Conjectures concerning the orders of the torsion subgroup, the arithmetic component groups, and the cuspidal subgroup

Amod Agashe

Florida State University
Department of Mathematics

March 5, 2016

Torsion and component groups

Torsion and component groups

Let E be an elliptic curve over the rationals that is optimal.

Torsion and component groups

Let E be an elliptic curve over the rationals that is optimal.
Thus $E : y^2 = x^3 + ax + b$, with $a, b \in \mathbf{Q}$

Torsion and component groups

Let E be an elliptic curve over the rationals that is optimal.
Thus $E : y^2 = x^3 + ax + b$, with $a, b \in \mathbf{Q}$
$L_E(s)$ = the L-function of E

Torsion and component groups

Let E be an elliptic curve over the rationals that is optimal.
Thus $E : y^2 = x^3 + ax + b$, with $a, b \in \mathbf{Q}$
$L_E(s) =$ the L-function of $E = C_E(s-1)^r +$ higher order terms

Torsion and component groups

Let E be an elliptic curve over the rationals that is optimal.
Thus $E: y^2 = x^3 + ax + b$, with $a, b \in \mathbf{Q}$
$L_E(s) =$ the L-function of $E = C_E(s-1)^r +$ higher order terms
$\Omega_E =$ period integral of E
$R_E =$ regulator of E

Torsion and component groups

Let E be an elliptic curve over the rationals that is optimal.
Thus $E : y^2 = x^3 + ax + b$, with $a, b \in \mathbf{Q}$
$L_E(s) =$ the L-function of $E = C_E(s-1)^r +$ higher order terms
$\Omega_E =$ period integral of E
$R_E =$ regulator of E

Conjecture (Birch and Swinnerton-Dyer)

$\frac{C_E}{\Omega_E \cdot R_E} \stackrel{?}{=}$

Torsion and component groups

Let E be an elliptic curve over the rationals that is optimal.
Thus $E : y^2 = x^3 + ax + b$, with $a, b \in \mathbf{Q}$
$L_E(s) =$ the L-function of $E = C_E(s-1)^r +$ higher order terms
$\Omega_E =$ period integral of E
$R_E =$ regulator of E

Conjecture (Birch and Swinnerton-Dyer)

$\frac{C_E}{\Omega_E \cdot R_E} \stackrel{?}{=} \frac{|Ш_E| \cdot \prod_p c_p(E)}{|E(\mathbf{Q})_{\mathrm{tor}}|^2}$, *where*

Torsion and component groups

Let E be an elliptic curve over the rationals that is optimal.
Thus $E : y^2 = x^3 + ax + b$, with $a, b \in \mathbf{Q}$
$L_E(s) =$ the L-function of $E = C_E(s-1)^r +$ higher order terms
$\Omega_E =$ period integral of E
$R_E =$ regulator of E

Conjecture (Birch and Swinnerton-Dyer)

$\frac{C_E}{\Omega_E \cdot R_E} \stackrel{?}{=} \frac{|Ш_E| \cdot \prod_p c_p(E)}{|E(\mathbf{Q})_{\mathrm{tor}}|^2}$, *where*

$E(\mathbf{Q})_{\mathrm{tor}} =$ the torsion subgroup of $E(\mathbf{Q})$

Torsion and component groups

Let E be an elliptic curve over the rationals that is optimal.
Thus $E : y^2 = x^3 + ax + b$, with $a, b \in \mathbf{Q}$
$L_E(s) =$ the L-function of $E = C_E(s-1)^r +$ higher order terms
$\Omega_E =$ period integral of E
$R_E =$ regulator of E

Conjecture (Birch and Swinnerton-Dyer)

$\frac{C_E}{\Omega_E \cdot R_E} \stackrel{?}{=} \frac{|Ш_E| \cdot \prod_p c_p(E)}{|E(\mathbf{Q})_{\mathrm{tor}}|^2}$, *where*

$E(\mathbf{Q})_{\mathrm{tor}} =$ the torsion subgroup of $E(\mathbf{Q})$
$c_p(E) =$ Tamagawa number

Torsion and component groups

Let E be an elliptic curve over the rationals that is optimal.
Thus $E : y^2 = x^3 + ax + b$, with $a, b \in \mathbf{Q}$
$L_E(s) =$ the L-function of $E = C_E(s-1)^r +$ higher order terms
$\Omega_E =$ period integral of E
$R_E =$ regulator of E

Conjecture (Birch and Swinnerton-Dyer)

$\frac{C_E}{\Omega_E \cdot R_E} \stackrel{?}{=} \frac{|\text{Ш}_E| \cdot \prod_p c_p(E)}{|E(\mathbf{Q})_{\rm tor}|^2}$, *where*

$E(\mathbf{Q})_{\rm tor} =$ the torsion subgroup of $E(\mathbf{Q})$
$c_p(E) =$ Tamagawa number
$=$ order of the arithmetic component group

Torsion and component groups

Let E be an elliptic curve over the rationals that is optimal.
Thus $E : y^2 = x^3 + ax + b$, with $a, b \in \mathbf{Q}$
$L_E(s) =$ the L-function of $E = C_E(s-1)^r +$ higher order terms
$\Omega_E =$ period integral of E
$R_E =$ regulator of E

Conjecture (Birch and Swinnerton-Dyer)

$\frac{C_E}{\Omega_E \cdot R_E} \stackrel{?}{=} \frac{|Ш_E| \cdot \prod_p c_p(E)}{|E(\mathbf{Q})_{\mathrm{tor}}|^2}$, *where*

$E(\mathbf{Q})_{\mathrm{tor}} =$ the torsion subgroup of $E(\mathbf{Q})$
$c_p(E) =$ Tamagawa number
$=$ order of the arithmetic component group $= [E(\mathbf{Q}_p) : E^0(\mathbf{Q}_p)]$.

Torsion and component groups

Let E be an elliptic curve over the rationals that is optimal.
Thus $E : y^2 = x^3 + ax + b$, with $a, b \in \mathbf{Q}$
$L_E(s) =$ the L-function of $E = C_E(s-1)^r +$ higher order terms
$\Omega_E =$ period integral of E
$R_E =$ regulator of E

Conjecture (Birch and Swinnerton-Dyer)

$\frac{C_E}{\Omega_E \cdot R_E} \stackrel{?}{=} \frac{|\text{Ш}_E| \cdot \prod_p c_p(E)}{|E(\mathbf{Q})_{\mathrm{tor}}|^2}$, *where*

$E(\mathbf{Q})_{\mathrm{tor}} =$ the torsion subgroup of $E(\mathbf{Q})$
$c_p(E) =$ Tamagawa number
$=$ order of the arithmetic component group $= [E(\mathbf{Q}_p) : E^0(\mathbf{Q}_p)]$.
may be thought of as the number of components in "E mod p"

Torsion and component groups

Let E be an elliptic curve over the rationals that is optimal.
Thus $E : y^2 = x^3 + ax + b$, with $a, b \in \mathbf{Q}$
$L_E(s) =$ the L-function of $E = C_E(s-1)^r +$ higher order terms
$\Omega_E =$ period integral of E
$R_E =$ regulator of E

Conjecture (Birch and Swinnerton-Dyer)

$\frac{C_E}{\Omega_E \cdot R_E} \stackrel{?}{=} \frac{|\text{Ш}_E| \cdot \prod_p c_p(E)}{|E(\mathbf{Q})_{\mathrm{tor}}|^2}$, *where*

$E(\mathbf{Q})_{\mathrm{tor}} =$ the torsion subgroup of $E(\mathbf{Q})$
$c_p(E) =$ Tamagawa number
$=$ order of the arithmetic component group $= [E(\mathbf{Q}_p) : E^0(\mathbf{Q}_p)]$.
may be thought of as the number of components in "E mod p"
is 1 for almost all p

Torsion and component groups

Let E be an elliptic curve over the rationals that is optimal.
Thus $E : y^2 = x^3 + ax + b$, with $a, b \in \mathbf{Q}$
$L_E(s) =$ the L-function of $E = C_E(s-1)^r +$ higher order terms
$\Omega_E =$ period integral of E
$R_E =$ regulator of E

Conjecture (Birch and Swinnerton-Dyer)

$\frac{C_E}{\Omega_E \cdot R_E} \stackrel{?}{=} \frac{|\text{Ш}_E| \cdot \prod_p c_p(E)}{|E(\mathbf{Q})_{\mathrm{tor}}|^2}$, *where*

$E(\mathbf{Q})_{\mathrm{tor}} =$ the torsion subgroup of $E(\mathbf{Q})$
$c_p(E) =$ Tamagawa number
$=$ order of the arithmetic component group $= [E(\mathbf{Q}_p) : E^0(\mathbf{Q}_p)]$.
may be thought of as the number of components in "E mod p"
is 1 for almost all p
$\text{Ш}_E =$ Shafarevich-Tate group of E

Cancellations

Recall BSD formula $\frac{C_E}{\Omega_E \cdot R_E} \stackrel{?}{=} \frac{|\text{Ш}_E| \cdot \prod_p c_p(E)}{|E(\mathbf{Q})_{\mathrm{tor}}|^2}$.

Cancellations

Recall BSD formula $\frac{C_E}{\Omega_E \cdot R_E} \stackrel{?}{=} \frac{|Ш_E| \cdot \prod_p c_p(E)}{|E(\mathbf{Q})_{\mathrm{tor}}|^2}$.

Theorem (Emerton): If the conductor of E is prime,

Cancellations

Recall BSD formula $\frac{C_E}{\Omega_E \cdot R_E} \stackrel{?}{=} \frac{|Ш_E| \cdot \prod_p c_p(E)}{|E(\mathbf{Q})_{\mathrm{tor}}|^2}$.

Theorem (Emerton): If the conductor of E is prime,

then $\prod_p c_p(E) = |E(\mathbf{Q})_{\mathrm{tor}}|$,

Cancellations

Recall BSD formula $\frac{C_E}{\Omega_E \cdot R_E} \stackrel{?}{=} \frac{|\text{Ш}_E| \cdot \prod_p c_p(E)}{|E(\mathbf{Q})_{\mathrm{tor}}|^2}$.

Theorem (Emerton): If the conductor of E is prime,

then $\prod_p c_p(E) = |E(\mathbf{Q})_{\mathrm{tor}}|$,

so there is quite a bit of cancellation on the right side.

Cancellations

Recall BSD formula $\frac{C_E}{\Omega_E \cdot R_E} \stackrel{?}{=} \frac{|Ш_E| \cdot \prod_p c_p(E)}{|E(\mathbf{Q})_{\mathrm{tor}}|^2}$.

Theorem (Emerton): If the conductor of E is prime,

then $\prod_p c_p(E) = |E(\mathbf{Q})_{\mathrm{tor}}|$,

so there is quite a bit of cancellation on the right side.

What happens more generally when the conductor is not prime?

Cancellations

Recall BSD formula $\frac{C_E}{\Omega_E \cdot R_E} \stackrel{?}{=} \frac{|Ш_E| \cdot \prod_p c_p(E)}{|E(\mathbf{Q})_{\mathrm{tor}}|^2}$.

Theorem (Emerton): If the conductor of E is prime,

then $\prod_p c_p(E) = |E(\mathbf{Q})_{\mathrm{tor}}|$,

so there is quite a bit of cancellation on the right side.

What happens more generally when the conductor is not prime?

Expect some cancellation based on theory and numerical data,

Cancellations

Recall BSD formula $\frac{C_E}{\Omega_E \cdot R_E} \stackrel{?}{=} \frac{|\text{Ш}_E| \cdot \prod_p c_p(E)}{|E(\mathbf{Q})_{\mathrm{tor}}|^2}$.

Theorem (Emerton): If the conductor of E is prime,

then $\prod_p c_p(E) = |E(\mathbf{Q})_{\mathrm{tor}}|$,

so there is quite a bit of cancellation on the right side.

What happens more generally when the conductor is not prime?

Expect some cancellation based on theory and numerical data,

which was first obtained from Cremona's tables,

Cancellations

Recall BSD formula $\frac{C_E}{\Omega_E \cdot R_E} \stackrel{?}{=} \frac{|\text{Ш}_E| \cdot \prod_p c_p(E)}{|E(\mathbf{Q})_{\rm tor}|^2}$.

Theorem (Emerton): If the conductor of E is prime,

then $\prod_p c_p(E) = |E(\mathbf{Q})_{\rm tor}|$,

so there is quite a bit of cancellation on the right side.

What happens more generally when the conductor is not prime?

Expect some cancellation based on theory and numerical data,

which was first obtained from Cremona's tables,

and then using SAGE (with W. Stein's help).

Conjectures

Conjectures

Recall BSD formula $\frac{C_E}{\Omega_E \cdot R_E} \stackrel{?}{=} \frac{|Ш_E| \cdot \prod_p c_p(E)}{|E(\mathbf{Q})_{\mathrm{tor}}|^2}$.

Conjectures

Recall BSD formula $\frac{C_E}{\Omega_E \cdot R_E} \stackrel{?}{=} \frac{|Ш_E| \cdot \prod_p c_p(E)}{|E(\mathbf{Q})_{\mathrm{tor}}|^2}$.

Conjecture

Let $\ell \geq 5$ be a prime. Then the order of the ℓ-primary part of $E(\mathbf{Q})_{\mathrm{tor}}$ divides $\prod_p c_p(E)$.

Conjectures

Recall BSD formula $\frac{C_E}{\Omega_E \cdot R_E} \stackrel{?}{=} \frac{|Ш_E| \cdot \prod_p c_p(E)}{|E(\mathbf{Q})_{\mathrm{tor}}|^2}$.

Conjecture

Let $\ell \geq 5$ be a prime. Then the order of the ℓ-primary part of $E(\mathbf{Q})_{\mathrm{tor}}$ divides $\prod_p c_p(E)$.

Was proved by D. Lorenzini,

Conjectures

Recall BSD formula $\frac{C_E}{\Omega_E \cdot R_E} \stackrel{?}{=} \frac{|Ш_E| \cdot \prod_p c_p(E)}{|E(\mathbf{Q})_{\mathrm{tor}}|^2}$.

Conjecture

Let $\ell \geq 5$ be a prime. Then the order of the ℓ-primary part of $E(\mathbf{Q})_{\mathrm{tor}}$ divides $\prod_p c_p(E)$.

Was proved by D. Lorenzini,

so part of $\prod_p c_p(E)$ gets cancelled.

Conjectures

Recall BSD formula $\frac{C_E}{\Omega_E \cdot R_E} \overset{?}{=} \frac{|\text{Ш}_E| \cdot \prod_p c_p(E)}{|E(\mathbf{Q})_{\mathrm{tor}}|^2}$.

Conjecture

Let $\ell \geq 5$ be a prime. Then the order of the ℓ-primary part of $E(\mathbf{Q})_{\mathrm{tor}}$ divides $\prod_p c_p(E)$.

Was proved by D. Lorenzini,

so part of $\prod_p c_p(E)$ gets cancelled.

But there is a part that remains in general in numerical examples.

Conjectures

Recall BSD formula $\frac{C_E}{\Omega_E \cdot R_E} \stackrel{?}{=} \frac{|\text{Ш}_E| \cdot \prod_p c_p(E)}{|E(\mathbf{Q})_{\rm tor}|^2}$.

Conjecture

Let $\ell \geq 5$ be a prime. Then the order of the ℓ-primary part of $E(\mathbf{Q})_{\rm tor}$ divides $\prod_p c_p(E)$.

Was proved by D. Lorenzini,

so part of $\prod_p c_p(E)$ gets cancelled.

But there is a part that remains in general in numerical examples.

What can one say about this part that remains?

Conjectures

Recall BSD formula $\frac{C_E}{\Omega_E \cdot R_E} \stackrel{?}{=} \frac{|Ш_E| \cdot \prod_p c_p(E)}{|E(\mathbf{Q})_{\mathrm{tor}}|^2}$.

Conjecture

Let $\ell \geq 5$ be a prime. Then the order of the ℓ-primary part of $E(\mathbf{Q})_{\mathrm{tor}}$ divides $\prod_p c_p(E)$.

Was proved by D. Lorenzini,

so part of $\prod_p c_p(E)$ gets cancelled.

But there is a part that remains in general in numerical examples.

What can one say about this part that remains?

Conjectures

There is a modular form $f = \sum_{n=1}^{\infty} a_n \exp(2\pi i \tau n)$

Conjectures

There is a modular form $f = \sum_{n=1}^{\infty} a_n \exp(2\pi i \tau n)$ such that for all primes p, $a_p = 1 + p - |E(\mathbf{F}_p)|$.

Conjectures

There is a modular form $f = \sum_{n=1}^{\infty} a_n \exp(2\pi i \tau n)$ such that for all primes p, $a_p = 1 + p - |E(\mathbf{F}_p)|$.

Recall BSD formula $\frac{C_E}{\Omega_E \cdot R_E} \stackrel{?}{=} \frac{|\text{Ш}_E| \cdot \prod_p c_p(E)}{|E(\mathbf{Q})_{\mathrm{tor}}|^2}$.

Conjectures

There is a modular form $f = \sum_{n=1}^{\infty} a_n \exp(2\pi i \tau n)$ such that for all primes p, $a_p = 1 + p - |E(\mathbf{F}_p)|$.

Recall BSD formula $\frac{C_E}{\Omega_E \cdot R_E} \stackrel{?}{=} \frac{|Ш_E| \cdot \prod_p c_p(E)}{|E(\mathbf{Q})_{\mathrm{tor}}|^2}$.

Conjecture

If an odd prime ℓ divides $c_p(E)$ for some prime p,

Conjectures

There is a modular form $f = \sum_{n=1}^{\infty} a_n \exp(2\pi i \tau n)$ such that for all primes p, $a_p = 1 + p - |E(\mathbf{F}_p)|$.

Recall BSD formula $\frac{C_E}{\Omega_E \cdot R_E} \stackrel{?}{=} \frac{|\text{Ш}_E| \cdot \prod_p c_p(E)}{|E(\mathbf{Q})_{\mathrm{tor}}|^2}$.

Conjecture

If an odd prime ℓ divides $c_p(E)$ for some prime p, then either ℓ divides $|E(\mathbf{Q})_{\mathrm{tor}}|$

Conjectures

There is a modular form $f = \sum_{n=1}^{\infty} a_n \exp(2\pi i \tau n)$ such that for all primes p, $a_p = 1 + p - |E(\mathbf{F}_p)|$.

Recall BSD formula $\frac{C_E}{\Omega_E \cdot R_E} \stackrel{?}{=} \frac{|\text{Ш}_E| \cdot \prod_p c_p(E)}{|E(\mathbf{Q})_{\mathrm{tor}}|^2}$.

Conjecture

If an odd prime ℓ divides $c_p(E)$ for some prime p, then either ℓ divides $|E(\mathbf{Q})_{\mathrm{tor}}|$ or the coefficients of f are congruent to those of another modular form of lower level "modulo ℓ".

Conjectures

There is a modular form $f = \sum_{n=1}^{\infty} a_n \exp(2\pi i \tau n)$ such that for all primes p, $a_p = 1 + p - |E(\mathbf{F}_p)|$.

Recall BSD formula $\frac{C_E}{\Omega_E \cdot R_E} \stackrel{?}{=} \frac{|Ш_E| \cdot \prod_p c_p(E)}{|E(\mathbf{Q})_{\mathrm{tor}}|^2}$.

Conjecture

If an odd prime ℓ divides $c_p(E)$ for some prime p, then either ℓ divides $|E(\mathbf{Q})_{\mathrm{tor}}|$ or the coefficients of f are congruent to those of another modular form of lower level "modulo ℓ".

Some of the numerical evidence was given by Randy Heaton.

Conjectures

There is a modular form $f = \sum_{n=1}^{\infty} a_n \exp(2\pi i \tau n)$ such that for all primes p, $a_p = 1 + p - |E(\mathbf{F}_p)|$.

Recall BSD formula $\frac{C_E}{\Omega_E \cdot R_E} \stackrel{?}{=} \frac{|\text{Ш}_E| \cdot \prod_p c_p(E)}{|E(\mathbf{Q})_{\mathrm{tor}}|^2}$.

Conjecture

If an odd prime ℓ divides $c_p(E)$ for some prime p, then either ℓ divides $|E(\mathbf{Q})_{\mathrm{tor}}|$ or the coefficients of f are congruent to those of another modular form of lower level "modulo ℓ".

Some of the numerical evidence was given by Randy Heaton.

Can prove some partial results towards this conjecture, using Ribet's level lowering theorem.

Cuspidal subgroup

Cuspidal subgroup

$N =$ conductor of E

Cuspidal subgroup

N = conductor of E = level of f

Cuspidal subgroup

$N =$ conductor of $E =$ level of f
$X_0(N) =$ modular curve;

Cuspidal subgroup

N = conductor of E = level of f
$X_0(N)$ = modular curve; so $X_0(N)(\mathbf{C}) = \mathfrak{H}/\Gamma_0(N)$

Cuspidal subgroup

$N =$ conductor of $E =$ level of f
$X_0(N) =$ modular curve; so $X_0(N)(\mathbf{C}) = \mathfrak{H}/\Gamma_0(N)$
$J_0(N) =$ Jacobian of $X_0(N)$;

Cuspidal subgroup

N = conductor of E = level of f
$X_0(N)$ = modular curve; so $X_0(N)(\mathbf{C}) = \mathfrak{H}/\Gamma_0(N)$
$J_0(N)$ = Jacobian of $X_0(N)$; so
$J_0(N)(\mathbf{C})$ = degree zero divisors on $X_0(N)$ modulo principal divisors

Cuspidal subgroup

N = conductor of E = level of f
$X_0(N)$ = modular curve; so $X_0(N)(\mathbf{C}) = \mathfrak{H}/\Gamma_0(N)$
$J_0(N)$ = Jacobian of $X_0(N)$; so
$J_0(N)(\mathbf{C})$ = degree zero divisors on $X_0(N)$ modulo principal divisors
Then $E \hookrightarrow J_0(N)$

Cuspidal subgroup

N = conductor of E = level of f
$X_0(N)$ = modular curve; so $X_0(N)(\mathbf{C}) = \mathfrak{H}/\Gamma_0(N)$
$J_0(N)$ = Jacobian of $X_0(N)$; so
$J_0(N)(\mathbf{C})$ = degree zero divisors on $X_0(N)$ modulo principal divisors
Then $E \hookrightarrow J_0(N)$
C = subgroup of $J_0(N)(\mathbf{C})$ generated by divisors supported on the cusps of $X_0(N)$,

Cuspidal subgroup

N = conductor of E = level of f
$X_0(N)$ = modular curve; so $X_0(N)(\mathbf{C}) = \mathfrak{H}/\Gamma_0(N)$
$J_0(N)$ = Jacobian of $X_0(N)$; so
$J_0(N)(\mathbf{C})$ = degree zero divisors on $X_0(N)$ modulo principal divisors
Then $E \hookrightarrow J_0(N)$
C = subgroup of $J_0(N)(\mathbf{C})$ generated by divisors supported on the cusps of $X_0(N)$, and is called the cuspidal subgroup.

Cuspidal subgroup

N = conductor of E = level of f
$X_0(N)$ = modular curve; so $X_0(N)(\mathbf{C}) = \mathfrak{H}/\Gamma_0(N)$
$J_0(N)$ = Jacobian of $X_0(N)$; so
$J_0(N)(\mathbf{C})$ = degree zero divisors on $X_0(N)$ modulo principal divisors
Then $E \hookrightarrow J_0(N)$
C = subgroup of $J_0(N)(\mathbf{C})$ generated by divisors supported on the cusps of $X_0(N)$, and is called the cuspidal subgroup.

Conjecture

If N is square-free, then $E(\mathbf{Q})_{\mathrm{tor}} \subseteq C$.

Cuspidal subgroup

N = conductor of E = level of f
$X_0(N)$ = modular curve; so $X_0(N)(\mathbf{C}) = \mathfrak{H}/\Gamma_0(N)$
$J_0(N)$ = Jacobian of $X_0(N)$; so
$J_0(N)(\mathbf{C})$ = degree zero divisors on $X_0(N)$ modulo principal divisors
Then $E \hookrightarrow J_0(N)$
C = subgroup of $J_0(N)(\mathbf{C})$ generated by divisors supported on the cusps of $X_0(N)$, and is called the cuspidal subgroup.

Conjecture

If N is square-free, then $E(\mathbf{Q})_{\mathrm{tor}} \subseteq C$.

Theorem

If N is square-free and r is a prime that does not divide $6N$, but divides $|E(\mathbf{Q})_{\mathrm{tor}}|$, then r divides $|C|$.

Cuspidal subgroup

N = conductor of E = level of f
$X_0(N)$ = modular curve; so $X_0(N)(\mathbf{C}) = \mathfrak{H}/\Gamma_0(N)$
$J_0(N)$ = Jacobian of $X_0(N)$; so
$J_0(N)(\mathbf{C})$ = degree zero divisors on $X_0(N)$ modulo principal divisors
Then $E \hookrightarrow J_0(N)$
C = subgroup of $J_0(N)(\mathbf{C})$ generated by divisors supported on the cusps of $X_0(N)$, and is called the cuspidal subgroup.

Conjecture

If N is square-free, then $E(\mathbf{Q})_{\rm tor} \subseteq C$.

Theorem

If N is square-free and r is a prime that does not divide $6N$, but divides $|E(\mathbf{Q})_{\rm tor}|$, then r divides $|C|$.

Question: Do the conjectures above generalize to arbitrary abelian subvarieties of $J_0(N)$ associated to modular forms?