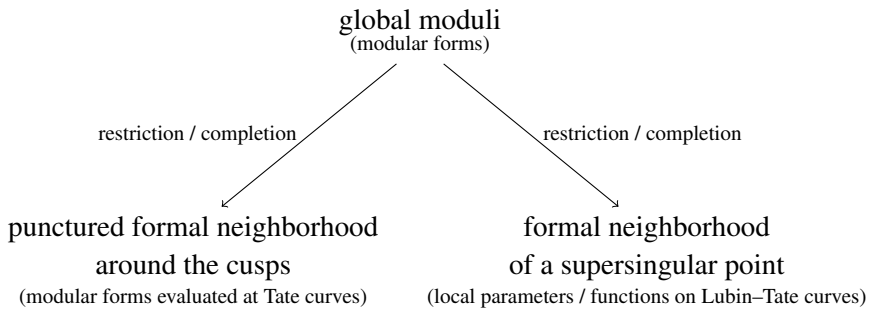
To be more precise, our results fit into the following framework.



In this diagram, the arrows between the boxed regions establish the aforementioned correspondences among modular curves, Lubin–Tate curves, and Dyler–Lashof algebras [Lubin–Serre–Tate1964, Ando–Hopkins–Strickland2004, Rezk2009]. Here, E is a Morava E-theory spectrum of height 2 at the prime p, $\mathbb{G}$ is the formal group of E as a Lubin–Tate universal deformation, and $\mathscr{C}_N$ is a universal ellip-

tic curve equipped with a level-$\Gamma_1(N)$ structure whose formal group is isomorphic to $\mathbb{G}$ (see Section 2 below). Conjecturally, the moduli of E should be the restriction of a moduli for a suitable equivariant elliptic cohomology theory $\mathcal{E}\ell\ell_G$ [Lurie2009, Schwede2018, Huan2018, Rezk2013b].

This paper represents an attempt to understand the above picture by working explicitly through the boxed regions. To obtain the local model for $X_0(p)$, our strategies can be summarized in the following diagram (cf. Figure 3.6 below). Here, we exploit the effectiveness of a modular form in terms of its calculable invariants, i.e., its weight, level, and a finite number of its first Fourier coefficients.



We now explain our main results in more detail and state the theorems in Sections 1.2 and 1.3, respectively, concerning aspects of algebraic geometry and algebraic topology.

1.2 Moduli of elliptic curves and of formal groups, and Theorem A

Known to Kronecker, the congruence

$$(j-\widetilde{j}^p)(\widetilde{j}-j^p)\equiv 0 \mod p \tag{1.1}$$

gives an equation for the modular curve $X_0(p)$ that represents (in a relative sense, cf. Section 2.2 below) the moduli problem $[\Gamma_0(p)]$ for elliptic curves over a perfect field of characteristic p. As a functor, this moduli problem associates to such an elliptic curve its finite flat subgroup schemes of rank p. A choice of such a subgroup scheme is equivalent to a choice of an isogeny from the elliptic curve with a prescribed kernel. The j-invariants of the source and target curves along this isogeny are parametrized by j and $\widetilde{j}$.

More precisely, this Kronecker congruence provides a *local* description for $[\Gamma_0(p)]$ at a supersingular point. For large primes p, the mod-p supersingular locus may consist

of more than one closed point. In this case, $X_0(p)$ does not have an equation in the simple form above. Only its completion at a single supersingular point has.

There are polynomials that describe $X_0(p)$ as a curve over $\mathrm{Spec}(\mathbb{Z})$. The computational algebra system `Magma` has Modular Polynomial Databases (`http://magma.maths.usyd.edu.au/magma/handbook/modular_curves`). There, *classical modular polynomials* lift and globalize the Kronecker congruence. In contrast, *canonical modular polynomials* appear simpler with a different pair of parameters. Below is a sample of the latter, where the first three modular curves are of genus 0 and the fourth is of genus 1.

$$
\begin{aligned}
X_0(2)\quad & x^3+48x^2+(768-j)x+2^{12}\\
&\equiv x(x^2-j) \bmod 2\\
X_0(3)\quad & x^4+36x^3+270x^2+(756-j)x+3^6\\
&\equiv x(x^3-j) \bmod 3\\
X_0(5)\quad & x^6+30x^5+315x^4+1300x^3+1575x^2+(750-j)x+5^3\\
&\equiv x(x^5-j) \bmod 5\\
X_0(11)\quad & x^{12}-5940x^{11}+14701434x^{10}+(-139755\,j-19264518900)x^9\\
&+(723797800\,j+13849401061815)x^8+(67496\,j^2-1327909897380\,j\\
&-4875351166521000)x^7+(2291468355\,j^2+1036871615940600\,j\\
&+40005097771307 4380)x^6+(-5346\,j^3+4231762569540\,j^2\\
&-310557763459301490\,j+12247115445643361 5800)x^5\\
&+(161201040\,j^3+755793774757450\,j^2+17309546645642506200\,j\\
&+651339173406982 4031615)x^4+(132\,j^4-49836805205\,j^3\\
&+6941543075967060\,j^2-64815179429761398660\,j\\
&+104264884483130180036700)x^3+(468754\,j^4+51801406800\,j^3\\
&+214437541826475\,j^2+77380735840203400\,j\\
&+804140494949359194)x^2+(-j^5+3732\,j^4-4586706\,j^3\\
&+2059075976\,j^2-253478654715\,j+2067305393340)x+11^6\\
&\equiv x\left(x^{11}-j^2(j-1)^3\right) \bmod 11
\end{aligned}
$$

In these canonical modular polynomials for $X_0(p)$, the variable

$$x = x(z) := p^s\left[\frac{\eta(pz)}{\eta(z)}\right]^{2s} \tag{1.2}$$

where η is the Dedekind η-function and $s = 12/\gcd(p-1,12)$ (s equals the exponent

in the constant term of each polynomial). The Atkin–Lehner involution (see Section 2.3 below) sends x to p^s/x. Computing these polynomials can be difficult. As Milne warns in [Milne2017, Section 6], "one gets nowhere with brute force methods in this subject." Fortunately, for our purpose, we need only a suitable *local* (but still integral) equation for $X_0(p)$ completed at a single mod-p supersingular point. We shall present this equation as a variant of the above polynomials in j and x.

Recall from Section 1.1 that the above completion of $X_0(p)$ is a Lubin–Tate curve, which is a moduli space for formal groups. Indeed, there is a connection between the moduli of formal groups and the moduli of elliptic curves. This connection is based on the Serre–Tate theorem. It states that p-adically, the deformation theory of an elliptic curve is equivalent to the deformation theory of its p-divisible group [Lubin–Serre–Tate1964, Section 6]. In particular, the p-divisible group of a supersingular elliptic curve is formal. Thus the local information provided by the Kronecker congruence (and its integral lifts) becomes useful for understanding deformations of formal groups of height 2.

Lubin and Tate developed the deformation theory for one-dimensional formal groups of finite height [Lubin–Tate1966, esp. Theorem 3.1]. More recently, with motivation from algebraic topology, Strickland studied the classification of finite subgroups of Lubin–Tate universal deformations. In particular, he proved a representability theorem for this moduli of deformations [Strickland1997, Theorem 42]. The representing objects are Gorenstein affine formal schemes. We call them *Lubin–Tate curves of level* $\Gamma_0(p^m)$, where p^m is the rank of the subgroups.

Our first main result gives an explicit model for Lubin–Tate curves of level $\Gamma_0(p)$ over the Witt ring $W(\overline{\mathbb{F}}_p)$. The special fiber is *semistable* in the sense that its only singularities are normal crossings. This model describes the complete local ring of the modular curve $X_0(p)$ at a mod-p supersingular point in terms of generators and relations.

Let $\mathbb{G}_0$ be a formal group over $\overline{\mathbb{F}}_p$ of height 2 and let $\mathbb{G}$ be its universal deformation over the Lubin–Tate ring. For each $m \geq 0$, denote by A_m the ring that classifies degree-p^m subgroups of the formal group $\mathbb{G}$. It is the ring of functions on the Lubin–Tate curve of level $\Gamma_0(p^m)$. In particular, write $A_0 \cong W(\overline{\mathbb{F}}_p)[\![h]\!]$ for the Lubin–Tate ring.

Theorem A *The ring* $A_1 \cong W(\overline{\mathbb{F}}_p)[\![h,\alpha]\!]/\big(w(h,\alpha)\big)$ *is determined by the polynomial*

$$w(h,\alpha) = (\alpha - p)\big(\alpha + (-1)^p\big)^p - \big(h - p^2 + (-1)^p\big)\alpha \tag{1.3}$$

which reduces to $w(h,\alpha) \equiv \alpha(\alpha^p - h) \mod p$.

Remark 1.4 The rings A_m are denoted by $\mathscr{O}_{\mathrm{Sub}_m(\mathbb{G})}$ in [Strickland1997]. The letter h stands for "Hasse" in the Hasse invariant (see Section 2.4 below). Due to a different choice of parameters, the last congruence above is not in the form (1.1) of Kronecker's. Section 2.4 discusses definitions and details of the parameters. Remark 2.25 discusses dependence of (1.3) on the choices involved for different primes p.

Remark 1.5 Let $\widetilde{\alpha}$ denote the image of α under the Atkin–Lehner involution (see Section 2.3 below). We will show in (2.24) that $\alpha \cdot \widetilde{\alpha} = (-1)^{p-1}p$ (cf. $xy = p$ in the Deligne–Rapoport model in Section 1.1). Note that the product equals the constant term of (1.3) as a polynomial in α of degree $p+1$. Thus factoring out α from the equation $w(h,\alpha) = 0$, we obtain a congruence

$$h \equiv \alpha^p + \widetilde{\alpha} \mod p$$

This congruence is a manifest of the Eichler–Shimura relation $T_p \equiv F + V \mod p$ between the Hecke, Frobenius, and Verschiebung operators. This relation reinterprets the Kronecker congruence for the moduli problem $[\Gamma_0(p)]$ in characteristic p (cf. [Katz–Mazur1985, pages ix–x] and see the discussion of dual isogenies in Section 2.5). Below in this remark we will give an explanation for the congruence $h \equiv T_p\,\alpha \mod p$.

The polynomial $w(h,\alpha)$ can be viewed as a local variant of a canonical modular polynomial, whose parameters are the j-invariant j and an eta-quotient x (1.2). These parameters correspond to h and α respectively. Indeed, for the key step (3.3) in our proof of Theorem A below, we adapt a technique with q-expansions that appeared in [Choi2006, Example 2.4, esp. (2.4)]. There, Choi worked with an eta-quotient ϕ_p, which almost equals the image $\widetilde{x}$ of x under the Atkin–Lehner involution. This function ϕ_p corresponds to $\widetilde{\alpha}$ in (3.3). The function $j_m^{(p)}$ in his equation (2.4) equals j if $m = 1$. When $m = p$ and $u = 1$, it corresponds to $\widetilde{h}$ in (3.4).

The sequence $\{j_m^{(p)}\}_{m=1}^{\infty}$ is an example of (l,N)-*type sequences* [ibid., Definition 3.1]. The latter generalize $\{j_n^{(p)}\}_{n=1}^{\infty}$ where $p \in \{2,3,5,7,13\}$[1] from [Ahlgren2003] and $\{j_m\}_{m=0}^{\infty}$ from [Bruinier–Kohnen–Ono2004]. These sequences each consist of Hecke translates of Hauptmodul. This sort of Hecke translates explains the analogous relation $h \equiv T_p\,\alpha \mod p$ above.

For comparison and later reference, we summarize the parameters in this remark as follows.

[1]Here the constraint on p is necessary for univalence of (global) modular functions on *zero-genus* congruence subgroups. Cf. Lemma 3.2 below, where we remove this constraint by working with local functions.

	canonical polynomial			classical polynomial
global	$(j,\, x)$	$(\widetilde{j},\, \widetilde{x})$	$(j_p^{(p)} = T_p j,\, \phi_p)$	$(\widetilde{j},\, j)$
local	$(h \equiv T_p\, \alpha,\, \alpha)$	$(\widetilde{h},\, \widetilde{\alpha})$		$(\widetilde{h},\, h)$

Table 1.6: Parameters for $[\Gamma_0(p)]$

1.3 Moduli of Morava E-theory spectra and Theorem C

The Adem relations

$$\mathrm{Sq}^i \mathrm{Sq}^j = \sum_{k=0}^{\lfloor \frac{i}{2} \rfloor} \binom{j-k-1}{i-2k} \mathrm{Sq}^{i+j-k} \mathrm{Sq}^k \qquad 0 < i < 2j \tag{1.7}$$

describe the rule of multiplication (composition of cohomology operations) for the Steenrod squares Sq^i. These Steenrod squares are power operations in ordinary cohomology with $\mathbb{F}_2$-coefficients. In general, for ordinary cohomology with $\mathbb{F}_p$-coefficients, the collection of its power operations has the structure of a graded Hopf algebra over $\mathbb{F}_p$, called the *mod-p Steenrod algebra* (cf. Dyer–Lashof operations in, e.g., [Bruner et al.1986, Theorem III.1.1] and see (2.1) below).

Quillen's work connects complex cobordism and the theory of one-dimensional formal groups [Quillen1969]. This connection leads to a *height filtration* for the stable homotopy category, which has turned out to be a highly effective principle since the 1980s for organizing large-scale periodic phenomena in the stable homotopy groups of spheres [Devinatz–Hopkins–Smith1988, Hopkins–Smith1998, Ravenel1992]. The height of a formal group indicates the filtration level of its corresponding generalized cohomology theory. Ordinary cohomology theories with $\mathbb{F}_p$-coefficients fit into this framework of *chromatic homotopy theory*, as theories concentrated at height ∞.

The power operation algebras for cohomology theories at other chromatic levels have been studied as well. In particular, central to the chromatic viewpoint is a family of Morava E-theories, one for each finite height n at a particular prime p. More precisely, given any formal group $\mathbb{G}_0$ of height n over a perfect field of characteristic p, there is a Morava E-theory associated to the Lubin–Tate universal deformation of $\mathbb{G}_0$. Via Bousfield localizations, these Morava E-theories determine the chromatic filtration of the stable homotopy category.

There is a connection between (stable) power operations in a Morava E-theory E and deformations of powers of Frobenius on its corresponding formal group $\mathbb{G}_0$. This con-

nection is via Rezk's theorem, which is built on the work of Ando, Hopkins, and Strickland [Ando1995, Strickland1997, Strickland1998, Ando–Hopkins–Strickland2004]. It gives an equivalence of categories between (i) graded commutative algebras over a Dyer–Lashof algebra for E and (ii) quasicoherent sheaves of graded commutative algebras over the moduli problem of deformations of $\mathbb{G}_0$ and Frobenius isogenies [Rezk2009, Theorem B]. Here, the Dyer–Lashof algebra is a collection of power operations that governs all homotopy operations on commutative E-algebra spectra [Rezk2009, Theorem A].

At height 2, information from the moduli of elliptic curves allows a concrete understanding of the power operation structure on Morava E-theories. Rezk computed the first example of a presentation for an E-theory Dyer–Lashof algebra, in terms of explicit generators and quadratic relations analogous to the Adem relations (1.7) [Rezk2008]. Moreover, he gave a presentation, which applies to E-theories at all primes p, for the mod-p reduction of their Dyer–Lashof algebras [Rezk2012, 4.8]. Underlying this presentation is the Kronecker congruence (1.1) [Rezk2012, Proposition 3.15].

Our second main result provides an "integral lift" of Rezk's mod-p presentation, with a different set of generators, in the same sense that Theorem A above lifts the Kronecker congruence. We begin with the following as a stepping-stone to this result.

Let E be a Morava E-theory spectrum of height 2 at the prime p. There is an additive total power operation $\psi^p\colon E^0 \to E^0(B\Sigma_p)/I$, or $W(\overline{\mathbb{F}}_p)[\![h]\!] \to W(\overline{\mathbb{F}}_p)[\![h,\alpha]\!]\big/\big(w(h,\alpha)\big)$, where I is a transfer ideal.

Theorem B *With the above notation, the following statements hold.*

(i) *The polynomial $w(h,\alpha) = w_{p+1}\alpha^{p+1} + \cdots + w_1\alpha + w_0$, $w_i \in E^0$, can be given as (1.3) from Theorem A. In particular, $w_{p+1} = 1$, $w_1 = -h$, $w_0 = (-1)^{p+1}p$, and the remaining coefficients*

$$w_i = (-1)^{p(p-i+1)}\left[\binom{p}{i-1} + (-1)^{p+1}p\binom{p}{i}\right]$$

(ii) *The image $\psi^p(h) = \sum_{i=0}^{p} Q_i(h)\,\alpha^i = \alpha + \sum_{i=0}^{p}\alpha^i \sum_{\tau=1}^{p} w_{\tau+1}\,d_{i,\tau}$, where*

$$d_{i,\tau} = \sum_{n=0}^{\tau-1}(-1)^{\tau-n}\,w_0^n \sum_{\substack{m_1+\cdots+m_{\tau-n}=\tau+i \\ 1\le m_s\le p+1 \\ m_{\tau-n}\ge i+1}} w_{m_1}\cdots w_{m_{\tau-n}}$$

In particular, $Q_0(h) \equiv h^p \mod p$.

The above theorem leads to the second main result of the paper. Continue with the notation in Theorem B. Let Γ be the Dyer–Lashof algebra for E, which is the ring of additive power operations on $K(2)$-local commutative E-algebras.

Theorem C *The Dyer–Lashof algebra Γ admits a presentation as the associative ring generated over $E^0 \cong W(\overline{\mathbb{F}}_p)[\![h]\!]$ by elements Q_i, $0 \le i \le p$, subject to the following set of relations.*

(i) Adem relations

$$Q_k Q_0 = -\sum_{j=1}^{p-k} w_0^j \, Q_{k+j} Q_j - \sum_{j=1}^{p} \sum_{i=0}^{j-1} w_0^i \, d_{k,j-i} \, Q_i Q_j \qquad \text{for } 1 \le k \le p$$

where the first summation is vacuous if $k = p$.

(ii) Commutation relations

$$Q_i \, c = (Fc) \, Q_i \quad \text{for } c \in W(\overline{\mathbb{F}}_p) \text{ and all } i, \text{ with } F \text{ the Frobenius automorphism}$$

$$Q_0 \, h = e_0 + (-1)^{p+1} r \sum_{m=0}^{p-1} s^m e_{p+m+1} + (-1)^p \left(e_p + r \, e_{2p} + \sum_{m=1}^{p} s^m e_{p+m} \right)$$
$$+ \sum_{j=1}^{p-1} (-1)^{pj} \left[e_j + r \, s^{p-j} e_{2p} + r \sum_{m=0}^{p-j-1} s^m \left(e_{p+j+m} + (-1)^{p+1} e_{p+j+m+1} \right) \right]$$

$$Q_k \, h = (-1)^{p(p-k)} \binom{p}{k} \left(e_p + r \, e_{2p} + \sum_{m=1}^{p} s^m e_{p+m} \right) + \sum_{j=k}^{p-1} (-1)^{p(j-k)} \binom{j}{k} \Bigg[e_j$$
$$+ r \, s^{p-j} e_{2p} + r \sum_{m=0}^{p-j-1} s^m \left(e_{p+j+m} + (-1)^{p+1} e_{p+j+m+1} \right) \Bigg] \quad \text{for } 0 < k < p$$

$$Q_p \, h = e_p + r \, e_{2p} + \sum_{m=1}^{p} s^m e_{p+m}$$

where $r = h - p^2 + (-1)^p$, $s = p + (-1)^p$, and

$$e_n = \sum_{m=n}^{p+1} (-1)^{(p+1)(m-n)} \binom{m}{n} Q_{m-1}$$
$$+ \sum_{m=n}^{2p} (-1)^{(p+1)(m-n)} \binom{m}{n} \sum_{\substack{i+j=m \\ 0 \le i,j \le p}} \sum_{\tau=1}^{p} w_{\tau+1} \, d_{i,\tau} \, Q_j$$

the first summation for e_n being vacuous if $p+2 \le n \le 2p$, and being vacuous in its term $m = 0$ if $n = 0$.

The Dyer–Lashof algebra Γ has the structure of a twisted bialgebra over E^0. The "twists" are described by the commutation relations above. The product structure satisfies the Adem relations. Certain Cartan formulas give rise to the coproduct structure as follows.

Theorem D *Let A be any $K(2)$-local commutative E-algebra. There are additive individual power operations $Q_k\colon \pi_0(A) \to \pi_0(A)$, $0 \le k \le p$, which satisfy the following Cartan formulas as well as the Adem and commutation relations from Theorem C. For each $0 \le k \le p$, $Q_k(xy)$ equals the expression on the right-hand side of the commutation relation for $Q_k h$, where $r = h - p^2 + (-1)^p$ and $s = p + (-1)^p$ as above, and*

$$e_n = \sum_{m=n}^{2p} (-1)^{(p+1)(m-n)} \binom{m}{n} \sum_{\substack{i+j=m \\ 0 \le i,j \le p}} Q_i(x)\, Q_j(y)$$

Proof In Section 4.2 below proving Theorem C, we will present a proof for the commutation relations, in such a way that the same formal procedure applies to give the stated Cartan formulas. □

Remark 1.8 Theorems C and D recover corresponding earlier results in [Rezk2008, Zhu2014, Zhu2015] for $p = 2$, 3, and 5 respectively.

To be more precise, for $p = 3$, the presentations do not coincide but are equivalent. Cf. Example 2.17 and Definition 2.23 below after we discuss models for the total power operation ψ^p. The equivalency will be addressed in Remark 2.25. Theorem B was stated with respect to a particular basis for the target ring $E^0(B\Sigma_p)/I$ of ψ^p as a free module over E^0 of rank $p+1$. Theorem C was stated with respect to a particular basis for the Dyer–Lashof algebra Γ as an associative ring over E^0 on $(p+1)$ generators.

For $p = 5$, in [Zhu2015, Example 4.1], we did not completely determine the Dyer–Lashof algebra due to constraints with our earlier methods (cf. [ibid., Example 2.14]). The issue was that, after a quadratic extension of $\mathbb{F}_5$, the mod-5 Hasse invariant factors into a pair of Galois conjugates (see Example 2.18 below). We calculated with global modular forms instead of local functions on Lubin–Tate curves. Thus we were unable to determine the image under ψ^p of $h \in E^0$ (denoted ibid. by u_1, with h standing for the global Hasse invariant), which corresponds to a local deformation parameter at one of the two supersingular points. Nevertheless, in fact, the current and earlier presentations for the Dyer–Lashof algebra in this case agree formally. This agreement is a manifest of the functoriality, with respect to base field extension, of the Dyer–Lashof algebra as a moduli space.

Caution 1.9 In this paper, we use the word "model" for two distinct but closely related objects. One is an algebraic curve with an explicit defining equation as customary in algebraic geometry. The other is a set of data involving formal groups and elliptic curves that is designed to facilitate explicit calculations in algebraic topology (Definitions 2.3, 2.6, and 2.23).

Remark 1.10 Let E be a Morava E-theory of height n. Recent work of Behrens and Rezk on spectral algebra models for unstable v_n-periodic homotopy theory has identified (i) the completed E-homology of the n'th Bousfield–Kuhn functor applied to an odd-dimensional sphere with (ii) the E-cohomology of the $K(n)$-localized André–Quillen homology of the spectrum of cochains on the odd-dimensional sphere valued in the $K(n)$-local sphere spectrum [Behrens–Rezk2017, Theorem 8.1]. The former (i) computes unstable v_n-periodic homotopy groups of spheres via a homotopy fixed point spectral sequence of Devinatz and Hopkins. By calculations of Rezk, (ii) can be identified at heights $n = 1$ and $n = 2$ via another spectral sequence, whose E_2-page consists of Ext-groups of certain rank-one modules over the Dyer–Lashof algebra of E (see [Rezk2013a, Example 2.13]).

We have applied Theorems A and B in this context of *unstable* chromatic homotopy theory to make these Ext-groups more explicit in [Zhu2018], with subsequent work partly joint with Wang towards general patterns in higher chromatic levels after [Rezk2012, Weinstein2016].

1.4 Acknowledgments

The author would like to thank Mark Behrens, Elden Elmanto, Paul Goerss, Michael Hopkins, Zhen Huan, Tyler Lawson, Haynes Miller, Charles Rezk, Joel Specter, Guozhen Wang, and Zhouli Xu for helpful discussions and encouragements. This work was partly supported by the National Natural Science Foundation of China grant 11701263.

1.5 Outline for the rest of the paper

In Section 2, we collect, streamline, and provide an in-depth analysis of necessary preliminary materials from [Zhu2015, Sections 2.1–2.3 and 3.1]. The presentation here is self-contained.

After a brief discussion of the homotopy-theoretic setup, we present in Sections 2.1 and 2.2 *models* for Morava E-theories of height 2 and their power operations, which are built from data of formal groups and elliptic curves. Section 2.3 is an interlude on the Atkin–Lehner involution, which becomes important later. We then introduce parameters for the local formal moduli in Section 2.4 and give a detailed analysis of their behavior at the cusps of the global moduli, as summarized in Lemma 2.15 and Definition 2.23.

Sections 3 and 4 are devoted to proving the main theorems stated in Sections 1.2 and 1.3 above, respectively, for the moduli spaces in algebraic geometry and in algebraic topology. The key ingredients for the proof in Section 3 are Lemmas 2.15 and 3.2.

2 Modeling Morava E-theories of height 2 via moduli spaces of elliptic curves

Given a formal group $\mathbb{G}_0$ over $\overline{\mathbb{F}}_p$ of height 2, let E be the Morava E-theory spectrum associated to $\mathbb{G}_0/\overline{\mathbb{F}}_p$ by the Goerss–Hopkins–Miller theorem [Goerss–Hopkins2004]. We have

$$\pi_*(E) = W(\overline{\mathbb{F}}_p)[\![\mu_1]\!][\mu^{\pm 1}]$$

with $|\mu_1| = 0$ and $|\mu| = 2$.

Let $x_E \in \widetilde{E}^2(\mathbb{C}P^\infty)$ be a class that extends to a complex orientation of E. Then $E^*(\mathbb{C}P^\infty) \cong E^*[\![x_E]\!]$ and the formal scheme $\mathrm{Spf}\big(E^0(\mathbb{C}P^\infty)\big)$ has a group structure [Hopkins1999, Section 1]. In particular, $x_E \cdot \mu$ is a coordinate on this formal group, i.e., a uniformizer for its ring of functions [Ando2000, Definition 1.4 and Remark 1.7].

The degree-0 coefficient ring $E^0 = W(\overline{\mathbb{F}}_p)[\![\mu_1]\!]$ is the Lubin–Tate ring that classifies formal deformations of $\mathbb{G}_0$ [Lubin–Tate1966, Theorem 3.1]. The formal group $\mathrm{Spf}\big(E^0(\mathbb{C}P^\infty)\big)$ is the universal deformation $\mathbb{G}$ of $\mathbb{G}_0$ over E^0.

As an E_∞-ring spectrum, E affords power operations constructed from the extended power functors $D_m(-) := \big(-\big)^{\wedge_E m}_{h\Sigma_m}$ on E-modules, for each integer $m \geq 0$, of taking the m-fold smash product over E modulo the action of the symmetric group Σ_m up to homotopy.

In particular, we have the (additive) *total* p-power operation

$$\psi^p\colon\ E^0 \to E^0(B\Sigma_p)/I \tag{2.1}$$

where $I = \bigoplus_{0<i<p} \operatorname{im}\big(E^0(B\Sigma_i \times B\Sigma_{p-i}) \to E^0(B\Sigma_p)\big)$ is the ideal generated by images of transfers. It gives rise to *individual* power operations $Q_i\colon \pi_0(A) \to \pi_0(A)$, $0 \le i \le p$, for any $K(2)$-local commutative E-algebra A (see [Bruner et al.1986, Definition I.4.2] and [Zhu2014, Definition 3.5]).

2.1 Models for an E-theory and Lubin–Tate curves of level 1

Given such an E-theory above, to carry out explicit calculations for its power operations, we work with elliptic curves as models (cf. [Zhu2015, Sections 2.1–2.2]).

First, let C_0 be a supersingular elliptic curve over $\overline{\mathbb{F}}_p$. Its formal completion $\widehat{C}_0$ at the identity section is a formal group of height 2 over $\overline{\mathbb{F}}_p$. By [Lazard1955, Théorème IV], $\widehat{C}_0$ is isomorphic to $\mathbb{G}_0$.

Next, to associate an elliptic curve to the universal formal deformation $\mathbb{G}$ of $\mathbb{G}_0$, we apply the Serre–Tate theorem [Lubin–Serre–Tate1964] (cf. [Katz–Mazur1985, 2.9.1]) and construct a universal deformation of the elliptic curve C_0. For representability, we equip C_0 with a level-$\Gamma_1(N)$ structure, $N \ge 3$ and $p \nmid N$.

More precisely, consider the representable moduli problem $\mathscr{P}_N$ of isomorphism classes of smooth elliptic curves over $\mathbb{Z}[1/N]$ with a choice of a point of exact order N and a nonvanishing 1-form. Let $\mathscr{M}_N$ be its representing scheme,[2] which is of relative dimension 1 over $\mathbb{Z}[1/N]$. Let $\mathscr{C}_N$ be the universal elliptic curve over this modular curve $\mathscr{M}_N$. In general, for p and N large, the supersingular locus of $\mathscr{M}_N$ at p consists of more than one closed point, and C_0 is the fiber of $\mathscr{C}_N$ over one of them. By the Serre–Tate theorem, the formal completion $\widehat{\mathscr{C}}_N$ of $\mathscr{C}_N$ at the identity section is isomorphic to the universal formal deformation $\mathbb{G}$ of $\mathbb{G}_0 \cong \widehat{C}_0$.

Remark 2.2 From the above discussion in this subsection, we see that up to isomorphism, the E-theory E associated to $\mathbb{G}_0/\overline{\mathbb{F}}_p$ does not depend on the choice of C_0 and $\mathscr{C}_N$ which model its formal group $\mathbb{G}$.

Definition 2.3 ([Zhu2015, Definition 2.9]) Let E be a Morava E-theory of height 2 at the prime p. With notation as above, a *$\mathscr{P}_N$-model for E* is the following set of data:

Mod. 1 a supersingular elliptic curve C_0 over $\overline{\mathbb{F}}_p$;

Mod. 2 a universal deformation $\mathscr{C}_N$ of C_0 over $\mathscr{M}_N$;

[2] See [Mahowald–Rezk2009, Proposition 3.2] and [Zhu2015, Examples 2.1–2.2] for explicit presentations in the cases when $N = 3$, 4, and 5.

Mod. 3 a coordinate u on the formal group $\widehat{\mathscr{C}}_N$;

Mod. 4 an isomorphism between $\mathrm{Spf}(E^0)$ and the formal completion of $\mathscr{M}_N$ at the supersingular point corresponding to C_0; and

Mod. 5 an isomorphism between $\mathrm{Spf}\big(E^0(\mathbb{C}P^\infty)\big)$ and $\widehat{\mathscr{C}}_N$ as formal groups over E^0, which sends $x_E \cdot \mu$ to u.

As discussed above, the existence of the isomorphisms in Mod. 4 and Mod. 5 follows from the Lubin–Tate theorem combined with the Serre–Tate theorem.

The formal schemes in Mod. 4 are each of relative dimension 1 over the formal completion $\mathrm{Spf}\big(W(\overline{\mathbb{F}}_p)\big)$ of $\mathrm{Spec}(\mathbb{Z})$ at p. We call them *Lubin–Tate curves of level* 1 (the level-$\Gamma_1(N)$ structure is auxiliary for our purpose).

2.2 Models for power operations on E and Lubin–Tate curves of level $\Gamma_0(p)$

By work of Ando, Hopkins, Rezk, and Strickland, power operations on E correspond to finite flat subgroup schemes of $\mathbb{G}$, or equivalently, to isogenies from $\mathbb{G}$ [Rezk2009, Theorem B]. Thus, again via the Serre–Tate theorem, we model the latter by isogenies between elliptic curves in order to obtain explicit formulas for the power operations.

More precisely, as the base ring E^0 is p-local, we need only work with the moduli problems $[\Gamma_0(p^r)]$ of isomorphism classes of elliptic curves with a choice of degree-p^r subgroup scheme. It suffices to analyze $[\Gamma_0(p)]$ and its Atkin–Lehner involution.[3] Indeed, the ring of (additive) power operations on any Morava E-theory is *quadratic* [Rezk2017, Main Theorem and Proposition 4.10]: with ring multiplication given by composition, the p^r-power operations are generated by the p-power ones, subject to quadratic relations that describe products of two generators.

The moduli problem $[\Gamma_0(p)]$ is *relatively* representable over the moduli stack of elliptic curves [Katz–Mazur1985, 4.2 and 5.1.1]. In particular, the simultaneous moduli problem $\mathscr{P}_N \times [\Gamma_0(p)]$ is representable by a scheme $\mathscr{M}_{N,p}$, which is finite flat over $\mathscr{M}_N$ of degree $p+1$.

Remark 2.4 The scheme $\mathscr{M}_{N,p}$ is of relative dimension 1 over $\mathbb{Z}[1/N]$. It is commonly referred to as *the* modular curve of level $\Gamma_0(p)$, whose compactification is

[3] See [Katz–Mazur1985, 11.3.1] with more details below in Section 2.3.

denoted by $X_0(p)$ in the literature. Up to base change, this modular curve is independent of the rigidification by $\mathscr{P}_N$ (for representability), or by any other types of level-N structure (cf. [Katz1973, Chapter 1, esp. 1.13] where full level-$\Gamma(N)$ structures are used). Also cf. [Katz–Mazur1985, 13.4.7] where $\mathscr{P}$ rigidifies $[\Gamma_0(p)]$. In particular, varying N will not change the local equation for $\mathscr{M}_{N,p}$ as a scheme over $\mathscr{M}_N$.

Now, we construct a universal degree-p isogeny over $\mathscr{M}_{N,p}$ as follows (cf. [Zhu2015, Construction 2.11]). Over $\mathscr{M}_{N,p}$, let $\mathscr{G}_N^{(p)}$ be the universal example of a degree-p subgroup scheme of $\mathscr{C}_N$ and write $\mathscr{C}_N^{(p)} := \mathscr{C}_N/\mathscr{G}_N^{(p)}$ for the quotient elliptic curve. Define $\Psi_N^{(p)}\colon \mathscr{C}_N \to \mathscr{C}_N^{(p)}$ over $\mathscr{M}_{N,p}$ by the formula

$$\widetilde{u}\big(\Psi_N^{(p)}(P)\big) = \prod_{Q \in \mathscr{G}_N^{(p)}} u(P-Q) \tag{2.5}$$

where u is a coordinate on $\mathscr{C}_N$ at the identity O and $\widetilde{u}$ is the coordinate on $\mathscr{C}_N^{(p)}$ induced by u (see [Ando2000, Section 4.3]).

This isogeny $\Psi_N^{(p)}$ is a *deformation of Frobenius* in the sense that its restriction over the supersingular point is the Frobenius isogeny $\mathrm{Frob}\colon C_0 \to C_0^{(p)}$, as the p-torsion subgroup scheme $C_0[p] = 0$.

Definition 2.6 Let ψ^p be the total power operation on E in (2.1). With notation as above, a *$\mathscr{P}_N$-model for ψ^p* is the data of Mod. 1–5 together with the following:

- Mod. 6 a universal deformation $\Psi_N^{(p)}\colon \mathscr{C}_N \to \mathscr{C}_N^{(p)}$ of $\mathrm{Frob}\colon C_0 \to C_0^{(p)}$ over $\mathscr{M}_{N,p}$; and
- Mod. 7 an isomorphism over E^0 between $\mathrm{Spf}\big(E^0(B\Sigma_p)/I\big)$ and the formal completion of $\mathscr{M}_{N,p}$ at the supersingular point corresponding to C_0.

Remark 2.7 The existence of the isomorphism in Mod. 7 follows from Strickland's theorem on Morava E-theories of symmetric groups in terms of rings of functions on the formal moduli [Strickland1998, Theorem 1.1], combined with the Serre–Tate theorem.

The formal schemes in Mod. 7 are each of relative dimension 1 over $\mathrm{Spf}\big(W(\overline{\mathbb{F}}_p)\big)$ and finite flat of degree $p+1$ over $\mathrm{Spf}(E^0)$. We call them *Lubin–Tate curves of level* $\Gamma_0(p)$ (again, the auxiliary N is omitted).

2.3 Atkin–Lehner involution on the global moduli

Instead of a universal deformation of Frobenius, an alternative viewpoint for modeling the total p-power operation is through an Atkin–Lehner involution.

Let us consider a $\mathscr{P}_N$-model for ψ^p as in Definition 2.6. With notation from last subsection, there is an automorphism on $\mathscr{M}_{N,p}$, induced by the map

$$\left(\mathscr{C}_N,\, P_0,\, du,\, \mathscr{G}_N^{(p)}\right) \mapsto \left(\mathscr{C}_N/\mathscr{G}_N^{(p)},\, \Psi_N^{(p)}(P_0),\, d\widetilde{u},\, \mathscr{C}_N[p]/\mathscr{G}_N^{(p)}\right)$$

of simultaneous level-$\big(\mathscr{P}_N, \Gamma_0(p)\big)$ structures on (distinct) elliptic curves, where $\mathscr{C}_N[p]$ denotes the p-torsion subgroup scheme of $\mathscr{C}_N$ (cf. [Katz–Mazur1985, 11.2 and 11.3.1]). We call this automorphism an *Atkin–Lehner involution* in connection with Atkin and Lehner's theory of modular forms on $\Gamma_0(p)$ [Atkin–Lehner1970, Lemmas 7–10]. It is an involution since $\mathscr{C}_N[p] \subset \mathscr{C}_N$ is of degree p^2.

Given $\Psi_N^{(p)}$ on $\mathscr{C}_N$, the Atkin–Lehner involution of $\mathscr{M}_{N,p}$ induces an isogeny on the quotient curve $\mathscr{C}_N^{(p)} = \mathscr{C}_N/\mathscr{G}_N^{(p)}$, namely,

$$\widetilde{\Psi}_N^{(p)}\colon\ \mathscr{C}_N^{(p)} \to \mathscr{C}_N^{(p)}/\widetilde{\mathscr{G}}_N^{(p)}$$

where $\widetilde{\mathscr{G}}_N^{(p)} = \mathscr{C}_N[p]/\mathscr{G}_N^{(p)}$.

As the p-divisible group of $\mathscr{C}_N$ sits in a short exact sequence of its formal (connected) and étale components [Tate1967, (4) in Section 2.2], the Atkin–Lehner involution interchanges these two sorts of formal and étale degree-p subgroups.

Via the correspondences in Mod. 4 and Mod. 7, given any $x \in E^0$, $\psi^p(x)$ is the image $\widetilde{x}$ of x under the Atkin–Lehner involution.

Remark 2.8 Note that since ψ^p acts on the scalars $W(\overline{\mathbb{F}}_p) \subset E^0$ as the p-power Frobenius automorphism, it is *not* an involution for this subring.

Convention 2.9 Henceforth whenever we write a tilde $\sim$ over a symbol, we mean the analogue of this symbol under an Atkin–Lehner involution.

2.4 h and α as deformation and norm parameters in the local moduli

In [Katz–Mazur1985, 7.7–7.8], various pairs of parameters are proposed for the local ring of $[\Gamma_0(p)]$ at a supersingular point, when one views the moduli problem as an "open arithmetic surface" (cf. [ibid., page xiii and 5.1.1]). More explicitly, a presentation for

this local ring over a perfect field of characteristic p is given in [ibid., 13.4.7], which Rezk applied to produce a mod-p presentation for the ring of power operations on E in [Rezk2012, 4.8].

We shall give an *integral* presentation for the local ring of $[\Gamma_0(p)]$ in terms of the parameters T and $\mathbf{N}\big(X(P)\big)$ from [Katz–Mazur1985, 7.7].

The parameter T is a uniformizer for the Lubin–Tate ring that carries the universal formal deformation (cf. [ibid., 5.2 (Reg. 4)]). We therefore call it a *deformation parameter* for the local moduli of $[\Gamma_0(p)]$. Via Mod. 4, it corresponds to $\mu_1 \in E^0$.

Globally over the moduli, the *Hasse invariant at* p is a modular form over $\mathbb{F}_p$ of level 1 and weight $p-1$ (see [ibid., 12.4] and [Silverman2009, V §4]). Up to p-torsion, it lifts to an integral modular form on $\mathscr{C}_N/\mathscr{M}_N$ for all p and all $N \geq 3$ prime to p (see [Calegari2013, Theorem 1.8.1], [Buzzard2003, journal p. 35], and [Meier2016]).[4]

The Hasse invariant vanishes precisely over the mod-p supersingular locus. Its restriction to a formal neighborhood of a supersingular point equals a deformation parameter T [Katz–Mazur1985, 12.4.4].

Convention 2.10 For the reason above, henceforth we will write h (the initial letter of "Hasse") for a deformation parameter and also for its corresponding element in $E^0 \subset E^0(B\Sigma_p)/I$.

The other parameter $\mathbf{N}\big(X(P)\big)$ is constructed as a norm [ibid., 7.5.2], where X is a coordinate on the formal group of a universal elliptic curve, and P a point on the curve of exact order p (see [ibid., 5.4]). We call $\mathbf{N}\big(X(P)\big)$ a *norm parameter* for the local moduli of $[\Gamma_0(p)]$. Via Mod. 7, it should correspond to an element in $E^0(B\Sigma_p)/I$ whose powers generate this ring as a free module over E^0 of rank $p+1$ (the degree of $\mathscr{M}_{N,p}$ over $\mathscr{M}_N$) by Weierstrass preparation.

Observe that from the definition (2.5) of the universal degree-p isogeny $\Psi_N^{(p)}$ over $\mathscr{M}_{N,p}$, setting

$$\alpha := \prod_{Q \in \mathscr{G}_N^{(p)} - \{O\}} u(Q) \tag{2.11}$$

we obtain a norm parameter for $[\Gamma_0(p)]$ associated with the coordinate u. This $\Gamma_0(p)$-*norm* is a modular form on $\mathscr{C}_N/\mathscr{M}_{N,p}$. We will also write α for the aforementioned

[4] See also [Zhu2015, Example 2.6] for an explicit calculation of the Hasse invariant when $p=5$ and $N=4$ as well as an illustration of the global-local moduli. We will return to this calculation below in Example 2.18.

element in $E^0(B\Sigma_p)/I$ that corresponds to the restriction of this modular form over the formal neighborhood of the supersingular point.[5]

Thus $E^0 \cong W(\overline{\mathbb{F}}_p)[\![h]\!]$ and by Weierstrass preparation there exists a unique monic polynomial $w(h,\alpha)$ in α of degree $p+1$ with coefficients in E^0 such that

$$E^0(B\Sigma_p)/I \cong E^0[\alpha]\,/\big(w(h,\alpha)\big) = W(\overline{\mathbb{F}}_p)[\![h,\alpha]\!]\,/\big(w(h,\alpha)\big) \tag{2.12}$$

Remark 2.13 We observe that this norm parameter α is the multiple which defines the relative cotangent map at the identity along $\Psi_N^{(p)}$, that is, $\big(\Psi_N^{(p)}\big)^* d\tilde{u} = \alpha \cdot du$.

2.5 The norm parameters α and $\tilde{\alpha}$ near the cusps of $X_0(p)$

Given the geometric interpretation for the norm parameter α from Remark 2.13, we next consider the compactified moduli $\overline{\mathscr{M}}_{N,p}$ over $\overline{\mathscr{M}}_N$ and determine the values of α, as a modular form, at the cusps of $\overline{\mathscr{M}}_{N,p}$ (cf. [Katz1973, 1.13 and 1.11]).

Recall that $\overline{\mathscr{M}}_{N,p} - \mathscr{M}_{N,p}$ is finite étale over $\mathbb{Z}[1/N]$. Over $\mathbb{Z}[1/N,\zeta_N]$ with ζ_N a primitive N'th root of unity, it is a disjoint union of sections, called the cusps of $\overline{\mathscr{M}}_{N,p}$, two of which lie over each cusp of $\overline{\mathscr{M}}_N$. Among each pair of the two cusps, one is étale over $\overline{\mathscr{M}}_N$, which corresponds to the (étale) subgroups H_i of the Tate curve $\mathrm{Tate}(q^N)$ generated by $(\zeta_p^i\, q^{1/p})^N$, with ζ_p a primitive p'th root of unity and $i = 0, 1, \ldots, p-1$. The other cusp is ramified over $\overline{\mathscr{M}}_N$, corresponding to the (formal) subgroup $\mathbb{\mu}_p$ of $\mathrm{Tate}(q^N)$ generated by ζ_p so that the quotient $\mathrm{Tate}(q^N)/\mathbb{\mu}_p = \mathrm{Tate}(q^{Np})$. These cusps appear in the literature as the unramified and ramified cusps of $X_0(p)$, respectively, without reference to the auxiliary level-N structure.

Recall from Section 2.3 that the Atkin–Lehner involution on $\mathscr{M}_{N,p}$ interchanges the two sorts of étale and formal degree-p subgroups of the p-divisible group. It thus extends to an automorphism on $\overline{\mathscr{M}}_{N,p}$ which interchanges the two sorts of unramified and ramified cusps, respectively.

[5] This is a footnote intended for the expert. In [Zhu2014, Zhu2015], we chose distinct symbols κ for the modular form constructed as a $\Gamma_0(p)$-norm, and α for the modular function as a multiple of κ by modular unit of weight p, passing from a weighted projective space to one of its affine local charts (cf. last footnote). As this perspective is not involved with addressing the central problem of the current paper, to ease notation and make the exposition more accessible, here we have suppressed the difference of symbols. This global-to-local procedure underlies Mod. 4, Mod. 5, and Mod. 7 as well as the choice of a nonvanishing 1-form in the moduli problem $\mathscr{P}_N$ (cf. [Katz–Mazur1985, 8.1.7.1], we work locally with $\mathbb{G}_m\backslash\mathscr{P}_N = \mathbb{G}_m\backslash\big(\Gamma_1(N)\times[\omega]\big) = \Gamma_1(N)$ auxiliary to $[\Gamma_0(p)]$).

In [ibid., 1.11], to discuss Hecke operators, Katz gave a detailed analysis of the degree-p isogenies π from Tate(q^N), each with one of the above subgroups as kernel. They are defined over the punctured formal neighborhood $\mathbb{Z}[1/N,\zeta_N][1/p,\zeta_p](\!(q^{1/p})\!)$ around the cusps. In particular, Katz calculated the cotangent maps to their dual isogenies $\check{\pi}$ and obtained $\check{\pi}^*(\omega_{\text{can}}) = \omega_{\text{can}}$ near the ramified cusps whereas $\check{\pi}^*(\omega_{\text{can}}) = p\cdot\omega_{\text{can}}$ near the unramified cusps [ibid., lines 4–5 on book p. 91]. Here, ω_{can} is the canonical 1-form on a Tate curve (cf. [Katz–Mazur1985, T.2 in 8.8]).

Recall from last subsection that the norm parameter α is the multiple which defines the cotangent map to the universal degree-p isogeny $\Psi_N^{(p)}$ over $\mathscr{M}_{N,p}$. We now determine the values of α, as a modular form, at the cusps from the above calculation of Katz. For this process, we need to carefully analyze the dual isogenies and 1-forms involved, by imposing conditions on the supersingular elliptic curve C_0 and the coordinate u on $\mathscr{C}_N$ of a $\mathscr{P}_N$-model as follows (cf. [Zhu2015, Section 3.1]).

Let us introduce the following strengthened version of Mod. 1:

Mod. 1^+ a supersingular elliptic curve C_0 over $\mathbb{F}_{p^2}$ whose p^2-power Frobenius endomorphism equals the map of multiplication by $(-1)^{p-1}p$, that is, $\text{Frob}^2 = (-1)^{p-1}[p]$.

Remark 2.14 By [Poonen2010], given any supersingular elliptic curve $C/\overline{\mathbb{F}}_p$, there exists such a C_0 isomorphic to C over $\overline{\mathbb{F}}_p$ (cf. [Baker et al.2005, Lemma 3.21], [Zhu2014, Remark 3.3], and [Rezk2012, 3.8]). In particular, the dual isogeny of $\text{Frob}\colon C_0 \to C_0^{(p)}$ is the Frobenius isogeny out of $C_0^{(p)}$ for all $p \neq 2$.

Lemma 2.15 *Let C_0 be in Mod. 1^+ and $\mathscr{C}_N$ be in Mod. 2. Then there exists a coordinate u^+ on $\mathscr{C}_N$ such that its associated modular form α in (2.11) equals p at the ramified cusps and $(-1)^{p-1}$ at the unramified cusps of $\overline{\mathscr{M}}_{N,p}$. The definition of u^+ may require an extension of scalars on $\mathscr{M}_{N,p}$.*

The proof is technical and will be given at the end of this section. Let us first move on to some examples.

Example 2.16 ([Rezk2008, Section 3]) Let $p = 2$ and $N = 3$. Rezk worked with a $\mathscr{P}_3$-model where $C_0\colon\ y^2 + y = x^3$ in Mod. 1^+, corresponding to the unique mod-2 supersingular point in the moduli. The universal curve $\mathscr{C}_3\colon\ y^2 + axy + y = x^3$ in Mod. 2 has a chosen 3-torsion point $(0,0)$ (cf. [Mahowald–Rezk2009, Proposition 3.2]). He then set $u = x/y$ in Mod. 3, which has the property in Lemma 2.15. Indeed, his deformation parameter a and norm parameter d satisfy $d^3 - ad - 2 = 0$. This

identity factors into $(d-2)(d+1)^2=0$ if $a=3$, which is an integral lift for the Hasse invariant 1 of the Tate curve.

Example 2.17 ([Zhu2014, Sections 2.1–3.1]) Let $p=3$ and $N=4$. We worked with a $\mathscr{P}_4$-model where $C_0\colon y^2+xy-y=x^3-x^2$ in Mod. 1 ($\mathrm{Frob}^2=[-3]$), corresponding to the unique mod-3 supersingular point in the moduli. The universal curve $\mathscr{C}_4\colon y^2+axy+aby=x^3+bx^2$ in Mod. 2 has a chosen 4-torsion point $(0,0)$. We set $u=x/y$ in Mod. 3. Our deformation parameter $h=a^2+b$ and norm parameter α satisfy $\alpha^4-6\alpha^2+(h-9)\alpha-3=0$, which factors into $(\alpha-3)(\alpha+1)^3=0$ if $h=1$.

Example 2.18 ([Zhu2015, Sections 2.1–2.3]) Let $p=5$ and $N=4$. We worked with a $\mathscr{P}_4$-model where $\mathscr{C}_4$ is the same curve as in Example 2.17. Its Hasse invariant at the prime 5 factors as

$$a^4-a^2b+b^2=\big(a^2+2(1+\eta)b\big)\big(a^2+2(1-\eta)b\big)$$

over $\overline{\mathbb{F}}_5$ with $\eta^2=2$. Thus the mod-5 supersingular locus consists of two closed points. We chose C_0 in Mod. 1^+ that corresponds to the first factor, and again $u=x/y$ in Mod. 3.

Setting $h=a^4-16a^2b+26b^2$ as an integral lift of the Hasse invariant above, we were only able to calculate that

$$\alpha^6-10\alpha^5+35\alpha^4-60\alpha^3+55\alpha^2-h\alpha+5=0 \tag{2.19}$$

where α is the (global) modular form constructed as a norm with the coordinate u. We were unable to deduce an equation for a lift of the factor $a^2+2(1+\eta)b$ of the Hasse invariant.

If we further set $h=26\equiv 1 \mod 5$, (2.19) then factors into $(\alpha-5)(\alpha-1)^5=0$. Thus u satisfies the property in Lemma 2.15. The relation (2.19) should specialize to one for the corresponding deformation and norm parameters at the chosen supersingular point.

Example 2.20 ([Rezk2015]) Let $p=5$ and $N=3$. We worked with a $\mathscr{P}_3$-model where $\mathscr{C}_3$ is the same curve as in Example 2.16. Its Hasse invariant at the prime 5 factors as

$$-a^4-a=-a(a+1)(a^2-a+1)$$

Thus the mod-5 supersingular locus consists of three closed points. We chose C_0 in Mod. 1 that corresponds to the first factor ($\mathrm{Frob}^2=[-5]$) and $u=x/y$ in Mod. 3.

Setting $h = -a^4 + 19a$ as an integral lift of the Hasse invariant above, we calculated that

$$\alpha^6 - 5a\alpha^4 + 40\alpha^3 - 5a^2\alpha^2 - h\alpha - 5 = 0 \tag{2.21}$$

where α is the (global) modular form constructed as a norm with the coordinate u. This identity factors into $(\alpha+5)(\alpha-1)^5 = 0$ if we set $a = 3$ so that $h = -24 \equiv 1 \mod 5$. Again, the relation (2.21) should specialize to one for the corresponding deformation and norm parameters at the chosen supersingular point, which is equivalent to the relation from Example 2.18 as an equation for a Lubin–Tate curve of level $\Gamma_0(5)$.

Remark 2.22 The coordinate u^+ in Lemma 2.15 (and u in Example 2.17) should restrict to a distinguished coordinate on the formal group $\widehat{\mathscr{C}}_N$ as well as to one on the formal group of Tate(q^N), which was originally studied by Ando [Ando1995, Theorem 2.5.7]. We have given an exposition of this fact in [Zhu2015, Section 3.1], with more details and greater generality in [Zhu2017]. Our results in the current paper are independent of the existence of Ando's coordinates.

Definition 2.23 ([Zhu2015, Definition 3.8]) Let ψ^p be the total power operation on E in (2.1). Continuing with Definition 2.6, we call the following set of data a *preferred model for* ψ^p:

- Mod. 0 an integer $N \geq 3$ that is prime to p;
- Mod. 1^+ a supersingular elliptic curve C_0 over $\mathbb{F}_{p^2}$ whose p^2-power Frobenius endomorphism equals the map of multiplication by $(-1)^{p-1}p$, that is, $\mathrm{Frob}^2 = (-1)^{p-1}[p]$;
- Mod. 2 a universal deformation $\mathscr{C}_N$ of C_0 over $\mathscr{M}_N$;
- Mod. 3^+ a coordinate u on the formal group $\widehat{\mathscr{C}}_N$ which extends to a coordinate on $\mathscr{C}_N$ satisfying the property that the associated modular form of $\Gamma_0(p)$-norm equals p at the ramified cusps and $(-1)^{p-1}$ at the unramified cusps of $\overline{\mathscr{M}}_{N,p}$;
- Mod. 4 an isomorphism between $\mathrm{Spf}(E^0)$ and the formal completion of $\mathscr{M}_N$ at the supersingular point corresponding to C_0;
- Mod. 5 an isomorphism between $\mathrm{Spf}\big(E^0(\mathbb{C}P^\infty)\big)$ and $\widehat{\mathscr{C}}_N$ as formal groups over E^0, which sends $x_E \cdot \mu$ to u;
- Mod. 6 a universal deformation $\Psi_N^{(p)}\colon \mathscr{C}_N \to \mathscr{C}_N^{(p)}$ of $\mathrm{Frob}\colon C_0 \to C_0^{(p)}$ over $\mathscr{M}_{N,p}$; and

Mod. 7 an isomorphism over E^0 between $\operatorname{Spf}\big(E^0(B\Sigma_p)/I\big)$ and the formal completion of $\mathscr{M}_{N,p}$ at the supersingular point corresponding to C_0.

As discussed above, the existence of the curve in Mod. 1^+ follows from Remark 2.14 and the existence of the coordinate in Mod. 3^+ follows from Lemma 2.15.

Analogous to [Zhu2014, Corollary 3.2], note that given a preferred model we have

$$\alpha \cdot \widetilde{\alpha} = (-1)^{p-1}p \tag{2.24}$$

where $\widetilde{\alpha}$ is the Atkin–Lehner involution of the norm parameter α, itself also a norm parameter (cf. [Katz–Mazur1985, row 7 for $[\Gamma_0(p^n)]$ of table in 7.7]).

Remark 2.25 Given Definition 2.23, let us summarize at this point the dependence on the various choices made therein of the stated formulas in Theorems A, B, and C.

Up to isomorphism, the height-2 Morava E-theory spectrum E is independent of the choice Mod. 1^+ (or Mod. 1) by Lazard's theorem and the Goerss–Hopkins–Miller theorem, and independent of Mod. 2 by the Lubin–Tate theorem (Remark 2.2). In particular, different choices between Mod. 1 and Mod. 1^+ may result in different but equivalent formulas in the theorems (see, e.g., the case $p = 3$ in Remark 1.8).

The choice Mod. 2, i.e., for different values of N, does not affect the coefficients in the modular equation (1.3) as long as Mod. 1^+ (or Mod. 1) has been fixed (Remark 2.4). Consequently, the formulas in Theorems B and C are independent of N.

The choice Mod. 3^+ (or Mod. 3) does affect the coefficients in (1.3) as its parameter α is built explicitly using a coordinate u. Different choices result in different bases in Theorem B for the target ring $E^0(B\Sigma_p)/I$ of ψ^p as a free module over E^0, and different bases in Theorem C for the Dyer–Lashof algebra Γ as an associative ring over E^0. This choice Mod. 3^+ can in fact be further strengthened and made unique, though we do not need it to be so here (Remark 2.22).

The rest Mod. 4–7 of the list are formal, which will not affect the formulas once the choices above have been made.

As we shall see in the proofs of the theorems below in Sections 3 and 4, for a fixed prime p, all *preferred* models for ψ^p from Definition 2.23 will give the *same* formulas as stated in the theorems.

Proof of Lemma 2.15 Let $[X, Y, Z]$ be the homogeneous Weierstrass coordinates of $\mathscr{C}_N$, with the identity section $O = [0, 1, 0]$. Let $u = X/Y$ so that $u(O) = 0$. Then

locally u is a coordinate on the formal group $\widehat{\mathscr{C}}_N$ (cf. [Silverman2009, IV § 1]).

Let $\Psi_N^{(p)}\colon \mathscr{C}_N \to \mathscr{C}_N^{(p)}$ over $\mathscr{M}_{N,p}$ be the universal degree-p isogeny from (2.5) constructed using the above coordinate u. Recall from earlier in this subsection Katz's calculation of degree-p isogenies on $\mathrm{Tate}(q^N)$ over $\mathbb{Z}[1/N,\zeta_N][1/p,\zeta_p](\!(q^{1/p})\!)$. Up to a unique isomorphism σ_p, the universal isogeny $\Psi_N^{(p)}$ restricts over a punctured disc around a ramified cusp as

$$\pi_p\colon \mathrm{Tate}(q^N) \to \mathrm{Tate}(q^N)/\!\!/\mu_p = \mathrm{Tate}(q^{Np}), \qquad q \mapsto q^p$$

with $\widetilde{\pi}_p^*(\omega_{\mathrm{can}}) = \omega_{\mathrm{can}}$ and thus $\pi_p^*(\omega_{\mathrm{can}}) = p\cdot\omega_{\mathrm{can}}$. Around an unramified cusp $\Psi_N^{(p)}$ restricts up to a unique isomorphism σ_0 as

$$\pi_0\colon \mathrm{Tate}(q^N) \to \mathrm{Tate}(q^N)/H_0 = \mathrm{Tate}(q^{N/p}), \qquad q \mapsto q^{1/p}$$

with $\widetilde{\pi}_0^*(\omega_{\mathrm{can}}) = p\cdot\omega_{\mathrm{can}}$ and thus $\pi_0^*(\omega_{\mathrm{can}}) = \omega_{\mathrm{can}}$.

Let λ be the unit in $\mathbb{Z}[1/N,\zeta_N]$ such that du restricts to $\lambda\cdot\omega_{\mathrm{can}}$ on $\mathrm{Tate}(q^N)$. Let ν_p and ν_0 be the units in $\mathbb{Z}[1/N,\zeta_N][1/p,\zeta_p]$ such that $d\widetilde{u}$ restricts to $\nu_p\cdot\lambda^p\cdot\omega_{\mathrm{can}}$ on $\mathrm{Tate}(q^{Np})$ and to $\nu_0\cdot\lambda^p\cdot\omega_{\mathrm{can}}$ on $\mathrm{Tate}(q^{N/p})$. The latter two units arise from the isomorphisms σ_p and σ_0 respectively. Since $\left(\Psi_N^{(p)}\right)^* d\widetilde{u} = \alpha\cdot du$, comparing this identity to those in last paragraph, we see that $\alpha = \nu_p\lambda^{p-1}p$ at a ramified cusp and $\alpha = \nu_0\lambda^{p-1}$ at an unramified cusp.

On the other hand, over the chosen supersingular point in the $\mathscr{P}_N$-model, by construction $\Psi_N^{(p)}$ restricts to $\mathrm{Frob}\colon C_0 \to C_0^{(p)}$. Thus by rigidity [Katz–Mazur1985, 2.4.2] the identity $\mathrm{Frob}^2 = (-1)^{p-1}[p]$ from Mod. 1^+ lifts to

$$\widetilde{\Psi}_N^{(p)} \circ \Psi_N^{(p)} = \tau\circ(-1)^{p-1}[p] \tag{2.26}$$

where $\widetilde{\Psi}_N^{(p)}\colon \mathscr{C}_N^{(p)} \to \mathscr{C}_N^{(p)}/\widetilde{\mathscr{G}}_N^{(p)}$ is the Atkin–Lehner involution of $\Psi_N^{(p)}$ from Section 2.3, with $\widetilde{\mathscr{G}}_N^{(p)} = \mathscr{C}_N[p]/\mathscr{G}_N^{(p)}$, and $\tau\colon \mathscr{C}_N/\mathscr{C}_N[p] \to \mathscr{C}_N^{(p)}/\widetilde{\mathscr{G}}_N^{(p)}$ is the canonical isomorphism inducing the identity map on relative cotangent spaces. Comparing (2.26) to $\widetilde{\pi}_p\circ\pi_p = \widetilde{\pi}_0\circ\pi_0 = [p]$ around the cusps [Katz1973, last line on book p. 90 and lines 1–3 on p. 91], we see that $v_0\cdot v_p = (-1)^{p-1}$ as $\widetilde{v}_p = v_0$.

Set $u^+ := \nu_p^{-1/(p-1)}\lambda^{-1}\cdot u = -\nu_0^{-1/(p-1)}\lambda^{-1}\cdot u$. It is straightforward to check that the $\Gamma_0(p)$-norm α associated to this coordinate u^+ takes the desired values at the cusps. □

3 Proof of Theorem A

Choose any preferred model as in Definition 2.23. We may assume that the j-invariant for the supersingular point of this model lies in $\mathbb{F}_p$. In fact, by a theorem of Deuring (see [Cox2013, Theorem 14.18, combined with Proposition 14.15]), there exists a supersingular elliptic curve over $\mathbb{F}_p$ for every $p > 3$. This existence is also true for $p \leq 3$ as shown by explicit examples [Silverman2009, beginning of V § 4 and Example 4.5]. Thus the corresponding j-invariant lies in $\mathbb{F}_p$. Since the condition on Frob^2 in Mod. 1^+ involves at most a substitution of supersingular curves via an isomorphism over $\overline{\mathbb{F}}_p$ (see Remark 2.14), the chosen j-invariant remains in $\mathbb{F}_p$.

Let $j_0 \in \mathbb{Z}$ be a lift of this supersingular j-invariant.

In the scheme $\mathscr{M}_{N,p}$ representing the simultaneous moduli problem $\mathscr{P}_N \times [\Gamma_0(p)]$, consider a formal neighborhood U that contains this single supersingular point. Note that $U \cong \mathrm{Spf}(A_1)$ by the Serre–Tate theorem (see Remark 2.7).

Define a modular function $h := j - j_0$, where $j(z) = q^{-1} + 744 + O(q)$ with $q = e^{2\pi i z}$ as usual. Since j_0 lifts a supersingular j-invariant, h then serves as a deformation parameter for A_0 and A_1. Locally, modulo p, it is a restriction of the Hasse invariant (cf. [Katz–Mazur1985, 12.4.4]).

Let α be the norm parameter (locally near the supersingular point) for A_1 associated with Mod. 3^+ of this model. By Weierstrass preparation there exists a unique polynomial

$$w(h,\alpha) = \alpha^{p+1} + \sum_{i=0}^{p} w_i\, \alpha^i \tag{3.1}$$

with $w_i \in W(\overline{\mathbb{F}}_p)[\![h]\!]$ such that $A_1 \cong A_0[\alpha] \big/ \big(w(h,\alpha)\big)$ (cf. (2.12)).

Write $\widetilde{h}$ and $\widetilde{\alpha}$ for the images of h and α under the Atkin–Lehner involution. Note that, as a function on the Lubin–Tate curve $\mathrm{Spf}(A_1)$, $\widetilde{\alpha}$ is only locally defined over the moduli scheme $\mathscr{M}_{N,p}$. Nevertheless, by construction as a norm parameter, it is the restriction of a globally defined modular form (the local uniformizer u in the construction can be taken as a fraction x/y between the affine Weierstrass coordinates x and y, up to a constant unit depending only on the elliptic curve $\mathscr{C}_N$, cf. the proof of Lemma 2.15). This local function $\widetilde{\alpha}$ thus has a q-expansion (at the unramified cusp ∞), though it may differ from the expansion of the global function.

The following technical lemma is crucial to our proof of the theorem. We postpone its

proof to the end of the section.

Lemma 3.2 *The local function $\widetilde{\alpha}$ has a q-expansion*

$$\widetilde{\alpha}(z) = \mu_0\, q^{-1} + O(1) = \mu_0(q^{-1} + a_0) + O(q)$$

for some $\mu_0 \in W(\overline{\mathbb{F}}_p)^\times \cap \mathbb{Z}$ and $a_0 \in \mathbb{Z}$ such that $a_0 \equiv 744 - j_0 \mod p$.

By this lemma, for $2 \le i \le p$, there exist *constants* $\widetilde{w}_i \in p\mathbb{Z}$ such that

$$\widetilde{\alpha}^p + \widetilde{w}_p\, \widetilde{\alpha}^{p-1} + \cdots + \widetilde{w}_2\, \widetilde{\alpha} = \mu_0^p q^{-p} + O(1) \tag{3.3}$$

On the other hand, we have

$$\widetilde{h}\,(z) = j\,(pz) - j_0 = q^{-p} + O(1) \tag{3.4}$$

Comparing the two displays above, we then have

$$\widetilde{\alpha}^p + \widetilde{w}_p\, \widetilde{\alpha}^{p-1} + \cdots + \widetilde{w}_2\, \widetilde{\alpha} = \mu_0^p\, \widetilde{h} + K + O(q)$$

for some $K \in \mathbb{Z}$. Passing to the mod-p reduction of this identity, we see that $K \in p\mathbb{Z}$. Therefore, by an abuse of notation, we can instead choose a deformation parameter h such that

$$\widetilde{\alpha}^p + \widetilde{w}_p\, \widetilde{\alpha}^{p-1} + \cdots + \widetilde{w}_2\, \widetilde{\alpha} = \widetilde{h} + O(q)$$

without changing $\widetilde{\alpha}$ and $\widetilde{w}_i$ that we already obtained. Multiplying $\widetilde{\alpha}$ to both sides of this identity, we obtain

$$\widetilde{\alpha}^{p+1} + \widetilde{w}_p\, \widetilde{\alpha}^p + \cdots + \widetilde{w}_2\, \widetilde{\alpha}^2 = \widetilde{h}\, \widetilde{\alpha} + O(1) \tag{3.5}$$

We claim that the last term $O(1)$ is constant. In fact, since A_1 is a free module over A_0 of rank $p+1$, $\widetilde{\alpha}^{p+1}$ can be expressed as a linear combination of $\widetilde{\alpha}^i$, $0 \le i \le p$, with coefficients polynomials in $\widetilde{h}$ over $W(\overline{\mathbb{F}}_p)$. Given the q-expansions of $\widetilde{h}$ in (3.4) and of $\widetilde{\alpha}$ from Lemma 3.2, we see that the term $O(1)$ must be a constant integer, corresponding to the basis element $\widetilde{\alpha}^i$, $i = 0$, with coefficient an integer.

Thus the terms $\widetilde{w}_i$ and $O(1)$ in (3.5) are all constant integers.

Applying the Atkin–Lehner involution to (3.5), we then conclude that except for $i = 1$, the coefficients w_i in (3.1) are all constant integers. It remains to determine their values. We apply Lemma 2.15 and exploit holomorphicity of the modular functions w_i over the complex-analytic moduli scheme. For this holomorphicity, we evoke GAGA and the Lefschetz principle (cf. the first paragraph of [Katz1973, Introduction]). Specifically, we move from the formal neighborhood of the supersingular point to the cusps via the global functions as in Figure 3.6. The two pictures illustrate the same process

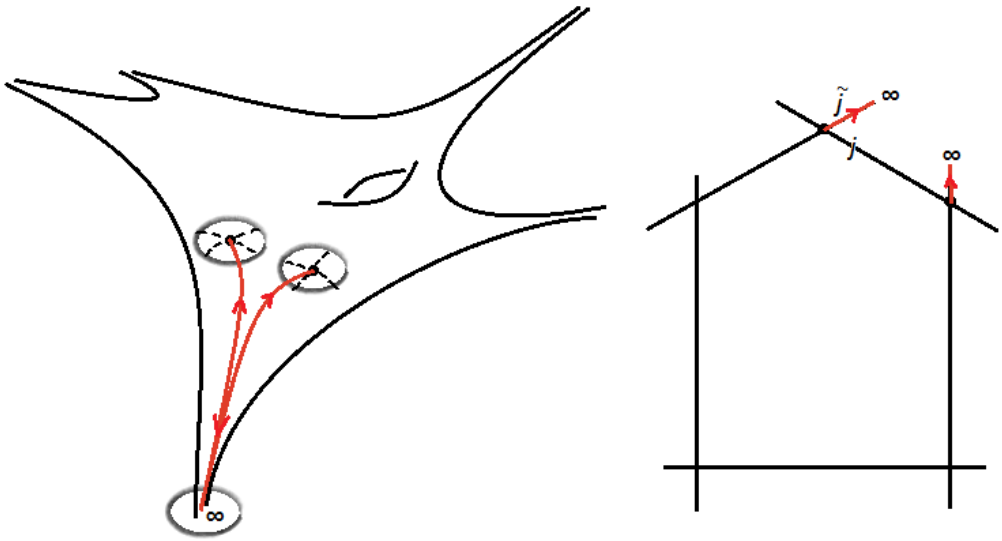


Figure 3.6: Transporting functions over the moduli

(cf. [Calegari2013, Figure 2] and [Deligne–Rapoport1973, book p. 290]) with $X_0(11)$ of genus 1 as an example. Explicitly, comparing the former local equation

$$\alpha^{p+1} + w_p\,\alpha^p + \cdots + w_2\,\alpha^2 - h\,\alpha + w_0 = 0$$

to the latter local equation

$$(\alpha - p)\big(\alpha - (-1)^{p-1}\big)^p = 0$$

we obtain the polynomial $w(h,\alpha)$ in Theorem A (h corresponds to $(-1)^{p^2+1} + p^2 \equiv 1 \mod p$, consistent with [Katz–Mazur1985, 12.4.2]). This completes the proof of Theorem A.

Proof of Lemma 3.2 First, note that $\widetilde{\alpha}$ has integral coefficients in its q-expansion, since α does by the q-expansion principle [Katz1973, Corollary 1.6.2] applied locally (in the sense above).

Recall from Remark 2.13 that the parameter α has a geometric interpretation as the multiple in the cotangent map along the p-power isogeny $\Psi_N^{(p)}\colon \mathscr{C}_N \to \mathscr{C}_N^{(p)} = \mathscr{C}_N/\mathscr{G}_N^{(p)}$. Under the Atkin–Lehner involution, the parameter $\widetilde{\alpha}$ then gives the cotangent map along $\widetilde{\Psi}_N^{(p)}\colon \mathscr{C}_N^{(p)} \to \mathscr{C}_N^{(p)}/\widetilde{\mathscr{G}}_N^{(p)}$ where $\widetilde{\mathscr{G}}_N^{(p)} = \mathscr{C}_N[p]/\mathscr{G}_N^{(p)}$. In particular, by rigidity, we have an identity

$$\widetilde{\Psi}_N^{(p)} \circ \Psi_N^{(p)} = \tau \circ (-1)^{p-1}[p]$$

that lifts $\mathrm{Frob}^2 = (-1)^{p-1}[p]$ over the supersingular point, where $\tau\colon \mathscr{C}_N/\mathscr{C}_N[p] \to \mathscr{C}_N^{(p)}/\widetilde{\mathscr{G}}_N^{(p)}$ is the canonical isomorphism. Thus, up to a unit in the global sections of $\mathscr{M}_{N,p}$, $\widetilde{\Psi}_N^{(p)}$ can be identified with the (Verschiebung) isogeny dual to the (Frobenius) isogeny $\Psi_N^{(p)}$ (cf. the proof of Lemma 2.15).

On the other hand, recall the Hasse invariant as defined in [Katz–Mazur1985, 12.4.1], modulo p, from the tangent map to Verschiebung. Since *locally* the deformation parameter $h = j - j_0$ is an integral lift of the Hasse invariant, we have

$$\widetilde{\alpha} \equiv \mu\, h \mod (p, \alpha) \tag{3.7}$$

for some unit $\mu \in A_0/(p)$. From this congruence, we deduce the q-expansion for $\widetilde{\alpha}$ as follows.

Let the lowest exponent of q in the expansion be $m \in \mathbb{Z}$.

Suppose $m < -1$. This leading term of $\widetilde{\alpha} \in A_1$ cannot come from an element in $h^2 \cdot A_0 \subset A_1$, because the neighborhood U contains a *single* supersingular point and a Hasse invariant has simple zeros (cf. [ibid., 12.4.3]). Thus it must come from an element in $\alpha \cdot A_1$.

Case 1. Let us suppose that the coefficient of q^m is not divisible by p. Since $\alpha \cdot \widetilde{\alpha} = (-1)^{p-1}p$ as in (2.24), the modular function α must then have a leading coefficient divisible by p, which leads to a contradiction (we deduced in last paragraph that the leading term of $\widetilde{\alpha}$ came from an element in $\alpha \cdot A_1$).

Case 2. If the coefficient of q^m is divisible by p, then $\alpha\cdot\widetilde{\alpha} = (-1)^{p-1}p$ implies that $\widetilde{\alpha} \equiv 0 \mod p$, as α becomes invertible in this case. This congruence is again a contradiction, since $\widetilde{\alpha}$ only becomes zero modulo p at precisely the closed supersingular point.

We have therefore shown that $m \geq -1$.

Now, by the argument from Case 2, we deduce that the coefficient of q^m is not divisible by p (there is no more contradiction in Case 1, now that $m \geq -1$). This time, $\alpha \cdot \widetilde{\alpha} = (-1)^{p-1}p$ implies that $\alpha \equiv 0 \mod p$,[6] as $\widetilde{\alpha}$ is invertible. Thus the congruence (3.7) strengthens to be

$$\widetilde{\alpha} \equiv \mu\, h \mod p$$

and the claimed q-expansion for $\widetilde{\alpha}$ follows. □

[6] More precisely, $\alpha \equiv 0 \mod p$ near the unramified cusps, not contradicting the stated congruence in Theorem A.

4 Proof of Theorems B and C

Theorem B (i) follows from [Strickland1998, Theorem 1.1]. We show the remaining parts in two steps below (Sections 4.1 and 4.2).

4.1 The total power operation formula and the Adem relations

To compute $\psi^p(h)$, we follow the recipe illustrated in [Zhu2015, Example 2.14] and generalize [ibid., proof of Proposition 4.4]. By (1.3) and (2.24), since

$$\begin{aligned} w(h,\alpha) &= w_{p+1}\alpha^{p+1} + \cdots + w_1\alpha + w_0 \\ &= w_{p+1}\alpha^{p+1} + \cdots - h\,\alpha + \widetilde{\alpha}\,\alpha \end{aligned}$$

is zero in the target ring of ψ^p, we have

$$h = w_{p+1}\alpha^p + \cdots + w_2\,\alpha + \widetilde{\alpha}$$

where $w_{p+1}, \ldots, w_2$ are constants, i.e., they do not involve h, as computed in Theorem B (i). Applying the Atkin–Lehner involution to this identity, we then obtain

$$\psi^p(h) = \widetilde{h} = w_{p+1}\,\widetilde{\alpha}^p + \cdots + w_2\,\widetilde{\alpha} + \alpha$$

For $1 \le \tau \le p$, we need only express each $\widetilde{\alpha}^\tau$ as a polynomial in α of degree at most p with coefficients in E^0. The constant terms $d_{0,\tau}$ of these polynomials have been computed as d_τ in [Zhu2015, proof of Proposition 4.4]. The same method there applies to give the stated formulas for the higher coefficients $d_{i,\tau}$ with $1 \le i \le p$.[7] This completes the proof of Theorem B.

To derive the Adem relations, we generalize [Zhu2014, proof of Proposition 3.6 (iv)] (cf. [Zhu2015, proof of Proposition 4.4]). In view of the relation $\alpha \cdot \widetilde{\alpha} = w_0$, we have

$$\begin{aligned} \psi^p\big(\psi^p(x)\big) &= \psi^p\Bigg(\sum_{j=0}^{p} Q_j(x)\,\alpha^j\Bigg) \\ &= \sum_{j=0}^{p} \psi^p\big(Q_j(x)\big)\,\psi^p(\alpha)^j \\ &= \sum_{j=0}^{p} \Bigg(\sum_{i=0}^{p} Q_iQ_j(x)\,\alpha^i\Bigg)\widetilde{\alpha}^j \end{aligned}$$

[7] In fact, those formulas hold for all $0 \le i \le p$ and $\tau \ge 1$ in expressing $\widetilde{\alpha}^\tau$ from α^i (with the convention that $w_\tau = 0$ if $\tau > p+1$).

$$= \sum_{j=0}^{p} \left(\sum_{i=0}^{j} w_0^i \, Q_i Q_j(x) \, \widetilde{\alpha}^{j-i} + \sum_{i=j+1}^{p} w_0^j \, Q_i Q_j(x) \, \alpha^{i-j} \right)$$
$$= \sum_{k=0}^{p} \alpha^k \left(\sum_{j=0}^{p} \sum_{i=0}^{j} w_0^i \, d_{k,j-i} \, Q_i Q_j(x) + \sum_{j=0}^{p-k} w_0^j \, Q_{k+j} Q_j(x) \right)$$

where $d_{k,0} = 0$ if $k > 0$ (and $d_{0,0} = 1$ from before). Write the expression in last line above as $\sum_{k=0}^{p} \Psi_k(x) \, \alpha^k$. For $1 \leq k \leq p$, the vanishing of each Ψ_k then gives the stated relation for $Q_k Q_0$.

4.2 The commutation relations

To facilitate computations, let us make a change of variables $\beta := \alpha + (-1)^p$. We then have

$$\begin{aligned}
\psi^p(hx) &= \psi^p(h) \, \psi^p(x) \\
&= \sum_{i=0}^{p} Q_i(h) \, \alpha^i \sum_{j=0}^{p} Q_j(x) \, \alpha^j \\
&= \sum_{m=0}^{2p} \left(\sum_{\substack{i+j=m \\ 0 \leq i,j \leq p}} Q_i(h) \, Q_j(x) \right) \alpha^m \\
&= \sum_{m=0}^{2p} \left(\sum_{\substack{i+j=m \\ 0 \leq i,j \leq p}} Q_i(h) \, Q_j(x) \right) \left(\beta + (-1)^{p+1} \right)^m \\
&= \sum_{m=0}^{2p} \left(\sum_{\substack{i+j=m \\ 0 \leq i,j \leq p}} Q_i(h) \, Q_j(x) \right) \sum_{n=0}^{m} \binom{m}{n} \beta^n (-1)^{(p+1)(m-n)} \\
&= \sum_{n=0}^{2p} e_n \, \beta^n
\end{aligned}$$

where

$$e_n = \sum_{m=n}^{2p} (-1)^{(p+1)(m-n)} \binom{m}{n} \sum_{\substack{i+j=m \\ 0 \leq i,j \leq p}} Q_i(h) \, Q_j(x)$$

Formulas for the terms $Q_i(h)$ above are given by Theorem B (ii). Note that $Q_1(h)$ includes a term of 1.

We now reduce $\psi^p(hx)$ above modulo $w(h,\alpha)$, by first rewriting the latter as a polynomial in β:

$$\begin{aligned} w(h,\alpha) &= (\alpha - p)\big(\alpha + (-1)^p\big)^p - \big(h - p^2 + (-1)^p\big)\alpha \\ &= \big(\beta + (-1)^{p+1} - p\big)\beta^p - \big(h - p^2 + (-1)^p\big)\big(\beta + (-1)^{p+1}\big) \\ &= \beta^{p+1} + v_p\,\beta^p + v_1\,\beta + v_0 \end{aligned}$$

where $v_p = (-1)^{p+1} - p$, $v_1 = -\big(h - p^2 + (-1)^p\big)$, and $v_0 = (-1)^{p+1}v_1$. We then carry out a long division of $\psi^p(hx)$ by $w(h,\alpha)$ with respect to β and obtain

$$\psi^p(hx) \equiv \sum_{j=0}^{p} f_j\,\beta^j \mod w(h,\alpha)$$

where

$$f_j = \begin{cases} e_p - v_1 e_{2p} + v_p \displaystyle\sum_{m=0}^{p-1} (-1)^{m+1} e_{p+1+m}\, v_p^m & j = p \\ e_j + v_0 \displaystyle\sum_{m=0}^{p-j-1} (-1)^{m+1} e_{p+j+1+m}\, v_p^m + v_1 \sum_{m=0}^{p-j} (-1)^{m+1} e_{p+j+m}\, v_p^m & 0 < j < p \\ e_0 + v_0 \displaystyle\sum_{m=0}^{p-1} (-1)^{m+1} e_{p+1+m}\, v_p^m & j = 0 \end{cases}$$

Thus we can rewrite

$$\begin{aligned} \psi^p(hx) &= \sum_{j=0}^{p} f_j \left(\alpha + (-1)^p\right)^j \\ &= \sum_{j=0}^{p} f_j \sum_{i=0}^{j} \binom{j}{i} \alpha^i\, (-1)^{p\,(j-i)} \\ &= \sum_{i=0}^{p} \left[\sum_{j=i}^{p} (-1)^{p\,(j-i)} \binom{j}{i} f_j \right] \alpha^i \end{aligned}$$

On the other hand, $\psi^p(hx) = \sum_{i=0}^{p} Q_i(hx)\,\alpha^i$. Comparing this identity to the last expression for $\psi^p(hx)$ above, term by term, we obtain the commutation relations as stated. This completes the proof of Theorem C.

References

[Ahlgren2003] Scott Ahlgren, *The theta-operator and the divisors of modular forms on genus zero subgroups*, Math. Res. Lett. **10** (2003), no. 6, 787–798. MR2024734

[Ando1995] Matthew Ando, *Isogenies of formal group laws and power operations in the cohomology theories E_n*, Duke Math. J. **79** (1995), no. 2, 423–485. MR1344767

[Ando2000] ———, *Power operations in elliptic cohomology and representations of loop groups*, Trans. Amer. Math. Soc. **352** (2000), no. 12, 5619–5666. MR1637129

[Ando–Hopkins–Strickland2004] Matthew Ando, Michael J. Hopkins, and Neil P. Strickland, *The sigma orientation is an H_∞ map*, Amer. J. Math. **126** (2004), no. 2, 247–334. MR2045503

[Atkin–Lehner1970] A. O. L. Atkin and J. Lehner, *Hecke operators on $\Gamma_0(m)$*, Math. Ann. **185** (1970), 134–160. MR0268123

[Baker et al.2005] Matthew H. Baker, Enrique González-Jiménez, Josep González, and Bjorn Poonen, *Finiteness results for modular curves of genus at least 2*, Amer. J. Math. **127** (2005), no. 6, 1325–1387. MR2183527

[Behrens–Rezk2017] Mark Behrens and Charles Rezk, *The Bousfield–Kuhn functor and topological André–Quillen cohomology*, available at `http://www3.nd.edu/~mbehren1/papers/BKTAQ8.pdf`.

[Bruinier–Kohnen–Ono2004] Jan H. Bruinier, Winfried Kohnen, and Ken Ono, *The arithmetic of the values of modular functions and the divisors of modular forms*, Compos. Math. **140** (2004), no. 3, 552–566. MR2041768

[Bruner et al.1986] R. R. Bruner, J. P. May, J. E. McClure, and M. Steinberger, *H_∞ ring spectra and their applications*, Lecture Notes in Mathematics, vol. 1176, Springer-Verlag, Berlin, 1986. MR836132

[Buzzard2003] Kevin Buzzard, *Analytic continuation of overconvergent eigenforms*, J. Amer. Math. Soc. **16** (2003), no. 1, 29–55. MR1937198

[Calegari2013] Frank Calegari, *Congruences between modular forms*, available at `http://swc.math.arizona.edu/aws/2013/2013CalegariLectureNotes.pdf`.

[Choi2006] D. Choi, *On values of a modular form on $\Gamma_0(N)$*, Acta Arith. **121** (2006), no. 4, 299–311. MR2224397

[Cox2013] David A. Cox, *Primes of the form $x^2 + ny^2$*, second ed., Pure and Applied Mathematics (Hoboken), John Wiley & Sons, Inc., Hoboken, NJ, 2013, Fermat, class field theory, and complex multiplication. MR3236783

[Deligne–Rapoport1973] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, 143–316. Lecture Notes in Math., Vol. 349. MR0337993

[Devinatz–Hopkins–Smith1988] Ethan S. Devinatz, Michael J. Hopkins, and Jeffrey H. Smith, *Nilpotence and stable homotopy theory. I*, Ann. of Math. (2) **128** (1988), no. 2, 207–241. MR960945

[Goerss–Hopkins2004] P. G. Goerss and M. J. Hopkins, *Moduli spaces of commutative ring spectra*, Structured ring spectra, London Math. Soc. Lecture Note Ser., vol. 315, Cambridge Univ. Press, Cambridge, 2004, pp. 151–200. MR2125040

[Hopkins1999] Mike Hopkins, *Complex oriented cohomology theories and the language of stacks*, available at http://web.math.rochester.edu/people/faculty/doug/otherpapers/coctalos.pdf.

[Hopkins–Smith1998] Michael J. Hopkins and Jeffrey H. Smith, *Nilpotence and stable homotopy theory. II*, Ann. of Math. (2) **148** (1998), no. 1, 1–49. MR1652975

[Huan2018] Zhen Huan, *Quasi-elliptic cohomology and its power operations*, J. Homotopy Relat. Struct. **13** (2018), no. 4, 715–767. MR3870771

[Katz1973] Nicholas M. Katz, *p-adic properties of modular schemes and modular forms*, Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1973, pp. 69–190. Lecture Notes in Mathematics, Vol. 350. MR0447119

[Katz–Mazur1985] Nicholas M. Katz and Barry Mazur, *Arithmetic moduli of elliptic curves*, Annals of Mathematics Studies, vol. 108, Princeton University Press, Princeton, NJ, 1985. MR772569

[Lazard1955] Michel Lazard, *Sur les groupes de Lie formels à un paramètre*, Bull. Soc. Math. France **83** (1955), 251–274. MR0073925

[Lubin–Serre–Tate1964] J. Lubin, J.-P. Serre, and J. Tate, *Elliptic curves and formal groups*, available at http://www.ma.utexas.edu/users/voloch/lst.html.

[Lubin–Tate1966] Jonathan Lubin and John Tate, *Formal moduli for one-parameter formal Lie groups*, Bull. Soc. Math. France **94** (1966), 49–59. MR0238854

[Lurie2009] J. Lurie, *A survey of elliptic cohomology*, Algebraic topology, Abel Symp., vol. 4, Springer, Berlin, 2009, pp. 219–277. MR2597740

[Mahowald–Rezk2009] Mark Mahowald and Charles Rezk, *Topological modular forms of level 3*, Pure Appl. Math. Q. **5** (2009), no. 2, Special Issue: In honor of Friedrich Hirzebruch. Part 1, 853–872. MR2508904

[Meier2016] Lennart Meier, *Lifting the Hasse invariant mod 2*, MathOverflow, http://mathoverflow.net/q/228497 (version: 2016-01-16).

[Milne2017] J.S. Milne, *Modular functions and modular forms*, available at http://www.jmilne.org/math/CourseNotes/MF.pdf.

[Poonen2010] Bjorn Poonen, *Supersingular elliptic curves and their "functorial" structure over $\mathbb{F}_{p^2}$*, MathOverflow, http://mathoverflow.net/a/19013 (version: 2010-03-22).

[Quillen1969] Daniel Quillen, *On the formal group laws of unoriented and complex cobordism theory*, Bull. Amer. Math. Soc. **75** (1969), 1293–1298. MR0253350

[Ravenel1992] Douglas C. Ravenel, *Nilpotence and periodicity in stable homotopy theory*, Annals of Mathematics Studies, vol. 128, Princeton University Press, Princeton, NJ, 1992, Appendix C by Jeff Smith. MR1192553

[Rezk2008] Charles Rezk, *Power operations for Morava E-theory of height 2 at the prime 2*. arXiv:0812.1320

[Rezk2009] ———, *The congruence criterion for power operations in Morava E-theory*, Homology, Homotopy Appl. **11** (2009), no. 2, 327–379. MR2591924

[Rezk2012] ———, *Modular isogeny complexes*, Algebr. Geom. Topol. **12** (2012), no. 3, 1373–1403. MR2966690

[Rezk2013a] ———, *Power operations in Morava E-theory: structure and calculations (Draft)*, available at `http://www.math.uiuc.edu/~rezk/power-ops-ht-2.pdf`.

[Rezk2013b] ———, correspondence, 2013.

[Rezk2015] ———, correspondence, 2015.

[Rezk2017] ———, *Rings of power operations for Morava E-theories are Koszul*. arXiv:1204.4831

[Schwede2018] Stefan Schwede, *Global homotopy theory*, New Mathematical Monographs, vol. 34, Cambridge University Press, Cambridge, 2018. MR3838307

[Silverman2009] Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR2514094

[Strickland1997] Neil P. Strickland, *Finite subgroups of formal groups*, J. Pure Appl. Algebra **121** (1997), no. 2, 161–208. MR1473889

[Strickland1998] ———, *Morava E-theory of symmetric groups*, Topology **37** (1998), no. 4, 757–779. MR1607736

[Tate1967] J. T. Tate, *p-divisible groups*, Proc. Conf. Local Fields (Driebergen, 1966), Springer, Berlin, 1967, pp. 158–183. MR0231827

[Weinstein2016] Jared Weinstein, *Semistable models for modular curves of arbitrary level*, Invent. Math. **205** (2016), no. 2, 459–526. MR3529120

[Zhu2014] Yifei Zhu, *The power operation structure on Morava E-theory of height 2 at the prime 3*, Algebr. Geom. Topol. **14** (2014), no. 2, 953–977. MR3160608

[Zhu2015] ———, *The Hecke algebra action and the Rezk logarithm on Morava E-theory of height 2*, updated at `https://yifeizhu.github.io/ho.pdf`. arXiv:1505.06377

[Zhu2017] ———, *Norm coherence for descent of level structures on formal deformations*, updated at `https://yifeizhu.github.io/nc.pdf`. arXiv:1706.03445

[Zhu2018] ———, *Morava E-homology of Bousfield–Kuhn functors on odd-dimensional spheres*, Proc. Amer. Math. Soc. **146** (2018), no. 1, 449–458. MR3723154