Rational torsion in elliptic curves and the cuspidal subgroup *

Amod Agashe
Florida State University

October 28, 2009

*Slides available at:
http://www.math.fsu.edu/~agashe/math.html

An elliptic curve E over $\mathbf{Q}$ is an equation of the form $y^2 = x^3 + ax + b$, where $a, b \in \mathbf{Q}$ and $\Delta(E) = -16(4a^3 + 27b^2) \neq 0$, along with a point O at infinity.

Example: The graph of $y^2 = x^3 - x$ over $\mathbf{R}$:

The abelian group $E(\mathbf{Q})$ is finitely-generated. By Mazur, $E(\mathbf{Q})_{\text{tor}}$ is one of the following 15 groups:
$\mathbf{Z}/m\mathbf{Z}$, with $1 \leq m \leq 10$ or $m = 12$;
$\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2m\mathbf{Z}$, with $1 \leq m \leq 4$.

$E =$ an elliptic curve over $\mathbf{Q}$.
Goal: To understand the torsion subgroup $E(\mathbf{Q})_{\mathsf{tor}}$ in terms of its modular parametrization.

$N =$ conductor of E.
$X_0(N) =$ modular curve over $\mathbf{Q}$; so
$X_0(N)(\mathbf{C}) = \Gamma_0(N)\backslash(\mathcal{H} \cup \mathbf{P}^1(\mathbf{Q}))$, where
$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) : N \mid c \right\}$.
$J_0(N) =$ Jacobian of $X_0(N)$; so
$J_0(N)(\mathbf{C}) =$ degree zero divisors on $X_0(N)(\mathbf{C})$ modulo divisors associated to functions.

Up to isogeny, E is a quotient of $J_0(N)$; assume it is an optimal quotient. Using the dual map, E can be viewed as an abelian subvariety of $J_0(N)$ (i.e., E is the abelian subvariety of $J_0(N)$ associated to a newform).

Cusps of $X_0(N) = \Gamma_0(N)\backslash\mathbf{P}^1(\mathbf{Q})$
Cuspidal subgroup, $C_N =$ degree zero divisors supported on cusps modulo divisors associated to functions; e.g., $(0) - (\infty) \in C_N$.
C_N is a finite group, and if N is square free, then $C_N \subseteq J_0(N)(\mathbf{Q})$.

Theorem (Mazur): If N is prime, then $J_0(N)(\mathbf{Q})_{\text{tor}} = C_N$; so $E(\mathbf{Q})_{\text{tor}} \subseteq C_N$, i.e. the cuspidal subgroup "accounts for" all of $E(\mathbf{Q})_{\text{tor}}$.

Theorem (Lorenzini, Ling): If N is a power of a prime ≥ 5, then $J_0(N)(\mathbf{Q})_{\text{tor}}^{(6N)} = C_N(\mathbf{Q})^{(6N)}$; so $E(\mathbf{Q})_{\text{tor}}^{(6N)} \subseteq C_N$.

Based on data of Cremona and Stein: suspect that $E(\mathbf{Q})_{\text{tor}} \subseteq C_N$ always.

Theorem: Suppose N is square-free. Let r be a prime such that $r \nmid 6N$. If r divides $|E(\mathbf{Q})_{\text{tor}}|$, then r divides $|C_N|$.
By Mazur's theorem, since $r \nmid 6$, $r = 5$ or 7, and $E(\mathbf{Q})_r$ is cyclic; so $E(\mathbf{Q})_{\text{tor}}^{(6N)} \subseteq C_N$.

Applications:
1) Computation of $|E(\mathbf{Q})_{\text{tor}}|$ (?): the proof implies that if r divides $|E(\mathbf{Q})_{\text{tor}}|$, then r divides $6 \cdot N \cdot \prod_{p|N}(p^2 - 1)$.
2) "Should" generalize to abelian subvarieties of $J_0(N)$ associated to newforms.
3) Relevant to the second part of the Birch and Swinnerton-Dyer conjecture.

$L(E,s) =$ the L-function of E
Suppose for simplicity that $L(E,1) \neq 0$. Then the second part of the Birch and Swinnerton-Dyer conjecture says

$$\frac{L(E,1)}{\Omega_E} = \frac{|\mathrm{Sha}_E| \cdot \prod_{p|N} c_p(E)}{|E(\mathbf{Q})_{\mathrm{tor}}|^2}, \text{where}$$

$\Omega_E =$ the real period (or two times it)
$\mathrm{Sha}_E =$ the Shafarevich-Tate group of E
$c_p(E) = [E(\mathbf{Q}_p) : E_{ns}(\mathbf{Q}_p)]$ is the arithmetic component group of E.

Theorem (Emerton): If N is prime, then the natural map $E \cap C_N \rightarrow \Phi_N(E)$ is an isomorphism (where $\Phi_N(E)$ is the "geometric" component group; in our situation, $c_N(E) = |\Phi_N(E)|$). So if N is prime, then $|E(\mathbf{Q})_{\mathrm{tor}}| = |E \cap C_N| = \prod_{p|N} c_p(E)$.

Thus the cuspidal group provides a link between $|E(\mathbf{Q})_{\mathrm{tor}}|$ and $\prod_{p|N} c_p(E)$.

Based on data of Cremona, suspect:
$|E(\mathbf{Q})_{\mathrm{tor}}^{(6)}|$ divides $\prod_{p|N} c_p(E)$ in general.

Proof of Theorem (sketch):
Recall that N is square-free, r is a prime s. t. $r \not| 6N$, and r divides $|E(\mathbf{Q})_{\text{tors}}|$. Need to show that r divides $|C_N|$. Let f be the cuspform corresponding to E.

Proposition: $r \not| a_r(f)$ and there is an Eisenstein series E_f such that $f \equiv E_f \bmod r$.
Then by a result of Tang, r divides $|E \cap C_N|$.

Proof of Proposition involves:
Lemma 1: If $\ell \not| N$, then $a_\ell(f) \equiv 1 + \ell \bmod r$ and if $p|N$, then $a_p(f) = -w_p = \pm 1$. In particular, since $r \not| N$, $r \not| a_r(f)$.

Lemma 2: There is an Eisenstein series E' such that for $\ell \not| N$, $a_\ell(E') = \ell + 1$, and for $p|N$, $a_p(E')$ can be chosen to be 1 or p provided at least one of them is 1.

Lemma 3: There is a $p|N$ such that $a_p(f) = 1$.

Lemma 4 (Dummigan): If $p|N$ is such that $a_p(f) = -1$, then $p \equiv -1 \bmod r$.