Trevor Arnold - Parity in Iwasawa Theory for CM Curves

By W. Stein

I. Ranks of Elliptic curves:

II Iwasawa theory

III Generalizations

I. Ranks

E/k elliptic curve over a number field k. $f(x,y)=0$.

We are interested in, for a number field F (which contains k),

$$E(F) = \{(x,y) \in F^2 : f(x,y)=0\} \cup \{\infty\}.$$

Thm (M-W): $E(F) \cong \mathbb{Z}^{r(E/F)} \oplus E(F)_{tors}$.

$E(F)_{tors}$ is well understood.

$r(E/F)$ is mysterious.

Question: How does $r(E/F)$ change as F changes?

Aside on Ш: If F is a number field, then there is an exact sequence (p = prime)

$$0 \to E(F) \otimes \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{\delta} \mathrm{Sel}(F, E[p^\infty]) \to Ш(E/F)[p^\infty] \to 0$$

$$(\mathbb{Q}_p/\mathbb{Z}_p)^{r(E/F)} \cong \qquad \mathrm{Sel}(F, E[p^\infty]) \subset H^1(F, E[p^\infty])$$

Ш-conj for F: $|Ш(E/F)[p^\infty]| < \infty$. Assume this for all F, E, etc.

Let K/k be a quadratic extension of number fields.

Let K_∞ be an infinite Galois extension of K s/t.

- $\mathrm{Gal}(K_\infty/K) \approx \mathbb{Z}_p$
- K_∞/k is Galois
- $1 \neq \tau \in \mathrm{Gal}(K/k)$ acts on $\mathrm{Gal}(K_\infty/K)$ by inversion.

<u>Theorem 1</u> (Mazur, Rubin, Nekovar) Assume p good ordinary for E, $E(K)_{tor} = 0$, $p \nmid c_v$ for all v.

<u>If $r(E/K)$ is odd, then $r(E/F) \geq [F:K]$ for $K \subseteq F \subseteq K_\infty$.</u>

<u>Recall</u>: E/F has <u>CM by L</u> (= quadratic imag. extension of $\mathbb{Q}$) if $\mathrm{End}_{\bar{\mathbb{Q}}}(E) \cong \mathcal{O}$ — rank 2 $\mathbb{Z}$-subalgebra of $\mathcal{O}_L$ (an "order").

Suppose E/k has CM by L and $K := Lk \neq k$.

<u>Fact</u> $\mathrm{End}_{\bar{\mathbb{Q}}} E = \mathrm{End}_K E$

Thus $E(K)$ is an $\mathcal{O}$-module, so $r(E/K)$ is <u>even</u>.

<u>Theorem 2</u>: Assume p is a good ordinary prime for E and above setup. If the $\mathcal{O}$-rank of $E(K)$ is odd, e.g. $r(E/K) \equiv 2 \pmod 4$, then

$$r(E/F) \geq 2\,[F:K]$$

for all $K \subseteq F \subseteq K_\infty$.

II. <u>Iwasawa</u> <u>theory</u>:

Thm 2 can be rephrased as a theorem about the structure of the module $X = \mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{Sel}(K_\infty, E[p^\infty]), \mathbb{Q}_p/\mathbb{Z}_p)$ over the ring $\Lambda = \mathbb{Z}_p[[\mathrm{Gal}(K_\infty/K)]] \cong \mathbb{Z}_p[[T]]$

Fact: X is a finitely generated Λ-module.

Structure of Λ modules.

If M f.g. Λ modules, then

$$M \longrightarrow \Lambda^{r(M)} \oplus \bigoplus_i \Lambda/(f_i) \oplus (\mathbb{Z}_p\text{-torsion module})$$

with finite kernel and cokernel, and the $f_i \in \Lambda$ ~~be~~ can be taken as polynomials w/ unit leading terms.

The numbers $r(M)$ and $\lambda(M) = \mathrm{rank}_{\mathbb{Z}_p} \Lambda/(f_i)$ are invariants — the rank and λ-invariant — are invariants of M.

(Same hypo as Thm 2.)

Thm 2': $\lambda(X) \equiv 0 \pmod 4$, in fact "each f_i appears in multiples of 4".

Finally $\text{Thm } 2' \underset{\text{(Mazur Control theorem)}}{\Longrightarrow} \text{Thm } 2$

Remarks about thm 2'.

Assumptions on $p \Rightarrow p\mathcal{O}_L = \mathfrak{p}\cdot\bar{\mathfrak{p}}$, so

$$E[p^\infty] \cong E[\mathfrak{p}^\infty] \oplus E[\bar{\mathfrak{p}}^\infty].$$

So $X = X_{\mathfrak{p}} \oplus X_{\bar{\mathfrak{p}}}$

I show $X_{\mathfrak{p}} \underset{\text{quasi-isom.}}{\sim} \Lambda^{r(X_{\mathfrak{p}})} \oplus \underbrace{M \oplus M}_{\text{cyclic}} \oplus (\mathbb{Z}_p\text{-torsion})$

III. Generalizations

More generally, suppose A/k of dim g with CM by F

F = CM field of dim $2g$ over $\mathbb{Q}$

Assume $K = kF^* = k$ and $1 \neq \tau \in \mathrm{Gal}(kF^*/k)$

F^* = reflex field

stabilizes F and $F^\tau = F^+$.

Thm: If $r(A/K) \equiv 2g \pmod{4g}$, then $r(A/L) \geq 4g[L:K]$

for any $K \leq L \leq K_\infty$.