RANKS OF ELLIPTIC CURVES

The goal of this seminar is to give an account of the main ideas entering in the proof of the following recent result by Bhargava, Skinner and Wei Zhang (see [BSZ] and the references therein), stating that

Theorem 0.1. *A positive proportion of elliptic curves over $\mathbb{Q}$ satisfies the Birch and Swinnerton-Dyer conjecture.*

More precisely, this paper shows that the Birch and Swinnerton-Dyer (BSD) conjecture holds for more than 66% of elliptic curves over $\mathbb{Q}$, ordered according to their naive height.

Given an elliptic curve E over $\mathbb{Q}$, let $E(\mathbb{Q})$ be the group of rational points of E – finitely generated by a theorem of Mordell – and let $Ш(E/\mathbb{Q})$ be the Shafarevich-Tate group of E. Write $L(E,s)$ for the Hasse-Weil L-series of E, defined by counting the number of points of E over all the finite fields of prime order. The work of Wiles, Taylor-Wiles, Breuil-Conrad-Diamond-Taylor (see e.g. [BCDT]), establishing the modularity of all elliptic curves over $\mathbb{Q}$, shows that $L(E,s)$ can be extended to an analytic function over the whole complex plane. The BSD conjecture for E states that the order of vanishing of $L(E,s)$ at $s=1$ is equal to the rank of $E(\mathbb{Q})$, and furthermore that $Ш(E/\mathbb{Q})$ is a finite group.

The strategy of proof of Theorem 0.1 goes along the following lines. Let p be a rational prime. Basic p-descent theory yields the existence of an exact sequence of finite abelian groups

$$0 \longrightarrow E(\mathbb{Q})/pE(\mathbb{Q}) \longrightarrow \mathrm{Sel}_p(E/\mathbb{Q}) \longrightarrow Ш(E/\mathbb{Q})_p \longrightarrow 0, \tag{1}$$

in which $\mathrm{Sel}_p(E/\mathbb{Q})$ is the p-Selmer group of E, and $Ш(E/\mathbb{Q})_p$ is the p-torsion of $Ш(E/\mathbb{Q})$.

Bhargava and Shankar [BS1], [BS2], [BS3], using delicate techniques in the geometry of numbers, have shown that

Theorem 0.2. *If $p \leq 5$, the average size of $\mathrm{Sel}_p(E/\mathbb{Q})$ is $p+1$.*

On the basis of parity considerations, this implies that the "generic" p-Selmer group has $\mathbb{F}_p$-dimension 0 or 1. In the former case $E(\mathbb{Q})$ is a finite group, while in the latter $E(\mathbb{Q})$ should have rank one if it has no p-torsion (in light of the fact that the order of $Ш(E/\mathbb{Q})$ is known to be a square when this group is finite).

Theorem 0.1 follows from Theorem 0.2, combined with the next "would-be" Theorem.

Theorem 0.3 ("Would-be" theorem)**.** *If $\mathrm{Sel}_p(E/\mathbb{Q})$ has either $\mathbb{F}_p$-dimension 0 or 1, then the Birch and Swinnerton-Dyer conjecture holds for E.*

The term "would-be" alludes to the fact that such a theorem is currently known to hold only under a host of arithmetic assumptions on the pair (E,p). The available versions are nonetheless sufficient to deduce Theorem 0.1.

As said, if $\mathrm{Sel}_p(E/\mathbb{Q}) = 0$, then $E(\mathbb{Q})$ has rank 0. In this case, Theorem 0.3 amounts to proving that $L(E,1)$ is non-zero and $Ш(E/\mathbb{Q})$ is finite. This follows from the work of Skinner-Urban [SU] on the so-called cyclotomic Iwasawa Main Conjecture for E, which requires in particular that p be of ordinary reduction for E.

If $\mathrm{Sel}_p(E/\mathbb{Q}) \simeq \mathbb{Z}/p\mathbb{Z}$, then one needs to show, in addition to the finiteness of $Ш(E/\mathbb{Q})$, that $L(E,s)$ has a simple zero at $s=1$. All the known proofs of this fact (see [S], [Z], [SZ] and [V]) make use of the so-called Euler system of Heegner points, and of the Gross-Zagier formula for $L'(E,1)$.

Plan. Roughly the same number of talks (details later) will be devoted to the following four parts in which the seminar is divided.

Part 1: Basic arithmetic theory of elliptic curves: Selmer groups, Shafarevich-Tate groups, proof of the Mordell-Weil theorem, Galois representations of an elliptic curve, associated L-series.

Part 2: Proof of Theorem 0.2.

Part 3: Modularity of elliptic curves. Strategy of proof of the theorem of Skinner-Urban, with emphasis on its precursors by Ribet, Mazur-Wiles, Wiles...

Part 4: The Euler system of Heegner points. The Gross-Zagier formula. Bounding Selmer groups. Idea of proof of (some of) the results in [S], [Z], [SZ] and [V].

Calendar of lectures.
April 9: Overview of the seminar.
April 16: Arithmetic theory of elliptic curves: rational points, Galois representations, Selmer groups, Shafarevich-Tate groups, the descent exact sequence.
April 23: Proof of the Mordell-Weil theorem.
April 30: Proof of Theorem 0.2, part I.
May 7: Proof of Theorem 0.2, part II.
May 21: Proof of Theorem 0.2, part III.
May 28: Modularity of elliptic curves, and the connection with their L-series.
June 11: A modular construction of unramified extensions, following Ribet.
June 18: The theorem of Skinner-Urban.
June 25: A modular construction of points on elliptic curves (Heegner points). The Gross-Zagier formula. Analytic theorems.
July 2: Bounding Selmer groups via Heegner points.
July 9: Conclusions.

References

[BS1] M. Bhargava, A. Shankar, *Binary quartic forms having bounded invariants, and the bound- edness of the average rank of elliptic curves,* http://arxiv.org/abs/1006.1002, Ann. of Math., to appear.

[BS2] M. Bhargava, A. Shankar, *Ternary cubic forms having bounded invariants and the existence of a positive proportion of elliptic curves having rank 0,* http://arxiv.org/abs/1007.0052, Ann. of Math., to appear.

[BS3] M. Bhargava, A. Shankar, *The average size of the 5-Selmer group of elliptic curves is 6, and the average rank of elliptic curves is less than 1,* http://arxiv.org/abs/1312.7859.

[BSZ] M. Bhargava, C. Skinner, Wei Zhang, *A majority of elliptic curves over $\mathbb{Q}$ satisfy the Birch and Swinnerton-Dyer conjecture*, arXiv:1407.1826v2.

[BCDT] C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises,* J. Amer. Math. Soc. 14 (2001), no. 4, 843 – 939.

[S] C. Skinner, *A converse to a theorem of Gross-Zagier-Kolyvagin,* http://arxiv.org/abs/1405.7294.

[SU] C. Skinner, E. Urban, *The Iwasawa main conjectures for GL2,* Invent. Math., 195 (2014), no. 1, 1 – 277.

[SZ] C. Skinner, W. Zhang, *Indivisibility of Heegner points in the multiplicative case,* http://arxiv.org /abs/1407.1099.

[V] R. Venerucci, *On the p-converse of the Kolyvagin-Gross-Zagier theorem,* http://arxiv.org/abs /1407.1816.

[Z] W. Zhang, *Selmer groups and the indivisibility of Heegner points,* http://math.columbia.edu/∼wzhang /math/online/Kconj.pdf, Cambridge J. Math., to appear.