A SUPERSINGULAR CONGRUENCE FOR MODULAR FORMS

ANDREW BAKER

ABSTRACT. Let $p > 3$ be a prime. In the ring of modular forms with q-expansions defined over $\mathbb{Z}_{(p)}$, the Eisenstein function E_{p+1} is shown to satisfy

$$(E_{p+1})^{p-1} \equiv -\left(\frac{-1}{p}\right)\Delta^{(p^2-1)/12} \bmod (p, E_{p-1}).$$

This is equivalent to a result conjectured by de Shalit on the polynomial satisfied by all the j-invariants of supersingular elliptic curves over $\overline{\mathbb{F}}_p$. It is also closely related to a result of Gross and Landweber used to define a topological version of elliptic cohomology.

INTRODUCTION

In [6], Gross and Landweber proved the following supersingular congruence in the ring of holomorphic modular forms for $\mathrm{SL}_2(\mathbb{Z})$ with q-coefficients in the ring of p-local integers $\mathbb{Z}_{(p)}$ for a prime $p > 3$:

$$u_2 \equiv \left(\frac{-1}{p}\right)\Delta^{(p^2-1)/12} \bmod (p, u_1). \tag{0.1}$$

The regular sequence p, u_1, u_2 is defined using the canonical formal group law F associated to the universal Weierstraß cubic whose p-series has the form

$$\begin{aligned}[p]_F(X) &= pX + \cdots + u_1X^p + \cdots + u_2X^{p^2} + (\text{higher order terms})\\ &\equiv u_1X^p + \cdots + u_2X^{p^2} + (\text{higher order terms}) && \bmod (p)\\ &\equiv u_2X^{p^2} + (\text{higher order terms}) && \bmod (p, u_1). \end{aligned} \tag{0.2}$$

In fact, u_1 is essentially the Eisenstein function E_{p-1}, in the sense that $u_1 \equiv E_{p-1} \bmod (p)$.

The main result of this paper is the following supersingular congruence for E_{p+1} which is closely related to Equation (0.1):

$$(E_{p+1})^{p-1} \equiv -\left(\frac{-1}{p}\right)\Delta^{(p^2-1)/12} \bmod (p, E_{p-1}). \tag{0.3}$$

These congruences are equivalent to equations that hold in the field of definition of a supersingular elliptic curve over a finite field of characteristic greater than 3, and our proof is couched in terms of this interpretation.

It turns out that our result is related to one conjectured by de Shalit [12] and described by Kaneko and Zagier in [4]. In fact, our original attempt at proving Theorem 1.4 involved a reduction to Equation (6.1). This unsuccessful strategy was aborted when Don Zagier pointed out the equivalence of the two results!

Our original motivation in studying this question and more generally isogenies of supersingular elliptic curves, lies in elliptic cohomology. Inspired by results of Robert [8] and of Gross and Landweber, we have determined the precise relationship between the category of isogenies and the stable operation algebra of supersingular elliptic cohomology. The details will appear in [1] which is currently in preparation. Like the present work, this makes use of Tate's theory, particularly that of the p-primary Tate module (never formally published by him but described in [17], see also the Woods Hole Notes [7]).

1991 *Mathematics Subject Classification.* 14K22 11G20.

Key words and phrases. Modular forms, supersingular elliptic curves.

Published in Acta Arithmetica **86** (1998), 91–100. [Version 13: 30/01/2003].

I would like to thank K. Buzzard, F. Clarke, I. Connell, J. Cremona, R. Odoni, R. Rankin, J. Tate and D. Zagier for help and encouragement on the subject matter of this paper and especially G. Robert for a never forgotten conversation of many years ago.

1. Recollections on modular forms and elliptic curves over finite fields

Background material for this section can be found in the articles of Serre [10, 11], Katz [5] and Tate [14]; see also the books by Husemoller and Silverman [3, 13].

Throughout, let $p > 3$ be a prime and let $\mathrm{S}(\mathbb{Z}_{(p)})_*$ (respectively $\mathrm{M}(\mathbb{Z}_{(p)})_*$) denote the graded ring of modular forms for $\mathrm{SL}_2(\mathbb{Z})$, holomorphic (respectively meromorphic) at ∞ and with q-coefficients in the ring of p-local integers $\mathbb{Z}_{(p)}$.

We will make use of the following modular forms which are determined by their q-expansions.

$$\begin{aligned}
P = E_2 &= 1 - 24\sum_{1\leqslant r}\sigma_1(r)q^r,\\
Q = E_4 &= 1 + 240\sum_{1\leqslant r}\sigma_3(r)q^r,\\
R = E_6 &= 1 - 504\sum_{1\leqslant r}\sigma_5(r)q^r,\\
\Delta &= \frac{Q^3 - R^2}{1728},\\
j &= \frac{Q^3}{\Delta},\\
A = E_{p-1} &= 1 - \frac{2(p-1)}{B_{p-1}}\sum_{1\leqslant r}\sigma_{p-2}(r)q^r,\\
B = E_{p+1} &= 1 - \frac{2(p+1)}{B_{p+1}}\sum_{1\leqslant r}\sigma_p(r)q^r.
\end{aligned}$$

Here, Q and R are modular forms of weights 4 and 6, while P is 'almost' modular of weight 2.

Theorem 1.1. *As graded rings,*

$$\begin{aligned}
\mathrm{S}(\mathbb{Z}_{(p)})_* &= \mathbb{Z}_{(p)}[Q,R],\\
\mathrm{M}(\mathbb{Z}_{(p)})_* &= \mathbb{Z}_{(p)}[Q,R,\Delta^{-1}].
\end{aligned}$$

Also,

$$\begin{aligned}
\mathrm{S}(\mathbb{Z}_{(p)})_0 &= \mathbb{Z}_{(p)},\\
\mathrm{M}(\mathbb{Z}_{(p)})_0 &= \mathbb{Z}_{(p)}[j].
\end{aligned}$$

There is a derivation ∂ on $\mathrm{M}(\mathbb{Z}_{(p)})_*$ which restricts to $\mathrm{S}(\mathbb{Z}_{(p)})_*$ and satisfies

$$\begin{aligned}
\partial P &= -Q - P^2,\\
\partial Q &= -4R,\\
\partial R &= -6Q^2,\\
\partial \Delta &= 0,\\
\partial j &= -12\frac{Q^2R}{\Delta}.
\end{aligned}$$

Theorem 1.2. *For the prime $p > 3$,*

1. *In the ring $\mathrm{S}(\mathbb{F}_p)_* = \mathrm{S}(\mathbb{Z}_{(p)})_*/(p)$, Δ is not a factor of A.*
2. *In the ring $\mathrm{S}(\mathbb{F}_p)_*$ each irreducible factor of A has multiplicity one, hence the same is true in the ring $\mathrm{M}(\mathbb{F}_p)_* = \mathrm{M}(\mathbb{Z}_{(p)})_*/(p)$.*

(3) *In each of the rings* $\mathrm{S}(\mathbb{F}_p)_*$ *and* $\mathrm{M}(\mathbb{F}_p)_*$*, every irreducible factor of* A *has one of the forms*

$$Q,\ R,\ Q^3-\alpha\Delta,\ Q^6+\beta\Delta Q^3+\gamma\Delta^2,$$

where $\alpha,\beta,\gamma\in\mathbb{F}_p$ *with* $\alpha\neq 0$ *and* $X^2+\beta X+\gamma\in\mathbb{F}_p[X]$ *irreducible.*

We also note the following calculational result.

Proposition 1.3. *For a prime* $p>3$*, in the ring* $\mathrm{M}(\mathbb{F}_p)_*$ *we have the identities modulo* p*:*

$$B\equiv\partial A,\quad \partial B\equiv -QA.$$

Now let $\mathbb{F}_q$ be the finite field of order $q=p^d$ where we continue to assume that $p>3$. An elliptic curve $\mathcal{E}$ over $\mathbb{F}_q$ is determined by its Weierstraß form,

$$\mathcal{E}\colon y^2=4x^3-ax-b.$$

The non-singularity of $\mathcal{E}$ is equivalent to the existence of a classifying ring homomorphism $\theta_{\mathcal{E}}\colon \mathrm{M}(\mathbb{F}_p)\longrightarrow\mathbb{F}_q$ for which $\theta_{\mathcal{E}}(Q)=12a$ and $\theta_{\mathcal{E}}(R)=-216b$. The curve is *supersingular* if $\theta_{\mathcal{E}}(A)=0$, or equivalently $\theta_{\mathcal{E}}$ factors through a homomorphism $\mathrm{M}(\mathbb{F}_p)_*/(A)\longrightarrow\mathbb{F}_q$ (which we will also denote by $\theta_{\mathcal{E}}$). For $x\in\mathrm{M}(\mathbb{Z}_{(p)})_*$ or $\mathrm{M}(\mathbb{F}_p)_*/(A)$ we will often write $x(\mathcal{E})=\theta_{\mathcal{E}}(x)$.

Given $u\in\mathbb{F}_q$, the curve

$$\mathcal{E}^u\colon y^2=4x^3-au^2x-bu^3$$

is the u-twist of $\mathcal{E}$. It is isomorphic (as an abelian variety over $\mathbb{F}_q$) to $\mathcal{E}$ if and only if u is a square in $\mathbb{F}_q$ and in that case, an isomorphism is provided by the completion of the affine map $\varphi_v\colon (x,y)\longmapsto(v^2x,v^3y)$ where $v^2=u$.

Associated to the Weierstraß form is the canonical invariant differential

$$\omega_{\mathcal{E}}=\frac{dx}{y}.$$

Notice that when $u=v^2$,

$$\varphi_v^*\omega_{\mathcal{E}^u}=v^{-1}\omega_{\mathcal{E}}.$$

Also, if $F\in\mathrm{M}(\mathbb{Z}_{(p)})_k$, then

$$F(\mathcal{E}^u)=v^kF(\mathcal{E}).$$

Using the above notation we restate our main result as the following:

Theorem 1.4. *For the prime* $p>3$*, in each of the rings* $\mathrm{S}(\mathbb{Z}_{(p)})_*$ *and* $\mathrm{M}(\mathbb{Z}_{(p)})_*$ *we have the congruence*

$$B^{p-1}\equiv-\left(\frac{-1}{p}\right)\Delta^{(p^2-1)/12}\bmod(p,A).$$

Equivalently, for a supersingular elliptic curve $\mathcal{E}$ *over a finite field* $\mathbb{F}_{p^d}$*,*

$$B(\mathcal{E})^{p-1}=-\left(\frac{-1}{p}\right)\Delta(\mathcal{E})^{(p^2-1)/12}.$$

2. Some supersingular isogeny invariants

Recall that for two elliptic curves $\mathcal{E}_1,\mathcal{E}_2$ defined over a field $\Bbbk$, an *isogeny* $\varphi\colon\mathcal{E}_1\longrightarrow\mathcal{E}_2$ *over* $\Bbbk$ is a non-zero morphism of abelian varieties. Using the *dual isogeny* $\widehat{\varphi}\colon\mathcal{E}_2\longrightarrow\mathcal{E}_1$, it is easily seen that the existence of an isogeny $\mathcal{E}_1\longrightarrow\mathcal{E}_2$ is equivalent to the existence of an isogeny $\mathcal{E}_2\longrightarrow\mathcal{E}_1$. Hence the notion of *isogeny* defines an equivalence relation on elliptic curves.

The next important result due to Tate [15], see also [3] Chapter 3 Theorem 8.4, allows us to determine isogeny classes of supersingular curves.

Theorem 2.1. *Two elliptic curves* $\mathcal{E}_1,\mathcal{E}_2$ *defined over a finite field* $\mathbb{F}_q$ *are isogenous over* $\mathbb{F}_q$ *if and only if*

$$|\mathcal{E}_1(\mathbb{F}_q)|=|\mathcal{E}_2(\mathbb{F}_q)|.$$

In particular, a supersingular curve defined over the prime field $\mathbb{F}_p$ has $|\mathcal{E}(\mathbb{F}_p)| = 1+p$, hence all such curves are isogenous over $\mathbb{F}_p$. For a more detailed analysis of the possible isogeny classes, see [16, 9].

For supersingular elliptic curves over finite fields, it turns out that there are some interesting isogeny invariants. In [6], Gross and Landweber in effect showed for two such curves $\mathcal{E}_1, \mathcal{E}_2$ defined and separably isogenous over $\mathbb{F}_{p^2}$,

$$\left(\frac{-1}{p}\right)\Delta(\mathcal{E}_1)^{(p^2-1)/12} = \left(\frac{-1}{p}\right)\Delta(\mathcal{E}_2)^{(p^2-1)/12}.$$

This follows from the facts that these two quantities are actually in $\mathbb{F}_p$ and by Equation (0.2) can be identified with the coefficients of the leading terms T^{p^2} in the $[p]$-series of the isomorphic canonical formal group laws associated to the local parameter $-2x/y$.

In order to identify another isogeny invariant, we will need Théorème B/Lemme 7 of Robert [8].

Lemma 2.2. *Let $\varphi\colon \mathcal{E}_1 \longrightarrow \mathcal{E}_2$ be a separable isogeny between supersingular elliptic curves. Then if $\varphi^*\omega_{\mathcal{E}_2} = \lambda\omega_{\mathcal{E}_1}$,*

$$B(\mathcal{E}_2) = \lambda^{-(p+1)}\deg\varphi B(\mathcal{E}_1).$$

Corollary 2.3.

$$B(\mathcal{E}_2)^{p-1} = \lambda^{-(p^2-1)}B(\mathcal{E}_1)^{p-1}.$$

In particular, if $\mathcal{E}_1, \mathcal{E}_2$ and φ are all defined over $\mathbb{F}_{p^2}$, then

$$B(\mathcal{E}_2)^{p-1} = B(\mathcal{E}_1)^{p-1}.$$

Using this corollary, together with the fact that for a supersingular curve $\mathcal{E}$ over a finite field $\mathbb{F}_{p^d}$, $j(\mathcal{E}) \in \mathbb{F}_{p^2}$ and there is supersingular curve $\mathcal{E}'$ defined over $\mathbb{F}_{p^2}$ and an isomorphism $\mathcal{E} \cong \mathcal{E}'$ defined over $\mathbb{F}_{p^d}$, we can reduce the proof of our main theorem to the case of curves defined over $\mathbb{F}_{p^2}$.

3. Constructing supersingular curves over the prime field

For completeness, in this section we outline details of a construction which seems to be well known but whose full details are not so readily found in the literature. A nice account of some aspects of this can be found in Cox [2].

Let $K = \mathbb{Q}(\sqrt{-p})$ and $\mathcal{O}_K$ be its ring of integers which is its unique maximal order.

Theorem 3.1. *For any prime $p > 11$, there are supersingular elliptic curves $\mathcal{E}$ defined over $\mathbb{F}_p$ and with $j(\mathcal{E}) \not\equiv 0, 1728 \bmod (p)$ and having $\mathcal{O}_K \subseteq \operatorname{End}\mathcal{E}$.*

Now $\mathcal{O}_K$ is a lattice in $\mathbb{C}$, hence we can define the torus $\mathbb{C}/\mathcal{O}_K$ which has a projective embedding as a Weierstraß cubic $\mathcal{E}_K$. Since $\mathcal{O}_K$ is an $\mathcal{O}_K$-module, $\mathcal{E}_K$ admits complex multiplication by $\mathcal{O}_K$.

Proposition 3.2. (1) *The j-invariant $j(\mathcal{O}_K) = j(\mathcal{E}_K)$ is an algebraic integer.*
(2) *The extension field $L = K(j(\mathcal{O}_K))$ is the Hilbert class field of K.*
(3) *The elliptic curve $\mathcal{E}_K$ is defined over L.*

A property of the Hilbert class field is that it is unramified at every principal prime ideal in $\mathcal{O}_K$. In particular, if $\mathfrak{p}$ is a prime in $\mathcal{O}_L$ lying above the prime $(\sqrt{-p})$ in $\mathcal{O}_K$, then the residue field is

$$\mathcal{O}_L/\mathfrak{p} \cong \mathbb{F}_p.$$

Hence,

$$j(\mathcal{O}_K) \bmod \mathfrak{p} \in \mathbb{F}_p. \tag{3.1}$$

Since the curve $\mathcal{E}_K$ can be defined over L, we can assume that it has the Weierstraß form

$$\mathcal{E}_K\colon y^2 = 4x^3 - ax - b$$

where $a, b \in \mathcal{O}_L$. Unfortunately, this might have discriminant Δ lying in some prime ideal $\mathfrak{p}$ over $(\sqrt{-p})$. To overcome this problem we pass to $\mathfrak{p}$-adic completions $K_{(\sqrt{-p})} \subseteq L_{\mathfrak{p}}$ which are complete local fields with maximal discrete valuation rings $\mathcal{O}_{K,(\sqrt{-p})} \subseteq \mathcal{O}_{L,\mathfrak{p}}$. We may pass to some finite extension $L'/L_{\mathfrak{p}}$ in which $\mathfrak{p}$ is totally ramified and the principal prime ideal $\mathfrak{p}' = (\pi) \lhd \mathcal{O}_{L'}$ satisfies

$$\Delta = \lambda \pi^{12k}$$

for some integer $k \geqslant 0$ and unit $\lambda \in \mathcal{O}_{L'}$. The curve

$$\mathcal{E}' \colon y^2 = 4x^3 - \pi^{-4k} a x - \pi^{-6k} b$$

is now defined over $\mathcal{O}_{L'} \subseteq L'$ and isomorphic to $\mathcal{E}_K$ over L'. Moreover its discriminant is λ, which reduces to a non-zero element of $\mathcal{O}_{L'}/(\pi)$, hence the reduced curve $\widetilde{\mathcal{E}'}$ is non-singular and so elliptic. We also have

$$\begin{aligned} j(\widetilde{\mathcal{E}'}) &= j(\mathcal{E}') && \bmod (\pi) \\ &= j(\mathcal{O}_K) && \bmod (\pi) \end{aligned}$$

with the latter lying in $\mathbb{F}_p$. Hence, $\widetilde{\mathcal{E}}$ is isomorphic over $\overline{\mathbb{F}}_p$ to an elliptic curve $\mathcal{E}$ defined over $\mathbb{F}_p$.

The endomorphism ring of $\mathcal{E}$ is at least as big as $\mathcal{O}_K$. Notice that it cannot contain the complex numbers i or ω since it would then have a commutative endomorphism ring of rank greater than 2. Thus we must have $j(\mathcal{O}_K) \not\equiv 0, 1728 \bmod (p)$, and using a straightforward change of variables, can actually assume that $\mathcal{E}$ has the form

$$\mathcal{E} \colon y^2 = 4x^3 - \frac{27 j(\mathcal{O}_K)}{j(\mathcal{O}_K) - 1728} x - \frac{27 j(\mathcal{O}_K)}{j(\mathcal{O}_K) - 1728}.$$

In fact, $\operatorname{End} \mathcal{E}$ is noncommutative since $\mathcal{E}$ is supersingular. To see this, notice that from general considerations of [15, 16, 17] the action of $\sqrt{-p}$ agrees with that of the Frobenius map. Applying Fr to the Tate module $\mathrm{T}_\ell \mathcal{E}$ for any prime $\ell \neq p$, we easily see that

$$\operatorname{Tr} \mathrm{Fr} = \sqrt{-p} - \sqrt{-p} = 0.$$

But this implies that

$$|\mathcal{E}(\mathbb{F}_p)| = p + 1 - \operatorname{Tr} \mathrm{Fr} = p + 1,$$

or equivalently that $\mathcal{E}$ is supersingular by standard results of [3, 13].

4. The case of supersingular curves over the prime field

In [6], Gross and Landweber proved that for a supersingular elliptic curve $\mathcal{E}$ defined over $\mathbb{F}_{p^2}$ the following identity holds whenever $j(\mathcal{E}) \not\equiv 0, 1728 \bmod (p)$.

$$\Delta(\mathcal{E})^{(p^2-1)/12} = \begin{cases} 1 & \text{if } \mathrm{Fr}^2 = [(-1/p)p]_{\mathcal{E}} \qquad \text{(Case A)}, \\ -1 & \text{if } \mathrm{Fr}^2 = [-(-1/p)]_{\mathcal{E}} \qquad \text{(Case B)}. \end{cases} \tag{4.1}$$

Here $\mathrm{Fr}^2 \colon \mathcal{E} \longrightarrow \mathcal{E}^{(p^2)} = \mathcal{E}$ is the relative Frobenius map and the stated possibilities are the only ones that can occur. They also observe if Case A holds, then

$$\mathcal{E}[4] \subseteq \mathcal{E}(\mathbb{F}_{p^2}).$$

Since $|\mathcal{E}[4]| = 16$, this means that $|\mathcal{E}(\mathbb{F}_{p^2})| \equiv 0 \bmod (16)$. In case B, a modification of their discussion shows that *none* of the elements of order 4 can be in $\mathcal{E}(\mathbb{F}_{p^2})$. On the other hand, in all cases,

$$\mathcal{E}[2] \subseteq \mathcal{E}(\mathbb{F}_{p^2}).$$

Let us now consider the case of such a curve actually defined over the prime $\mathbb{F}_p$. Then it is well known that the number of points over $\mathbb{F}_p$ is $|\mathcal{E}(\mathbb{F}_p)| = 1 + p$. Using the form of the zeta function over $\mathbb{F}_p$ given by the Weil Conjectures, we easily find that

$$|\mathcal{E}(\mathbb{F}_{p^2})| = 1 + 2p + p^2 = (1+p)^2 \equiv \begin{cases} 4 \bmod (8), & \text{if } p \equiv 1 \bmod (4), \\ 0 \bmod (8), & \text{if } p \equiv 3 \bmod (4). \end{cases}$$

Hence, for such a curve, we have

$$\begin{array}{rcl} \text{Case A holds} & \iff & p \equiv 3 \bmod (4), \\ \text{Case B holds} & \iff & p \equiv 1 \bmod (4). \end{array}$$

Since $B(\mathcal{E}) \in \mathbb{F}_p$

$$B(\mathcal{E})^{p-1} = 1.$$

In Case A, we have $(-1/p) = -1$, and so by (4.1)

$$-\left(\frac{-1}{p}\right)\Delta(\mathcal{E})^{(p^2-1)/12} = 1 = B(\mathcal{E})^{p-1}.$$

In case B, $(-1/p) = 1$, and by (4.1),

$$-\left(\frac{-1}{p}\right)\Delta(\mathcal{E})^{(p^2-1)/12} = 1 = B(\mathcal{E})^{p-1}.$$

Hence we have proved the following.

Theorem 4.1. *For a supersingular elliptic curve $\mathcal{E}$ defined over $\mathbb{F}_p$ and satisfying $j(\mathcal{E}) \not\equiv 0, 1728 \bmod (p)$,*

$$B(\mathcal{E})^{p-1} = -\left(\frac{-1}{p}\right)\Delta(\mathcal{E})^{(p^2-1)/12}.$$

5. The case of supersingular curves over the field of order p^2

Having dealt with supersingular curves over the prime field, we now turn to those defined over $\mathbb{F}_{p^2}$. For $p > 11$, choose a supersingular elliptic curve $\mathcal{E}_0$ defined over $\mathbb{F}_p$ with $j(\mathcal{E}) \not\equiv 0, 1728 \bmod (p)$– this is always possible courtesy of Theorem 3.1.

Let $\mathcal{E}$ be a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$ and with $j(\mathcal{E}) \not\equiv 0, 1728 \bmod (p)$. By [16],

$$|\mathcal{E}(\mathbb{F}_{p^2})| = 1 \pm 2p + p^2 = (1 \pm p)^2.$$

By the Weil Conjectures, any curve defined over $\mathbb{F}_p$ has $|\mathcal{E}(\mathbb{F}_{p^2})| = (1+p)^2$. By Theorem 2.1, if $|\mathcal{E}(\mathbb{F}_{p^2})| = (1+p)^2$, there is an isogeny $\mathcal{E}_0 \longrightarrow \mathcal{E}$ defined over $\mathbb{F}_{p^2}$. There is a unique factorization of the form $\varphi = {}_s\varphi \circ \mathrm{Fr}^k$, where

$$\mathrm{Fr}^k \colon \mathcal{E}_0 \longrightarrow \mathcal{E}_0^{(p^k)} = \mathcal{E}_0$$

is the k-fold iterated Frobenius map, and ${}_s\varphi \colon \mathcal{E}_0 \longrightarrow \mathcal{E}$ is separable. Hence we might as well assume that φ itself is separable.

Now applying Corollary 2.3 we may deduce that

$$B(\mathcal{E})^{p-1} = B(\mathcal{E}_0)^{p-1} = 1.$$

Notice that if $p \equiv 1 \bmod (4)$ then case B of Section 4 applies to $\mathcal{E}$, while if $p \equiv 3 \bmod (4)$ then case A applies. Thus we find that

$$B(\mathcal{E})^{p-1} = 1 = -\left(\frac{-1}{p}\right)\Delta^{(p^2-1)/12}.$$

If $|\mathcal{E}(\mathbb{F}_{p^2})| = (1-p)^2$, we may twist by any non-square u in $\mathbb{F}_{p^2}$ to obtain a curve

$$\mathcal{E}^u \colon y^2 = 4x^3 - au^2x - bu^3$$

which can easily be seen to have $|\mathcal{E}^u(\mathbb{F}_{p^2})| = (1+p)^2$. If $v \in \mathbb{F}_{p^4}$ with $v^2 = u$, $(x, y) \longmapsto (v^2x, v^3)$ defines an isomorphism $\varphi_v \colon \mathcal{E} \cong \mathcal{E}^u$ over $\mathbb{F}_{p^4}$, and we have $\varphi_v^*\omega_{\mathcal{E}^u} = \omega_{\mathcal{E}}$. By the above result for $\mathcal{E}^u$ together with Corollary 2.3, and the fact that $\Delta(\mathcal{E}^u) = u^6\Delta(\mathcal{E}^u)$, we now see that

$$B(\mathcal{E})^{p-1} = -B(\mathcal{E}^u)^{p-1} = \left(\frac{-1}{p}\right)\Delta(\mathcal{E}^u)^{(p^2-1)/12} = -\left(\frac{-1}{p}\right)\Delta(\mathcal{E})^{(p^2-1)/12}.$$

Similar arguments allow our identity to be proved directly for supersingular curves with $j(\mathcal{E}) \equiv 0, 1728 \bmod (p)$. Hence for primes $p \not\equiv 1 \bmod (12)$ we can avoid the use of Theorem 3.1, however when $p \equiv 1 \bmod (12)$, we do require this result.

6. Relations with other work

In [4], Kaneko and Zagier discuss the *supersingular polynomial*

$$\mathrm{ss}_p(X) = \prod_{\mathcal{E}}(X - j(\mathcal{E})),$$

where the product is taken over all isomorphism classes of supersingular curves over $\overline{\mathbb{F}}_p$. Thus in the ring $\mathrm{M}(\mathbb{F}_p)_*$ we have

$$A = \frac{Q^\delta R^\varepsilon \,\mathrm{ss}_p(j)\Delta^{m_p}}{j^\delta(j-1728)^\varepsilon},$$

where we write $p = 12m_p + 4\delta + 6\varepsilon + 1$ with $\delta, \varepsilon \in \{0, 1\}$. Using Proposition 1.3 we obtain a formula for B in terms of the derivation ∂.

If $\alpha \not\equiv 0, 1728 \bmod p$ is a root of $\mathrm{ss}_p(X)$, then there is a supersingular elliptic curve

$$\mathcal{E}\colon y^2 = 4x^3 - \frac{27\alpha}{(\alpha-1728)}x - \frac{27\alpha}{(\alpha-1728)}$$

with $j(\mathcal{E}) = \alpha$. Then for some $\lambda \in \mathbb{F}_p$,

$$B(\mathcal{E}) = \lambda\frac{\alpha^{\varepsilon+1}\,\mathrm{ss}_p'(\alpha)\Delta^{m_p}}{(\alpha-1728)^{\delta+\varepsilon}}.$$

Combining this with Theorem 1.4 gives

$$\mathrm{ss}_p'(\alpha)^{p-1} = (-1)^{\varepsilon-1}\alpha^{2(\delta-1)(p-1)/3}(\alpha-1728)^{(\varepsilon-1)(p-1)/2} \tag{6.1}$$

which is the conjectured result [4], equation (40). Thus we have also proved the equivalent conjectural equation (39) of de Shalit.

References

[1] A. Baker, Isogenies of supersingular elliptic curves over finite fields and operations in elliptic cohomology, Glasgow University Mathematics Department preprint 98/39.
[2] D. A. Cox, Primes of the form x^2+ny^2. Fermat, class field theory and complex multiplication, Wiley (1989).
[3] D. Husemoller, Elliptic Curves, Springer-Verlag (1987).
[4] M. Kaneko and D. Zagier, Supersingular j-invariants, hypergeometric series, and Atkin's orthogonal polynomials, AMS/IP Studies in Advanced Mathematics **7** (1998), 97–126.
[5] N. M. Katz, p-adic properties of modular schemes and modular forms, Lecture Notes in Mathematics **350** (1973), 69–190.
[6] P. S. Landweber, Supersingular elliptic curves and congruences for Legendre polynomials, Lecture Notes in Mathematics **1326** (1988), 69–93.
[7] J. Lubin, J-P. Serre and J. Tate, Elliptic curves and formal groups, mimeographed notes from the Woods Hole conference, available at `http://www.ma.utexas.edu/~voloch/lst.html`.
[8] G. Robert, Congruences entre séries d'Eisenstein, dans le cas supersingular, Invent. Math. **61** (1980), 103–158.
[9] H-G. Rück, A note on elliptic curves over finite fields, Math. Comp. **49** (1987), 301–4.
[10] J-P. Serre, Congruences et formes modulaires (après H. P. F. Swinnerton-Dyer), Sém. Bourbaki 24$^{\mathrm{e}}$ Année, (1971/2) No. 416, Lecture Notes in Mathematics **317** (1973), 319–38.
[11] J-P. Serre, Formes modulaires et fonctions zeta p-adiques, Lecture Notes in Mathematics **350** (1973), 191–268.
[12] E. de Shalit, Kronecker's polynomial, supersingular elliptic curves, and p-adic periods of modular curves, Contemporary Math. **165** (1994), 135–148.
[13] J. Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag (1986).
[14] J. Tate, The arithmetic of elliptic curves, Invent. Math. **23** (1974), 179–206.
[15] J. Tate, Endomorphisms of abelian varieties over finite fields, Invent. Math. **2** (1966), 134–144.
[16] W. C. Waterhouse, Abelian varieties over finite fields, Ann. Sci. Ecole Norm. Sup. (4) **2** (1969), 521–560.
[17] W. C. Waterhouse & J. S. Milne, Abelian varieties over finite fields, Proc. Sympos. Pure Math. **XX** (1971), 53–64.

Department of Mathematics, University of Glasgow, Glasgow G12 8QW, Scotland.
E-mail address: `a.baker@maths.gla.ac.uk`
URL: `http://www.maths.gla.ac.uk/~ajb`