Recent results towards the BSD conjecture for elliptic curves over $\mathbb{Q}$

Seminar in the winter semester 2014/15 at Universität Heidelberg

Prof Dr. Gebhard Böckle, Dr. Juan Cerviño, Dr. Patrik Hubschmid

1 Introduction

In his works on the analytic theory of quadratic forms, "Siegel has shown that the density of rational points on a quadratic surface can be expressed in terms of the densities of p-adic points; which for almost all primes p depends directly on the number of solutions of the corresponding equation in the finite field with p elements. [...] It is natural to hope that something similar will happen for the elliptic curve

$$y^2 = x^3 - Ax - B,$$

where A, B are rational. In particular, one hopes that if for most p the curve [above] has unusually many points in the finite field with p elements, then it will have a lot of rational points."
This is extracted from the first lines of the work of B.J. Birch and H.P.F. Swinnerton-Dyer [5]. It is in fact this idea of calculating densities of rational points of quadrics via local densities – which goes back to Minkowski –, what is at the core of the BSD-conjecture, as Birch and Swinnerton-Dyer stress.

It was Birch and Swinnerton-Dyer's desire to compute the rank of an elliptic curve over $\mathbb{Q}$ via 'local' computations (of *local densities*). In practice, this can be often done by bounding the rank of the elliptic curve via explicit computation of the 2-Selmer group $S_2(E)$:

$$0 \to E(\mathbb{Q})/2E(\mathbb{Q}) \to S_2(E) \to Ш_E[2] \to 0,$$

as implemented in Cremona's famous `mwrank` program. This program is based on the calculation of the 2-coverings representing the elements of the 2-Selmer group, the so called 2-*descent*.

In this seminar, we will study the recent work of Bhargava and Shankar [1] which in particular implies that the limsup average rank of elliptic curves over $\mathbb{Q}$ is at most 1.5. This follows, after looking at the exact sequence above, from their actual main result about the average size of 2-Selmer groups of elliptic curves over $\mathbb{Q}$. Using a representation of the elements of the 2-Selmer group by certain integral binary quartic forms, Bhargava and Shankar deduce the mentioned main result by reducing the calculations to previous results of Bhargava on the density of discriminants of quartic rings – yet again, a result based on his famous earlier contributions on *Higher Composition Laws*.

We will start the seminar by studying several results counting equivalence classes of integral binary quartic forms with bounded invariants satisfying certain congruence conditions. Then we will prove in detail the correspondence between the elements of the 2-Selmer group of an elliptic curve over $\mathbb{Q}$ and certain integral binary quartic forms. In the following, we will prove the main result of Bhargava-Shankar about the average size of the 2-Selmer group of elliptic curves over $\mathbb{Q}$ by applying the results of the first part of the seminar to the sets of integral binary quartic forms corresponding to the elements of the 2-Selmer groups of the involved elliptic curves.

At the end of the seminar, we will give an outlook to further results of Bhargava and his coauthors. In particular, we will study the recent result by Bhargava-Skinner-Zhang saying that a majority (in fact $> 66\%$) of all elliptic curves over $\mathbb{Q}$, when ordered by height, satisfy the BSD conjecture. This result relies on the Iwasawa-Greenberg main conjecture proven by Skinner and Urban.

2 Talks

The first four talks all follow the article [1]. All citations without further specification refer to this article.

Talk 1 (Counting integral binary quartic forms I)**.**
Introduce the vector space $V_{\mathbb{R}}$ of binary quartic forms over $\mathbb{R}$, the natural action of $\mathrm{GL}_2(\mathbb{R})$ on $V_{\mathbb{R}}$ and the relative invariants I and J for this action. Say a few words about invariant theory in general and mention the case of binary quadratic forms for comparison.

After introducing the height of binary quartic forms in $V_{\mathbb{R}}$ and the lattice $V_{\mathbb{Z}} \subset V_{\mathbb{R}}$ of integral binary quartic forms, formulate Theorem 2.1. Then follow §2.1 concerning reduction theory of binary quartic forms. Subdivide your presentation into the following steps:

- Describe fundamental sets $L^{(i)}$ of binary quartic forms over $\mathbb{R}$ with discriminant $\neq 0$ for the action of $\mathrm{GL}_2(\mathbb{R})$.
- Give a description of the $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of binary quartic forms over $\mathbb{R}$ using the fundamental sets $L^{(i)}$ and Gauss's usual fundamental domain for $\mathrm{GL}_2(\mathbb{Z}) \setminus \mathrm{GL}_2(\mathbb{R})$.
- Reduce the proof of Theorem §2.1 to calculate a weighted number of irreducible integral points in a certain multiset $\mathcal{R}_X(h \cdot L^{(i)})$.
- If time permits, try to say a few words about the proof of the facts cited from [7] at the beginning of §2.1 which are needed for the description of the fundamental sets $L^{(i)}$. The reference [9], which we discuss in Talk 5, might also be useful for this.

References: [1, pp. 6-9], maybe [7] and [9].
Date: October 22, 2014 **Speaker: N.N.**

Talk 2 (Counting integral binary quartic forms II)**.**
First prove an upper bound for the number of reducible integral points in the multiset $\mathcal{R}_X(h \cdot L^{(i)})$ from the last talk (Lemma 2.3). Then cite Lemma 2.4 without proof. Explain that this lemma says that it is "relatively rare" that the weights in the weighted number from the end of the last talk are different from 1.

Follow §2.3 and explain how averaging over a compact set allows to reduce the computation of the above weighted number to counting integral points in a certain bounded region $\mathcal{R}_X(L^{(i)})$ (up to an error term). Finally apply a result of Davenport to estimate this number with the volume of this bounded region.

References: [1, §§2.2-2.3].
Date: October 29, 2014 **Speaker: Yujia Qiu**

Talk 3 (Counting integral binary quartic forms III)**.**
In the first part of the talk finish the proof of Theorem 2.1 computing the volume of $\mathcal{R}_X(L^{(i)})$ following §2.4. You can cite Proposition 2.8 without proof because a proof of this variable transformation formula will be given in a later talk. Also give a proof of Theorem 1.8 concerning the average number of $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of binary quartic forms with fixed invariants I and J including the proof of Theorem 1.7 given in §2.8.

Then follow §2.5 to estimate the number of integral binary quartic forms with bounded invariants satisfying finitely many congruence conditions (Theorem 2.11). Also mention the weighted version of this result (Theorem 2.12).

Finally, as a preparation for the next talk, explain the embedding of the space of integral binary quartic forms into the space of pairs of integral ternary quadratic forms and the action of $\mathrm{PGL}_2(\mathbb{Z})$ and $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$ on these spaces following §2.6. Conclude your talk with a proof of Theorem 2.14.

References: [1, §§2.4-2.6, 2.8].
Date: November 5, 2014 **Speaker: N.N.**

Talk 4 (Counting integral binary quartic forms IV)**.**
The first 45-60 minutes of this talk should be devoted to give a survey about the proof of Theorem 2.13 that bounds the number of $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of integral binary quartic forms whose discriminant is divisible by a square of some large prime. Since the proof of this theorem is quite technical and it makes use of deep results concerning binary cubic forms and pairs of ternary quadratic forms, it suffices to present the ideas and to explain the results which are cited in §2.6.

In the rest of the talk, you should show how Theorems 2.12 and 2.13 imply the "squarefree sieve" 2.21 which is a version of Theorem 2.12 including weights which are defined by infinitely many congruence conditions.

References: [1, §§2.6-2.7].
Date: November 12, 2014 **Speaker: N.N.**

The goal of the next two talks is to establish an explicit correspondence between equivalence classes of certain binary quartic forms and the elements of the 2-Selmer group of a given elliptic curve over $\mathbb{Q}$ (cf. Theorem 3.5). The *'connecting'* objects between the mentioned equivalences of binary quartics and the elements of the 2-Selmer group are the 2-coverings of elliptic curves.

Talk 5 (Binary quartic forms and 2-coverings of elliptic curves I)**.**
In this talk we concentrate on the article [9]. In particular, we give a complete proof of Theorem 3.2, based on op.cit. – the reference given in [1] is (mainly) to [8], which contains some mistakes, corrected in [9], the paper we discuss in this talk.

After summarizing Sections 1 and 2 (from [9]) on invariants and covariants of binary quartics – stressing the definition of the *irrational invariant* $z(\cdot)$ –, explain the group action of $\mathrm{GL}_2 \times \mathrm{GL}_1$ on *non-degenerate* binary quartics as well as Lemmas 4 and 5. Next give a proof of Theorem 11, which characterizes properly equivalent binary quartics (among those with the same invariants) via the irrational invariant $z(\cdot)$. Give also the more practical result: Theorem 12 – the speaker may skip the details of the proof, if time is short; i.e., if there is something from this talk's description the speaker needs to skip (due to time constraints), then skip this proof. Complete the presentation of the paper, give all the details from Section 6 (Theorem 13), proving so [1, Theorem 3.2].

References: [9]. One may also consult [8], [1], as well as the very classical work [10].
Date: November 19, 2014 **Speaker: N.N.**

Talk 6 (Binary quartic forms and 2-coverings of elliptic curves II)**.**
Our Leitfaden here is the fundamental paper [5], and the goal is to prove [1, Theorem 3.5] – as outlined in [1], by proving first Proposition 3.3 and Lemma 3.4 therein.

The talk should be divided in two parts. The first part contains the basic "abstract nonsense" (using words of Cassels on the theme) on Galois cohomology for elliptic curves: definitions of Selmer- and Shafarevich-Tate groups, the *fundamental short exact sequence* relating these two, and the interpretation of the Selmer group elements via 2-coverings. All these is already contained in the work of Cassels [6], but we suggest to follow more modern expositions as in [16, §1] and/or in [11] – see also [1, §1.3].
The second part proves [1, Theorem 3.5] as explained above, following the original paper of [5]: Lemmas 1–5 (on the last two, one may just show only one case!) and the first part of Theorem 1 ibid., which lead to Proposition 3.3 and Lemma 3.4 of [1].

References: [5], [1, §3.1], [16, §1]. The speaker may also want to – does not have to – consult [11], [15, Ch. X], [13, Ch. III, §1].
Date: November 26, 2014 **Speaker: N.N.**

After having focused on general facts about binary quartics and its relation with the Selmer group of elliptic curves, we go back to the main theorem of [1], in order to prove that "the" average size of 2-Selmer groups of elliptic curves over $\mathbb{Q}$ is 3.

Talk 7 (Statement of the main theorem, a weighted set $S(F)$ of integral binary quartics)**.**
The talk begins with the exposition from §3, page 22, where we precisely explain the main result to be

proven in the next talks (Theorem 3.1). After this, the talk proceeds with all details of Section 3.2 (in particular the proof of Proposition 3.6).

In the remaining time, the speaker could cover (at least) the statements of Proposition 3.7 and Corollary 3.8.

References: [1, §3].
Date: December 3, 2014 **Speaker: N.N.**

Talk 8 (Local densities of $S(F)$ and change-of-measure formula I)**.**
The speaker should continue with the proof of Corollary 3.8 (following from Proposition 3.7 and the results from Section 3.1, presented in talks 5 and 6), and then state and prove Proposition 3.9.

From now on, the aim will be to prove Proposition 3.7, for which we need several statements, in particular a change-of-measure formula, also needed much earlier in the seminar. Follow all proofs until the statement of Proposition 3.13 – if time permits, one may continue until Remark 3.14 on page 30.

References: [1, §3].
Date: December 10, 2014 **Speaker: N.N.**

Talk 9 (Change-of-measure formula II and the number of elliptic curves of bounded height in F)**.**
The first part of the talk is devoted to finish the proof of Proposition 3.7, and so finishing Section 3.4.

In the second part, the speaker should go through Section 3.5, and if time permits, prove also Proposition 3.18.

References: [1, §3].
Date: December 17, 2014 **Speaker: N.N.**

Talk 10 (Proof of the main theorems and first outlook)**.**
Give complete proofs of the remaining results from Section 3.6 and finally deduce Theorem 3.1 from this. Also shortly explain, how Theorem 3.1 implies that the average (algebraic) rank of elliptic curves over $\mathbb{Q}$ is at most 1.5, when ordered by height.

In the remaining time, if any, present a survey of further results of Bhargava and his coauthors regarding Selmer groups and the BSD conjecture. In particular, you could give a survey of the main results of [2] and [3] and the methods used therein. The first of these articles computes the average rank of the 3-Selmer group of an elliptic curve over $\mathbb{Q}$ by counting ternary cubic forms having bounded invariants and the second one the average rank of the 5-Selmer group of an elliptic curve over $\mathbb{Q}$. Also explain the consequences of these results for the average rank of elliptic curves over $\mathbb{Q}$ and the correctness of the BSD conjecture.
References: [1, §3], [2], [3].
Date: January 7, 2015 **Speaker: N.N.**

Talk 11 (A majority of elliptic curves over $\mathbb{Q}$ satisfy the BSD conjecture I)**.**
Start your talk with a reminder on reduction theory of elliptic curves. You should cover the following topics:

- Minimal Weierstrass equations for elliptic curves over local fields
- Definitions: Good reduction (ordinary/supersingular) and bad reduction (multiplicative/additive) of an elliptic curve at a prime
- Explain how to read off the reduction type of an elliptic curve from a minimal Weierstrass equation

You can use the book of Silverman [15] as a reference, in particular §VII.5.1 and Theorem V.4.1.

Continue to explain (without proof) the p-adic conditions for an elliptic curve to have algebraic and analytic rank 0 from [4, §2.2] which rely on deep results from Iwasawa theory.

Then state the result of Dokchitser-Dokchitser [4, Theorem 15] concerning the connection between the root number and the parity of the corank of the p^∞-Selmer group of an elliptic curve. For a better explanation of the necessary definitions see [12, §1.4]. Finally, explain the content of [4, Theorems 13 and 16] (without proof).

References: [4, §2], [15], [12, §1.4].
Date: January 14, 2015 **Speaker: N.N.**

Talk 12 (A majority of elliptic curves over $\mathbb{Q}$ satisfy the BSD conjecture II)**.**
The goal of this talk is to give an overview of the recent result by Bhargava-Skinner-Zhang [4] that a majority (in fact $> 66\%$) of all elliptic curves over $\mathbb{Q}$, when ordered by height, satisfy the Birch and Swinnerton-Dyer conjecture. The focus of your talk should lie on the presentation of the proof of [4, Corollary 22] saying that at least 16.5% of elliptic curves over $\mathbb{Q}$, when ordered by height, have both algebraic and analytic rank 0 assuming the results explained in the previous talk.

Start with the definition of the family $S_0(5)$ of elliptic curves over $\mathbb{Q}$ and the lower bound of its density (§3.1 and Lemma 17). Continue with the proof of Lemma 20 saying that a density of 100% of elliptic curves over $\mathbb{Q}$, when ordered by height, satisfy two of the four p-adic conditions from [4, §2.2] mentioned in the previous talk. Also explain well the parts of this proof which are not worked out completely in [4] (application of Hilbert irreducibility, ramification criterion mentioned in Remark 7 including reference to [14, §V.6], computation of the density of $S(L)$). Then follow §3.3 to conclude Corollary 22.

Finish your talk mentioning the lower bounds for the proportion of elliptic curves having algebraic and analytic rank 1 resp. 0 or 1. If there is some time left, you can give a very quick survey of their proofs.

References: [4, §3], [14, §V.6].
Date: January 21, 2015 **Speaker: N.N.**

References

[1] Bhargava, M. and Shankar, A. (2013), *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, preprint. [pdf]

[2] Bhargava, M. and Shankar, A. (2013); *Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank* 0, [pdf].

[3] Bhargava, M. and Shankar, A. (2013); *The average size of the 5-Selmer group of elliptic curves is 6, and the average rank is less than 1*, [pdf].

[4] Bhargava, M.; Skinner, C. and Zhang, W. (2014); *A majority of elliptic curves over* $\mathbb{Q}$ *satisfy the Birch and Swinnerton-Dyer conjecture*, preprint. [pdf].

[5] Birch, B. J. and Swinnerton-Dyer, H. P. F., *Notes on elliptic curves.* I, J. Reine Angew. Math. **212** (1963), 7–25.

[6] Cassels, J. W. S., Arithmetic on curves of genus 1. I. *On a conjecture of Selmer*, J. Reine Angew. Math. **202** (1959), 52–99. II. *A general result*, J. Reine Angew. Math. **203** (1960), 174–208. III. The Tate-Šafarevič and Selmer groups, Proc. London Math. Soc. (3) **12** (1962), 259–296. IV. *Proof of the Hauptvermutung*, J. Reine Angew. Math. **211** (1962), 95–112.

[7] Cremona, J. E. (1999), *Reduction of binary cubic and quartic forms*, LMS J. Comput. Math. **2**., pp. 64–94.

[8] Cremona, J. E., *Classical invariants and 2-descent on elliptic curves*, J. Symbolic Comput. **31** (2001), no. 1-2, 71–87.

[9] Cremona, J. E. and Fisher, T. (2009), *On the equivalence of binary quartics*, Journal of Symbolic Computation **44**, pp. 673–682.

[10] Hilbert, D., *Theory of algebraic invariants*, translated from the German and with a preface by Reinhard C. Laubenbacher, Cambridge Univ. Press, Cambridge, 1993.

[11] Poonen, B. (2002), *The Selmer group, the Shafarevich-Tate group, and the weak Mordell-Weil theorem*, Lecture Notes from Arizona Winter School 1999. [pdf]

[12] Poonen, B. (2012); *Average rank of elliptic curves*, Séminaire Bourbaki, 2011-2012, 64ème année, no. 1049.

[13] Serre, J.-P., *Galois cohomology*, translated from the French by Patrick Ion and revised by the author, Springer, Berlin, 1997.

[14] Silverman, J. H. (1994); *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics **151**, Springer-Verlag.

[15] Silverman, J. H., *The arithmetic of elliptic curves*, second edition, Graduate Texts in Mathematics, 106, Springer, Dordrecht, 2009.

[16] Stoll, M., *Descent on elliptic curves*, in *Explicit methods in number theory*, 51–80, Panor. Synthèses, 36, Soc. Math. France, Paris. [pdf]