Elliptic Curves and Modularity

Jack Thorne
University of Cambridge

Mordell's equation:

$$y^2 = x^3 + a,$$

where a is a non-zero integer.

What are the solutions $(x, y) \in \mathbb{Z}^2$?

$$y^2 = x^3 + a$$

Mordell (1920): there are finitely many solutions $(x, y) \in \mathbb{Z}^2$.

Baker (1967): any solution $(x, y) \in \mathbb{Z}^2$ satisfies

$$\log |x|, \log |y| \leq (10^{10}|a|)^{10^4}.$$

von Känel, Matschke (2016): any solution $(x, y) \in \mathbb{Z}^2$ satisfies

$$\log |x|, \frac{2}{3} \log |y| \leq 1728|a|(\log |a| + 4).$$

Today we will discuss:

- What is the modularity conjecture for elliptic curves over a number field K;
- Why the modularity conjecture is important in number theory;
- How to prove new cases of the modularity conjecture.

Let K be a number field.

Definition

An elliptic curve E over K is a smooth, projective curve of genus 1 with a marked rational point $\infty \in E(K)$.

Any such curve can be represented by a *Weierstrass equation*

$$E : y^2 = x^3 + ax + b$$

for some $a, b \in \mathcal{O}_K$.

The points of E naturally form a group, and $E(K)$ is finitely generated (Mordell–Weil theorem).

In order to simplify statements, we now assume that K has class number 1. The counterpart to elliptic curves in the modularity conjecture is the cohomology of congruence subgroups of $\mathrm{GL}_2(\mathcal{O}_K)$.

For any non-zero ideal $\mathfrak{n} \leq \mathcal{O}_K$, we consider the congruence subgroup

$$\Gamma_1(\mathfrak{n}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}_K) \mid c \equiv 0 \bmod \mathfrak{n}, d \equiv 1 \bmod \mathfrak{n} \right\}.$$

The group cohomology groups $H^*(\Gamma_1(\mathfrak{n}), \mathbb{Q})$ are finite-dimensional $\mathbb{Q}$-vector spaces.

We can also think of these as the cohomology groups of certain manifold quotients $\Gamma_1(\mathfrak{n})\backslash X_K$, where X_K is a generalisation of the complex upper half-plane.

For any non-zero prime ideal $\mathfrak{p} \leq \mathcal{O}_K$ not dividing $\mathfrak{n}$, there is an associated Hecke operator

$$T_{\mathfrak{p}} : H^*(\Gamma_1(\mathfrak{n}), \mathbb{Q}) \to H^*(\Gamma_1(\mathfrak{n}), \mathbb{Q}).$$

This is a commuting family of operators, and it is of great interest to study the spectral decomposition of $H^*(\Gamma_1(\mathfrak{n}), \mathbb{Q})$.

Modularity conjecture

Let E be an elliptic curve over K. Then there is a non-zero element $c_E \in H^*(\Gamma_1(\mathfrak{n}), \mathbb{Q})$ such that

$$T_{\mathfrak{p}}(c_E) = a_{\mathfrak{p}}(E)c_E$$

for all but finitely many prime ideals $\mathfrak{p} \leq \mathcal{O}_K$, where

$$a_{\mathfrak{p}}(E) = N(\mathfrak{p}) + 1 - |E(\mathcal{O}_K/\mathfrak{p})|.$$

If c_E exists, we say that the curve E is *modular*.

Note: elliptic curves E, E' are isogenous over K if and only if $a_{\mathfrak{p}}(E) = a_{\mathfrak{p}}(E')$ for all but finitely many prime ideals $\mathfrak{p} \leq \mathcal{O}_K$.

One class of applications of the modularity conjecture is the solution of Diophantine equations.

Let $p \geq 5$ be a prime, and consider a non-trivial solution

$$a^p + b^p = c^p$$

to the Fermat equation with $(a, b, c) \in \mathbb{Z}^3$. We can associate to this solution the (Frey–Hellegoarch) elliptic curve

$$E_{a,b,c} : y^2 = x(x - a^p)(x + b^p).$$

Theorem (Şengün, Siksek)

Let $d > 0$ be an even square-free integer, and let $K = \mathbb{Q}(\sqrt{-d})$. Assume a strengthened version of the modularity conjecture for elliptic curves over K.
Then the asymptotic Fermat's Last Theorem holds over K: there is a constant B_K such that for each prime $p > B_K$, the equation $a^p + b^p = c^p$ has no non-trivial solution with $(a, b, c) \in \mathcal{O}_K^3$.

Theorem (von Känel, Matschke)

Let $a \in \mathbb{Z}$ be non-zero. Then any solution $(x, y) \in \mathbb{Z}^2$ to $y^2 = x^3 + a$ satisfies

$$\log |x|, \frac{2}{3} \log |y| \leq 1728|a|(\log |a| + 4).$$

Modularity is also important in the study of the arithmetic of elliptic curves.

Birch–Swinnerton-Dyer conjecture

Let E be an elliptic curve over K, and let

$$L(E,s) \doteq \prod_{\mathfrak{p}} (1 - a_{\mathfrak{p}}(E) N(\mathfrak{p})^{-s} + N(\mathfrak{p})^{1-2s})^{-1}$$

be its associated L-function. Then:

1. $L(E,s)$ admits an analytic continuation to $\mathbb{C}$.
2. The order of vanishing of $L(E,s)$ at the point $s = 1$ equals the rank of the finitely generated abelian group $E(K)$.

Theorem (Hecke, Weil, Jacquet–Langlands)

Let E be a modular elliptic curve over a number field K. Then $L(E, s)$ admits an analytic continuation to $\mathbb{C}$.

Theorem (Gross–Zagier, Kolyvagin, Zhang)

Let K be a totally real number field, and let E be a modular elliptic curve over K. If $[K : \mathbb{Q}]$ is even, suppose that E has a prime of multiplicative reduction.
Then if the order of vanishing of $L(E, s)$ at the point $s = 1$ is at most 1, then the Birch–Swinnerton-Dyer conjecture holds for E.

Theorem (Wiles, Taylor–Wiles, Breuil–Conrad–Diamond–Taylor)

The modularity conjecture is true when $K = \mathbb{Q}$.

Let E be an elliptic curve over the number field K. The absolute Galois group $G_K = \mathrm{Gal}(\overline{K}/K)$ acts on the set of points $E(\overline{K})$.

In particular, if ℓ is a prime number then G_K acts on $E[\ell](\overline{K})$, which is an $\mathbb{Z}/\ell\mathbb{Z}$-vector space of dimension 2. A choice of basis determines a continuous representation

$$\rho_{E,\mathbb{Z}/\ell\mathbb{Z}} : G_K \to \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}).$$

If $n \geq 1$ then $E[\ell^n](\overline{K})$ is a free $\mathbb{Z}/\ell^n\mathbb{Z}$-module of rank 2. By passage to limit, we see that G_K acts continuously on

$$V_\ell E = \left(\varprojlim_n E[\ell^n](\overline{K}) \right) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell,$$

which is a $\mathbb{Q}_\ell$-vector space of dimension 2. A choice of basis determines a continuous representation

$$\rho_{E,\mathbb{Q}_\ell} : G_K \to \mathrm{GL}_2(\mathbb{Q}_\ell).$$

If $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ not dividing ℓ and at which E has good reduction, then this representation $\rho_{E,\mathbb{Q}_\ell}$ is unramified at $\mathfrak{p}$ and

$$\mathrm{tr}\, \rho_{E,\mathbb{Q}_\ell}(\mathrm{Frob}_\mathfrak{p}) = a_\mathfrak{p}(E).$$

Definition

We say that a representation $\rho : G_K \to \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is modular if there exists an ideal $\mathfrak{n} \leq \mathcal{O}_K$ and a non-zero class $c_\rho \in H^*(\Gamma_1(\mathfrak{n}), \mathbb{Z}/\ell\mathbb{Z})$ such that for almost all prime ideals $\mathfrak{p} \leq \mathcal{O}_K$,

$$T_\mathfrak{p}(c_\rho) = (\mathrm{tr}\, \rho(\mathrm{Frob}_\mathfrak{p}))c_\rho.$$

Definition

We say that a representation $\rho : G_K \to \mathrm{GL}_2(\mathbb{Q}_\ell)$ is modular if there exists an ideal $\mathfrak{n} \leq \mathcal{O}_K$ and a non-zero class $c_\rho \in H^*(\Gamma_1(\mathfrak{n}), \mathbb{Q}_\ell)$ such that for almost all prime ideals $\mathfrak{p} \leq \mathcal{O}_K$,

$$T_\mathfrak{p}(c_\rho) = (\mathrm{tr}\, \rho(\mathrm{Frob}_\mathfrak{p}))c_\rho.$$

Key observations:

- E is modular if and only if each of its associated representations $\rho_{E,\mathbb{Q}_\ell}$ is modular.
- Any representation $\rho : G_K \to \mathrm{GL}_2(\mathbb{Q}_\ell)$ has an associated residual representation $\overline{\rho} : G_K \to \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, with

$$\mathrm{tr}\,\overline{\rho}(\mathrm{Frob}_{\mathfrak{p}}) = \mathrm{tr}\,\rho(\mathrm{Frob}_{\mathfrak{p}}) \bmod \ell$$

  for almost all primes ideals $\mathfrak{p} \leq \mathcal{O}_K$.
- If ρ is modular, then so is $\overline{\rho}$.

Modularity Lifting Theorem Schema

Let $\rho : G_K \to \mathrm{GL}_2(\mathbb{Q}_\ell)$ be a representation satisfying the following conditions:

- $\overline{\rho}$ is modular.
- ρ satisfies the necessary local conditions to be modular.

Then ρ is modular.

Wiles and Taylor proved the first modularity lifting theorems in the case $K = \mathbb{Q}$.

To apply a modularity lifting theorem, one needs a supply of modular residual representations $\overline{\rho}$. Wiles observed that if E is an elliptic curve, then $\rho_{E,\mathbb{Z}/3\mathbb{Z}}$ is necessarily modular. This relies on the following three facts:

- The reduction map $\mathrm{GL}_2(\mathbb{Z}_3) \to \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ splits, so $\rho_{E,\mathbb{Z}/3\mathbb{Z}}$ lifts to a representation $\widetilde{\rho} : G_K \to \mathrm{GL}_2(\mathbb{C})$ of finite image.
- The group $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ is solvable, so $\widetilde{\rho}$ corresponds to a weight 1 modular form.
- There exist plentiful congruences between weight 1 modular forms and modular forms of weight 2 (which contribute to the cohomology of congruence subgroups).

The strongest generalisations of these ideas exist when K is a totally real field.

Theorem (Kisin, Barnet-Lamb–Gee–Geraghty)

Let K be a totally real number field, and let E be an elliptic curve over K. Suppose that there is an odd prime ℓ such that:

- $\rho_{E,\mathbb{Z}/\ell\mathbb{Z}}$ *is modular.*
- $\rho_{E,\mathbb{Z}/\ell\mathbb{Z}}|_{G_{K(e^{2\pi i/\ell})}}$ *is absolutely irreducible (Taylor–Wiles hypothesis).*

Then E is modular.

Using a generalisation of Wiles' idea, one can show that the modularity of $\rho_{E,\mathbb{Z}/\ell\mathbb{Z}}$ is automatic when $\ell = 3, 5$ or 7. Thus if an elliptic curve E fails to be modular, then there exists a prime $\ell \in \{3, 5, 7\}$ such that $\rho_{E,\mathbb{Z}/\ell\mathbb{Z}}|_{G_{K(e^{2\pi i/\ell})}}$ is reducible.

Theorem (Freitas, Le Hung, Siksek, 2015)

If K is a real quadratic field, then every elliptic curve E over K is modular.

Strategy of the proof: write down a finite collection of modular curves Y_i such that if E is a non-modular elliptic curve, then E determines a point of $Y_i(K)$. They all have genus > 1, hence have finitely many rational points by Faltings' theorem.

For example, this collection includes the modular curve $Y_0(105)$ which parameterises elliptic curves together with a subgroup of order $3 \times 5 \times 7 = 105$.

Then compute all points of the curves Y_i defined over real quadratic fields and check by hand that they correspond to modular elliptic curves.

Theorem (T., 2019)

Let p be a prime. If K is a totally real field such that $K/\mathbb{Q}$ is abelian of degree p^n and unramified outside p, then every elliptic curve E over K is modular.

Strategy of the proof: first prove a new modularity lifting theorem which implies:

Theorem

Let K be a totally real field such that $\sqrt{5} \notin K$. If E is an elliptic curve over K such that $\rho_{E,\mathbb{Z}/5\mathbb{Z}}$ is irreducible, then E is modular.

Theorem (T., 2019)

Let p be a prime. If K is a totally real field such that $K/\mathbb{Q}$ is abelian of degree p^n and unramified outside p, then every elliptic curve E over K is modular.

Then look at the modular curves Y_i which parameterize elliptic curves for which 3-adic and 5-adic modularity lifting theorems fail to prove the modularity. It turns out there are two, which are of genus 1, and they are both isogenous to $X_0(15)$.

Any field K as in the statement of the theorem is contained in the Iwasawa $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty/\mathbb{Q}$. We can use the Iwasawa theory of elliptic curves to understand $X_0(15)(\mathbb{Q}_\infty)$. (More precisely, results of Kato and Skinner on the Main Conjecture.)

It turns out that for any prime p, $X_0(15)(\mathbb{Q}_\infty) = X_0(15)(\mathbb{Q})$.

Theorem (Derickx, Najman, Siksek, 2020)

Let K be a totally real cubic number field. Then every elliptic curve E over K is modular.

Strategy of proof: similar to the real quadratic case, using new modularity lifting theorems due to T. and Kalyanswamy.

What about number fields which are not totally real? This case is much harder for a number of related reasons:

- When K is totally real, the groups $H^*(\Gamma_1(\mathfrak{n}), \mathbb{Q}_\ell)$ are essentially the étale cohomology groups of algebraic varieties over K. In particular, the group G_K acts. When K is not totally real, there is no clear link to algebraic geometry.
- When K is totally real, the groups $H^*(\Gamma_1(\mathfrak{n}), \mathbb{Z}_\ell)$ are essentially torsion-free, so passing to $H^*(\Gamma_1(\mathfrak{n}), \mathbb{Q}_\ell)$ does not lose information. When K is not totally real, there are many non-trivial torsion classes.
- The Taylor–Wiles method for proving modularity lifting theorems requires a "numerical coincidence" to hold: two Selmer groups are required to have the same dimension.

Calegari–Geraghty (2018) made the beautiful realisation that the "numerical coincidence" should be replaced by an equality between the difference in the dimension of these Selmer groups and the range of degrees in which the cohomology groups $H^*(\Gamma_1(\mathfrak{n}), \mathbb{Z}/\ell\mathbb{Z})$ can be non-zero. They showed how one could prove modularity lifting theorems assuming two conjectures:

- Conjecture A: each non-zero class in $H^*(\Gamma_1(\mathfrak{n}), \mathbb{Z}_\ell)$ (including ℓ^n-torsion classes) which is an eigenvector for the Hecke operators $T_\mathfrak{p}$ gives rise to a Galois representation satisfying certain local conditions.
- Conjecture B: for each $i \in \mathbb{Z}$, the "interesting part" of $H^i(\Gamma_1(\mathfrak{n}), \mathbb{Z}/\ell\mathbb{Z})$ is non-zero only if the "interesting part" of $H^i(\Gamma_1(\mathfrak{n}), \mathbb{Q}_\ell)$ is non-zero.

The Calegari–Geraghty framework was implemented to prove unconditional modularity lifting theorems, leading to the following:

Theorem (Allen–Caraiani–Calegari–Gee–Helm–Le Hung–Newton–Scholze–Taylor–T.)

Let K be a CM field (e.g. an imaginary quadratic extension of a totally real field). Then each elliptic curve E over K is potentially modular, in the sense that there exists a finite CM extension L/K such that the base change curve E_L is modular.

Key ingredients in proof: work of Scholze and Caraiani–Scholze on the cohomology of unitary Shimura varieties forms the basis for a proof of most of Calegari–Geraghty's Conjecture A.
Observations due to Khare–T. form the basis of a strategy to avoid proving Conjecture B.
The story of the proof of this theorem was the subject of an article in Quanta magazine.

What about establishing the modularity, as opposed to potential modularity, of elliptic curves over CM fields? We need a supply of modular residual representations $\overline{\rho} : G_K \to \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. Recall the ingredients to show that if E is an elliptic curve over a totally real field K, then $\rho_{E,\mathbb{Z}/3\mathbb{Z}}$ is modular:

- The reduction map $\mathrm{GL}_2(\mathbb{Z}_3) \to \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ splits, so $\rho_{E,\mathbb{Z}/3\mathbb{Z}}$ lifts to a representation $\widetilde{\rho} : G_K \to \mathrm{GL}_2(\mathbb{C})$ of finite image.
- The group $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ is solvable, so $\widetilde{\rho}$ corresponds to a weight 1 modular form.
- There exist plentiful congruences between weight 1 modular forms and modular forms of weight 2 (which contribute to the cohomology of congruence subgroups).

When K is a CM field, the last point fails!

Nevertheless, we can prove:

Theorem (Allen–Khare–T.)

Let K be an imaginary quadratic field. Then a positive proportion of elliptic curves E over K are modular.

It seems reasonable to hope that the next 10 years will bring a proof of the modularity of all elliptic curves over imaginary quadratic fields. After that – who knows!