Modularity, Level Lowering, Frey Curves and Fermat's Last Theorem

Samir Siksek

11 July 2016

Monday & Tuesday

Prerequistes:

(i) Basic knowledge of elliptic curves and modular forms.

(ii) In fact you can get away with knowing nothing about modular forms, except for a few facts that can be taken as black boxes.

Plan:

- **Talk 1:** Modularity, Level lowering and the proof of FLT.
- **Talk 2:** The equation $x^p + L^r y^p + z^p = 0$.
- **Monday afternoon:** Exercises—work in groups.
- **Monday late afternoon:** Presentations of solutions.
- **Talk 3:** The Method of Kraus.
- **Talk 4:** Galois Representations.
- **Tuesday afternoon:** Exercises—work in groups.
- **Tuesday late afternoon:** Presentations of solutions.

Facts about Newforms I

Definition

A **newform of level** N is an element of the space $S_2^{\mathrm{new}}(N)$ that is a simultaneous eigenvector for all the Hecke operators, normalized so that the q-expansion at infinity begins with $q + c_2 q^2 + \cdots$.

Facts:

1. $N \geq 1$ is an integer called the level.
2. There are finitely many newforms of level N (and weight 2).
3. There are algorithms implemented in `SAGE` and `Magma` for computing the newforms of level N.
4. A newform is given by its q-expansion

$$f = q + \sum_{n \geq 2} c_n q^n \,.$$

Facts about Newforms II

1. A newform is given by its q-expansion

$$f = q + \sum_{n \geq 2} c_n q^n \,.$$

2. $K = \mathbb{Q}(c_2, c_3, \ldots)$ is a totally real finite extension of $\mathbb{Q}$.
3. $c_i \in \mathcal{O}_K$.
4. (Deligne) If ℓ is a prime then

$$|\sigma(c_\ell)| \leq 2\sqrt{\ell}, \qquad \text{for all embeddings } \sigma : K \hookrightarrow \mathbb{R}.$$

Theorem

There are no newforms at levels

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 22, 25, 28, 60 \,.$$

Example

The newforms at a fixed level N can be computed using the modular symbols algorithm (Cremona, Stein, ...) implemented in `Magma` and `SAGE`. For example, the newforms at level 110 are

$$\begin{aligned} f_1 &= q - q^2 + q^3 + q^4 - q^5 - q^6 + 5q^7 + \cdots, \\ f_2 &= q + q^2 + q^3 + q^4 - q^5 + q^6 - q^7 + \cdots, \\ f_3 &= q + q^2 - q^3 + q^4 + q^5 - q^6 + 3q^7 + \cdots, \\ f_4 &= q - q^2 + \theta q^3 + q^4 + q^5 - \theta q^6 - \theta q^7 + \cdots. \end{aligned}$$

f_1, f_2, f_3 have coefficients in $\mathbb{Z}$.
f_4 has coefficients in $\mathbb{Z}[\theta]$ where $\theta = (-1+\sqrt{33})/2$.
There is a fifth newform at level 110 which is the conjugate of f_4.

f_1, f_2, f_3 are **rational** newforms, whereas f_4 is irrational.

The Modularity Theorem

We call a newform **rational** if all its coefficients are in $\mathbb{Q}$, otherwise it is **irrational**.

The Modularity Theorem (Wiles and many others). There is a bijection:

$$\text{level } N \text{ rational newforms} \longleftrightarrow \text{isogeny classes of elliptic curves over } \mathbb{Q} \text{ of conductor } N$$

$$f = q + \sum_{n \geq 2} c_n q^n \quad \mapsto \quad E_f$$

such that

$$c_\ell = a_\ell(E_f), \qquad a_\ell(E_f) = \ell + 1 - \#E_f(\mathbb{F}_\ell),$$

for all primes $\ell \nmid N$.

‘arises from’

Definition

Let

- E be an elliptic curve of conductor N,
- $f = q + \sum_{n \geq 2} c_n q^n$ be a newform of level N',
- $K = \mathbb{Q}(c_2, c_3, \ldots)$,
- $\mathcal{O}_K$ the ring of integers of K,
- p a prime.

We say that E **arises from** f **mod** p and write $E \sim_p f$ if there is some prime ideal $\mathfrak{P} \mid p$ of $\mathcal{O}_K$ such that for all primes ℓ

(i) if $\ell \nmid pNN'$ then $a_\ell(E) \equiv c_\ell \pmod{\mathfrak{P}}$, and

(ii) if $\ell \nmid pN'$ and $\ell \,||\, N$ then $\ell + 1 \equiv \pm c_\ell \pmod{\mathfrak{P}}$.

If f is rational then it corresponds to an elliptic curve E'. In which case we write $E \sim_p E'$.

Ribet's Level Lowering Theorem

Let

1. $E/\mathbb{Q}$ be an elliptic curve,
2. $\Delta = \Delta_{\min}$ be the discriminant of a minimal model of E,
3. N be the conductor of E,
4. for a prime p let

$$N_p = N \Big/ \prod_{\substack{q \| N, \\ p \mid \mathrm{ord}_q(\Delta)}} q.$$

Theorem (A simplified special case of Ribet's Theorem)

- *Let $p \geq 3$ be a prime.*
- *Suppose E does not have any p-isogenies.*
- *Suppose E is modular.*

Then there exists a newform f of level N_p such that $E \sim_p f$.

An Example

$$E \ : \quad y^2 = x^3 - x^2 - 77x + 330 \qquad \texttt{132B1}$$

Then

$$\Delta_{\min} = 2^4 \times 3^{10} \times 11, \qquad N = 2^2 \times 3 \times 11.$$

The only isogeny the curve E has is a 2-isogeny. Recall

$$N_p = N \Big/ \prod_{\substack{q || N, \\ p \mid \mathrm{ord}_q(\Delta)}} q.$$

So

$$N_5 = \frac{2^2 \times 3 \times 11}{3} = 44, \qquad N_p = 132 \text{ for } p \neq 5.$$

Example (continued)

$$E \;:\quad y^2 = x^3 - x^2 - 77x + 330 \qquad \text{only 2-isogenies}$$

$$N_5 = \frac{2^2 \times 3 \times 11}{3} = 44, \qquad N_p = 132 \text{ for } p \neq 5.$$

Apply Ribet's Theorem with $p = 5$.

There is only one newform at level 44 which corresponds to the elliptic curve

$$F \;:\quad y^2 = x^3 + x^2 + 3x - 1 \qquad \text{44A1.}$$

Thus $E \sim_5 F$.

ℓ	2	3	5	7	11	13	17	19
$a_\ell(E)$	0	-1	2	2	-1	6	-4	-2
$a_\ell(F)$	0	1	-3	2	-1	-4	6	8

Fermat's Last Theorem

Suppose a, b, c are integers, $p \geq 5$ prime satisfying

$$a^p + b^p + c^p = 0, \qquad abc \neq 0\,.$$

Without loss of generality

$$\gcd(a, b, c) = 1, \qquad 2 \mid b, \qquad a^p \equiv -1 \pmod 4.$$

Let

$$E \ : \ Y^2 = X(X - a^p)(X + b^p), \qquad \text{Frey curve.}$$

(For $E \ : \ Y^2 = X(X - u)(X - v)$ we have $\Delta = 16u^2v^2(u - v)^2$.)

Thus

$$\Delta = 16a^{2p}b^{2p}(a^p + b^p)^2 = 16a^{2p}b^{2p}c^{2p}.$$

FLT continued

Applying Tate's algorithm:

$$\Delta_{\min} = \frac{a^{2p} b^{2p} c^{2p}}{2^8}, \qquad N = \prod_{\ell \mid abc} \ell \,.$$

Absence of Isogenies

Theorem (Mazur)

Let $E/\mathbb{Q}$ be an elliptic curve, and p a prime satisfying **at least one** *of the following conditions:*

- $p > 163$,
- *or $p \geq 5$ and $\#E(\mathbb{Q})[2] = 4$ and the conductor of E is squarefree.*

Then E does not have p-isogenies.

$$E \; : \; Y^2 = X(X - a^p)(X + b^p), \qquad \text{Frey curve.}$$

Then

$$\Delta_{\min} = \frac{a^{2p} b^{2p} c^{2p}}{2^8}, \qquad N = \prod_{\ell \mid abc} \ell \, .$$

By Mazur, for $p \geq 5$, the Frey curve does not have p-isogenies.

FLT (continued)

$$\Delta_{\min} = \frac{a^{2p} b^{2p} c^{2p}}{2^8}, \qquad N = \prod_{\ell \mid abc} \ell \,.$$

$$N_p = N \Big/ \prod_{\substack{q \| N, \\ p \mid \mathrm{ord}_q(\Delta)}} q \qquad \Longrightarrow \qquad N_p = 2.$$

Theorem (Ribet)

- *Let $p \geq 3$ be a prime.*
- *Suppose E does not have any p-isogenies.*
- *Suppose E is modular.*

Then there exists a newform f of level N_p such that $E \sim_p f$.

By Ribet, there is a newform f of level 2 such that $E \sim_p f$.

FLT (continued)

By Ribet, there is a newform f of level 2 such that such that $E \sim_p f$.

Theorem

There are no newforms at levels

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 22, 25, 28, 60\,.$$

Contradiction!

Frey Curves

Given a Diophantine equation, suppose it has a solution, and associate with it an elliptic curve E called a **Frey curve**, if possible. The key properties of the Frey curve are

- The coefficients of the elliptic curve somehow depend on the solution to the Diophantine equation.
- The minimal discriminant can be written in the form $\Delta = C \cdot D^p$ where D depends on the solution. The factor C **does not depend on the solutions but only on the Diophantine equation**.
- E has multiplicative reduction at the primes dividing D. (i.e. if $p \mid D$ then $p \parallel N$).

We conclude

1. The conductor N of E is divisible by primes dividing C and D (depends on the equation and the solution).
2. The primes dividing D can be removed when we write down N_p (depends only on the equation).
3. There are only finitely many possibilities for N_p.
4. For each N_p, there are only finitely many newforms f of level N_p.

Frey Curve

1. The conductor N of E is divisible by primes dividing C and D (depends on the equation and the solution).
2. The primes dividing D can be removed when we write down N_p (depends only on the equation).
3. There are only finitely many possibilities for N_p.
4. For each N_p, there are only finitely many newforms f of level N_p.

Applying Wiles, Ribet and Mazur, we have $E \sim_p f$ for one of finitely many f.

What can we learn about the solution to the Diophantine equation from knowing the finitely many f?

Frey Curve

1. The conductor N of E is divisible by primes dividing C and D (depends on the equation and the solution).
2. The primes dividing D can be removed when we write down N_p (depends only on the equation).
3. There are only finitely many possibilities for N_p.
4. For each N_p, there are only finitely many newforms f of level N_p.

Applying Wiles, Ribet and Mazur, we have $E \sim_p f$ for one of finitely many f.

What can we learn about the solution to the Diophantine equation from knowing the finitely many f?

Find out in the next lecture!