Kleine AG: Modularity of elliptic curves

Organisation:
Paul Jonas Hamacher[1]
Timo Keller[2]

In the 1950s Taniyama and Shimura conjectured that every elliptic curve over $\mathbb{Q}$ is modular. Nowadays the statement is proven in full generality; Wiles gave the proof for semistable elliptic curves and the general case was subsequently deduced by works of Breuil, Conrad, Diamond, Taylor and Wiles. The most famous "application" of this assertion is the proof of Fermat's Last Theorem using arguments of Frey, Serre and Ribet.

The aim of this kleine AG is to understand the assertion of the Shimura-Taniyama conjecture rather than its proof. We will follow the paper [DDT] of Darmon, Diamond and Taylor. Unless stated otherwise all references in the program refer to it.

We remark that our program is very similar to the program of a past kleine AG about the same topic. You can find it at `http://www.math.uni-bonn.de/ag/kleineag/Modulare-Elliptische-Kurven/programm.pdf`

1. Modular curves and elliptic curves over $\mathbb{C}$ (60 minutes)

The aim of this talk is to recall the basics of elliptic curves over $\mathbb{C}$ and modular forms.

- Recall briefly the correspondence of elliptic curves over $\mathbb{C}$ and lattices (see for example [Sil1], ch. 6 for a detailed exposition).
- Recall the definition of $Y(\Gamma)$ resp. $X(\Gamma)$ as complex manifolds(p. 23) and give the moduli interpretation for $\Gamma = \Gamma_0(N), \Gamma_1(N)$ (p. 24).
- Recall the definition of modular forms and cusp forms and explain the interpretation of cusp forms of weight 2 as differential forms on $X(\Gamma)$ (p. 25 f).
- Define the Hecke-operators. Also explain their modular interpretation in the case $\Gamma = \Gamma_1(N)$ (p. 28 f).
- Define eigenforms and prove Prop. 1.17
- Introduce oldforms and newforms and explain Theorem 1.22.

2. Modularity: Geometric definition (45 minutes)

- Define the Jacobian and the Abel-Jacobi map as in p. 27f.
- Review the correspondence of complex projective manifolds and projective nonsingular varieties over $\mathbb{C}$ via the GAGA functor (see [GAGA],§19). In particular we can view $X(\Gamma)$ and their Jacobians as varieties over $\mathbb{C}$.
- State (without proof) that $X(\Gamma)$ and their Hecke correspondences can be canonically defined over $\mathbb{Q}$.

[1] `<Nachname>@ma.tum.de`
[2] `<Vorname>.<Nachname>@mathematik.uni-regensburg.de`

- Explain integral modular forms and the q-expansion principle (1.31-1.33)
- Give Shimura's construction of an abelian variety associated to a newform f (Def. 1.44) and explain Lemma 1.46 and Prop. 1.49.
- Define modularity as the (equivalent) properties given in Prop. 1.53. Also, give its proof (except $a \Rightarrow b$). *Note:* The conductor of an elliptic curve will be defined in the third talk. For now it suffices to know that it is some integer associated to an elliptic curve.

3. Modularity: Analytic definition (45-60 minutes)

- Define the L-function of a modular form (§ 1.4) and show Proposition 1.54: If $E = A_f$ is modular, then $L(E/\mathbb{Q}, s) = L(f, s)$.
- State the analytic version of the modularity: For any elliptic curve E over $\mathbb{Q}$ is modular if exists an eigenform f such that $L(E/\mathbb{Q}, s) = L(f, s)$. *Note:* For now, it is only clear that the geometric definition of modularity implies the analytic one. The other direction will be proven in the forth talk, continuing the second half of this talk.
- Introduce ℓ-adic Galois representations as in §2.1. In particular:
  - Deduce Proposition 2.6(c) from the Čebotarev's density theorem.
  - Give the definition of Galois representation unramified at p.
  - Give the definition of the conductor.
- Define the representation associated to an elliptic curve.
- Explain how to calculate the conductor of an elliptic curve (§1.1, also [Sil2, § V.9-11] for details). The most important result is [Sil2, Thm. 10.2]. The calculation of the wild part of the conductor is explained in [Sil2, Rem. 11.1.2].
- State Proposition 2.11(a) and Proposition 2.8(b).

4. Modularity: Arithmetic definition (45 minutes)

- Give the moduli interpretation of $X_0(N)$ resp. $X_1(N)$ and define models over $\mathbb{Q}$ and $\mathbb{Z}$ (§ 1.5).
- State the Eichler-Shimura relation (Thm. 1.29).
- Define the Galois representation associated to an eigenform f and state Thm. 3.1 (a),(b),(c),(d) and prove (a) and (b).
- Conclude that ρ_E is modular if and only if $L(E/\mathbb{Q}, s) = L(f, s)$ for some eigenform f.
- Show Proposition 3.20.

5. Lowering the level and Fermat's Last Theorem (30 minutes)

State the Ribet's theorem about lowering the level ([Rib, Thm. 1.1]) and deduce Fermat's last theorem from it ([Rib, Cor. 1.2]). Give a detailed proof, in particular make all necessary calculations (see also [vDdB] for more details or [Sil2, § V.9] for Tate's algorithm for calculating the special fibre for arbitrary elliptic curves).

References

[DDT] Darmon H., Diamond F., Taylor R.: *Fermats Last Theorem*, http://modular.math.washington.edu/edu/2011/581g/misc/Darmon-Diamond-Taylor-Fermats_Last_Theorem.pdf

[GAGA] Serre J.P.: Géométrie algébrique et géoétrie analytique, *Annales de l'institut Fourier* **6** (1955–56), pp. 1–42

[Rib] Ribet, K.A.: On modular representations of Gal($\overline{\mathbf{Q}}/\mathbf{Q}$) arising from modular forms, *Invent. Math.* **100** (1990), no. 2, pp. 431–476

[Sil1] Silverman J.: *The Arithmetic of Elliptic Curves*, 2nd edition.[3]

[Sil2] Silverman J.: *Advanced Topics in the Arithmetic of Elliptic Curves*.[4]

[vDdB] van Dobben de Bruyn R.: *The modularity theorem*, Bachelor thesis,`http://www.math.leidenuniv.nl/scripties/DobbendeBruynBach.pdf`

[3]Note the errata `http://www.math.brown.edu/~jhs/AEC/AECErrata.pdf`
[4]Note the errata `http://www.math.brown.edu/~jhs/ATAEC/ATAECErrata.pdf`