On Howard's Main Conjecture and the Heegner point Kolyvagin system

Murilo Corato Zanarella

Massachusetts Institute of Technology

January 17, 2020

Elliptic curves

For a number field K (e.g. $K = \mathbb{Q}$), an elliptic curve is a diophantine equation of the form

$$E\colon y^2 = x^3 + ax + b, \quad a, b \in K.$$

Elliptic curves

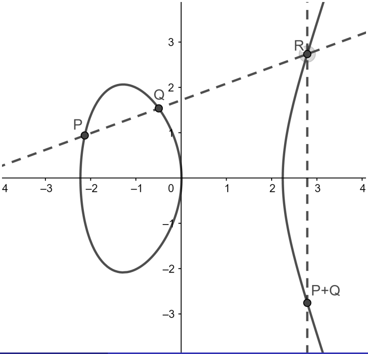
For a number field K (e.g. $K = \mathbb{Q}$), an elliptic curve is a diophantine equation of the form

$$E\colon y^2 = x^3 + ax + b, \quad a, b \in K.$$

Theorem (Mordell–Weil'28)

$E(K)$ is a finitely generated abelian group. (So $E(K) \simeq \mathbb{Z}^r \oplus E(K)_{\mathrm{tor}}$)

We call r the *algebraic rank* $r_{\mathrm{alg}}(E/K)$.



Elliptic curves

The main problem about elliptic curves is to understand $r_{\text{alg}}(E/K)$.

Elliptic curves

The main problem about elliptic curves is to understand $r_{\text{alg}}(E/K)$.

The Birch and Swinnerton-Dyer conjecture relates it with the L-function $L(E/K, s)$, an analogue of $\zeta(s)$ for E/K.

Elliptic curves

The main problem about elliptic curves is to understand $r_{\mathrm{alg}}(E/K)$.

The Birch and Swinnerton-Dyer conjecture relates it with the L-function $L(E/K, s)$, an analogue of $\zeta(s)$ for E/K.

In the case $K = \mathbb{Q}$, it is

$$L(E/\mathbb{Q}, s) = \prod_p{}' \frac{1}{1 - a_p p^{-s} + p^{1-2s}}$$

where $a_p = p + 1 - \#E(\mathbb{F}_p)$. It converges absolutely for $\mathrm{Re}(s) > 3/2$.

Birch and Swinnerton-Dyer conjecture

Conjecture (BS-D/K)

1. *$L(E/K, s)$ extends holomorphically to $\mathbb{C}$.*
2. $r_{alg}(E/K) = \mathrm{ord}_{s=1} L(E/K, s)$.
3. $\frac{L^{(r)}(E/K,1)}{r!} = \frac{\Omega_{E/K} \cdot R_{E/K} \cdot \#\text{Ш}(E/K) \cdot \prod_{l|N} c_l(E/K)}{(\#E(K)_{\mathrm{tor}})^2}$.

Birch and Swinnerton-Dyer conjecture

Conjecture (BS-D/K)

1. *$L(E/K, s)$ extends holomorphically to $\mathbb{C}$.*
2. $r_{alg}(E/K) = \mathrm{ord}_{s=1} L(E/K, s)$.
3. $\frac{L^{(r)}(E/K,1)}{r!} = \frac{\Omega_{E/K} \cdot R_{E/K} \cdot \#\text{Ш}(E/K) \cdot \prod_{l|N} c_l(E/K)}{(\#E(K)_{\mathrm{tor}})^2}$.

For $K = \mathbb{Q}$, the following is known:

Birch and Swinnerton-Dyer conjecture

Conjecture (BS-D/K)

1. *$L(E/K, s)$ extends holomorphically to $\mathbb{C}$.*
2. $r_{alg}(E/K) = \mathrm{ord}_{s=1} L(E/K, s)$.
3. $\frac{L^{(r)}(E/K,1)}{r!} = \frac{\Omega_{E/K} \cdot R_{E/K} \cdot \#Ш(E/K) \cdot \prod_{l|N} c_l(E/K)}{(\#E(K)_{\mathrm{tor}})^2}$.

For $K = \mathbb{Q}$, the following is known:

1. Follows from Modularity (Taylor–Wiles'94, Breuil–Conrad–Diamond–Taylor'99).

Birch and Swinnerton-Dyer conjecture

Conjecture (BS-D/K)

1. $L(E/K, s)$ *extends holomorphically to* $\mathbb{C}$.
2. $r_{alg}(E/K) = \mathrm{ord}_{s=1} L(E/K, s)$.
3. $\frac{L^{(r)}(E/K,1)}{r!} = \frac{\Omega_{E/K} \cdot R_{E/K} \cdot \# \text{Ш}(E/K) \cdot \prod_{l|N} c_l(E/K)}{(\# E(K)_{\mathrm{tor}})^2}$.

For $K = \mathbb{Q}$, the following is known:

1. Follows from Modularity (Taylor–Wiles'94, Breuil–Conrad–Diamond–Taylor'99).
2. Known if $r_{an}(E/\mathbb{Q}) \leq 1$ by Gross–Zagier'86 + Kolyvagin'89.

Birch and Swinnerton-Dyer conjecture

Conjecture (BS-D/K)

1. *$L(E/K, s)$ extends holomorphically to $\mathbb{C}$.*
2. $r_{alg}(E/K) = \mathrm{ord}_{s=1} L(E/K, s)$.
3. $\frac{L^{(r)}(E/K,1)}{r!} = \frac{\Omega_{E/K} \cdot R_{E/K} \cdot \#\text{Ш}(E/K) \cdot \prod_{l|N} c_l(E/K)}{(\#E(K)_{\mathrm{tor}})^2}$.

For $K = \mathbb{Q}$, the following is known:

1. Follows from Modularity (Taylor–Wiles'94, Breuil–Conrad–Diamond–Taylor'99).
2. Known if $r_{an}(E/\mathbb{Q}) \leq 1$ by Gross–Zagier'86 + Kolyvagin'89.
3. There is progress if $r_{an}(E/\mathbb{Q}) \leq 1$.

Heegner points

Let $E/\mathbb{Q}$ and let $K = \mathbb{Q}[\sqrt{-D}]$ with $D > 4$ satisfying

$$N_E \text{ is a product of primes split in } K. \tag{Heeg}$$

Heegner points

Let $E/\mathbb{Q}$ and let $K = \mathbb{Q}[\sqrt{-D}]$ with $D > 4$ satisfying

$$N_E \text{ is a product of primes split in } K. \tag{Heeg}$$

By modularity, we have a nontrivial map

$$X_0(N_E) \to E.$$

The condition (Heeg) guarantees the existence of "special" (CM) points in $X_0(N_E)$, and one can map them to a collection of points

$$z_n \in E(K[n])$$

defined over rings class fields of K.

Heegner points

For certain primes p, Kolyvagin used such points to produce a collection

$$\kappa = \{\kappa_n \in \mathrm{H}^1(K, T_pE/I_n)\}$$

that controls the Selmer group $\mathrm{Sel}_{p^\infty}(E/K)$, which lies in an exact sequence

$$0 \to E(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{Sel}_{p^\infty}(E/K) \to Ш(E/K)[p^\infty] \to 0.$$

Theorem (Kolyvagin)

If $\kappa \neq 0$, then κ "controls" $\mathrm{Sel}_{p^\infty}(E/K)$.

Heegner points

Together with

Theorem (Gross–Zagier)

If $r_{an}(E/\mathbb{Q}) \leq 1$, *one can choose* K *such that* $\kappa_1 \neq 0$.

Kolyvagin could prove

Theorem

$r_{an}(E/\mathbb{Q}) \leq 1 \implies r_{an}(E/\mathbb{Q}) = r_{alg}(E/\mathbb{Q})$.

Heegner points

Kolyvagin could only prove $\kappa \neq 0$ in the previous cases, but he conjectured:

Conjecture (Kolyvagin)

κ is always nontrivial.

He also proved

Theorem (Kolyvagin)

If $r_{an}(E/K) = 1$, then assuming the BS-D formula, we have

$$\kappa \not\equiv 0 \mod p \iff p \nmid \prod_{l|N} c_l(E/K).$$

Howard's Main Conjecture

Let E, K, p be as before.

The anticyclotomic extension is the unique sequence of number fields

$$K = K_0 \subset K_1 \subset \cdots$$

Galois over $\mathbb{Q}$ such that $[K_{i+1} : K_i] = p$ and such that $\mathrm{Gal}(K_n/\mathbb{Q})$ is dihedral.

Howard's Main Conjecture

Howard's Main Conjecture deals with the behaviour of $E(K_n)$ when n varies:

Howard's Main Conjecture

Howard's Main Conjecture deals with the behaviour of $E(K_n)$ when n varies:

$$HMC \text{ "="} \text{ limiting behaviour of BS-D}/K_n \text{ as } n \to \infty.$$

Howard's Main Conjecture

Howard's Main Conjecture deals with the behaviour of $E(K_n)$ when n varies:

$$HMC \text{ "="} \text{ limiting behaviour of BS-D}/K_n \text{ as } n \to \infty.$$

It is known in certain cases by Howard'04 + Wan'14.

Howard's Main Conjecture

Howard's Main Conjecture deals with the behaviour of $E(K_n)$ when n varies:

$$HMC \text{ "="} \text{ limiting behaviour of BS-D}/K_n \text{ as } n \to \infty.$$

It is known in certain cases by Howard'04 + Wan'14.

It is an essential ingredient in the progress made on the BS-D formula for $r_{\mathrm{an}}(E/\mathbb{Q}) = 1$.

Main Result

Theorem (Z.'19)

Let E, K as before. Assume p is a good ordinary prime for E, that p splits in K and that $p \nmid \#E(\mathbb{F}_p)$. Assume also $G_{\mathbb{Q}} \to \mathrm{Aut}(E[p])$ is surjective. Then

$$\kappa \not\equiv 0 \mod p \iff HMC \text{ and } p \nmid \prod_{l|N} c_l(E/K).$$

Main Result

Theorem (Z.'19)

(...). Then

$$\kappa \not\equiv 0 \mod p \iff \text{HMC and } p \nmid \prod_{I|N} c_I(E/K).$$

1. Extends Kolyvagin's conjectural description of when $\kappa \not\equiv 0 \mod p$ to higher rank.

Main Result

Theorem (Z.'19)

(...). Then

$$\kappa \not\equiv 0 \mod p \iff \textit{HMC and } p \nmid \prod_{l|N} c_l(E/K).$$

1. Extends Kolyvagin's conjectural description of when $\kappa \not\equiv 0 \mod p$ to higher rank.
2. Proves new cases of HMC due to

Theorem (Wei Zhang'14)

$(...) \implies \kappa \not\equiv 0 \mod p.$

Ideas of proof

Step 1: prove $\kappa \not\equiv 0 \mod p \implies HMC$.

Ideas of proof

Step 1: prove $\kappa \not\equiv 0 \mod p \implies HMC$.

This is done by improving the methods of Kolyvagin and Howard to obtain the second implication below

$$\kappa \not\equiv 0 \mod p \implies \kappa^{\mathrm{Hg}} \text{ is } \Lambda\text{-primitive} \implies HMC.$$

Ideas of proof

Step 2: prove $\kappa \not\equiv 0 \mod p \overset{HMC}{\iff} p \nmid \prod_{l|N} c_l(E/K)$.

Ideas of proof

Step 2: prove $\kappa \not\equiv 0 \mod p \overset{HMC}{\Longleftrightarrow} p \nmid \prod_{l|N} c_l(E/K)$.

The main idea is to study twists of E by anticyclotomic characters $\chi\colon \mathrm{Gal}(K_n/K) \to \mathbb{C}^\times$.

Ideas of proof

Step 2: prove $\kappa \not\equiv 0 \mod p \overset{HMC}{\iff} p \nmid \prod_{l|N} c_l(E/K)$.

The main idea is to study twists of E by anticyclotomic characters $\chi\colon \mathrm{Gal}(K_n/K) \to \mathbb{C}^\times$.

Such characters are trivial modulo p, so it suffices to prove

$$\kappa^\chi \not\equiv 0 \mod p \iff p \nmid \prod_{l|N} c_l(E^\chi/K)$$

for one such character.

Ideas of proof

Step 2: prove $\kappa \not\equiv 0 \mod p \overset{HMC}{\iff} p \nmid \prod_{l|N} c_l(E/K)$.

The main idea is to study twists of E by anticyclotomic characters $\chi \colon \mathrm{Gal}(K_n/K) \to \mathbb{C}^\times$.

Such characters are trivial modulo p, so it suffices to prove

$$\kappa^\chi \not\equiv 0 \mod p \iff p \nmid \prod_{l|N} c_l(E^\chi/K)$$

for one such character.

Choosing χ with $r_{\mathrm{an}}(E^\chi/K) = 1$, one can adapt the methods of Kolyagin to deduce this from HMC.

Thank you!