Computing Higher Heegner Points

(joint work with K. Lauter and W. Stein)

Dimitar Jetchev
University of California, Berkeley

SAGE Days 5, October 2, 2007

Motivation

- Computing rational points (Elkies, Watkins, Delauney)

Motivation

- Computing rational points (Elkies, Watkins, Delauney)
- Explicit points over certain abelian extensions

Motivation

- Computing rational points (Elkies, Watkins, Delauney)
- Explicit points over certain abelian extensions
- Explicit Selmer classes (Kolyvagin's method)

Motivation

- Computing rational points (Elkies, Watkins, Delauney)
- Explicit points over certain abelian extensions
- Explicit Selmer classes (Kolyvagin's method)
- Elliptic curves of high analytic rank

Motivation

- Computing rational points (Elkies, Watkins, Delauney)
- Explicit points over certain abelian extensions
- Explicit Selmer classes (Kolyvagin's method)
- Elliptic curves of high analytic rank

- In a joint work with K. Lauter and W. Stein, we tried to address the last application.

Elliptic curves of high analytic rank

The Birch and Swinnerton-Dyer conjecture implies

Conjecture

$$r_{\mathrm{an}}(E/\mathbb{Q}) \geq 2 \Longrightarrow \mathrm{corank}_p \, \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) \geq 2.$$

There are no currently known results about this conjecture! Our project is motivated by a conjecture of Kolyvagin which has implications on the above conjecture.

Kolyvagin's conjecture

E - elliptic curve over $\mathbb{Q}$ (usually non-CM)

$K = \mathbb{Q}(\sqrt{-D})$ - a quadratic imaginary field, such that

$$q \mid N \Rightarrow q \text{ splits in } K.$$

Under mild technical hypothesis on a prime p, Kolyvagin constructs explicit classes $\kappa_{c,m} \in \mathrm{H}^1(K, E[p^m])$ from Heegner points for certain special square-free positive integers c and certain integers m bounded by a function of c.

Conjecture (Kolyvagin)

There exists c and m, such that $\kappa_{c,m} \neq 0$.

Kolyvagin's conjecture is a consequence of the Gross-Zagier formula if $r_{\mathrm{an}}(E/\mathbb{Q}) \leq 1$. We know very little if $r_{\mathrm{an}}(E/\mathbb{Q}) \geq 2$.

The conjecture is similar in flavor to Mazur's conjecture on Heegner points in Iwasawa extensions, except that the ergodic methods of Ratner used by Cornut and Vatsal are inapplicable in the setting of Kolyvagin.

WARNING: Whenever $r_{\mathrm{an}}(E/\mathbb{Q}) \geq 2$ (when the Gross-Zagier formula says the basic Heegner point must be torsion), higher Heegner points ARE NOT USELESS! Do not throw them away!

Consequences

Follows from results of Kolyvagin, Waldspurger, Nekovář, Murty-Murty, Bump-Friedberg-Hoffstein.

Corollary

Assume Kolyvagin's conjecture for a fixed E and p, and any Heegner discriminant D, $(D, p) = 1$. Then

1. *If $r_{\mathrm{an}}(E/\mathbb{Q})$ is nonzero then*

$$\operatorname{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) \geq 2.$$

Consequences

Follows from results of Kolyvagin, Waldspurger, Nekovář, Murty-Murty, Bump-Friedberg-Hoffstein.

Corollary

Assume Kolyvagin's conjecture for a fixed E and p, and any Heegner discriminant D, $(D, p) = 1$. Then

1. *If $r_{\mathrm{an}}(E/\mathbb{Q})$ is nonzero then*

$$\operatorname{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) \geq 2.$$

2. *If $r_{\mathrm{an}}(E/\mathbb{Q}) \geq 3$ is odd then*

$$\operatorname{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) \geq 3.$$

Definition of higher Heegner points

$E, K = \mathbb{Q}(\sqrt{-D}), N$ are as before

$\mathcal{O}_K$ - ring of integers of K (maximal order)

$\mathcal{O}_c = \mathbb{Z} + c\mathcal{O}_K$ - order of conductor c (c coprime to D and N)

$\mathfrak{n} \subset \mathcal{O}_K$ an ideal with $\mathcal{O}_K/\mathfrak{n} \simeq \mathbb{Z}/N\mathbb{Z}$

$\mathfrak{n}_c = \mathcal{O}_c \cap \mathfrak{n}$ - invertible ideal of $\mathcal{O}_c$.

$x_c = [\mathbb{C}/\mathcal{O}_c \to \mathbb{C}/\mathfrak{n}_c^{-1}] \in X_0(N)(K[c])$ - higher Heegner point
$K[c]$ - ring class field of conductor c
Let $\varphi : X_0(N) \to E$ - fixed optimal parametrization
$y_c = \varphi(x_c) \in E(K[c])$

In particular, $y_K = \mathrm{Tr}_{K[1]/K}(y_1) \in E(K)$ - classical Heegner point

What do we want to do?

Compute y_c (note: the computation would automatically produce the ring class field $K[c]/K$)

Compute the *derived Heegner points*

$$P_c = D_0 D_c y_c,$$

$D_c \in \mathbb{Z}[\mathrm{Gal}(K[c]/K)]$ - certain group ring element
$D_0 = \sum_{\sigma \in S} \sigma$, S - a set of liftings of $\mathrm{Gal}(K[1]/K)$ to $\mathrm{Gal}(K^{\mathrm{ab}}/K)$.

Remark

The definition of P_c's is HIGHLY non-canonical (depends on choices of generators of $\mathrm{Gal}(K[c]/K[c/\ell])$ and on the choice of S)

Basic idea

f - modular form, associated to E, $f = \sum_{n=1}^{\infty} a_n q^n, q = e^{2\pi i z}$

Λ - complex lattice for E
$\mathfrak{h}^\times = \mathfrak{h} \cup \mathbb{P}^1(\mathbb{Q}) \cup \{i\infty\}$
$X_0(N)_{/\mathbb{C}} \cong \Gamma_0(N) \backslash \mathfrak{h}^\times$

$\varphi : \mathfrak{h}^\times \xrightarrow{I_\varphi} \mathbb{C}/\Lambda \xrightarrow{(\wp, \wp')} E$ - modular parametrization

$$I_\varphi(\tau) = \int_\tau^{i\infty} f(z)dz = \sum_{n \geq 1} \frac{a_n}{n} q^n, \ q = e^{2\pi i \tau} \qquad (1)$$

We would like to compute the τ's corresponding to the orbit $\mathrm{Gal}(K[c]/K)y_c$.

Main steps

- Compute structure and generators for $\mathrm{Pic}(\mathcal{O}_c)$ in terms of primitive and reduced binary quadratic forms

Main steps

- Compute structure and generators for $\mathrm{Pic}(\mathcal{O}_c)$ in terms of primitive and reduced binary quadratic forms
- For each $[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O}_c)$, let $I = \mathfrak{a}$, $J = \mathfrak{a}\mathfrak{n}_c^{-1}$. Compute a $\mathbb{Z}$-basis $\{\omega_1, \omega_2\}$ of I, such that $\{\omega_1, \omega_2/N\}$ is a $\mathbb{Z}$-basis for J. Set $\tau_{[\mathfrak{a}]} = \omega_2/\omega_1$ or ω_1/ω_2 depending on which one is in $\mathfrak{h}$.

Main steps

- Compute structure and generators for $\mathrm{Pic}(\mathcal{O}_c)$ in terms of primitive and reduced binary quadratic forms
- For each $[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O}_c)$, let $I = \mathfrak{a}$, $J = \mathfrak{a}\mathfrak{n}_c^{-1}$. Compute a $\mathbb{Z}$-basis $\{\omega_1, \omega_2\}$ of I, such that $\{\omega_1, \omega_2/N\}$ is a $\mathbb{Z}$-basis for J. Set $\tau_{[\mathfrak{a}]} = \omega_2/\omega_1$ or ω_1/ω_2 depending on which one is in $\mathfrak{h}$.
- Choose the class $[\mathfrak{a}]$, such that $\mathrm{Im}(\tau_{[\mathfrak{a}]})$ is maximal

Main steps

- Compute structure and generators for $\mathrm{Pic}(\mathcal{O}_c)$ in terms of primitive and reduced binary quadratic forms
- For each $[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O}_c)$, let $I = \mathfrak{a}$, $J = \mathfrak{a}\mathfrak{n}_c^{-1}$. Compute a $\mathbb{Z}$-basis $\{\omega_1, \omega_2\}$ of I, such that $\{\omega_1, \omega_2/N\}$ is a $\mathbb{Z}$-basis for J. Set $\tau_{[\mathfrak{a}]} = \omega_2/\omega_1$ or ω_1/ω_2 depending on which one is in $\mathfrak{h}$.
- Choose the class $[\mathfrak{a}]$, such that $\mathrm{Im}(\tau_{[\mathfrak{a}]})$ is maximal
- Compute $I_\varphi(\tau_{[\mathfrak{a}]})$ with sufficiently many terms and up to sufficiently many digits and try to recognize $\wp(I_\varphi(\tau_{[\mathfrak{a}]}))$ as an algebraic number (we know the degree $[K[c] : K]$)

Main steps

- Compute structure and generators for $\mathrm{Pic}(\mathcal{O}_c)$ in terms of primitive and reduced binary quadratic forms
- For each $[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O}_c)$, let $I = \mathfrak{a}$, $J = \mathfrak{a}\mathfrak{n}_c^{-1}$. Compute a $\mathbb{Z}$-basis $\{\omega_1, \omega_2\}$ of I, such that $\{\omega_1, \omega_2/N\}$ is a $\mathbb{Z}$-basis for J. Set $\tau_{[\mathfrak{a}]} = \omega_2/\omega_1$ or ω_1/ω_2 depending on which one is in $\mathfrak{h}$.
- Choose the class $[\mathfrak{a}]$, such that $\mathrm{Im}(\tau_{[\mathfrak{a}]})$ is maximal
- Compute $I_\varphi(\tau_{[\mathfrak{a}]})$ with sufficiently many terms and up to sufficiently many digits and try to recognize $\wp(I_\varphi(\tau_{[\mathfrak{a}]}))$ as an algebraic number (we know the degree $[K[c] : K]$)
- Alternatively: compute minimal polynomial of $\wp(I_\varphi(\tau_{[\mathfrak{a}]}))$ and recognize coefficients as K-rational numbers

How can we turn this into an algorithm?

We aim for a proof that the computed point is the correct one! One needs to know the following in advance:

1) minimal number d of digits after the decimal point, such that one can recognize $x(y_c)$

2) minimal number of Fourier terms in order to correctly compute $\wp(I_\phi(\tau))$ up the d-th digit after the decimal point.

Since 2) is controlled by 1) and bounds on $\frac{a_n}{n}$ and 1) is controlled by the logarithmic height $h(y_c)$, we need an upper bound on $h(y_c)$.

Estimating the canonical height

$\chi : \mathrm{Gal}(K[c]/K) \to \mathbb{C}^\times$ - ring class character
$e_\chi \in \mathbb{C}[\mathrm{Gal}(K[c]/K)]$ - associated eidempotent projector

Theorem (Zhang-GZ)

$$\widehat{h}(e_\chi y_c) \sim L'(f,\chi,1)\frac{\sqrt{-D}}{(f,f)},$$

where $L(f,\chi,s)$ *is the Rankin-Selberg L-function for* f *and* χ

Dokchitser's method (also, Mark's talk) can be used to compute $L'(f,\chi,1)$ up to any precision for any χ. Finally,

$$\widehat{h}(y_c) = \sum_\chi \widehat{h}(e_\chi y_c),$$

since $\widehat{h}$ is a quadratic form and e_χ's are orthogonal.

Estimating the naïve height

Height difference bounds (Silverman, Cremona, Siksek)
F - number field
v - non-archimedian place of K, $n_v = [F_v : \mathbb{Q}_v]$
M_F^∞ - all archimedian places of F

Theorem (Cremona-Prickett-Siksek)

Let $P \in E(F)$ and suppose that $P \in E^0(F_v)$ for every non-archimedian place v of F. Then

$$\frac{1}{3[F:\mathbb{Q}]} \sum_{v \in M_F^\infty} n_v \log \delta_v \leq h(P) - \widehat{h}(P) \leq \frac{1}{3[F:\mathbb{Q}]} \sum_{v \in M_F^\infty} n_v \log \varepsilon_v,$$

for some explicit constants ε_v and δ_v.

The elliptic curve **389a1**

389a1: The elliptic curve with label **389a1** is

$$y^2 + y = x^3 + x^2 - 2x$$

The associated modular form is

$$f_E(q) = q - 2q^2 - 2q^3 + 2q^4 - 3q^5 + 4q^6 - 5q^7 + q^9 + 6q^{10} + \cdots .$$

We know $r_{\mathrm{an}}(E/\mathbb{Q}) \geq 2$.

$D = 7$ - Heegner discriminant for E
$c = 5$ - conductor

Minimal polynomial of the $x(y_5)$:

$$\begin{aligned} F(x) &= x^6 + \frac{10}{7}x^5 - \frac{867}{49}x^4 - \frac{76}{245}x^3 + \\ &+ \frac{3148}{35}x^2 - \frac{25944}{245}x + \frac{48771}{1225}. \end{aligned}$$

If α is a root of $F(x)$ then $y_5 = (\alpha, \beta)$ where

$$\begin{aligned} \beta &= \frac{280}{7761}\sqrt{-7}\alpha^5 + \frac{1030}{7761}\sqrt{-7}\alpha^4 - \frac{12305}{36218}\sqrt{-7}\alpha^3 - \\ &- \frac{10099}{15522}\sqrt{-7}\alpha^2 + \frac{70565}{54327}\sqrt{-7}\alpha + \frac{-18109 - 33814\sqrt{-7}}{36218}. \end{aligned}$$

The elliptic curve **709a1**

The curve **709a1** has Weierstrass equation

$$E : y^2 + y = x^3 - x^2 - 2x,$$

and an associated modular form

$$f_E(q) = q - 2q^2 - q^3 + 2q^4 - 3q^5 + 2q^6 - 4q^7 - 2q^9 + \cdots .$$

We know $r_{\mathrm{an}}(E/\mathbb{Q}) \geq 2$.

Heegner discriminant: $D = 7$

Conductor $c = 5$

Minimal polynomial for $x(y_5)$:

$$\begin{aligned} F(x) &= \frac{1}{5^2 \cdot 7^2 \cdot 19^2}(442225x^6 - 161350x^5 - 2082625x^4 - \\ &- 387380x^3 + 2627410x^2 + 18136030x + 339921), \end{aligned}$$

If α is a root of $F(x)$ then $y_5 = (\alpha, \beta)$ for

$$\begin{aligned}\beta &= \frac{341145}{62822}\sqrt{-7}\alpha^5 - \frac{138045}{31411}\sqrt{-7}\alpha^4 - \\ &- \frac{31161685}{1319262}\sqrt{-7}\alpha^3 + \frac{7109897}{1319262}\sqrt{-7}\alpha^2 + \frac{39756589}{1319262}\sqrt{-7}\alpha + \\ &+ \frac{-219877 + 4423733\sqrt{-7}}{439754}.\end{aligned}$$

Elliptic curve **53a1**

Let $E_{/\mathbb{Q}}$ be the elliptic curve with label **53a1** in Cremona's database. Explicitly,

$$E : y^2 + xy + y = x^3 - x^2.$$

$$f_E(q) = q - q^2 - 3q^3 - q^4 + 3q^6 - 4q^7 + 3q^8 + 6q^9 + \cdots.$$

$D = 43$ - Heegner discriminant
$c = 5$ - conductor

Minimal polynomial of $x(y_5)$

$$F(x) = x^6 - 12x^5 + 1980x^4 - 5855x^3 + 6930x^2 - 3852x + 864.$$

$K[5] = K[\alpha] \cong K[x]/\langle F(x)\rangle$, α - root.

$$\begin{aligned} y_5 &= \big(\alpha, -4/315\alpha^5 + 43/315\alpha^4 - 7897/315\alpha^3 + \\ &+ 2167/35\alpha^2 - 372/7\alpha + 544/35\big) \in E(K[5]). \end{aligned}$$

QUESTIONS?