Rational torsion in elliptic curves and the cuspidal subgroup *

Amod Agashe
Florida State University

April 27, 2006

*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 $\mathbf{R}$:

Reducing the equation modulo a prime p gives a curve $\tilde{E}$ over $\mathbf{F}_p$. The reduced curve can be
non-singular – good reduction
have a node – multiplicative reduction
have a cusp – additive reduction

Mordell-Weil theorem:
The abelian group $E(\mathbf{Q})$ is finitely-generated.

Goal: To understand the torsion subgroup $E(\mathbf{Q})_{\text{tor}}$.

Mazur's theorem:
$E(\mathbf{Q})_{\text{tor}}$ 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 $1 \leq m \leq 4$.

$|E(\mathbf{Q})_{\text{tor}}|$ can be computed,
e.g., using the Lutz-Nagell theorem,
and by reducing modulo primes.

Theorem: Suppose E does not have additive reduction at any prime, and let N be the product of the primes of multiplicative reduction. Let ℓ be a prime that divides $|E(\mathbf{Q})_{\text{tor}}|$. Then ℓ divides $6 \cdot N \cdot \prod_{p|N}(p^2 - 1)$.

Applications:
1) Computation of $|E(\mathbf{Q})_{\text{tor}}|$?
2) Should generalize to certain abelian varieties associated to modular forms.
3) Relevant to the second part of the Birch and Swinnerton-Dyer conjecture.

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

$N =$ conductor of E.
Assume that N is square free and > 5.
$X_0(N) =$ 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 since N is square-free, $C_N \subseteq J_0(N)(\mathbf{Q})$.

Theorem (Emerton, Mazur): If N is prime, then $E(\mathbf{Q})_{\text{tor}} \subseteq C_N$.

Based on calculations of Cremona and Stein: Expect that $E(\mathbf{Q})_{\text{tor}} \subseteq C_N$ more generally if N is square-free (perhaps away from the prime 2, and perhaps even for arbitrary N).

Theorem: Let ℓ be a prime such that $\ell \nmid 6N$. If ℓ divides $|E(\mathbf{Q})_{\text{tor}}|$, then ℓ divides $|C_N|$.

Applications:
1) Computation of $|E(\mathbf{Q})_{\text{tor}}|$ (?): the proof implies that if ℓ divides $|E(\mathbf{Q})_{\text{tor}}|$, then ℓ 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.

Let $C_E = E \cap C_N$.

Theorem (Emerton): If N is prime, then the natural map $C_E \to \Phi_N(E)$ 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 $|E(\mathbf{Q})_{\mathrm{tor}}| = |C_E| = \prod_{p|N} c_p(E)$.

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

Based on calculations of Cremona and Stein, and theoretical considerations, expect that $|E(\mathbf{Q})_{\mathrm{tor}}|$ divides $\prod_{p|N} c_p(E)$ in general.

Proof of Theorem (sketch):

Let ℓ be a prime such that $\ell \nmid 6N$ and ℓ divides $|E(\mathbf{Q})_{\mathrm{tors}}|$. Need to show that ℓ divides $|C_N|$.

Let V be an irreducible constituent in the Jordan-Holder filtration of $A[\ell]$ as a $\mathbf{T}[G]$ module. Let $\mathbf{m} = \mathrm{Ann}_{\mathbf{T}}(V)$, which is a maximal ideal of $\mathbf{T}$ containing ℓ.

Let f be the cuspform corresponding to E. If $p \nmid N$, then $T_p - (p+1) \in \mathbf{m}$ and if $p \mid N$, then $U_p - w_p \in \mathbf{m}$, where $w_p =$ eigenvalue of W_p acting on f.

Dummigan defines an explicit cuspidal divisor $Q \in C_N$ such that the Hecke operators act the same way on Q modulo ℓ.

Associated to Q is an Eisenstein series E such that $\mathrm{ord}(Q) = a_0(E)$, and the above implies that $a_n(f) \equiv a_n(E) \bmod \mathbf{m}$ $\forall n \geq 1$. By a lemma of Mazur, $a_0(E) \in \mathbf{m}$, so $\ell \mid \mathrm{ord}(Q)$, i.e., ℓ divides $|C_N|$.