Stark-Heegner points: a status report

Invited talk

Midwest Number Theory Conference

University of Chicago, Chicago

October 23-24 2004

Stark's conjecture

$K=$ number field.

$v_1, v_2, \ldots, v_n =$ Archimedean place of K.

Assume: $v_2, \ldots, v_n$ real.

$$s(x) = \mathsf{sign}(v_2(x)) \cdots \mathsf{sign}(v_n(x)).$$

$$\zeta(K, \mathcal{A}, s) = \mathsf{N}(\mathcal{A})^s \sum_{x \in \mathcal{A}/(\mathcal{O}_K^+)^\times} s(x) \mathsf{N}(x)^{-s}.$$

$H =$ Narrow Hilbert class field of K.

$\tilde{v}_1 : H \longrightarrow \mathbf{C}$ extending $v_1 : K \longrightarrow \mathbf{C}$.

Conjecture (Stark) There exists $u(\mathcal{A}) \in \mathcal{O}_H^\times$ such that

$$\zeta'(K, \mathcal{A}, 0) \doteq \log |\tilde{v}_1(u(\mathcal{A}))|.$$

$u(\mathcal{A})$ is called a *Stark unit* attached to H/K.

Is there a stronger form?

Stark Question: Is there an *explicit analytic formula* for $\tilde{v}_1(u(\mathcal{A}))$, and not just its *absolute value*?

Some evidence that the answer is "Yes" : Sczech-Ren. (Also, ongoing work of Charollois-D.)

If $\tilde{v}_1$ is real,

$$\tilde{v}_1(u(\mathcal{A})) \stackrel{?}{=} \pm \exp(\zeta'(K, \mathcal{A}, 0)).$$

If $\tilde{v}_1$ is complex, it is harder to recover $\tilde{v}_1(u(\mathcal{A}))$ from its absolute value.

$$\log(\tilde{v}_1(u(\mathcal{A}))) = \log|\tilde{v}_1(u(\mathcal{A}))| + i\theta(\mathcal{A}) \in \mathbf{C}/2\pi i\mathbf{Z}.$$

Applications to *Hilbert's Twelfth problem* $\Rightarrow$ *Explicit class field theory for K*.

The **Stark Question** has an analogue for elliptic curves.

Elliptic Curves

$E=$ elliptic curve over K

$L(E/K,s)$ = its Hasse-Weil L-function.

Birch and Swinnerton-Dyer Conjecture. If $L(E/K,1)=0$, then there exists $P\in E(K)$ such that

$$L'(E/K,1)=\hat{h}(P)\cdot(\text{ explicit period}).$$

Stark-Heegner Question: Fix $v:K\longrightarrow\mathbf{C}$.

$\Omega=$ Period lattice attached to $v(E)$.

Is there an *explicit analytic formula* for P, or rather, for

$$\log_E(v(P))\in\mathbf{C}/\Omega?$$

A point P for which such an explicit analytic recipe exists is called a *Stark-Heegner point*.

The prototype: Heegner Points

Modular parametrisation attached to E:

$$\Phi : \mathcal{H}/\Gamma_0(N) \longrightarrow E(\mathbf{C}).$$

$K = \mathbf{Q}(\sqrt{-D}) \subset \mathbf{C}$ a *quadratic imaginary field*.

$$\log_E(\Phi(\tau)) = \int_{i\infty}^{\tau} 2\pi i f(z) dz = \sum_{n=1}^{\infty} \frac{a_n}{n} e^{2\pi i n \tau}.$$

Theorem. If τ belongs to $\mathcal{H} \cap K$, then $\Phi(\tau)$ belongs to $E(K^{\mathrm{ab}})$.

This theorem produces a *systematic* and *well-behaved* collection of algebraic points on E defined over class fields of K.

Heegner points

Given $\tau \in \mathcal{H} \cap K$, let

$$F_\tau(x, y) = Ax^2 + Bxy + Cy^2$$

be the primitive binary quadratic form with

$$F_\tau(\tau, 1) = 0, \quad N|A.$$

Define $\mathrm{Disc}(\tau) := \mathrm{Disc}(F_\tau)$.

$$\mathcal{H}^D := \{\tau \text{ s.t. } \mathrm{Disc}(\tau) = D.\}.$$

$H_D =$ ring class field of K attached to D.

Theorem 1. If τ belongs to $\mathcal{H}^D$, then $P_D := \Phi(\tau)$ belongs to $E(H_D)$.

2. (Gross-Zagier)

$$L'(E/K, \mathcal{O}_K, 1) = \hat{h}(P_D) \cdot (\text{period})$$

The Stark-Heegner conjecture

General setting: E defined over F;

$K =$ auxiliary quadratic extension of F;

The Stark-Heegner points belong (*conjecturally*) to ring class fields of K.

So far, three contexts have been explored:

1. $F =$ totally real field, $K =$ ATR extension ("Almost Totally Real").

2. $F = \mathbf{Q}$, $K =$ real quadratic field

3. $F =$ imaginary quadratic field.

(Trifkovic, Balasubramaniam, in progress).

ATR extensions

E of conductor 1 over a totally real field F,

$\omega_E =$ associated Hilbert modular form on $(\mathcal{H}_1 \times \cdots \times \mathcal{H}_n)/\mathbf{SL}_2(\mathcal{O}_F)$.

$K =$ quadratic ATR extension of F; ("Almost Totally Real"): v_1 complex, $v_2, \ldots, v_n$ real.

D-Logan: A "modular parametrisation"

$$\Phi : \mathcal{H}/\mathbf{SL}_2(\mathcal{O}_F) \longrightarrow E(\mathbf{C})$$

is constructed, and $\Phi(\mathcal{H} \cap K) \overset{?}{\subset} E(K^{\mathrm{ab}})$.

Φ defined analytically from periods of ω_E.

- Experimental evidence (Logan);

- Replacing ω_E with a weight two Eisenstein series yields a conjectural *affirmative* answer to the **Stark Question** for K (work in progress with Charollois).

Real quadratic fields

E defined over $\mathbf{Q}$, of conductor pM.

$K =$ real quadratic field in which p is non-split.

$\Rightarrow$ p-adic construction of points on E over ring class fields of K.

Advantages of a p-adic context:

1. The setting is more basic.

2. More tools at our disposal:

- Iwasawa Theory

- p-adic uniformisation

- Hida Theory

- Overconvergent modular forms

- Deformations of Galois representations...

Real quadratic fields

Set-up: E has conductor $N = pM$, with $p \not| M$.

$\mathcal{H}_p := \mathbf{C}_p - \mathbf{Q}_p$ (A p-adic analogue of $\mathcal{H}$)

K = real quadratic field, embedded both in $\mathbf{R}$ and $\mathbf{C}_p$.

Motivation for $\mathcal{H}_p$: $\mathcal{H} \cap K = \emptyset$, but $\mathcal{H}_p \cap K$ need not be empty!

Goal: Define a p-adic "modular parametrisation"

$$\Phi : \mathcal{H}_p^D / \Gamma_0(M) \stackrel{?}{\longrightarrow} E(H_D),$$

for *positive* discriminants D.

In defining Φ, I follow an approach suggested by *Dasgupta's thesis*.

Hida Theory

$U = p$-adic disc in $\mathbf{Q}_p$ with $2 \in U$;

$\mathcal{A}(U) =$ ring of p-adic analytic functions on U.

Hida. There exists a unique q-expansion

$$f_\infty = \sum_{n=1}^{\infty} \underline{a}_n q^n, \qquad \underline{a}_n \in \mathcal{A}(U),$$

such that $\forall k \geq 2$, $k \in \mathbf{Z}$, $k \equiv 2 \pmod{p-1}$,

$$f_k := \sum_{n=1}^{\infty} \underline{a}_n(k) q^n$$

is an eigenform of weight k on $\Gamma_0(N)$, and

$$f_2 = f_E.$$

For $k > 2$, f_k arises from a newform of level M, which we denote by $f_k^\dagger$.

Heegner points for real quadratic fields

Definition. If $\tau \in \mathcal{H}_p/\Gamma_0(M)$, let $\gamma_\tau \in \Gamma_0(M)$ be a generator for $\mathrm{Stab}_{\Gamma_0(M)}(\tau)$.

Choose $r \in \mathbf{P}_1(\mathbf{Q})$, and consider the "Shimura period" attached to τ and $f_k^\dagger$:

$$J_\tau^\dagger(k) := \Omega_E^{-1} \int_r^{\gamma_\tau r} (z-\tau)^{k-2} f_k^\dagger(z) dz.$$

This does not depend on r.

Proposition. There exist $\lambda_k \in \mathbf{C}^\times$ such that $\lambda_2 = 1$ and

$$J_\tau(k) := \lambda_k^{-1} (a_p(k)^2 - 1) J_\tau^\dagger(k)$$

takes values in $\bar{\mathbf{Q}} \subset \mathbf{C}_p$ and extends to a p-adic anaytic function of $k \in U$.

The definition of Φ

Note: $J_\tau(2) = 0$. We define:

$$\log_E \Phi(\tau) := \frac{d}{dk} J_\tau(k)|_{k=2}.$$

There are more precise formulae giving $\Phi(\tau)$ itself, and not just its formal group logarithm.

Conjecture 1. If τ belongs to $\mathcal{H}_p^D$, then $P_D := \Phi(\tau)$ belongs to $E(H_D)$.

2. ("Gross-Zagier")

$$L'(E/K, \mathcal{O}_K, 1) = \hat{h}(P_D) \cdot (\text{period})$$

Computational Issues

The definition of Φ is well-suited to *numerical calculations*. (Green (2000), Pollack (2004)).

Magma package `shp`: software for calculating Stark-Heegner points on elliptic curves of prime conductor.

`http://www.math.mcgill.ca/darmon/programs/shp/shp.html`

H. Darmon and R. Pollack. *The efficient calculation of Stark-Heegner points via overconvergent modular symbols*. Israel Math Journal, submitted.

The *key new idea* in this efficient algorithm is the theory of *overconvergent modular symbols* developped by Stevens and Pollack.

Numerical examples

$E = X_0(11) : y^2 + y = x^3 - x^2 - 10x - 20.$

$>$ HP,P,hD := stark_heegner_points(E,8,Qp);

The discriminant D = 8 has class number 1

Computing point attached to quadratic form (1,2,-1)

Stark-Heegner point (over Cp) =

$$(-2088624084707821, 1566468063530870w + 2088624084707825) + O(11^{15})$$

This point is close to $[9/2, 1/8(7s - 4), 1]$

$(9/2 : 1/8(7s - 4) : 1)$ is a global point on E(K).

A second example

$E = 37A : y^2 + y = x^3 - x, \quad D = 1297.$

> ,,hD := stark_heegner_points(E,1297,Qp);

The discriminant D = 1297 has class number 11

1 Computing point for quadratic form (1,35,-18)

2 Computing point for quadratic form (-4,33,13)

3 Computing point for quadratic form (16,9,-19)

4 Computing point for quadratic form (-6,25,28)

5 Computing point for quadratic form (-8,23,24)

6 Computing point for quadratic form (2,35,-9)

7 Computing point for quadratic form (9,35,-2)

8 Computing point for quadratic form (12,31,-7)

9 Computing point for quadratic form (-3,31,28)

10 Computing point for quadratic form (12,25,-14)

11 Computing point for quadratic form (14,17,-18)

Sum of the Stark-Heegner points (over Cp) =

$(0 : -1 : 1)) + (37^{100})$

This p-adic point is close to $[0, -1, 1]$

$(0 : -1 : 1)$ is indeed a global point on E(K).

Polynomial hD satisfied by the x-ccordinates:

$$\begin{aligned} 961x^{11} &- 4035x^{10} - 3868x^9 + 19376x^8 + 13229x^7 \\ &- 27966x^6 - 21675x^5 + 11403x^4 + 11859x^3 \\ &+ 1391x^2 - 369x - 37 \end{aligned}$$

> G := GaloisGroup(hD);

Permutation group G acting on a set of cardinality 11

(1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11)

(1, 10)(2, 9)(3, 8)(4, 7)(5, 6)

> #G;

22

A theoretical result

$$\chi : G_D := \mathrm{Gal}(H_D/K) \longrightarrow \pm 1$$

$$\zeta(K, \chi, s) = L(s, \chi_1) L(s, \chi_2).$$

$$P(\chi) := \sum_{\sigma \in G_D} \chi(\sigma) \Phi(\tau^\sigma), \quad \tau \in \mathcal{H}_p^D.$$

$H(\chi) :=$ extension of K cut out by χ.

Theorem (Bertolini, D).

If $a_p(E)\chi_1(p) = -\mathrm{sign}(L(E, \chi_1, s))$, then

1. $\log_E P(\chi) = \log_E \tilde{P}(\chi)$, with $\tilde{P}(\chi) \in E(H(\chi))$.

2. The point $\tilde{P}(\chi)$ is of infinite order, if and only if $L'(E/K, \chi, 1) \neq 0$.

The proof rests on an idea of Kronecker ("Kronecker's solution of Pell's equation in terms of the Dedekind eta-function").

Kronecker's Solution of Pell's Equation

$D =$ *negative* discriminant.

Replace $\mathcal{H}_p^D/\Gamma_0(N)$ by $\mathcal{H}^D/\mathbf{SL}_2(\mathbf{Z})$.

Replace Φ by

$$\eta^*(\tau) := |D|^{-1/4}\sqrt{\mathrm{Im}(\tau)}|\eta(\tau)|^2.$$

$\chi =$ genus character of $\mathbf{Q}(\sqrt{D})$, associated to

$$D = D_1 D_2, \quad D_1 > 0, \quad D_2 < 0.$$

Theorem (Kronecker, 1865).

$$\prod_{\sigma \in G_D} \eta^*(\tau^\sigma)^{\chi(\sigma)} = \epsilon^{2h_1h_2/w_2},$$

where

$h_j =$ class number of $\mathbf{Q}(\sqrt{D_j})$.

$\epsilon =$ Fundamental unit of $\mathcal{O}_{D_1}^\times$.

Kronecker's Proof

Three key ingredients:

1. Kronecker limit formula:

$$\zeta'(K, \chi, 0) = \sum_{\sigma \in G_D} \chi(\sigma) \log \eta^*(\tau^\sigma).$$

2. Factorisation Formula:

$$\zeta(K, \chi, s) = L(s, \chi_{D_1}) L(s, \chi_{D_2}).$$

In particular

$$\zeta'(K, \chi, 0) = L'(0, \chi_{D_1}) L(0, \chi_{D_2}).$$

3. Dirichlet's Formula.

$$L'(0, \chi_{D_1}) = h_1 \log(\epsilon), \qquad L(0, \chi_{D_2}) = 2h_2/w_2.$$

Note: Complex multiplication is not used!

The Stark-Heegner setting

Assume $\chi =$ trivial character.

$P_K =$ "trace" to K of P_D.

1. A "Kronecker limit formula"

$$\frac{d^2}{dk^2} L_p(f_k/K, k/2) = \frac{1}{4} \log_p(P_K + a_p(E)\bar{P}_K)^2.$$

If $a_p(E) = -\text{sign}(L(E/\mathbf{Q}, s)$, then

$$\frac{d^2}{dk^2} L_p(f_k/K, k/2) = \log_p(P_K)^2.$$

2. Factorisation formula:

$$L_p(f_k/K, k/2) = L_p(f_k, k/2) L_p(f_k, \chi_D, k/2).$$

$L_p(f_k, k/2) =$ specialisation to the critical line $s = k/2$ of $L_p(f_k, k, s)$ (Mazur's two-variable p-adic L-function.)

An analogue of Dirichlet's Formula

Suppose $a_p = -\text{sign}(L(E/\mathbf{Q}, s)) = 1$.

Theorem over $\mathbf{Q}$ (Bertolini, D)

The function $L_p(f_k, k/2)$ vanishes to order ≥ 2 at $k = 2$, and there exists $P_{\mathbf{Q}} \in E(\mathbf{Q}) \otimes \mathbf{Q}$ such that

1. $\frac{d^2}{dk^2} L_p(f_k, k/2) = -\log^2(P_{\mathbf{Q}})$.

2. $P_{\mathbf{Q}}$ is of infinite order iff $L'(E/\mathbf{Q}, 1) \neq 0$.

Proof of theorem over $\mathbb{Q}$

Introduce a suitable auxiliary imaginary quadratic field K.

A "Kronecker limit formula"

$$\frac{d^2}{dk^2} L_p(f_k/K, k/2) = \log_p(P_K)^2,$$

where P_K is a *Heegner point* arising from a Shimura curve parametrisation.

Key Ingredients: Cerednik-Drinfeld Theorem.

M. Bertolini and H. Darmon, *Heegner points, p-adic L-functions and the Cerednik-Drinfeld uniformisation*, Invent. Math. **131** (1998).

M. Bertolini and H. Darmon, *Hida families and rational points on elliptic curves*, in preparation.

End of Proof

We now use the factorisation formula

$$L_p''(f_k/K, k/2) = L_p''(f_k, k/2) L_p(f_k, \chi_D, 1)$$

to conclude.

The structure of the argument

Heegner points + Cerednik-Drinfeld

$\Rightarrow$ Theorem for K imaginary quadratic

$\Rightarrow$ Theorem for $\mathbf{Q}$

$\Rightarrow$ Theorem for K real quadratic.

This argument seems to shed no light on the rationality of the Stark-Heegner point P_D (unless the class group has exponent two).