Atkin Memorial Workshop,
Chicago, 28/4/12
2pm

# Elusive Isogenies and Unusual Modular Curves

(Joint with B. Banwait, and following A.V. Sutherland).

In a recent paper (to appear in JNTB) Sutherland asked the question

"If an elliptic curve $E$ defined over a number field $K$ admits an $\ell$-isogeny locally everywhere, must $E$ admit an $\ell$-isogeny over $K$?"

giving a criterion and a complete answer for $K = \mathbb{Q}$. BB and I have been extending Sutherland's results, and in particular will show that the answer is "no" when $\ell = 5$ and $K = \mathbb{Q}(\sqrt{5})$ for infinitely many values $j(E) \in K$.

---

- $\ell$ will denote a prime number throughout. Recall that $E$ is said to "admit an $\ell$-isogeny over $K$" if there is an isogeny $E \to E'$ of degree $\ell$ defined over $K$, or equivalently if $E(\bar{K})$ has a subgroup of order $\ell$ stable under the action of $G_K = \mathrm{Gal}(\bar{K}/K)$.

- Such a subgroup is necessarily one of the $\ell+1$ subgroups of order $\ell$ in $E[\ell]$, on which $G_K$ acts via the "projective mod-$\ell$" Galois representation

$$\bar{\rho}_{E,\ell} : G_K \xrightarrow{GL(2,\mathbb{F}_\ell)} PGL(2, \mathbb{F}_\ell)$$

(after fixing a basis for $E[\ell]$)

which we may view as giving a permutation action of $G_K$ on $\mathbb{P}^1(\mathbb{F}_\ell)$.

- $E$ admits an $\ell$-isogeny over $K$ iff this action has a fixed point, i.e. $H := \bar{\rho}_{E,\ell}(G_K) \subset \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \subset PGL(2,\ell)$.

If $\mathfrak{p}$ is a prime of $K$ where $E$ has good reduction & $\mathfrak{p} \nmid \ell$ then $\bar{\rho}_{E,\ell}(\mathrm{Frob}_\mathfrak{p})$ is well-defined up to conjugacy, and

"E admits an $\ell$-isogeny modulo $\mathfrak{p}$" means that the reduction of E mod $\mathfrak{p}$, which is an elliptic curve over the finite field $\mathcal{O}_K/\mathfrak{p}$, admits an $\ell$-isogeny; this is if and only if

$$\bar{\rho}_{E,\ell}(\mathrm{Frob}_{\mathfrak{p}}) \quad \text{has a fixed point in } \mathbb{P}^1(\mathbb{F}_\ell).$$

- So clearly if E admits an $\ell$-isogeny over K then " " " " mod $\mathfrak{p}$ for almost all $\mathfrak{p}$ and Sutherland asks if the converse holds.

- If E admits an $\ell$-isogeny then so do all twists of E, so the question only depends on $j(E)$. We say that a pair ~~$(j,\ell)$~~ $(\ell, j)$ with $j \in K$ is <u>exceptional</u> for K if (all) $E/K$ with $j(E) = j$ <u>do</u> admit $\ell$-isogenies mod $\mathfrak{p}$ for almost all $\mathfrak{p}$, but <u>do not</u> admit " over K itself.

<u>Theorem</u> (Sutherland) When $K = \mathbb{Q}$, the only exceptional pair is

$$(\ell, j) \; \cancel{(j,\ell)} = \left(17, \frac{2268945}{128}\right).$$

<u>Theorem</u> (BB & JC) Over $K = \mathbb{Q}(\sqrt{5})$, $(5, j)$ is exceptional if and only if $\exists s \in K$:

$$j = \left((s+5)(s^2-5)(s^2+5s+10)\right)^3 / (s^2+5s+5)^5$$

(where $s \in K$) and $\sqrt{s^2-20} \notin K^*$.

To see where these results come from we must study

- Group theory, in particular subgroups of $PGL(2,\ell)$ & how they act on $\mathbb{P}^1(\mathbb{F}_\ell)$
- Modular curves of level $\ell$.

Group theory • Elements $^{\neq 1}$ of $PGL(2,\ell)$ have 0, 1 or 2 fixed pts (= # of eigenvalues of associated matrix) and for orders coprime to $\ell$, only 0 or 2.

• $PSL(2,\ell) \leq PGL(2,\ell)$ with index 2 ($\ell \geq 3$)

& image $H \subseteq PSL(2,\ell) \Leftrightarrow \sqrt{\ell^*} \in K$ where $\ell^* = \pm \ell \equiv 1 \pmod 4$.

Let $G$ be the image of $G_K$ in $GL(2,\ell)$ & $H$ its image in $PGL(2,\ell)$. Properties of the Weil pairing + Galois theory imply: $\zeta_\ell \in K \Leftrightarrow G \leq SL(2,\ell)$
$\sqrt{\ell^*} \in K \Leftrightarrow H \leq PSL(2,\ell)$. } independent of $E$

Assume $\ell \nmid \# G$. Then the well-known classification gives:
either (a) $H$ cyclic, $G \leq$ Cartan (split or non-split)
or (b) $H$ dihedral, $G \leq$ Normalizer of Cartan, $\not\leq$ Cartan
or (c) $H \cong A_4, S_4, A_5$.
The last 3 we'll call "unusual". NB $A_4, A_5$ cannot occur $/\mathbb{Q}$ since necessarily $\leq PSL$

Sutherland's main group-theoretical result is:
**Prop^n** (AVS) Assume $H \not\leq PSL(2,\ell)$, every $h \in H$ has a fixed pt and no pt is fixed by all of $H$. Then
(1) $H$ is dihedral, $\# H = 2n$, $n > 1$, $n$ odd, $2n \mid \ell - 1$.
(2) $G \lneq$ normalizer of a split Cartan
(3) $\ell \equiv 3 \pmod 4$
(4) $H$ has an orbit of size 2 on $\mathbb{P}^1(\mathbb{F}_\ell)$.

From this he derives
**Theorem** (AVS) If $\sqrt{\ell^*} \notin K$ and $E/K$ admits an $\ell$-isogeny mod $p$ for a set of primes of density 1, then • $E$ admits an $\ell$ isogeny over a quadratic ext^n of $K$
• If $\ell \equiv 1 \pmod 4$ or $\ell < 7$ then $E$ admits $\ell$-isog. $/K$.

For counterexamples in Sutherland's scenario $\sqrt{\ell^*} \notin K$ take $\ell \equiv 3 \pmod 4$, $\ell \geq 7$ & let $H$ be the image in PGL of the subgp of GL of the form

$$\left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}, \begin{pmatrix} 0 & \alpha \\ \beta & 0 \end{pmatrix} \right\}$$

with $\alpha, \beta \in \mathbb{F}_\ell^*$ both squares or both non-squares i.e. $\alpha\beta = \square$

(so $\begin{pmatrix} 0 & \alpha \\ \beta & 0 \end{pmatrix}$ has fixed pts $\pm\sqrt{\alpha/\beta}$)

which $\not\subseteq$ PSL since $-1 \neq \square$

Taking $\ell = 7$, elliptic curves whose mod-$\ell$ rep$^{\underline{n}}$ are contained in this subgroup are parametrized by a quotient of the modular curve $X(7)$, of genus 1, which turns out to be (as explained by Elkies in his article in the book on the Klein quartic) a twist of $X_0(49)$ [with eqn

$$-7y^2 = x^4 + 2x^3 - 9x^2 - 10x - 3 \,]$$

which is $\cong$ 49a3, which only has 2 rational pts, yielding one $j$ invariant as stated.

To rule out $\ell > 7$ one uses a result of Parent to show that $E$ must have CM & then rule out that. (on $X_0^+(\ell^2)(\mathbb{Q})$)

---

What if $\sqrt{\ell^*} \in K$? eg $K = \mathbb{Q}(\sqrt{5})$, $\ell = 5$?

<u>Prop$^{\underline{n}}$</u> (BB) $\sqrt{\ell^*} \in K$, $(\ell, E)$ exceptional $\Rightarrow$

<u>either</u> $H \cong A_4$, $\ell \equiv 1 \pmod{12}$

<u>or</u> $H \cong A_5$, $\ell \equiv 1 \pmod{60}$

<u>or</u> [Similar to Sutherland] $H \cong D_{2n}$, $n > 1$, $2n \mid \ell - 1$, $G \leq$ normalizer of a split Cartan, $\ell \equiv 1 \ (4)$

In the last case, $E$ comes from a $K$-rational non-cuspidal point on $X_{split}(\ell)$.

**The $\ell=5$ case** Now $H \cong V_4$ (Klein 4-group)

$X_{split}(5) \cong X_0^+(25)$ (via) induced by $\tau \mapsto 5\tau$ on $\mathfrak{h}$

Let $t_N$ be a Hauptmodul for $X_0(N)$ (when its genus is 0).
Then

$$j(5\tau) = (t_5^2 + 250t_5 + 3125)^3/t_5^5 \qquad \text{[Klein, 1879]}$$

while $$t_5 = t_{25}(t_{25}^4 + 5t_{25}^3 + 15t_{25}^2 + 25t_{25} + 25)$$

This gives the j-invariant of our curve in terms of $t_{25}$, but $X_0^+(25) = X_0(25)/w_{25}$ & $w_{25} : t_{25} \mapsto 5/t_{25}$ so we set $s = t_{25} + 5/t_{25}$ & find that

$$j(5\tau) = ((s+5)(s^2-5)(s^2+5s+10))^3/((s^2+5s+5))^5$$

is the j-invariant of an $E$ whose projective mod 5 rep$^n$ is contained in the normalizer of the split Cartan (order 8, $\cong D_4$). For it not to be contained in the split Cartan itself ($\Rightarrow E$ has a $K$-rational 5-isogeny) we require $t_{25} \notin K$, and since $t_{25}^2 - st_{25} + 5$ has discriminant $s^2-20$ this is where the extra condition $s^2-20 \notin K^2$ comes from. & when $\sqrt{5} \in K$ the image $\subseteq D_4 \cap PSL = V_4$.

**$A_4$, $A_5$ examples?** To get an $A_4$ image with an exceptional curve we require $\ell \equiv 1 \pmod{12}$
(since $\ell \equiv 1$ (3) $\Leftrightarrow$ elts of order 3 have fixed pts,
$\ell \equiv 1$ (4) $\Leftrightarrow$ " " " 2 " " " ).
When $\ell = 13$ this gives a modular curve $X_{A_4}(13)$ which has genus 3. We are close to finding a model for this curve over $\mathbb{Q}(\mathbb{J}_{13}^+)$, but not there yet

$\square$