HEEGNER POINTS AND CONGRUENT NUMBERS

OBERSEMINAR IM WINTERSEMESTER 2013

Content

A positive square-free integer n is called a congruent number if it is the area of a right-angled triangle, all of whose sides have rational length. It is well known that n is congruent precisely if the elliptic curve $E^{(n)}\colon ny^2 = x^3 - x$ has non-zero algebraic rank. The BSD conjecture predicts that this is always the case if n is congruent to 5, 6, or 7 modulo 8. In his remarkable article [Tia12a], Tian proves the following partial result in this direction.

Theorem 1. *For any given integer $k \geq 0$, there are infinitely many square-free congruent numbers n with exactly $k+1$ odd prime divisors in each residue class of 5, 6, and 7 modulo 8.*

Maybe more importantly, he shows that for those infinitely many n, the analytic rank of $ny^2 = x^3 - x$ is 1, such that by the Gross-Zagier-Kolyvagin theorem, the algebraic rank agrees with the analytic rank and the Shafarevich-Tate group of $E^{(n)}$ is finite. At the same time, his method also yields that the 2-part of the Shafarevich-Tate group is trivial. Thus, taking results of Perrin-Riou and Kobayashi into account, the p-part of the full BSD conjecture holds for $E^{(n)}$ for all p not dividing n. Since the appearance of Tian's article, his methods have been successfully extended to other elliptic curves [CKLZ13] and there is ongoing research trying to extend these results even further.

The main ingredients of the proof are the general theory of Heegner points, Zhang's automorphic interpretation of the Gross-Zagier formula, and certain estimates of the 2-valuation of special values of L-functions provided by Zhao. Zhaos result applies to elliptic curves $E^{(m)}$ with m congruent to 1 modulo 8, for which the BSD conjecture predicts almost surely algebraic rank 0. The corresponding L-values are then used to compare the height of two Heegner points on $E^{(1)}(\mathbb{Q}(\sqrt{nm}))$ via the Gross-Zagier formula, one of which corresponds to a point in $E^{(n)}(\mathbb{Q})$, the other to a point in $E^{(nm)}(\mathbb{Q})$. By induction one proves that these points are of infinite order.

This seminar serves as an introduction to this circle of ideas. The first five talks are overview talks, which introduce to congruent numbers and the BSD conjecture, complex multiplication, Heegner points, and the Gross-Zagier formula. In the four talks of the second part of the seminar, we will study Tian's article in detail and prove the above theorem for $n \equiv 5 \mod 8$.

Time and place

Thursday, 11 – 13 h, INF 288, HS 4.

Contact

Dr. Malte Witte, INF 288, Raum 109
witte@mathi.uni-heidelberg.de, Tel. +49-6221-54-5642

Distribution of the talks

Please contact me directly if you want to have Talk 1 or 2. The other talks will be distributed at the end of the first session on Thursday, 17/10/14.

Talks

Talk 1: Congruent Numbers and the BSD Conjecture
V. Nicolas (1 session)

Formulate the congruent number problem and introduce the full BSD conjecture for elliptic curves over $\mathbb{Q}$. In particular, briefly recall the definition of the L-function, the canonical height pairing, the Shafarevich-Tate group, the local Tamagawa factors, and the conductor of an elliptic curve over $\mathbb{Q}$. Explain how the BSD conjecture implies the solution of the congruent number problem and state Tian's main results in [Tia12a, §1]. Good sources for the BSD conjecture are [Coa13, §4–5], [Dar04, Chap. I], and [Sil09, App. §16]. For the congruent number problem, use Wikipedia and [Kob93, Prop. I.17, Prop. II.12].

Talk 2: The Theory of Complex Multiplication
U. Schmitt, C. Rüschoff (2 sessions)

Review the theory of complex multiplication. Central for our application is the main theorem of complex multiplication [Dar04, Thm. 3.5]. We also need to introduce the Grössencharacter of a CM elliptic curve, and its L-function [Sil94, §9, §10]. Nice surveys are given in [Dar04, §3.1], [Coa13, §8] and [Ser67]. Silverman [Sil94, Ch. II] considers mainly the case that the elliptic curve has complex multiplication by the full ring of integers. Another good reference might be [Cox89, Ch. III].

Talk 3: Modular Parametrisations
M. Fütterer, M. Witte (2 sessions)

Introduce the modular curve $X_0(N)$, give the modular description of its points [Mil06, Thm. V.2.7], and sketch how to associate to each normalised Hecke eigenform f of level N and weight 2 with integral coefficients an elliptic curve E_f and a modular parametrisation $\phi_f \colon X_0(N) \to E_f$ [Mil06, §V.6]. By Wiles' modularity theorem any elliptic curve over $\mathbb{Q}$ with conductor N is isogenous to such an E_f. Hence, modular parametrisations exist for all elliptic curves over $\mathbb{Q}$. We can certainly not give all the details. A good account is given in [Mil06, Ch. V], more details can be found in [Kna92]. See also [Dar04, Ch. II] for a summary.

Talk 4: Heegner Points on $X_0(N)$
C. Ruiz-Toscano (1 session)

This talk is about [Dar04, §3.2 – 3.9]. Introduce Heegner points and Heegner systems [Dar04, §3.4, §3.5], state the Gross-Zagier formula [YZZ12, Thm. 1.1], formulate Kolyvagin's theorem [Dar04, Thm. 3.21], and sketch the proof of the Gross-Zagier-Kolyvagin theorem [Dar04, §3.9]. Some more background material is given in [Gro84].

Talk 5: The Gross-Zagier Formula
K. Maurischat (2 sessions)

For Talk 7 we will need Zhang's reformulation of the Gross-Zagier formula in terms of automorphic forms [YZZ12, Thm. 1.2]. This works for arbitrary Shimura curves, but we may concentrate on the classical case of modular curves. Introduce the notation and terminology needed in Talk 7. If possible, sketch the connection to the classical formulation given in the previous talk and the general strategy of the proof of the formula. The main reference is [YZZ12], especially Chapter I.

Talk 6: Modular Parametrisation of $y^2 = x^3 - x$
J. Anschütz (1 session)

This talk is about [Tia12a, §2]. We will restrict to the case $n \equiv 5 \mod 8$. The elliptic curve $E\colon y^2 = x^3 - x$ has a modular parametrisation by $X_0(32)$. The curve $X_0(32)$ is itself an elliptic curve, which can be given the Weierstrass equation $y^2 = x^3 + 4x$. We will introduce a certain Heegner point z_n depending on n and study its properties. It turns out that z_n is defined over the Hilbert class field H_n of $K_n = \mathbb{Q}(\sqrt{-2n})$.

Talk 7: Comparison of Heegner Points
S. Shekhar (1 session)

This talk is about [Tia12a, §3]. Again, we will restrict to the case $n \equiv 5 \mod 8$. For $d \mid n$, $d \equiv 5 \mod 8$ set $y_d = \mathrm{Tr}_{H_n/K_n(\sqrt{d})}\, z$, $y_d^0 = \mathrm{Tr}_{H_d/K_d(\sqrt{d})}\, z$. Both points are defined over $\mathbb{Q}(\sqrt{d})$. The aim of the talk is to show that the 2-divisibility of $4y_d$ is bounded below by the 2-divisibility of $4y_d^0$. This uses Kolyvagin's theorem, the Gross-Zagier formula and a result of Zhao on 2-divisibilities of L-values. (Replace $2s - 1$ by $2s$ in Prop. 3.8.(2).) It may be considered as the centre piece of Tian's method.

Talk 8: 2-Divisibilities of L-Values
A. Riedel (1 session)

This talk is about [Zha01, Thm. 1], with back references to [Zha97]. In the end, we only need the estimate, not the equality condition. This might simplify matters. We should feel free to shorten technical calculations (e. g. the proof of Lemma 2 and 3). For the central ideas, see also [CKLZ13].

Talk 9: Induction on Quadratic Twists
O. Thomas (1 session)

This talk is about [Tia12a, §4.1, §5]. As before, we will concentrate on the case $n \equiv 5 \mod 8$. Under the condition that the ideal class group of K_n has no elements of order 4 we show by induction that y_n is a point of infinite order. From this, we conclude that the 2-part of the Shafarevich-Tate group of $E^{(n)}\colon ny^2 = x^3 - x$ vanishes and that n is a congruent number.

References

[CKLZ13] J. Coates, M. Kim, Z. Liang, and C. Zhao, *On the 2-part of the birch-swinnerton-dyer conjecture for elliptic curves with complex multiplication*, preprint, arXiv:1303.5218v2, 2013.

[Coa13] J. Coates, *Lectures on the Birch-Swinnerton-Dyer conjecture*, preprint, 2013.

[Cox89] David A. Cox, *Primes of the form x^2+ny^2*, A Wiley-Interscience Publication, John Wiley & Sons Inc., New York, 1989, Fermat, class field theory and complex multiplication. MR 1028322 (90m:11016)

[Dar04] Henri Darmon, *Rational points on modular elliptic curves*, CBMS Regional Conference Series in Mathematics, vol. 101, Published for the Conference Board of the Mathematical Sciences, Washington, DC, 2004.

[Gro84] Benedict H. Gross, *Heegner points on $X_0(N)$*, Modular forms (Durham, 1983), Ellis Horwood Ser. Math. Appl.: Statist. Oper. Res., Horwood, Chichester, 1984, pp. 87–105. MR 803364 (87f:11036b)

[Kna92] Anthony W. Knapp, *Elliptic curves*, Mathematical Notes, vol. 40, Princeton University Press, Princeton, NJ, 1992.

[Kob93] Neal Koblitz, *Introduction to elliptic curves and modular forms*, second ed., Graduate Texts in Mathematics, vol. 97, Springer-Verlag, New York, 1993. MR 1216136 (94a:11078)

[Mil06] J. S. Milne, *Elliptic curves*, BookSurge Publishers, Charleston, SC, 2006.

[Ser67] J.-P. Serre, *Complex multiplication*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 292–296.

[Sil94] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994.

[Sil09] ———, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.

[Tia12a] Y. Tian, *Congruent numbers and Heegner points*, preprint, arXiv:1210.8231v1, 2012.

[Tia12b] ———, *Congruent numbers with many prime factors*, Proc. Natl. Acad. Sci. USA **109** (2012), 21256–21258.

[YZZ12] X. Yuan, S. Zhang, and W. Zhang, *The Gross-Zagier formula*, Annals of Mathematics Studies, no. 184, Princeton University Press, Princeton NJ, 2012.

[Zha97] Chunlai Zhao, *A criterion for elliptic curves with lowest* 2*-power in $L(1)$*, Math. Proc. Cambridge Philos. Soc. **121** (1997), no. 3, 385–400.

[Zha01] ———, *A criterion for elliptic curves with second lowest 2-power in $L(1)$*, Math. Proc. Cambridge Philos. Soc. **131** (2001), no. 3, 385–404.

[Zha03] ———, *A criterion for elliptic curves with lowest 2-power in $L(1)$. II*, Math. Proc. Cambridge Philos. Soc. **134** (2003), no. 3, 407–420.