Yet More Nontrivial Elements in Shafarevich-Tate Groups of Fermat Curves

William McCallum
University of Arizona

May 9, 2006

Fermat curves

- p an odd prime, ζ a primitive p-th root of unity
- $$F_s : y^p = x^s(1-x), \quad 1 \le s \le p-2,$$
  genus $(p-1)/2$
- J_s the jacobian of F_s, complex multiplication by $\mathbb{Z}[\zeta]$
- $\lambda = 1-\zeta$, Selmer groups $S_{\lambda^k}(J,K)$
- $$0 \to J(K)/\lambda^k J(K) \to S_{\lambda^k}(J,K) \to Ш[\lambda^k] \to 0$$
- $$S_{\lambda^k}(J,K) \subset H^1(G, J[\lambda^k]),$$
  G the Galois group of the maximal extension of K unramified outside p

What does the Selmer group look like?

- First consider $k = 1$. Then

$$J[\lambda] \simeq \mathbb{Z}/p\mathbb{Z} \simeq \mu_p,$$

so we have (non-canonically), where E is the group of p-units

$$E/E^p \subset H^1(G, J[\lambda]) \subset K^\times/K^{\times p}.$$

- For $0 \leq i \leq p+1$, we define a local condition at $\mathfrak{p}$, the prime above p, by demanding, for $x \in H^1(G, J[\lambda])$, that $x_\mathfrak{p} \in (1 + \mathfrak{p}^i \mathcal{O}_\mathfrak{p})$ mod local p-th powers, and denote the corresponding "Selmer group" by S_i. Then Faddeev showed that

$$\mathrm{Sel}_{(p+3)/2} \subset S_\lambda(J, K) \subset \mathrm{Sel}_{(p-1)/2}\,.$$

- $\omega : G_\mathbb{Q} \to \mathbb{Z}_p^\times$ the Teichmüller character, $K = \mathbb{Q}(\zeta)$

Early nontriviality result

Theorem (McCallum)

If $p \equiv 1 \pmod 4$, does not divide $B_{(p-1)/2}B_{(p+3)/2}$, and if F_s is wild split, then $\text{Ш} \supset (\mathbb{Z}/p\mathbb{Z})^2$.

- The elements of Ш in question are cyclotomic units $\eta_{(p-1)/2}$ and $\eta_{(p+3)/2}$, where

  $$\eta_i = (1-\zeta)^{\epsilon_i}, \quad \epsilon_i \text{ the projector onto the } \omega^i \text{ eigenspace.}$$

  Fact: $\eta_i \in \mathrm{Sel}_i$.
- Wild split is a condition on the reduction type of F_s.
- Method was to calculate the Cassels pairing (computer helped).
- E.g., $y^{17} = x(1-x)$.

Later nontriviality result

Theorem (McCallum-Tzermias)

Suppose that $p \geq 19$ is regular, $p \equiv 3 \pmod 4$, F_s is tame or wild non-split and

$$q(s^s/(s+1)/(s+1))^3 - s(s+1)B_{p-3} \not\equiv 0 \pmod p, \quad (1)$$

where $q(x) = (x^{p-1} - 1)/p$. Then $Ш(J, K) \supset (\mathbb{Z}/p\mathbb{Z})^4$.

- Works with Cassels pairing between $Ш[\lambda^3]$ and $Ш[\lambda]$.
- Greenberg showed $J[\lambda^3] \simeq (\mathbb{Z}/p\mathbb{Z})^3$ as G-modules, so we identify $H^1(G, J[\lambda^3])$ with a finite subgroup of $(K^\times/K^{\times p})^3$, which contains $(E/E^p)^3$
- E.g, $y^{19} = x^2(1-x)$

Most recent nontriviality result

- Let

$$\langle\ ,\ \rangle : H^1(G, \mu_p) \times H^1(G, \mu_p) \to H^2(G, \mu_p) \otimes \mu_p$$

be the cup product pairing. Yields a pairing

$$E \times E \to C/pC \otimes \mu_p,$$

where C is the ideal class group.

Theorem (Levitt-McCallum)

Suppose p divides B_r, $p - r + 3 \geq \frac{p+1}{2}$, F_s is wild nonsplit or tame, and $\langle \eta_{p-r+3}, \eta_{p-3} \rangle \neq 0$. Then $(1, 1, \eta_{p-r+3}) \in S_{\lambda^3}(J, K)$ and its image in $Ш(J, K)$ is nontrivial.

- The pairing was *computed* by McCallum and Sharifi for $p = 37$ and found to be nontrivial, and Sharifi subsequently showed nontriviality of the pairing for $p \leq 15{,}000$
- Does not use Cassels pairing
- E.g., $y^{691} = x^5(1-x)^{29}$

Consider the diagram

$$\begin{array}{ccccc}
J(K)/\lambda^4 J(K) & \longrightarrow & J(K)/\lambda^3 J(K) & & \\
\downarrow & & \downarrow & & \\
S_{\lambda^4}(K,J) & \xrightarrow{\lambda_*} & S_{\lambda^3}(K,J) & \xrightarrow{\delta} & H^2(G, J[\lambda]) \\
& & \downarrow & & \\
& & Ш(K,J)[\lambda^3] & & \\
& & \downarrow & & \\
& & 0 & &
\end{array}$$

where δ is the coboundary for

$$0 \longrightarrow J[\lambda] \xrightarrow{i} J[\lambda^4] \xrightarrow{\lambda} J[\lambda^3] \longrightarrow 0 \, .$$

The method is to show that $\delta(1, 1, \eta_{p-r+3}) = \langle \eta_{p-r+3}, \eta_{p-3} \rangle$.

- The η_{p-3} comes from yet another theorem of Greenberg, and subsequent work of Kashiwahara, showing
$$K(J[\lambda^4]) = K(\eta_{p-3}^{1/p}).$$
- Key point: if you have an extension
$$0 \to \mathbb{Z}/p\mathbb{Z} \to M \to \mathbb{Z}/p\mathbb{Z} \to 0$$
given by the character of χ, then the coboundary is cup product with χ.
- Moral of the story: take a random non-zero element of the Selmer group, it's probably non-zero in Ш.