# L-functions and arithmetic, notes and remarks

**by Eduardo Ruiz Duarte**

University of Groningen  
e.ruiz.duarte@rug.nl

## Contents

1. **Selmer Group Heuristics (Björn Poonen)**  
   1.1 Preamble on Hasse principle with adeles and Selmer Groups (Eduardo Ruiz) . .  
   1.2 Talk Begins: Motivation (Björn Poonen) . . . . . . . . . . . . . . . . . . . . . . . .  
   1.3 Random Linear Algebra . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .  
   1.4 Selmer Groups . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .  
   1.5 Variants . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .  
   1.6 Consequences of conjecture . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .  
   1.7 How to model ranks . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .  

2. **Some questions about the fields of definition of endomorphisms of abelian varieties (Kiran Kedlaya)**  
   2.1 Talk Begins (Kiran Kedlaya) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .  
   2.2 Introduction . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .  
   2.3 Where do these bounds come from? . . . . . . . . . . . . . . . . . . . . . . . . . . . .  
   2.4 Results . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .  
   2.5 Why the discrepancy for Fermat primes? . . . . . . . . . . . . . . . . . . . . . . . . .  

3. **On the Conjecture of Birch-Swinnerton-Dyer for Elliptic curves with CM (John Coates)**  
   3.1 Preamble on Grossencharacters, Hilbert Class fields and Artin Map (Eduardo Ruiz)  
   3.2 Talk begins (John Coates) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .  
   3.3 Example . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .  
   3.4 Consequences for the congruent number problem . . . . . . . . . . . . . . . . . . . .  
   3.5 Statement of results . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .  

## Abstract

This is a document which has the notes from my favourite talks at the congress *L-Functions and arithmetic*, at Harvard on June 9-13, 2016. The information of this document was made with all the pictures of slides I took and notes from the blackboard according to my understanding, and my questions to the speaker, I have added more information according to my holes in the theory and my lack of definitions in order to be clearer for me. Errors might exist, but I would like in some way to share my experience to one of the best conferences I have ever been.

I will start with three talks, I have must of them, but it takes a while to make the notes because sometimes I need to go to the book to review what I am writing, or maybe find on the internet stuff that the speaker remarks as similar or “consequence of”. If you are interested in a particular talk, just write me and is almost a fact that I have the notes from it.
1. Selmer Group Heuristics (Björn Poonen)

In this talk, Bjorn showed statements that have been proved or conjectured about the distribution of Selmer groups of elliptic curves over global fields, with important consequences to the standard conjectures.

A lot of things that Bjorn said are complemented in this text according to my "holes" in definitions and theory in fact I begin here defining two important objects, and we are going to assume that $k$ is a number field, usually $\mathbb{Q}$.

1.1. Preamble on Hasse principle with adeles and Selmer Groups (Eduardo Ruiz)

Adeles and Hasse principle

The question is, when, given an algebraic variety $X/k$ (that is, a finite type separated scheme over $\text{Spec } k$) has a rational point?, (whether there is a $k$–morphism $\text{Spec } k \rightarrow X$).

The classical approach to attack this question is the local-global principle, which helps you to find obstructions to the existence of these rational points, explaining why $X(k) = \emptyset$.

The idea is to look at the $k_v$ points of $X$, where $k_v$ as usually, is the completion of $k$ at a place $v$. So if $\text{Spec } k_v \rightarrow \text{Spec } k$ you get an injection $X(K) \rightarrow X(k_v)$ and observe that the absence of $k_v$–points $X(k_v) = \emptyset$ implies the absence of $k$–points of $X$, doing this for all places $v$ one gets the following injection:

$$X(k) \hookrightarrow \prod_v X(k_v) \quad (1)$$

And observe that this injection factors through the adelic points of $X$ (points over the spectrum of the ring of adeles $A$) which is defined as follows:

$$A := \prod_v (k_v, O_v) = \{(x_v) \in \prod_v k_v \mid v \text{ for all but finitely many } v \text{ one has } x_v \in O_v\}$$

Where $O_v$ is the valuation ring at $k_v$ as usually for a non-archimedean place $v$.

$$X(k) \hookrightarrow X(\text{Spec } A) \rightarrow \prod_v X(k_v) \quad (2)$$

So, $X$ has no $k$–points if it has no adelic points, and searching for obstructions in terms of local points $X(k_v)$ is natural in the sense that it is usually much easier to decide whether $X(k_v) = \emptyset$, because using Hensel’s lemma, the search for a $k_v$–point can be often reduced to a search for a $\mathbb{F}_q$–point for some finite field $\mathbb{F}_q$ (and a different $X$) which is a finite computation.

The converse implication does not always hold, namely the claim that "$X$ has a rational point whenever it has an adelic point" in fact we know that it always work for quadric hypersurfaces on $\mathbb{P}^n$, which is the Hasse-Minkowski theorem.

Selmer Group

If $E$ is an elliptic curve over $k$ and $k$ is a subfield of $\overline{Q}$ and $E_{\text{tors}}$ is the torsion of $E(\overline{Q}) \cong (\mathbb{Q}/\mathbb{Z})^2$. We have that $\text{Gal}(\overline{Q}/k) =: G_k$ act naturally on $E_{\text{tors}}$, the intuition is that the Selmer group of $E$ is a certain subgroup of $H^1(G_k, E_{\text{tors}})$.
Suppose that \( P \in E(k) \) and \( n \geq 1 \). Then there is a \( Q \in E(\overline{Q}) \) such that \( nQ = P \), and in fact, there are \( n^2 \) such points \( Q \), all differ by points in \( E_{\text{tors}} \) of order dividing \( n \). \( \gamma \in G_k \) and \( Q' = \gamma(Q) \) then \( nQ' = P \), and then \( \gamma(Q) - Q \in E_{\text{tors}} \). The map \( \phi : G_k \to E_{\text{tors}} \) defined by \( \phi(g) = g(Q) - Q \) is of course a 1-cocycle and defines a class \([\phi] \in H^1(G_k, E_{\text{tors}})\), so with this we define the Kummer map.

\[
\kappa : E(k) \otimes \mathbb{Z} (Q/\mathbb{Z}) \to H^1(G_k, E_{\text{tors}})
\]

With this map we have that the image of \( P \otimes \mathbb{Z} (\frac{1}{n} + \mathbb{Z}) \) is defined to be \([\phi]\), and \( \kappa \) is an injective homomorphism.

Now we can define similarly the \( v \)-adic Kummer map

\[
\kappa_v : E(k_v) \otimes \mathbb{Z} (Q/\mathbb{Z}) \to H^1(G_{k_v}, E_{\text{tors}})
\]

Is easy to identify \( G_{k_v} \) with a subgroup of \( G_k \) if you choose an embedding of \( \overline{Q} \) into an algebraic closure of \( \mathbb{Q} \), which extends the embedding of \( \mathbb{Q} \) into \( \mathbb{Q} \) and then we can define a restriction map from \( H^1(G_k, E_{\text{tors}}) \to H^1(k_v, E_{\text{tors}}) \), so we have that map for each prime \( v \) of \( k \), so we define the Selmer group of \( E \) as:

\[
\text{Sel}_E(k) := \ker \{ \sigma : H^1(k, E_{\text{tors}}) \to \bigoplus_v H^1(k_v, E_{\text{tors}})/\text{Im}\kappa_v \}
\]

Where \( v \) runs in all the places of \( k \).

We also have that \( \text{III} := \text{Sel}_E(k)/\text{Im}(\kappa) \)

The next sections are now what Bjorn Poonen explained.

1.2. Talk Begins: Motivation (Bjorn Poonen)

If we have \( E/\mathbb{Q} \), then \( s(E) := \dim_{F_2} \text{Sel}_E - \dim_{F_2} E(\mathbb{Q})[2] \)

**Theorem 1.1 (Heath-Brown, 1994)** Let \( d \geq 1 \), as \( E \) varies over quadratic twists of \( y^2 = x^3 - x \).

\[
\text{Prob}(s(E) = d) \propto \prod_{j=1}^d \frac{2}{2^j - 1}
\]

And the normalizing constant (because is a proportionality relation) is \( \prod_{j \geq 0} (1 + 2^{-j})^{-1} \)

This motivated the thinking about distribution of “random” \( F_2 \) vector spaces.

1.3. Random Linear Algebra

Let \( V := F_p^{2n} \), and \( Q : V \to F_p \) be a quadratic form, i.e.

\[
(x_1, \ldots, x_n, y_1, \ldots, y_n) \mapsto \sum x_i y_i
\]

We can associate a bilinear form to this:

\[
\langle v, w \rangle := Q(v + w) - Q(v) - Q(w)
\]
Definition 1 A subspace $Z \subset V$ is maximal isotropic $\iff Z^\perp = Z$ and $Q\rvert_Z = 0$.

Second condition is needed in characteristic 2.

Proposition 1.2 Let $Z, W \subset V$ be random maximal isotropic spaces, then:

$$
\lim_{n \to \infty} \text{Prob}(\dim(Z \cap W) = d) = \prod_{j=0}^{d}(1 + p^{-j})^{-1} \cdot \prod_{j=1}^{d} \frac{p}{p^j - 1}
$$

This carries an obvious resemblance to Heath-Brown’s theorem, and is interesting. Why is this happening?

1.4. Selmer Groups

Let $k$ be a global field, $\mathbb{A}$ the adele ring of $k$, $E/k$ and elliptic curve over $k$ and $p \neq \text{char}(k)$ a prime.

$$
\begin{array}{ccc}
E(k)/pE(k) & \xrightarrow{a} & H^1(k, E[p]) \\
\downarrow & \downarrow & \downarrow \\
E(\mathbb{A})/pE(\mathbb{A}) & \xrightarrow{\beta} & H^1(\mathbb{A}, E[p])
\end{array}
$$

Here we see $H^1(\mathbb{A}, E[p])$ as notation for restricted product

$$
\prod_v (H^1(k_v, E[p]), H^1(O_v, E[p]))
$$

Here is not trivial but is true that $\beta$ is an injection.

Definition 2 We define the Selmer group

$$
\text{Sel}_p := \beta^{-1}(\text{Im}a) \cong \text{Im}(a) \cap \text{Im}(\beta)
$$

Theorem 1.3 (Poonen-Rains) There exists a quadratic form $Q : H^1(\mathbb{A}, E[p]) \to \mathbb{Q}/\mathbb{Z}$ for which $\text{Im}a$ and $\text{Im}\beta$ are maximal isotropic

this shows that Selmer group is the intersection of two maximal isotropic subspaces in an infinite-dimensional vector space, which harmonizes with the random linear algebra, but ... what is $Q$? In the interest of time, Bjorn does not answer this. but he explained an associated bilinear form given by the Weil pairing:

$$
E[p] \times E[p] \to \mathbb{G}_m
$$

We have an induced pairing

$$
\langle \cdot , \cdot \rangle : H^1(\mathbb{A}, E[p]) \times H^1(\mathbb{A}, E[p]) \to H^2(\mathbb{A}, \mathbb{G}_m)
$$

Now we have that $H^2(\mathbb{A}, \mathbb{G}_m) = Br(\mathbb{A})$, because the Brauer Groups of $O_v$ turn out to be trivial if they are isomorphic to $\oplus_v Br(k_v)$, then the pairing is the sum of the invariant maps to $\mathbb{Q}/\mathbb{Z}$.

Example: How should $\text{dimSel}_pE$ be distributed as $E$ varies in an algebraic family whose generic member has rank 18 over $\mathbb{Q}(i)$?
We can adjust the model to guess the answer to such a question. The 18 rational point generator map to a 18-dimensional subspace of $H^1(A,E[p])$ containing $\text{Im} x$ and $\text{Im} y$. This suggests the following model.

Let $R \leq V$ be isotropic of dimension 18. Then the answer should be conditional probability.

$$\lim_{n \to \infty} \text{Prob}(\text{dim}(Z \cap W) = r : Z, W \supset R)$$

(14)

The result is that the distribution on $\mathbb{N}$ shifts by +18.

1.5. Variants

What about $\text{Sel}_{p^n} E$?

Theorem holds also, but we need to know what is a "random maximal isotropic subgroup of $((\mathbb{Z}/4\mathbb{Z})^2)^n, \sum x_i y_i$.

In the $p$–Selmer case, automorphisms acted transitively on maximal isotropic subspaces, but in this case, the maximal isotropic subgroups can even have different shapes, even as abelian groups are different. Should $((\mathbb{Z}/4\mathbb{Z})^n \times \{0\})$ and $(2\mathbb{Z}/4\mathbb{Z})^{2n}$ be equally likely?.

The only solution with the model for $p$–Selmer groups is to only consider direct summands, this means to assign probability 0 to $(2\mathbb{Z}/4\mathbb{Z})^{2n}$. With this, the automorphisms acts transitively on such subgroups, and the same model applies.

Consider the following sequence:

$$0 \to E(k) \otimes \frac{p^{-e} \mathbb{Z}_p}{\mathbb{Z}_p} \to \text{Sel}_{p^n} E \to \text{III}[p^e] \to 0$$

(15)

If we take the direct limit over $e$ we have:

$$0 \to E(k) \otimes \frac{Q_p}{\mathbb{Z}_p} \to \text{Sel}_{p^n} E \to \text{III}[p^\infty] \to 0$$

(16)

The question here was can one model the "distribution" of this whole short exact sequence?

Let $(V \cong \mathbb{Z}_p^{2n}, Q = \sum x_i y_i)$ be a quadratic space.

**Definition 3** A Lagrangian submodule $Z$ is a rank $n$ submodule such that

- $Z$ is a direct summand
- $Q|Z = 0$

Chose a Lagrangian subspace $Z, W \subset V$ at random, and form:

$$0 \to (Z \cap W) \otimes \frac{Q_p}{\mathbb{Z}_p} \to Z \otimes \frac{Q_p}{\mathbb{Z}_p} \cap W \otimes \frac{Q_p}{\mathbb{Z}_p} \to T \to 0$$

(17)

Here, the intuition behind $R$ is as a model for the rational points, $S$ is the model for the Selmer Group, and $T$ is the Tate-Shafarevich group in (16) after we let $n \to \infty$

**Theorem 1.4** The limit

$$\lim_{n \to \infty}(\text{distribution of } 0 \to R \to S \to T \to 0)$$

(18)

exists
Conjecture 1.1 The limit is the distribution of (16) as $E$ varies over all elliptic curves over $k$ ordered by height.

1.6. Consequences of conjecture

- 50% of $E/k$ have rank 0 and 50% rank 1 which can be compared with Goldfeld,Katz-Sarnak work, I found what he meant here http://math.stanford.edu/~fthorne/ec-ranks.pdf

- $\#Sel_nE$ has average size $\sigma_n(n)$ (sum of divisors of $n$), with $n$ a prime power, this has been proven by Bhargava-Shankar for $n = 2, 3, 4, 5$, here I found $n = 4$ http://arxiv.org/pdf/1312.7333v1.pdf

- $\text{III}[p^\infty]$ is finite for 100% of $E$, if $E$ ranges over its rank $r$, the distribution of $\text{III}[p^\infty]$ is as conjecture by Delaunay in 2001,2007 (at least for $r = 0, 1$, ther is a variant for higher $r$, here I found Delaunay's doc here https://projecteuclid.org/download/pdf_1/euclid.em/999188631

The model for $\text{III}$ for large $n \equiv r \mod 2$ is done as follows: choose $A \in M_n(\mathbb{Z}_p)$ subject to $A^T = -A$ and $\text{rank}_{\mathbb{Z}}(\ker A) = r$. then $\text{coker}(\mathbb{Z}_p^n \rightarrow^A \mathbb{Z}_p^n)_{\text{tors}}$ is a model for $\text{III}$.

Theorem 1.5 Fix $r$, The following distributions coincide:

- The distribution of $T$ in theorem (1.4)
- Delaunay's distribution
- $\lim_{n \to \infty} \left( \text{dist. of } \text{coker}(\mathbb{Z}_p^n \rightarrow^A \mathbb{Z}_p^n)_{\text{tors}} \right)_{\text{tors}}$ where $n \equiv r \mod 2$

1.7. How to model ranks

The theorem suggests that the rank of the elliptic curve is modelled by the the rank of $A$. This predicts that 100% of ranks should be as small as possible (0 or 1). We can restrict to matrices of bounded height, and ask how quickly the percentage of higher ranks goes to 0. To model $E/Q$ of height $H := \max(|4A^2|, |27B^2|)$. choose a random variable $A \in M_n(\mathbb{Z})$ with $A^T = -A$, and the entries are bounded in absolute value by $X$, where $n = n(H)$ and $X = X(H)$ are functions of height such that $n \mod 2$ is random and $X^a = H^{1/12+o(1)}$. (This is calibrated so that the average size of $\text{III}$ for rank 0 curves is a predicted by standard conjectures.)

Conjecture 1.2 "$(\text{coker}A)_{\text{tors}}$ models $\text{III}$" and "$\text{rank}_{\mathbb{Z}}(\ker A)$ models rank of $E(Q)$"

The amazing thing is this followed by finiteness of second part of conjecture.

Theorem 1.6 With probability $1$.
\[ \{E/Q : \text{rank}_{\mathbb{Z}}(\ker A_E) > 21\} \text{ is finite} \]
this suggests that:
\[ \{E/Q : \text{rank}_{\mathbb{Z}}E/Q > 21\} \text{ is finite} \]
2. Some questions about the fields of definition of endomorphisms of abelian varieties (Kiran Kedlaya)

2.1. Talk Begins (Kiran Kedlaya)

Let $A$ be an abelian variety of genus $g$ over a number field $K$. Let $L$ be the minimal extension of $K$ over which all of the geometric endomorphisms of $A$ become defined. It is an old observation of Silverberg that $L/K$ is a finite Galois extension whose order can be bounded in terms of the orders of certain matrix groups over finite fields (by analogy with the Schur-Minkowski theorem on finite groups of integer matrices). Kiran discuss an attempt to sharpen this bound, with somewhat surprising results.

2.2. Introduction

Let $A/K$ be an abelian variety of dimension $g$ over a number field $K$. Define the endomorphism field of $K$ to be “the” minimal field extension $L$ of $K$ such that:

$$\text{End}(A_L) \cong \text{End}(A_K)$$

Then $L/K$ is a finite Galois extension.

**Example:** If $E$ is a CM elliptic curve over $K/Q$ then $L$ is an imaginary quadratic field.

**Question.** For fixed $g$, how large $|L : K|$ be?

**Theorem 2.1 (Silverberg 1992)** The degree $[L : K]$ divides $2 \prod_p p^{r(g,p)}$ where $r(g,p) = \sum_{n=0}^{\infty} \lfloor \frac{2g}{p^n-1} \rfloor$

**Proof**

For each prime $\ell \geq 2$, $Gal(L/K)$ can be identified with a subquotient of $GSp(2g, \mathbb{F}_\ell)$ via the action of $\Gamma$ in $\ell$-torsion points. The claimed bound then results from taking the gcd over $\ell$.

This looks like Minkowski’s method for bounding the order of a finite subgroup of $GL(n, \mathbb{Q})$. The method is to reduce mod $\mathbb{F}_\ell$ and take the gcd in a similar way. The conclusion is that the order divides

$$\prod_p p^{\lfloor \frac{2g}{p} \rfloor + \lfloor \frac{g}{p-1} \rfloor + \ldots}$$

But for $p = 2$, the direct gcd gives the wrong answer, because one must add in archimidean considerations.

**Comparison of bounds.** We compare Silverberg’s bound with the lcm of $[L : K]$ over all $A/K$

<table>
<thead>
<tr>
<th>$g$</th>
<th>Silverberg bound</th>
<th>Optimal bound</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$2^4 \times 3$</td>
<td>$2$</td>
</tr>
<tr>
<td>2</td>
<td>$2^8 \times 3^2 \times 5$</td>
<td>$2^4 \times 4$</td>
</tr>
<tr>
<td>3</td>
<td>$2^{11} \times 3^4 \times 5 \times 7$</td>
<td>$2^6 \times 3^3 \times 7$</td>
</tr>
</tbody>
</table>
Is not a surprise that there’s an issue at 2. However, Silverberg’s bound is also off by factors of 3 and 5, but at least in the $g = 3$ case is right for $p = 7$. This was the starting point of the project.

2.3. Where do these bounds come from?

The optimal bound for $g = 2$

For $g = 1$, the optimal bound is easy (either the curve has CM or not).

For $g = 2$, one enumerates all the options for $\text{Gal}(L/K)$ for abelian surfaces. In joint work with Fité-Rotger-Kedlaya-Sutherland, we did this by classification of Sato-Tate groups of abelian surfaces.

**Conjecture 2.1 (Sato-Tate)** Let $E/\mathbb{Q}$ be an elliptic curve without CM. Setting

$$a_p := \text{Tr} \text{Frob}_p = p + 1 - \#E(\mathbb{F}_p)$$

(21)

The distribution of $\frac{a_p}{\sqrt{p}} \in [-2, 2]$ is the distribution of the trace of a random matrix in $SU(2)$.

For $A$ an abelian variety over $K$, we can define a compact Lie group $ST(A)$ for which one expects an analogous equidistribution statement for the characteristic polynomials of Frobenius. The recipe for this is essentially written in Serre’s paper in the Motives volume, and is written somewhat more explicitly in my first paper with Bonaszak.

The Group $ST(A)$ is defined in terms of Hodge cycles. If you know the Mumford-Tate conjecture for $A$ then you can express it in terms of $\ell$-adic Galois representations.

The group of connected components of $ST(A)$ surjects onto $\text{Gal}(L/K)$, and is an isomorphism if $g \leq 3$.

Unfortunately, this classification seems to be hard for $g \geq 3$. Instead, we use another interpretation of the group of connected components of $ST(A)$.

2.4. Results

Strategy

$ST(A)$ arises as a compact form of a certain reductive algebraic group over $\mathbb{Q}$, called the algebraic Sato-Tate Group $AST(A)$. In particular the group of connected components of $ST(A)$ and $AST(A)$ coincide.

The plan is to use a form of the Minkowski method for $AST(A)$, plus archimedean considerations.

We described Minkowski’s method for finite groups, but it turns out to work pretty well for algebraic groups. You look for integral models, and reduce modulo primes. So, what we have to do is:

- Realize $AST(A) \subset Sp(2g)_{\mathbb{Q}}$ over $\mathbb{Z}[1/N]$
- Realize the component group as a subquotient of $Sp(2g, \mathbb{F}_t)$
- Look closely at extreme cases (occurring when the connected part is as small as possible
Statement of results

**Theorem 2.2 (G-K)** For $A$ an abelian variety of dimension $g$ with endomorphism field $L$, $[L : K]$ divides $\prod p^{r(g,p)}$ where:

$$r'(g,p) = \sum_{i=0}^{\infty} \left\{ \begin{array}{ll} r(g,p) - g - 1 & \text{if } p = 2 \\ \max\{0, r(g,p) - 1\} & \text{if } p = \text{Fermat prime} \\ r(g,p) & \text{if otherwise} \end{array} \right. \tag{22}$$

and this is the best possible.

2.5. Why the discrepancy for Fermat primes?

To extremize the power of $p$ in $[L : K]$, you are forced to take $A$ to be a twist of a power of a CM abelian variety. We can find an exact sequence

$$1 \to G_1 \to \pi_0(AST(A)) \to G_2 \to 0 \tag{23}$$

Where $G_1$ is the component group of $AST(A) \cap AST(A)^\circ \cdot \mathbb{Z}$. So the point is to separate into the part that commutes with the connected component and the part that doesn’t. The analysis of $G_2$ is combinatorial, while the $G_1$ is something in the domain of Minkowski’s method.

To beat the bound $r(g,p)$ the point is that there is not enough room in $G_1$ unless $AST(A)^\circ$ is abelian. This forces you into CM situations. In particular $A_K \cong A_0$ where $A_0$ has CM in some subfield of $\mathbb{Q}(\zeta_p)$. In order to match this bound exactly, the subfield must be a proper subfield.

(The reason is that we’re looking inside $\text{PGL}$ instead of $\text{GL}$, so the center doesn’t contribute).

The reason **Fermat primes** arise is that they are precisely the primes for which there is no CM subfield of $\mathbb{Q}(\zeta_p)$ which is proper.

For $p = 2$, similar issue occurs.

3. **On the Conjecture of Birch-Swinnerton-Dyer for Elliptic curves with CM (John Coates)**

This lecture describes recent joint work with Y. Kezuka, Y. Li and Y. Tian. Let $E$ be any elliptic curve defined over $\mathbb{Q}$ which is a quadratic twist of the modular curve $X_0(49)$. Let $E(\mathbb{Q})$ be the group of rational points of $E$, $\text{III}(E/\mathbb{Q})$ its Tate-Shafarevich group, and $L(E/\mathbb{Q}, s)$ its complex $L$-series. He begins by discussing the proof of the following generalization of earlier work of K. Rubin and C.D. Gonzalez-Aviles.

**Theorem 3.1** We have $L(E/\mathbb{Q}, 1) \neq 0$ if and only if both $E(\mathbb{Q})$ and the $2$–primaty subgroup of $\text{III}(E/\mathbb{Q})$ are finite. When these equivalent conditions holds, the full Birch-Swinnerton-Dyer conjecture is valid for $E$.

Then John discusses a partial generalization to a large family of quadratic twists of the Gross curves $A(q)$ with complex multiplication by the ring of integers of an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-q})$, where $q$ is any prime which is congruent to $7$ modulo $8$.

3.1. Preamble on Grossencharacters, Hilbert Class fields and Artin Map (Eduardo Ruiz)

First I will define here some of the concepts needed for me in this talk.
Grossencharacters

Let $K$ be a number field; and $\mathcal{O}_K$ the integers of $K$, let $\mathbb{A}_K$ be the adeles of $K$ (as described in my preamble of the talk by Bjorn Poonen).

**Definition 4** A Grossencharacter is a continuous group homomorphism

$$K^\times \setminus \mathbb{A}_K^\times \to \mathbb{C}^\times$$

Equivalently (by definition of quotient topology), a Grossencharacter is a continuous group homomorphism $\mathbb{A}_K^\times \to \mathbb{C}^\times$ with $K^\times$ in its kernel.

Example 1: First we recall how to normalize a norm. If $K$ is a finite extension of the $p$-adics or reals, then $K$ has an additive Haar measure $dx$ and we define $|a|$ by $|a|dx = d(ax)$. This is a completely canonical norm of such a field. Explicitly: if $K$ is a finite extension of the $p$-adics then define a norm on $K$ by letting the norm of a uniformiser be the reciprocal of the size of the residue field. If $K$ is the reals, then put the usual norm on it. If $K$ is the complexes, put the square of the usual norm on it. Define the global norm $||x||$ of an idele $x$ as the product of the local norms. Then the norm of an element of $K^\times$ is 1 and so $||.||$ define a Grossencharacter (which takes values on the positive reals).

Example 2: If $t$ is a positive real and $z$ is a complex number, then $t^z$ is of course defined to be $\exp(z \log(t))$. So $||.||^z$ is a Grossencharacter.

Example 3: If $\chi$ is a Grossencharacter, then $\psi$ defined by $\psi(x) = |\chi(x)|$ is one too, where here $|.|$ denotes the usual norm on the complex numbers, for example if $\chi$ is $||.||^z$ then $|\chi|$ is $||.||^{|Re(z)|}$

Hilbert class fields

First to define the Hilber class field we will do it through the Artin map.

**Definition 5** Let $K$ be a number field and $L$ and abelian extension. Form a prime divisor $m$ that is divides by all ramified primes of the extension $L/K$. Now define a map $\phi_{L/K}$ from the fractional ideals relatively prime to $m$ to $Gal(L/K)$ sending an ideal $\alpha = \prod_p p^{n_p} \mapsto ((L/K), \alpha) = (L/K, \prod_p p^{n_p}) := \prod_p c_p^{e_p}$ this map is called the **Artin map**

The importance of the map defined before lies in its kernel, which is the Artin’s reciprocity theorem which states that it contains all fractional ideals that are only composed of primes that split completely in the extension $L/K$.

**Definition 6** Given a number field $K$, the Hilbert class field is the abelian extension $H_K$ of $K$ such that the Artin map of $H_K/K$ induces an isomorphism between the ideal class group of $K$ and $Gal(H_K/K)$.

Something cool here from the definition is that $H_K$ has the property that a prime ideal $p$ of $\mathcal{O}_K$ splits completely in $\mathcal{O}_{H_K}$ if and only if it is principal. Another thing is that $H_K$ is the unique maximal unramified abelian extension of $K$ and it contains all other unramified abelian extensions of $K$.

The degree $[H_K : K]$ is the class number of $K$.

This is something important from the definition before:
3.2. Talk begins (John Coates)

Let $E$ be an elliptic curve over $\mathbb{Q}$. Let $g_E$ be the rank of $E(\mathbb{Q})$. We write $r_E = \text{ord}_s = 1 L(E, s)$. A special case of a more general theorem that is going to be announced in this talk is:

**Theorem 3.2** If $r_E = 0$ then $g_E = 0$

How do we prove the converse, $g_E = 0 \Rightarrow r_E = 0$? Even today, we know surprisingly little about this.

The main conjecture tells us:

**Theorem 3.3** If $p$ is a sufficiently large good ordinary prime, then $L(E(1)) = 0$, $g_E = 0$ and $\text{III}(E)[p]$ is finite.

The problem with this theorem is that it is precisely for the primes $p$ as in the hypothesis that we do not know how to show that the $p$-primary part $\text{III}(E)[p]$ is finite. We would like to have a statement such as:

**Conjecture 3.1** $L(E, 1) \neq 0 \Leftrightarrow g_E = 0$ and $\text{III}(E)[2]$ is finite.

(Of course we would also like to have the result with 2 replaced by some other prime as well). One reason why we would like this, is that we could then use descent to prove specific cases of BSD which are currently out of reach. The methods we will discuss are Isasawa-theoretic. Morally we think that they should be able to reach the result with $p$ being any good ordinary prime.

3.3. Example

Let $A$ be a fixed elliptic curve and $M$ the discriminant of a quadratic extension $\mathbb{Q}(\sqrt{M})/\mathbb{Q}$. Let $E = A(M)$ be the twist of $A$ by $\mathbb{Q}(\sqrt{M})/\mathbb{Q}$. Consider $A = X_0(49)$ which has minimal equation $y^2 + xy = x^3 - x^2 - 2x - 1$ and discriminant $\Delta = -7^3$. It has CM by $K = \mathbb{Q}(\sqrt{7})$. The prime 2 is a good ordinary for this curve, so it is in some sense the simplest of elliptic curves.

**Theorem 3.4 (Rubin,Gonzalez-Aviles)** Let $E$ be any quadratic twist of $X_0(49)$. Then $L(E, 1) \neq 0 \Leftrightarrow g_E = 0$ and $\text{III}(E)[2]$ is finite. Moreover, when $L(E, 1) \neq 0$ then $\#\text{III}(E)$ is finite and as predicted by BSD.

As far as I know, this is the only family of elliptic curves for which we can prove such a theorem.

**Corollary 3.5** Assume $E$ is a quadratic twist of $X_0(49)$. Then $g_E = 0$ and $\text{III}(E)[2] = 0$ if and only if it is predicted by BSD (in other words, if and only if $L(E, 1) \neq 0$)

This has some interesting numerical consequences. Let

$$\mathcal{M} = \{M = q_1 \cdots q_r : \text{distinct primes } \equiv 1 \mod 4, \text{inert in } K\}$$  \hspace{1cm} (25)

Let $E = A^{(M)}$ for some $M \in \mathcal{M}$. The theorem says that $E(\mathbb{Q})$ is finite and $\text{III}(E)[2] = 0 \Rightarrow L(E, 1) \neq 0$

For another example, a consequence of this result is that any odd prime $p \neq 2357$, there exists a $M \in \mathcal{M}$ such that $E = A^{(M)}$ has $\text{III}(E)$ of order $p^2$.  


3.4. Consequences for the congruent number problem

Let $C$ be the elliptic curve $y^2 = x^3 - x$ (this is the oldest elliptic curve; its quadratic twists control congruent numbers)

Theorem 3.6 (Tian, Yuan, Zhang) Assume $E$ is a quadratic twist of $C$. Then $g_E = 0$ and $\text{III}(E)[2] = 0 \Leftrightarrow$ it is predicted by BSD

Remark: The Tian-Yuan-Zhang proof is not Isasawa-Theoretic; they use an explicit form of formula of Waldspurger.

Let $N$ be any square-free positive integer. By combining the preceding results with analytic results of Heath-Brown, A. Smith showed that for $N \equiv 1, 2, 3 \pmod{8}$ (i.e. when the root number of the twist $C^{(N)}$ is $+1$) roughly $50\%$ are not congruent numbers (i.e. $g=0$). For $N \equiv 5, 6, 7 \pmod{8}$ roughly $50\%$ are congruent numbers. Conjecturally, in the first case $100\%$ are not congruent, and in the second case all are congruent.

3.5. Statement of results

Let $K = \mathbb{Q}(\sqrt{-q})$ where $q \equiv 7 \pmod{8}$ (prime). Let $h$ be the class number of $K$ (which is odd because the discriminant is prime). Let $H$ be the Hilbert class field of $K$; we know that $H = K(j(O))$. Write $J = \mathbb{Q}(j(O))$. Since $j(O)$ is real (Eduardo: Why?) this comes with an embedding $J \hookrightarrow \mathbb{R}$. We also fix some embedding $K \hookrightarrow \mathbb{C}$.

Theorem 3.7 (Gross) There exists a unique elliptic curve $A = A(q)$ defined over $J$ such that

- $\text{End}_H(A) = O$
- The minimal discriminant of $A/H$ is the ideal $(-q^3)$
- $A$ is isogenous to all of its conjugates over $H$

In fact, Gross proved that this $A(q)$ has a global minimal Weierstrass equation.

Example: For $J = \mathbb{Q}(\alpha)$, with minimal equation $\alpha^3 - \alpha - 1 = 0$, the global minimal equation of $A$ is:

$$y^2 + \alpha^3 xy + (\alpha + 2)y = x^3 + 2\alpha^2 - (12\alpha^2 + 27\alpha + 16)x - (73\alpha^2 + 99\alpha + 62) \quad (26)$$

Write $\Psi_{A/H}$ for the Grossencharacter of $A/H$. (So the $L$-series of $A/H$ is the product of that for $\Psi_{A/H}$ and its conjugate). Gross proved that $g_{A/H} = 0$ by 2-descent. Rohrlich showed that $L(A/H, 1) \neq 0$, which by the result before gives another proof of this fact.

We would like to have an analogue of the theorem which we established for quadratic twists of $X_0(49)$. Careful: we cannot consider ALL quadratic extensions of $K$, but only those twists coming from quadratic extensions of $K$.

So let $Q(A)$ be the set of twists of $A$ by quadratic extensions of $H$ of the form $HK'/H$, where $K'/K$ is a quadratic extension of conductor prime to $2q$.

Let $E \in Q(A)$. Write $\Psi_{E/H}$ for the Grossencharacter of $E/H$, which is $\phi \circ N_{H/K}$, where $\phi$ is a Grossencharacter of $K$ (in fact, the one attached to the restriction of scalars of $A$ from $H$ to $K$). Let $g$ be the conductor of $\phi$.

Now I’ll describe joint work with Y. Kezuka, Y. Li, and Y. Tian. Let $\omega$ be the Neron differential, which will be a generator of the differentials for the global minimal Weierstrass equation. Let $L$
be the period lattice of $\omega$, which is of the form $\omega = \Omega_\infty O$ for some $\Omega_\infty \in \mathbb{C}^*$. Let $a$ be an integral ideal of $K$ and $c_a$ be the Artin symbol in $G = G(H/K)$ for $(a, g) = 0$. Then we have a canonical:

$$\eta_E(a) : E \to E^a$$

(27)

Let $E_a := \text{Ker} \eta_E(a)$. The Néron differential of $E^a_\infty$ will be denoted by $\omega^a_\infty$.

We define $\xi(a) \in H^*$ by

$$\eta_E(a)(\omega^a_\infty) = \xi(a)\omega$$

(28)

Let

$$\Omega_\infty(E/H) = \prod_a \xi(a)\Omega_\infty$$

(29)

Fact: for all $n \geq 1$, $\Omega_\infty(E/H)^{-n}L(\Psi_{E/H}^n, n) \in K$.

Consider a prime $p$ split in $K$, suppose $pO = pp^\infty$. Suppose $E$ has good reduction abobe $p$, and $(p, h) = 1$. Let $F_\infty = H(E[p^\infty])$.

For time reasons, John Coates will state a simplified result. Assume $p = 2$. Let $M_\infty$ be the maximal abelian $p$-extension of $K$ unramified outside $p$.

$$K \to H \xrightarrow{\pi} F_\infty \xrightarrow{\pi} M_\infty$$

In this case it can be proven that $X_\infty$ is a finitely generated $\mathbb{Z}_2$-module. We have that $\mathfrak{S} \cong O_p^*$, so $\mathfrak{S} = \Gamma \times \Delta$ where $\Delta = \{1, \delta\}$ is cyclic of order 2. Let $Y_\infty = X_\infty/(\delta + 1)X_\infty$

**Theorem 3.8** Assume $L(E/H, 1) \neq 0$. Then

$$\text{ord}_p(\Omega_\infty(E/H)^{-1}L(\Psi_{E/H}^p, 1)) \leq \text{ord}_p(\#\text{III}(E/H)(p)) + \#B - 2$$

(30)

Where $B$ is the set of bad primes of $E/H$. Moreover, we have equality if and only if $Y_\infty$ has no non-zero finite $\Gamma$-submodule.

**Remark:** We do not know how to prove the nonexistence of such a submodule, although it’s an old theorem of Greenberg for $X_\infty$ itself. This problem dissapears for $X_0(49)$, because then $(1 + \delta)X_\infty = 0$