Growth of Selmer rank in nonabelian extensions of number fields

Karl Rubin

Selmer groups, L-functions, and Galois deformations

UCLA

3-25-2008

Joint work with Barry Mazur Rubin

K = # field, $p > 2$ prime

$$\begin{tikzcd} F \arrow[d, dash, "p^n"', "G"] \arrow[dd, dash, bend right=60, "\text{Galois}"'] \\ K \arrow[d, dash, "2"'] \\ k \end{tikzcd}$$

F/k Galois of degree $2p^n$

$G = \mathrm{Gal}(F/K)$

$c = \mathrm{Gal}(F/k)$ order 2.

$$c : G \longrightarrow G$$
$$g \longmapsto cgc = g^c$$

$$G^+ = \{ g \in G : g^c = g \}$$

E/k elliptic curve

$$0 \longrightarrow E(F) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow \mathrm{Sel}_{p^\infty}(E/F) \longrightarrow Ш_{E/F}[p^\infty] \longrightarrow 0$$

$$\mathrm{rk}_p(E/F) = \mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(E/F).$$

Conjecturally, $\mathrm{rk}_p(E/F) = \mathrm{rank}\, E(F)$.

<u>Theorem:</u> Suppose ① $\mathrm{rk}_p(E/K)$ is odd

② $\forall$ prime $v \nmid p$ of k where E has bad reduction either v splits in K/k or v unram in F/K.

③ $\forall$ prime $v \mid p$ of k either E has good ordinary reduction at v or v splits in K/k, or ...

Then $\mathrm{rk}_p(E/F) \geq [G : G^+]$.

More precisely,

$$\mathrm{Hom}(\mathrm{Sel}_{p^\infty}(E/F), \mathbb{Q}_p/\mathbb{Z}_p) \otimes \mathbb{Q}_p$$

contains a copy of $\mathbb{Q}_p[G/G^+]$.

In fact, every irreducible constituent of $\mathbb{Q}_p[G/G^+]$ occurs with odd multiplicity in $\mathrm{Hom}(\mathrm{Sel}_{p^\infty}(E/F), \mathbb{Q}_p/\mathbb{Z}_p) \otimes \mathbb{Q}_p$.

Remark: 1) $L(E/F, s) = \prod_{\substack{\text{irred} \\ \rho \text{ of } G}} L(E \otimes \rho, s)^{\dim \rho}$

Can produce $[G:G^+]$ zeros of from functional equations.

2) Where do these Selmer classes and hopefully rational points come from?

Examples: 0) F/k abelian, then $G^+ = G$, so this says $rk_p(E/F) \geq 1$, which is not new since we assumed it to be odd.

1) F/k dihedral, $\mathrm{Gal}(F/k) = D_{2p^n}$.

Then $G^+ = \{1\}$, so $rk_p(E/F) \geq [F:K]$.

2) $A/\mathbb{Q}$, $E/\mathbb{Q}$ elliptic curve, no CM, with a rational point of order p. Suppose E has good ordinary reduction at p, every prime where both E and A have bad reduction has odd order in $\mathbb{F}_p^\times$.

If $-N_E$ is not a square in $\mathbb{F}_p^\times$, then $\exists\, c > 0$ independent of E, n s.t.

$$\mathrm{rk}_p\,(E/\mathbb{Q}(A[p^n])) \geq C p^{2n}.$$

<u>Proof:</u> $K = \mathbb{Q}(\mu_p)$,

$k = \mathbb{Q}(\mu_p)^+$

$F = \mathbb{Q}(A[p^n])$

$G \subset \left\{ \gamma \in GL_2(\mathbb{Z}/p^n\mathbb{Z}) : \gamma \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \bmod p \right\}$

$G^+ = G \cap (\text{diagonal matrices})$ $\square$

$E = A = 91A1 =$

$y^2 + y = x^3 + x^2 + 13x + 42$

$p = 3$

$\mathrm{rk}_p(E/\mathbb{Q}(E[p^n])) \geq p^{2n-2}$.

3) $k = \mathbb{Q}$, K imaginary quadratic

$H_0 = K$, H_{n+1} = maximal abelian unram. p-ext of H_n.

<u>Thm:</u> Suppose $\chi_K(N_E) = 1$ and either p splits in K or (p is inert in K and $p > 3$), then

$$\mathrm{rk}_p(E/H_{2n-1}) \geq \sum_{i=1}^{n} [H_{2n-1} : H_{2n-2}].$$

<u>Ex:</u> $p = 5$, $K = \mathbb{Q}(\sqrt{-51213139})$. If N_E is a square modulo 51213139, then

$$\mathrm{rk}_p(E/H_n) \to \infty.$$

Proof of Main Thm: Goes in 2 steps:

1) Dihedral case

2) Use 1) and pure group theory to deduce the general case.

We start with 1):

$$\begin{array}{c} F \\ {\scriptstyle \mathbb{Z}/p^r\mathbb{Z}}\Big| \; G \\ K \\ \Big| \\ k \end{array}$$

restriction of scalars

$$\mathrm{Res}^F_K E \simeq E \times A_1 \times \cdots \times A_n \quad , A_i \text{ abelian vars.}$$

$$\dim(A_r) = p^r - p^{r-1}$$

$$\mathbb{Z}[\zeta_{p^r}] \subset \mathrm{End}_K(A_r)$$

$$\pi_r = \zeta_{p^r} - 1$$

$$\mathrm{Sel}_{p^\infty}(E/F) \simeq \mathrm{Sel}_{p^\infty}((\mathrm{Res}^F_K E)/K)$$

$$\simeq \mathrm{Sel}_{p^\infty}(E/K) \times \cdots \times \mathrm{Sel}_{p^\infty}(A_n/K)$$

Key fact: $E[p] \simeq A_r[\pi_r]$ as Galois-modules.

$$\begin{array}{ccc} \mathrm{Sel}_p(E/K) & \subset & H^1(K, E[p]) \\ & & \wr\!\wr \\ \mathrm{Sel}_{\pi_r}(A_r/K) & \in & H^1(K, A_r[\pi_r]) \end{array}$$

Thm: Under hypotheses of main thm,

$$\dim_{\mathbb{F}_p}(\mathrm{Sel}_p(E/K)) \equiv \dim_{\mathbb{F}_p}(\mathrm{Sel}_{\pi_r}(A_r/K)) \pmod 2.$$

Assuming this theorem, and assuming $E(K)[p] = 0$, we have

$$\mathrm{rk}_p(E/K) \equiv \dim_{\mathbb{F}_p}(\mathrm{Sel}_p(E/K)) \pmod 2$$

Cassels pairing

$$\equiv \dim_{\mathbb{F}_p}(\mathrm{Sel}_{\pi_r}(A_r/K)) \pmod 2$$

$$\equiv \operatorname{corank}_{\mathbb{Z}_p[\zeta_{p^r}]} \mathrm{Sel}_{p^\infty}(A_r/K) \pmod 2$$

$\uparrow$

Tricky A_r has no polarization of degree prime to p.

This is where the dihedral nature is used.

$$\equiv \mathrm{rk}_p(A_r/K) \big/ (p^r - p^{r-1}) \pmod 2$$

So $\mathrm{rk}_p(E/K)$ odd $\Rightarrow$ $\mathrm{rk}_p(A_r/K) \geq p^r - p^{r-1}$ and so

$$\mathrm{rk}_p(E/F) = \mathrm{rk}_p(E/K) + \sum_{r=1}^{n} \mathrm{rk}_p(A_r/K) \geq p^n.$$

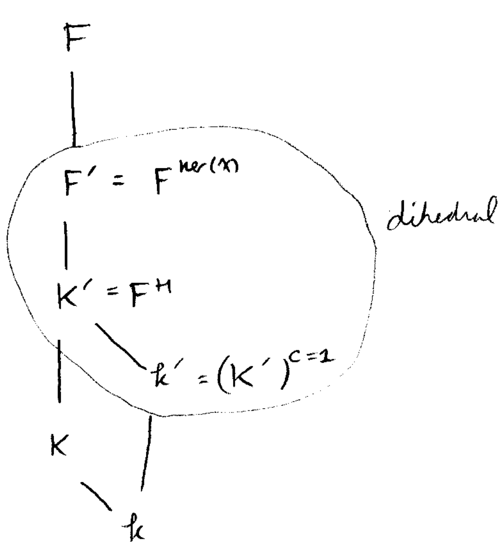
We now return to the general case 2):

$$\mathbb{X} = \{ \text{irred. complex chars. of } G \text{ s.t. } \chi(gc) = \bar{\chi}(g) \ \forall g \in G \}$$

<u>Prop:</u> $\mathrm{Ind}_{G^+}^{G} \mathbb{1}_{G^+} = \sum_{\chi \in \mathbb{X}} \chi$.

<u>Prop:</u> If $\chi \in \mathbb{X}$, then $\exists$ subgroup $H \subset G$, $H^c = H$ and a 1-dim. character $\Psi : H/H^+ \longrightarrow \mathbb{C}^\times$ s.t. $\chi = \mathrm{Ind}_H^G \Psi$.

Let $\chi \in \mathbb{X}$, H, Ψ.



check the hypotheses of theorem apply to

$$\begin{array}{c} F' \\ | \\ K' \\ | \\ k' \end{array}.$$

By the dihedral case we conclude ψ occurs in

$$\mathrm{Hom}\left(\mathrm{Sel}_{p^\infty}(E/F'), \mathbb{Q}_p/\mathbb{Z}_p\right)$$

as a $\mathrm{Gal}(F'/K')$-module

$\Rightarrow$ ψ occurs in $\mathrm{Hom}\left(\mathrm{Sel}_{p^\infty}(E/F), \mathbb{Q}_p/\mathbb{Z}_p\right)$

as H-module.

$\Rightarrow$ $\chi = \mathrm{Ind}_H^G \psi$ occurs in $\mathrm{Hom}\left(\mathrm{Sel}_{p^\infty}(E/F), \mathbb{Q}_p/\mathbb{Z}_p\right)$

as G-module.

This holds $\forall\, \chi \in X$, so $\mathrm{Ind}_{G^+}^G \mathbb{1}_{G^+}$ occurs in

$$\mathrm{Hom}\left(\mathrm{Sel}_{p^\infty}(E/F), \mathbb{Q}_p/\mathbb{Z}_p\right). \quad \blacksquare$$