UCLA Fall 2007

Kolyvagin's Euler system for elliptic curves and its application in recent work of Ciperjani-Wiles

Organization: G. Böckle, C.. Khare Mon 3–4.15 pm, MS 6227

Programme

In the recent preprint [CW], Çiperiani and Wiles begin a program whose aim it is to prove that any genus one curve C defined over $\mathbb{Q}$ has a solvable point. An important role in this is the investigation of the Tate-Shafarevich group $Ш(E, \mathbb{Q})$ where E is the elliptic curve (over $\mathbb{Q}$) that is the Jacobian of C. The group $Ш(E, \mathbb{Q})$ is the obstruction to a local-global principle for points on E. In particular, if C has local points at all places, then C yields a class c in $Ш(E, \mathbb{Q})$ and C will have a global point over every field extension of $\mathbb{Q}$ which trivializes c – over any such C and E will be isomorphic. A main tool in their study of $Ш(E, \mathbb{Q})$ is Kolyvagin's Heegner point Euler system. The cohomology classes produced by it split over a solvable extension of $\mathbb{Q}$. So one would like to show that the above class c is a linear combination of Kolyvagin's classes.

Kolyvagin's Euler system is well understood if the analytic rank of E is at most one. Then it proves the finiteness of $Ш(E, \mathbb{Q})$. The main surprise in the work of Çiperiani and Wiles is their use of such classes without this restriction on the rank! This they achieve by cleverly exploiting work of Cornut and Vatsal on Heegner points in anticyclotomic towers as well as a variant of the Wiles-Taylor method which was instrumental in the proof of Fermat's last theorem.

The initial use of Kolyvagin's Heegner point Euler system was to the Birch and Swinnertion-Dyer conjecture (BSD): In the mid 60's Birch and Swinnerton-Dyer conjectured an interpretation for the leading term of the L-function of an elliptic curve at $s = 1$ in terms of arithmetic invariants of the curve. This could be viewed as an analogue of the classical class number formula relating the residue at $s = 1$ of the Dirichlet ζ-function of a number field to its arithmetic invariants such as the class number, the regulator, the discriminant, etc. Some of the depth of BSD is succinctly described by the following quote of Tate from 1972: "This remarkable conjecture [BSD] relates the behavior of a function L where it is not known to be defined to the order of a group Ш not known to be finite".

As a consequence of the proof of the Taniyama-Shimura conjecture, it is now known that for elliptic curves over $\mathbb{Q}$ the L-function in question is an entire function on the complex plane and thus defined at $s = 1$. The Tate-Shafarevich group Ш still remains mysterious and its finiteness is a hard open conjecture. The strongest theoretical evidence toward BSD is a consequence (of variants) of Kolyvagin's Heegner point Euler system – combined with (generalizations of) the Gross-Zagier formula, and some analytic results due to Waldschmidt, Bump-Friedberg-Hoffstein, Murty-Murty. In particular, BSD holds for elliptic curves whose analytic rank is at most one.

The main aim of the seminar will be to study Kolyvagin's Heegner point Euler system and learn about Kolyvagin's proof, cf. [Ko1, Ko2], of the finiteness of $Ш(E/\mathbb{Q})$ provided that the so-called basic Heegner has infinite order, and its application to BSD. We will follow some notes by T. Weston [Wes] which in turn are based on the expository article [Gro] by B. Gross. The idea is to present the proof of Kolyvagin's result in as much detail a possible, also recalling some background on Galois cohomology, elliptic curves with complex multiplication and modular curves. The final portion of the seminar aims at covering some parts of the preprint [CW] of Çiperiani and Wiles.

A remark on referencing: There are detailed references in [Wes]. I will not repeat them below, but only give further references that are not mentioned therein.

01.10.07 **1. Introduction and statement of BSD**

Formulation of the conjecture of Birch and Swinnerton-Dyer, including a recall of the necessary invariants of an elliptic curve needed to state it. Statement of the main results of Kolyvagin. Deduction of the consequences for BSD modulo some auxiliary results due to Gross-Zagier, Waldschmidt, etc. (which we will not cover in the seminar). Maybe a very rough sketch of Kolyvagin's argument.

If time permits, I shall try to give some glimpses on the work of Çiperiani and Wiles.

G. Böckle

08.10.07 **2. Local Galois cohomology**

This is [Wes], § 2. I suggest to present the results in the same three steps Weston does it. That way we see very clearly what's important. The aim of the talk will be to explain, motivate, prove, etc. some of these results.

Note, so we won't forget: **the prime p is almost always different from** 2

On 2.1: Recall the 5-term inflation-restriction sequence. Why is it shorter in 2.1 (1)? Another reference for (2) is [NSW], Ch.7., or perhaps even better: [Neu], Aufgabe V.2.4. A sketch of proof for the unramified duality is given in [Pap], Prop 1.3. (Papikian's E_p can be any T. Assuming (2) one also needs to check that the cokernel of (1) for T has the same dimension as the kernel of (1) for the Cartier dual $T^* = \mathrm{Hom}(T, \mu_p)$.)

On 2.2. This is easy and mainly notation. Explain (4): This is a consequence of (2) for a vector space and its dual.

On 2.3: Perhaps one could recall the definition of the Weil pairing and explain its Galois equivariance. Thereby one proves what Weston calls **Duality**.

The first sequence on p. 5 (in local and global form) is fundamental. Explain how by using cohomology, one obtains the second formula. Explain the map κ. This is a good point to recall the description of H^1 in terms of 1-cycles. (κ is obtained from this description and the Snake Lemma). Also, in [Pap] it is explained how the second sequence on page 5 is exactly the sequence (1) in 2.1; this explains **Compatibility**

TBA

15.10.07 **3. Global Galois cohomology and interpretations of Selmer groups**

This talk has two goals. One is to introduce the notation of global Selmer groups, the other to interprete them in our situations as groups describing certain Galois extensions.

Expose [Wes], §3.1–3.3. Emphasize the case we are interested in and the geometric local Selmer structure. Perhaps indicate a proof of Prop. 3.1 from the better known Poitou-Tate duality theorem (see also [NSW], 8.6.13, and proof of 8.6.20).

After exposing this material, the remainder of the talk should serve to provide a concrete interpretation in the case we are interested. The main source is [Gro], § 9 (beginning up to the second line of p. 251; a diagram like (9.4) might be helpful), but, **please**, stick to the notation of Weston. (Note E_p(Gross)= $E[p]$(Weston), L(Gross)=L_0(Weston), etc.): Prove [Gro], 9.1, 9.2 and 9.3. (I think here K can be any number field, $L = K(E[p])$; one needs $\mathrm{Gal}(L/K) \cong \mathrm{GL}_2(\mathbb{F}_p)$! Some of the proofs are written down in more detail in [Wes], Lemmas 4.5 and 4.6)

The key point for us is that any finite $\mathbb{F}_p$-vector subspace $S \subset H^1(K, E[p])$ defines a finite Galois extension of L_0 with Galois group isomorphic to $E[p]^{\dim_{\mathbb{F}_p} S} \cong \mathbb{Z}/(p)^{2\dim_{\mathbb{F}_p} S}$. Now one can reinterpret $S_{\mathfrak{a}}$ and $S^{\mathfrak{a}}$ of Weston (for $S = \mathrm{Sel}(\ldots)$ and $T = E[p] \cong T^*$) as classes describing Galois extensions. Local classes being zero means that certain Frobenius elements are trivial, local classes being unrestricted means that ramification is allowed.

Note: If one tries to compare [Gro] with [Wes] it's mainly just reordering the material. However some parts of Gross seem to disappear. One of them is the proof of [Gro], Prop. 8.2, where Gross uses a global pairing that goes into the Brauer group and then makes use of the fact that for a given global class the sum of its local classes is zero. This is contained in the sequence (6), i.e., the main global duality result in [Wes], 3.3

TBA

22.10.07 **4. Bounding Selmer groups by local conditions**

After the concrete interpretations above, we now want to bound the size of Selmer groups $S^{\mathfrak{a}}$ by restricting the Frobenius elements at suitable places. Most of the talk should be dedicated to the proofs of [Wes], 3.4 and 3.5, perhaps after briefly recalling the notation. Weston's arguments are quite complete. Before entering 3.5 it might be good to recall whats on page 3 last paragraph and page 4 first. In 3.5 it suffices to assume, from the start, that K is an imaginary quadratic extension of $K_0 = \mathbb{Q}$. (One could at the end mention that everything works more generally.)

The talk should end with [Wes], §4.2, i.e. by explaining how the action of $\mathrm{Gal}(K/\mathbb{Q})$ decomposes $E[p]$ as well as the singular local groups into plus and minus parts, and also the sequence (11). Thus from now on, we may investigate plus and minus parts separately.

TBA

29.10.07 **5. Reduction of the main result to the construction of certain cohomology classes**

Present the remaining parts of [Wes], § 4 (various things need to be recalled from previous talks). The upshot of this is: If by some magic (= Kolyvagin), we can produce suitable cohomology classes, then the proof of Theorem 4.1 (our main goal) will be completed. The proof is thus 'reduced' to proving Prop. 4.8 and 4.12

TBA

05.11.07 **6. Heegner points on modular curves**

It might be good to start out by briefly presenting the aim of this and parts of the following talk: Let K be an imaginary quadratic field and E an elliptic curve over $\mathbb{Q}$. We want to construct points in $E(L)$ for certain abelian extensions L of K. The idea is to use a modular parameterization $X_0(N) \to E$ where N is the conductor of E. That such a parameterization should exist is the conjecture of Taniyama-Shimura and was only proved in the aftermath to the proof of FLT. So we have $X_0(N)(L) \to E(L)$. The special points on $X_0(N)$ that are defined on abelian extensions of K are elliptic curves with CM by an order of K (and an N-isogeny). This yields the so called Heegner points on E.

The present talk should lay foundations and cover [Wes], §5, up to and including Proposition 5.1. Thus it should contain some background on class field theory over imaginary quadratic fields, on CM elliptic curves and the curve $X_0(N)$. Obviously one can't expose everything in great detail - but one should do quite a bit more than what Weston did. For instance one can remind us of the CM theory – like why $j(\mathbb{C}/\mathfrak{a})$ is algebraic – ring class fields, etc. The reminder about $X_0(N)$ could be rather brief.

There is a good survey in [Dar], §3.1 and 3.2. To fill in some details in [Dar] a very good source is [Si2], II, Ch.2 (The action of ideals for an order $\mathcal{O}$ of K on elliptic curves for that order should certainly be presented.). Another longer survey of the CM theme is Kedlaya's senior thesis [Ke1] or its 'condensed' version [Ke2]. Finally, there is also the book [Cox].

For modular curves I recommend [DI], §7 and §8.

A remark: I think in [Wes], p. 16, line 3, Weston would like to define the reduction not only for E, but also for $J_0(N)$, the Jacobian of $X_0(N)$. (Else Proposition 5.1 doesn't make sense)

TBA

14.11.07 7. Heegner points on elliptic curves and Kolyvagin's Euler system
please note: Nov 12 is a holiday; we'll probably meet on Wednesday

Let E be an arbitrary (non-CM) elliptic curve and choose a modular parameterization $X_0(N) \to E$ (see [Kna], XI.11, XII.1–2). By changing E within its isogeny class (which does not alter the applications to BSD, see [Si1], 16.5.2), we may assume if necessary that we have a strong modular parameterization (see also [Edi]). Having a modular parameterization, we obtain $y_n \in E(K_n)$ as the image of $x_n \in X_0(K_n)$. The first aim of this talk to to complete the list of properties of the points y_n, namely [Wes], Prop. 5.2, and thereby explain the remainder of [Wes], §5. This should not

be hard since Prop. 5.1 was covered in the previous talk. (Further references on §5 are [DI], also [Cla], and obviously [Gro], Prop. 3.7.)
The larger part of the talk should introduce Kolyvagin's Euler system for elliptic curves (formed by the classes $c(n)$) and prove its basic properties. One should cover [Wes], §6.1, §6.2 and give the proof of Lemma 6.6 in the case where the place does not divide the level N. Weston's presentation seems pretty complete. For the construction of $c(n)$ (and also $d(n)$ and $\tilde{d}(n)$) the diagram (4.2) in [Gro] is perhaps useful. The main Lemma 6.6 says that the cohomology classes $c(n)$ of Kolyvagin (n a suitable square free integer) are unramified at all primes of K not dividing n. Apart from Weston and Gross, a good source for this is also [And], proof of Prop 2.1, (1)

TBA

19.11.07 **8. Unramifiedness of Kolyvagin's classes at bad primes of E**
This talk should give the proof of Lemma 6.6 in the case where v divides the level. This is well-documented in [And] - but might require further literature on Néron models (see also [Si2], IV and references therein) and $X_0(N)$ over $\operatorname{Spec}\mathbb{Z}$. The proof in [Gro], Prop. 6.2 is quite short.

TBA

26.11.07 **9. Ramification of Kolyvagin's classes**
Now comes a crucial part: Analyze the ramification of the classes $c(n)$ at places dividing n. This is [Wes], §6.3, except for Lemma 6.6. The main result is Lemma 6.8. One can also consult [Gro], Prop 6.2, and [And], Prop 2.2(2)

TBA

03.12.07 **10. The completion of Kolyvagin's proof and examples**
Finish! It's now easy to prove the missing propositions and thus complete the results. The reference is [Wes], §6.4
This is perhaps also a good point to review the entire proof!
It would be very nice to give some details on the example in [Wes], §7. Or to dig up some further examples, e.g. [Wat].

TBA

10.12.07 **11. The results of Ciperiani-Wiles I**

TBA

10.12.07 **12. The results of Ciperiani-Wiles II**

TBA

References

[And] F. Andreatta, *A criterion for local triviality*, in [SEM], under *Neron Models and Local Triviality of Classes*.

[Cla] P. Clark, *Lecture notes on Eichler-Shimura*, in [SEM], under *Hecke Correspondence, Eichler-Shimura Congruence*.

[CW] M. Çiperiani and A. Wiles, *Solvable points on genus one curves*, preprint.

[Cox] D. Cox, *Primes of the form* $x^2 + ny^2$.

[Dar] H. Darmon, *Rational points on modular elliptic curves*, CBMS Regional Conf. Ser. in Math. **101**.

[DI] F. Diamond, J. Im, *Modular forms and modular curves*, in "Seminar on Fermat's Last Theorem", CMS conference proceedings, vol. **17**.

[Edi] B. Edixhoven, *On the Manin constants of modular elliptic curves*, in "Arithmetic Algebraic Geometry (Texel 1989)", 25–40.

[Gro] B. Gross, *Kolyvagin's work on modular elliptic curves*, in "L-functions and arithmetic (Durham, 1989)", 235–256, LMS Lecture Notes **153**.

[Ke1] K. Kedlaya, *Complex multiplication and explicit class field theory*, senior thesis http://www-math.mit.edu/∼kedlaya/math/other.html#expository

[Ke2] K. Kedlaya, *Complex multiplication lectures*, in [SEM].

[Ko1] V. Kolyvagin, *Finiteness of* $E(\mathbb{Q})$ *and* $Ш(E, \mathbb{Q})$ *for a subclass of Weil curves*, (transl.) Math. USSR-Izv. **32** (1989), no. 3, 523–541.

[Ko2] V. Kolyvagin, *The Mordell-Weil and Shafarevich-Tate groups for Weil elliptic curves*, (transl.) Math. USSR-Izv. **33** (1989), no. 3, 473–499

[Kna] A. Knapp, *Elliptic Curves*.

[NSW] J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of Number Fields*.

[Neu] J. Neukirch, *Algebraische Zahlentheorie*.

[Pap] M. Papikian, *On Tate local duality*, in [SEM] under *Constructing the local pairing*.

[SEM] *Kolyvagin's Application of Euler Systems to Elliptic Curves*, Graduate Number Theory Seminar by K. Kedlaya, Lecture Notes Section, math.ucdavis.edu/∼osserman/semold/

[Si1] J. Silverman, *Arithmetic of Elliptic Curves*, GTM **106**.

[Si2] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, GTM **151**.

[Wat] M. Watkins, *Some remarks on Heegner point computations*, http"//arxiv.org/pdf/math/0506325

[Wes] T. Weston, *The Euler system of Heegner points*, http://www.math.umass.edu/∼weston/oldpapers/hp.pdf

[Wes2] T. Weston, *The modular curves* $X_0(11)$ *and* $X_1(11)$, http://www.math.umass.edu/∼weston/oldpapers/mc.ps