Slide 1

Isogenies of elliptic curves and operations in elliptic cohomology

Andrew Baker, Glasgow

Oberwolfach talk: 14 September, 1998

Slide 2

1 Elliptic curves and elliptic cohomology

If $\Bbbk$ is a commutative ring then an *oriented elliptic curve* $(\mathcal{E}, \omega)$ over $\Bbbk$ is a 1-dimensional irreducible abelian variety $\mathcal{E}$ equipped with a non-vanishing invariant 1-from ω. Two such curves $(\mathcal{E}, \omega)$, $(\mathcal{E}', \omega')$ are deemed to be equivalent if there is an isomorphism of abelian varieties $\varphi\colon \mathcal{E} \longrightarrow \mathcal{E}'$ under which $\varphi^*\omega' = \omega$. The notation $(\mathcal{E}, \omega)$ will signify the equivalence class of such an elliptic curve.

Associated to such a curve $(\mathcal{E}, \omega)$ is a unique realisation in $\mathrm{P}^2(\Bbbk)$ as the projectivisation of a Weierstraß cubic

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where ω corresponds to the standard invariant differential

$$\frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y}.$$

Slide 3

The invertible sheaf of 1-forms $\Omega^1(\mathcal{E})$ and its tensor powers $\Omega^1(\mathcal{E})^{\otimes k}$ have regular sections. A rule which assigns to each equivalence class of oriented elliptic curves $(\mathcal{E}, \omega)$ a section $F(\mathcal{E}, \omega)$ of $\Omega^1(\mathcal{E})^{\otimes k}$ is called a *modular form of weight* k over $\Bbbk$ if it transforms under a morphism of abelian varieties $\varphi\colon \mathcal{E}_1 \longrightarrow \mathcal{E}_2$ under which $\varphi^*\omega_2 = \lambda\omega_1$ according to the rule

$$\varphi^*(F(\mathcal{E}_2, \omega_2)) = F(\mathcal{E}_1, \omega_1).$$

Writing $F(\mathcal{E}, \omega) = f(\mathcal{E}, \omega)\omega^{\otimes k}$, we see that

$$\begin{aligned} \varphi^*(f(\mathcal{E}_2, \omega_2)\omega_2^{\otimes k}) &= f(\mathcal{E}_1, \omega_1)\omega_1^{\otimes k}, \\ \text{i.e.,} \quad f(\mathcal{E}_2, \omega_2) &= \lambda^{-k} f(\mathcal{E}_1, \omega_1). \end{aligned}$$

Slide 4

Theorem 1.1 *If* $\Bbbk$ *is a commutative unital ring containing* $1/6$*, then the graded ring of modular forms is* $\Bbbk[Q, R, \Delta^{-1}]$*, where* $\operatorname{wt} Q = 4$*,* $\operatorname{wt} R = 6$ *and* $\Delta = (Q^3 - R^2)/1728$ *has* $\operatorname{wt} \Delta = 12$*.*

In fact, if $\Bbbk$ contains $1/6$, then oriented elliptic curves are classified by the graded ring $E\ell\ell_* = \mathbb{Z}[1/6][Q, R, \Delta^{-1}]$ in which $E\ell\ell_{2n}$ consists of the elements of weight n. Here the ring homomorphism $\varphi\colon E\ell\ell_* \longrightarrow \Bbbk$ is equivalent to the Weierstraß cubic

$$y^2 = 4x^3 - \frac{1}{12}\varphi(Q) + \frac{1}{216}\varphi(R)$$

4 with its canonical invariant 1-form dx/y.

The formal group law associated to the local parameter $t = -x/y$ is induced from a universal Weierstraß formal group law over $E\ell\ell_*$ and hence a genus $\varphi_{E\ell\ell}\colon MU_* \longrightarrow E\ell\ell_*$.

Slide 5

Elliptic homology and cohomology are defined using the following consequence of Landweber's Exact Functor Theorem.

Theorem 1.2 *The functors*

$$E\ell\ell_*(\ ) = E\ell\ell_* \underset{MU_*}{\otimes} MU_*(\ )$$
$$E\ell\ell^*(\ ) = E\ell\ell_* \underset{MU_*}{\otimes} MU^*(\ ).$$

are dual complex oriented multiplicative homology and cohomology theories.

These are actually level 1 versions of the level 2 theories defined by Landweber, Ravenel and Stong.

Slide 6

2 Isogenies and Hecke operators

An *isogeny* $\varphi\colon (\mathcal{E}_1, \omega_1) \longrightarrow (\mathcal{E}_2, \omega_2)$ consists of a finite degree morphism of abelian varieties $\varphi\colon \mathcal{E}_1 \longrightarrow \mathcal{E}_2$; on 1-forms it induces $\varphi^*\omega_2 = \lambda_\varphi \omega_1$ for some $\lambda_\varphi \in \Bbbk$. If $\lambda_\varphi = 1$ then φ is a *strict isogeny*.

Such an isogeny φ factors uniquely as

$$\mathcal{E}_1 \longrightarrow \mathcal{E}_1/\ker\varphi \xrightarrow{\cong} \mathcal{E}_2,$$

where the second arrow is a strict isogeny which is an isomorphism, hence gives an equivalence $(\mathcal{E}_1/\ker\varphi, \omega_1) \longrightarrow (\mathcal{E}_2, \omega_2)$. Hence, for each $n \geqslant 1$, the isogenies out of $\mathcal{E}$ are essentially determined by the subgroups of $\mathcal{E}$ of 'size' n. Here we need to be careful when working in finite characteristic since inseparable isogenies do not have the correct number of points in their kernels and we need to work with finite subgroup schemes.

Slide 7

In fact the category of oriented elliptic curves over $\mathbb{C}$ and their isogenies can be used to describe a large part of the stable operation algebra $E\ell\ell^* E\ell\ell$; more precisely, the dual object $E\ell\ell_* E\ell\ell$ is a certain algebra of functions on this category with suitable arithmetic conditions on their q-expansions.

Slide 8

If we fix $n \geqslant 1$, then in characteristic 0, the generic case, for an elliptic curve $\mathcal{E}$ over $\Bbbk$ we have

$$\mathcal{E}[n] = \ker[n] \colon \mathcal{E} \longrightarrow \mathcal{E}$$

which has rank n^2 and is essentially $(\mathbb{Z}/n)^2$ as a group. We can define for each subgroup S of size n an isogeny $\mathcal{E} \longrightarrow \mathcal{E}/S$. If $\mathcal{E}$ is defined over $\Bbbk$, then $\mathcal{E}/S$ is defined over a finite extension $\Bbbk'$ containing $\Bbbk[1/n, \zeta_n]$ where $\zeta_n = e^{2\pi i/n}$. The classifying maps $E\ell\ell_* \longrightarrow \Bbbk'$ of $\mathcal{E}$ and $\mathcal{E}/S$ turn out to induce strictly isomorphic formal group laws on $\Bbbk'$ and hence extend to a ring homomorphism $\Phi_S \colon E\ell\ell_* E\ell\ell \longrightarrow \Bbbk'$. Averaging over all of these gives a left $E\ell\ell_*$-linear map

$$\widetilde{\Phi} = \frac{1}{n} \sum_{S} \Phi_S.$$

Slide 9

In the universal case this gives

$$\mathrm{T}_n \in \mathrm{Hom}_{E\ell\ell_*}(E\ell\ell_* E\ell\ell, E\ell\ell_*[1/n])$$

which is just a stable operation $E\ell\ell^*(\ ) \longrightarrow E\ell\ell[1/n]^*(\ )$. There are also multiplicative Adams operations $\psi^n\colon E\ell\ell^*(\ ) \longrightarrow E\ell\ell[1/n]^*(\ )$ with the usual properties.

Theorem 2.1 *The stable operations* T_n, ψ^n $(n \geqslant 1)$ *satisfy*

a) *For all* m, n *such that* $\mathrm{T}_m, \mathrm{T}_n$ *are defined,* $\mathrm{T}_m\mathrm{T}_n = \mathrm{T}_n\mathrm{T}_m$.

b) *For all coprime* m, n, $\mathrm{T}_m\mathrm{T}_n = \mathrm{T}_{mn}$.

c) *For a prime* p *and* $r \geqslant 1$,

$$\mathrm{T}_{p^{r+1}} = \mathrm{T}_{p^r}\mathrm{T}_p - \frac{1}{p}\psi^p \circ \mathrm{T}_{p^{r-1}}.$$

d) *On the coefficient ring* $E\ell\ell_*$, *each* T_n *agrees with the classical Hecke operator* T_n *and* $\psi^n F = n^k F$ *if* $F \in E\ell\ell_{2k}$.

Slide 10

For example, if $p \nmid n$ there are stable operations

$$T_n, \psi^n\colon E\ell\ell^*_{(p)}(\ ) \longrightarrow E\ell\ell^*_{(p)}(\ ),$$
$$T_n, \psi^n\colon E\ell\ell/p^*(\ ) \longrightarrow E\ell\ell/p^*(\ ).$$

There is another type of operation U_p in $v_1^{-1}E\ell\ell/p^*(\ )$ extending Atkin's operator and this lifts to a sort of p-adic completion of $v_1^{-1}E\ell\ell^*(\ )$.

On q-expansions, Hecke operators have the following effect for a prime p:

$$\mathrm{T}_p\Big(\sum_j a_j q^j\Big) = \sum_j a_{jp}q^j + p^{k-1}\sum_j a_j q^{jp}, \tag{2.1}$$

$$\mathrm{U}_p\Big(\sum_j a_j q^j\Big) = \sum_j a_{jp}q^j. \tag{2.2}$$

3 An application

An important problem is to calculate the E_2-term of the Adams spectral sequence

$$\mathrm{E}_2^{*,*}(X) = \mathrm{Ext}^{*,*}_{E\ell\ell_* E\ell\ell}(E\ell\ell_*, E\ell\ell_*(X)) \text{ `}\Longrightarrow\text{' } \pi_*(X),$$

Slide 11

where '$\Longrightarrow$' means converges in an appropriate sense. For $X = S = S^0$ this can be reduced to familiar cohomological objects. However, Hecke operators give a 'neo-classical' calculation of Ext^1.

Theorem 3.1 *For $n \in \mathbb{Z}$,*

$$\mathrm{Ext}^{1,2n}_{E\ell\ell_* E\ell\ell}(E\ell\ell_*, E\ell\ell_*) \cong \begin{cases} \mathbb{Z}[1/6]/\mathrm{m}(n) & \text{if } n > 0, \\ 0 & \text{otherwise,} \end{cases}$$

where $\mathrm{m}(n) = \mathrm{denom}\, \dfrac{B_n}{2n}$.

An important ingredient in proving this is the following.

Proposition 3.2 *Let $x \in \mathrm{Ext}^{0,k}_{E\ell\ell_* E\ell\ell}(E\ell\ell_*, M_*)$. Then for $r > 0$ and any prime ℓ, we have*

$$\mathrm{T}_\ell x = (1 + \ell^{-1})x,$$
$$\psi^r x = x.$$

Slide 12

Furthermore, if $pM_* = 0$, then

$$\mathrm{U}_p x = x.$$

The proof of Theorem 3.1 now proceeds in three steps.

Slide 13

Step 1: Reduce to $\mathrm{Ext}^{0,2n}_{E\ell\ell_* E\ell\ell}(E\ell\ell_*, E\ell\ell_*/p)$ for $p > 3$ a prime, using a standard argument.
Step 2: Show that this group vanishes for $n \leqslant 0$ by applying Proposition 3.2 and Equations (2.1), (2.2) to show that elements of this Ext^0 group are represented by holomorphic q-expansions, thus must be in non-negative degrees.
Step 3: Use the Adams operation $\psi^{r(1+p)}$ for suitable $\overline{r} \in \mathbb{Z}/p^\times$ to show that $(p-1) \mid n$. Then $A = E_{p-1} \in (E\ell\ell_{2(p-1)})_{(p)}$ has q-expansion $A(q) \equiv 1 \bmod (p)$ and $A^k \in \mathrm{Ext}^{0,2(p-1)k}_{E\ell\ell_* E\ell\ell}(E\ell\ell_*, E\ell\ell_*/p)$ if $k \geqslant 1$. For $F \in \mathrm{Ext}^{0,2(p-1)k}_{E\ell\ell_* E\ell\ell}(E\ell\ell_*, E\ell\ell_*/p)$, subtracting a suitable multiple of A^k gives a cusp form F_0. Proposition 3.2 together with a result of Serre shows that $F_0 = \lambda\theta_p$ where $\theta_p(q) = \dfrac{A(q)^p - A(q)}{p}$. Serre also showed that this is not the reduction of the q-expansion of a modular form, so $F_0 = 0$.

Slide 14

4 Supersingular elliptic cohomology

Let $(\mathcal{E}, \omega)$ be an oriented elliptic curve over a $\Bbbk \subseteq \overline{\mathbb{F}}_p$, classified by a ring homomorphism $\varphi\colon E\ell\ell_*/(p) \longrightarrow \overline{\mathbb{F}}_p$. The element $A = E_{p-1} \in (E\ell\ell_{2(p-1)})_{(p)}$ gives rise to $A(\mathcal{E}, \omega) = \varphi(A) \in \overline{\mathbb{F}}_p$, the *Hasse invariant* of $\mathcal{E}$. If $A(\mathcal{E}, \omega) = 0$, $\mathcal{E}$ is *supersingular.* This is equivalent to $\mathrm{End}\,\mathcal{E} = \mathrm{End}_{\overline{\mathbb{F}}_p}\mathcal{E}$ being noncommutative, actually a maximal order in a quaternion algebra over $\mathbb{Q}$.

${}^{\mathrm{ss}}E\ell\ell_* = E\ell\ell_*/(p, A)$ is the coefficient ring of a multiplicative complex oriented cohomology theory ${}^{\mathrm{ss}}E\ell\ell^*(\ )$ which has a multiplicative splitting

$$ {}^{\mathrm{ss}}E\ell\ell^*(\ ) = \prod_j L[j]^*(\ ), $$

with finite indexing set and $L[j]^*(\ )$ a finite extension of $K(2)^*(\ )$.

Slide 15

5 Stable operations in supersingular elliptic cohomology

The category $\mathbf{SepIsog}_{\mathrm{ss}}$ of separable isogenies of oriented supersingular elliptic curves over $\overline{\mathbb{F}}_p$ with morphisms being separable isogenies $(\varphi, \lambda_\varphi)\colon (\mathcal{E}_1, \omega_1) \longrightarrow (\mathcal{E}_2, \omega_2)$ with $\varphi^*\omega_2 = \lambda_\varphi \omega_1$.

There is a contravariant functor $\mathcal{T}_p$ which assigns to each supersingular elliptic curve $\mathcal{E}$, its *Tate module* $\mathcal{T}_p\mathcal{E}$, which is a free topological $\mathbb{W}(\Bbbk)$-module of rank 2 and also a module over the *Dieudonné algebra*

$$\mathbb{D}_\Bbbk = \mathbb{W}(\Bbbk)\,\langle \mathrm{F}, \mathrm{V}\rangle\,,$$
$$\mathrm{FV} = \mathrm{VF} = p,\ \mathrm{F}a = a^{(p)}\mathrm{F},\ a\mathrm{V} = \mathrm{V}a^{(p)} \quad \text{for } a \in \mathbb{W}(\Bbbk).$$

Slide 16

Theorem 5.1 (Tate) *Let $\mathcal{E}$, $\mathcal{E}'$ be elliptic curves over $\Bbbk \subseteq \overline{\mathbb{F}}_p$. Then the natural map*

$$\mathrm{Hom}_\Bbbk(\mathcal{E}, \mathcal{E}') \longrightarrow \mathrm{Hom}_{\mathbb{D}_\Bbbk}(\mathcal{T}_p\mathcal{E}', \mathcal{T}_p\mathcal{E}')$$

is injective and the induced map

$$\mathrm{Hom}_\Bbbk(\mathcal{E}, \mathcal{E}') \otimes \mathbb{Z}_p \longrightarrow \mathrm{Hom}_{\mathbb{D}_\Bbbk}(\mathcal{T}_p\mathcal{E}', \mathcal{T}_p\mathcal{E}')$$

is an isomorphism. If $\mathcal{E}$ is supersingular, then $\mathrm{End}\,\mathcal{E} \otimes \mathbb{Z}_p$ is a maximal order in the unique quaternion algebra over $\mathbb{Q}_p$.

We can identify the separable isogenies $\mathcal{E} \longrightarrow \mathcal{E}'$ with a subset of $\mathrm{Hom}_{\mathbb{D}_\Bbbk}(\mathcal{T}_p\mathcal{E}', \mathcal{T}_p\mathcal{E}')$, we can 'complete' $\mathbf{SepIsog}_{\mathrm{ss}}$ to the category $\widetilde{\mathbf{SepIsog}}_{\mathrm{ss}}$ with the same objects but for morphisms

$$\widetilde{\mathbf{SepIsog}}_{\mathrm{ss}}(\mathcal{E}, \mathcal{E}') = \mathrm{InvtHom}_{\mathbb{D}_\Bbbk}(\mathcal{T}_p\mathcal{E}', \mathcal{T}_p\mathcal{E}).$$

Slide 17

The category $\widetilde{\mathbf{SepIsog}}_{\mathrm{ss}}$ is a topological groupoid, and the morphism sets are complete in the natural 'p-adic' topology.

It is possible to describe the non-Bockstein part of the algebra ${}^{\mathrm{ss}}E\ell\ell_*{}^{\mathrm{ss}}E\ell\ell$ as an algebra of continuous functions on this category taking values in $\overline{\mathbb{F}}_p$ and possessing a suitable equivariance under the action of the Frobenius on the domain and codomain.

For $p \nmid n$ there are Hecke-like operations T_n in ${}^{\mathrm{ss}}E\ell\ell^*(\ )$ just as before, constructed using geometric isogenies. There are other operations originating with the 'connected pro-schemes'

$$\widetilde{\mathbf{SepIsog}}_{\mathrm{ss}}(\mathcal{E},\mathcal{E}) = \mathrm{InvtHom}_{\mathbb{D}_{\Bbbk}}(\mathcal{T}_p\mathcal{E},\mathcal{T}_p\mathcal{E}).$$

Slide 18

Theorem 5.2 *The separable isogeny categories* $\mathbf{SepIsog}_{\mathrm{ss}}$ *and* $\widetilde{\mathbf{SepIsog}}_{\mathrm{ss}}$ *are connected.*

The following stronger result gives more information about the global structure. The quotient category $\mathbf{C} = \widetilde{\mathbf{SepIsog}}_{\mathrm{ss}}/\mu_{p^2-1}$ has object set consisting of ring homomorphisms ${}^{\mathrm{ss}}E\ell\ell_*{}^{\mu_{p^2-1}} \longrightarrow \overline{\mathbb{F}}_p$, where μ_{p^2-1} acts on ${}^{\mathrm{ss}}E\ell\ell_{2n}$ by $\alpha \cdot x = \alpha^n x$.

Theorem 5.3 *Let* $\mathcal{E}_0$ *be an object of* $\mathbf{C}$. *Then there is a continuous map* $\sigma\colon \mathbf{C} \longrightarrow \mathrm{Obj}\,\mathbf{C}$ *for which*

$$\mathrm{dom}\,\sigma(\mathcal{E}) = \mathcal{E}_0, \quad \mathrm{codom}\,\sigma(\mathcal{E}) = \boldsymbol{\mathcal{E}}.$$

Hence there is a splitting of topological groupoids

$$\mathbf{C} \cong \mathrm{Obj}\,\mathbf{C} \rtimes \mathrm{Aut}_{\mathbf{C}}\,\mathcal{E}_0.$$

Slide 19

For each prime p there is always a supersingular elliptic curve $\mathcal{E}_0$ defined over $\mathbb{F}_p$, and then $\mathrm{Aut}_{\mathbf{C}}\,\mathcal{E}_0 \cong \mathbb{S}_2$, the Morava stabilizer group. This gives

Theorem 5.4 *There is an equivalence between the Hopf algebroids $(E\ell\ell_*/(p, A), E\ell\ell_*E\ell\ell/(p, A))$ and $(K(2)_*, K(2)_*K(2))$. Hence, there is an isomorphism*

$$\mathrm{Ext}^{*,*}_{E\ell\ell_*E\ell\ell}(E\ell\ell_*, E\ell\ell_*/(p, A)) \cong \mathrm{Ext}^{*,*}_{K(2)_*K(2)}(K(2)_*, K(2)_*)$$

Slide 20

References

[1] A. Baker, Operations and cooperations in elliptic cohomology, Part I: Generalized modular forms and the cooperation algebra, New York J. Math. **1** (1995), 39–74.

[2] A. Baker, Hecke algebras acting on elliptic cohomology, to appear in Contemp. Math., 'Homotopy theory via algebraic geometry and group representations', edited by M. Mahowald and S. Priddy.

[3] A. Baker, Hecke operations and the Adams E_2-term based on elliptic cohomology, to appear in Can. Bull. Math.

[4] A. Baker, Isogenies of supersingular elliptic curves over finite fields and operations in elliptic cohomology, Glasgow University Mathematics Department preprint 98/39.