The modular and symplectic methods

Mike Daas

Universiteit Leiden

November 25, 2021

Fermat's Last Theorem

- In 1637: if $n > 2$ and $x, y, z \in \mathbb{Z}$ satisfy

$$x^n + y^n = z^n,$$

then $xyz = 0$.

Fermat's Last Theorem

- In 1637: if $n > 2$ and $x, y, z \in \mathbb{Z}$ satisfy

$$x^n + y^n = z^n,$$

  then $xyz = 0$.
- First proof completed in 1994 mainly by Andrew Wiles.
- We need to introduce *elliptic curves* ~~and modular forms~~ to understand the method.

Elliptic Curves

Definition

An *elliptic curve* over a field k with $\mathrm{char}(k) \neq 2, 3$ is given by an equation of the form $y^2 = x^3 + ax + b$ with $a, b \in k$. Its points $E(L)$ over a field L consist of the solutions $(x, y) \in L^2$ and a point at infinity.

Elliptic Curves

Definition

An *elliptic curve* over a field k with $\mathrm{char}(k) \neq 2, 3$ is given by an equation of the form $y^2 = x^3 + ax + b$ with $a, b \in k$. Its points $E(L)$ over a field L consist of the solutions $(x, y) \in L^2$ and a point at infinity.

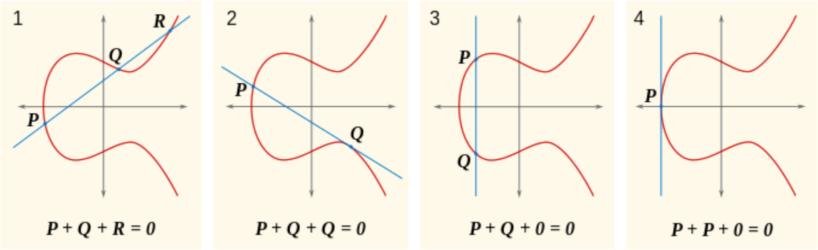
- Define the discriminant $\Delta = -16(4a^3 + 27b^2)$.
- An elliptic curve must be *non-singular*: $\Delta \neq 0$.

Elliptic Curves

Definition

An *elliptic curve* over a field k with $\mathrm{char}(k) \neq 2, 3$ is given by an equation of the form $y^2 = x^3 + ax + b$ with $a, b \in k$. Its points $E(L)$ over a field L consist of the solutions $(x, y) \in L^2$ and a point at infinity.

- Define the discriminant $\Delta = -16(4a^3 + 27b^2)$.
- An elliptic curve must be *non-singular*: $\Delta \neq 0$.
- The points of an elliptic curve form a *group*:



Conductor

- Let E be an elliptic curve over $\mathbb{Q}$ and let p be a prime number.
- Intuitively, by reducing the equation for E modulo p, we obtain the *reduction* of E modulo p. Denote this by $\tilde{E}$.

Conductor

- Let E be an elliptic curve over $\mathbb{Q}$ and let p be a prime number.
- Intuitively, by reducing the equation for E modulo p, we obtain the *reduction* of E modulo p. Denote this by $\tilde{E}$.
- If $p \mid \Delta_{\text{min}}$, then $\tilde{E}$ is singular $\implies$ E has *bad reduction*.
- Two types: *multiplicative reduction* and *additive reduction*.

Conductor

- Let E be an elliptic curve over $\mathbb{Q}$ and let p be a prime number.
- Intuitively, by reducing the equation for E modulo p, we obtain the *reduction* of E modulo p. Denote this by $\tilde{E}$.
- If $p \mid \Delta_{\min}$, then $\tilde{E}$ is singular $\implies$ E has *bad reduction*.
- Two types: *multiplicative reduction* and *additive reduction*.

Definition

We define the *conductor* of E by

$$N = \prod_{p \mid \Delta_{\min}} p^{f_p + \delta_p} \quad \text{where} \quad f_p = \begin{cases} 1 & \text{if } E \text{ has mult. reduction at } p; \\ 2 & \text{if } E \text{ has add. reduction at } p, \end{cases}$$

and where $\delta_p = 0$ for $p \geqslant 5$ and for δ_2, δ_3 use *Tate's algorithm*.

Galois representations

- An elliptic curve over $\mathbb{Q}$ can have *torsion* points; those of finite order. Write $E[n] := E(\overline{\mathbb{Q}})[n]$ for the n-torsion over $\overline{\mathbb{Q}}$.

Galois representations

- An elliptic curve over $\mathbb{Q}$ can have *torsion* points; those of finite order. Write $E[n] := E(\overline{\mathbb{Q}})[n]$ for the n-torsion over $\overline{\mathbb{Q}}$.

Theorem

The $\mathbb{C}$-points of an elliptic curve are given by $E(\mathbb{C}) \cong \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$ for some $\tau \in \mathcal{H}$. In particular, $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$.

Galois representations

- An elliptic curve over $\mathbb{Q}$ can have *torsion* points; those of finite order. Write $E[n] := E(\overline{\mathbb{Q}})[n]$ for the n-torsion over $\overline{\mathbb{Q}}$.

Theorem

The $\mathbb{C}$-points of an elliptic curve are given by $E(\mathbb{C}) \cong \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$ for some $\tau \in \mathcal{H}$. In particular, $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$.

- The group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on the n-torsion points $E[n]$.
- For any prime ℓ, this gives a representation

$$\rho_E^\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(E[\ell]) \cong \mathrm{GL}_2(\mathbb{F}_\ell).$$

Level Lowering

- For any prime p, let $v_p(n)$ denote the number of factors of p in n.

(slightly false) Level Lowering Theorem (Ribet, 1990)

Let $E/\mathbb{Q}$ be an elliptic curve with conductor N and discriminant $\Delta_{\min}$. Let $\ell \geqslant 3$ be a prime number such that ρ_E^ℓ is irreducible. Define

$$N_\ell = N \Big/ \prod_{p \| N,\ \ell | v_p(\Delta_{\min})} p.$$

Then there exists another elliptic curve $F/\mathbb{Q}$ with conductor N_ℓ such that their mod-ℓ representations are isomorphic.

Level Lowering

- For any prime p, let $v_p(n)$ denote the number of factors of p in n.

(slightly false) Level Lowering Theorem (Ribet, 1990)

Let $E/\mathbb{Q}$ be an elliptic curve with conductor N and discriminant $\Delta_{\min}$. Let $\ell \geqslant 3$ be a prime number such that ρ_E^ℓ is irreducible. Define

$$N_\ell = N \Big/ \prod_{p \| N,\ \ell | v_p(\Delta_{\min})} p.$$

Then there exists another elliptic curve $F/\mathbb{Q}$ with conductor N_ℓ such that their mod-ℓ representations are isomorphic.

- **Example:** if $N = 2 \cdot 3 \cdot 5$ and $\Delta = 2^2 \cdot 15^\ell$, then $N_\ell = 2$.
- Now we are ready for Fermat's Last Theorem!

Fermat's Last Theorem

- It suffices to show that $x^\ell + y^\ell + z^\ell = 0$ has no non-trivial solutions for all odd primes $\ell \geqslant 5$.
- Suppose we have a non-trivial solution and consider

$$E\colon Y^2 = X(X - x^\ell)(X + y^\ell).$$

Fermat's Last Theorem

- It suffices to show that $x^\ell + y^\ell + z^\ell = 0$ has no non-trivial solutions for all odd primes $\ell \geqslant 5$.
- Suppose we have a non-trivial solution and consider

$$E\colon Y^2 = X(X - x^\ell)(X + y^\ell).$$

- One may compute that

$$\Delta_{\mathrm{min}} = (xyz)^{2\ell}/2^8 \quad \text{and} \quad N = \mathrm{rad}(xyz),$$

where $\mathrm{rad}(n)$ is the product of all the primes dividing n.

Fermat's Last Theorem

- It suffices to show that $x^\ell + y^\ell + z^\ell = 0$ has no non-trivial solutions for all odd primes $\ell \geqslant 5$.
- Suppose we have a non-trivial solution and consider

$$E\colon Y^2 = X(X - x^\ell)(X + y^\ell).$$

- One may compute that

$$\Delta_{\min} = (xyz)^{2\ell}/2^8 \quad \text{and} \quad N = \operatorname{rad}(xyz),$$

  where $\operatorname{rad}(n)$ is the product of all the primes dividing n.
- Level lowering: $N_\ell = 2$, so E corresponds to a rational elliptic curve of conductor 2.

Fermat's Last Theorem

- It suffices to show that $x^\ell + y^\ell + z^\ell = 0$ has no non-trivial solutions for all odd primes $\ell \geqslant 5$.
- Suppose we have a non-trivial solution and consider

$$E\colon Y^2 = X(X - x^\ell)(X + y^\ell).$$

- One may compute that

$$\Delta_{\min} = (xyz)^{2\ell}/2^8 \quad \text{and} \quad N = \mathrm{rad}(xyz),$$

  where $\mathrm{rad}(n)$ is the product of all the primes dividing n.
- Level lowering: $N_\ell = 2$, so E corresponds to a rational elliptic curve of conductor 2.
- **Lemma:** There exist no elliptic curves with conductor 2. $\square$

The symplectic method

- **Problem:** often elliptic curves after level lowering *do* still exist.
- **Idea:** still derive a contradiction based on the information that their mod-ℓ representations are supposed to be isomorphic.

The symplectic method

- **Problem:** often elliptic curves after level lowering *do* still exist.
- **Idea:** still derive a contradiction based on the information that their mod-ℓ representations are supposed to be isomorphic.
- **The symplectic method:** we have an isomorphism $E[\ell] \to F[\ell]$. What do we know about its determinant?
- **First:** we need canonical bases.

Symplectic types

- For some $\tau \in \mathcal{H}$, the $\mathbb{C}$-points of an elliptic curve are given by

$$E(\mathbb{C}) \cong \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z}).$$

Symplectic types

- For some $\tau \in \mathcal{H}$, the $\mathbb{C}$-points of an elliptic curve are given by

$$E(\mathbb{C}) \cong \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z}).$$

- Let $\varphi : E[\ell] \to F[\ell]$ be a morphism and γ the matrix sending

$$\gamma : \{1/\ell, \tau_F/\ell\} \mapsto \{\varphi(1/\ell), \varphi(\tau_E/\ell)\}.$$

- Define $r(\varphi) = \det(\gamma)$.

Symplectic types

- For some $\tau \in \mathcal{H}$, the $\mathbb{C}$-points of an elliptic curve are given by

$$E(\mathbb{C}) \cong \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z}).$$

- Let $\varphi : E[\ell] \to F[\ell]$ be a morphism and γ the matrix sending

$$\gamma : \{1/\ell, \tau_F/\ell\} \mapsto \{\varphi(1/\ell), \varphi(\tau_E/\ell)\}.$$

- Define $r(\varphi) = \det(\gamma)$. This is well-defined, because any two bases for a lattice $\cong \mathbb{Z}^2$ differ by an element in $\mathrm{GL}_2(\mathbb{Z})$.
- By insisting on $\tau \in \mathcal{H}$, we force $\det = 1$.

Symplectic types

- For some $\tau \in \mathcal{H}$, the $\mathbb{C}$-points of an elliptic curve are given by

$$E(\mathbb{C}) \cong \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z}).$$

- Let $\varphi : E[\ell] \to F[\ell]$ be a morphism and γ the matrix sending

$$\gamma : \{1/\ell, \tau_F/\ell\} \mapsto \{\varphi(1/\ell), \varphi(\tau_E/\ell)\}.$$

- Define $r(\varphi) = \det(\gamma)$. This is well-defined, because any two bases for a lattice $\cong \mathbb{Z}^2$ differ by an element in $\mathrm{GL}_2(\mathbb{Z})$.
- By insisting on $\tau \in \mathcal{H}$, we force $\det = 1$.
- Clearly, for any scalar $a \in \mathbb{F}_\ell$, we have $r(a \cdot \varphi) = a^2 r(\varphi)$.

Definition

We say φ is *symplectic* if $r(\varphi)$ is a square modulo ℓ.
If not, we say it is *anti-symplectic*.

A symplectic theorem

Proposition (Kraus, Oesterlé, 1992)

Let $E/\mathbb{Q}$ and $F/\mathbb{Q}$ be elliptic curves such that $E[\ell] \cong F[\ell]$ for some ℓ. Let $p \neq \ell$ be a prime such that both E and F have mult. reduction at p, and such that neither $v_p(\Delta_{\min}(E))$ nor $v_p(\Delta_{\min}(F))$ is divisible by ℓ.

Then $E[\ell]$ and $F[\ell]$ are symplectically isomorphic if and only if $v_p(\Delta_{\min}(E)) \,/\, v_p(\Delta_{\min}(F))$ is a square modulo ℓ.

A symplectic theorem

Proposition (Kraus, Oesterlé, 1992)

Let $E/\mathbb{Q}$ and $F/\mathbb{Q}$ be elliptic curves such that $E[\ell] \cong F[\ell]$ for some ℓ. Let $p \neq \ell$ be a prime such that both E and F have mult. reduction at p, and such that neither $\nu_p(\Delta_{\min}(E))$ nor $\nu_p(\Delta_{\min}(F))$ is divisible by ℓ.

Then $E[\ell]$ and $F[\ell]$ are symplectically isomorphic if and only if $\nu_p(\Delta_{\min}(E)) \,/\, \nu_p(\Delta_{\min}(F))$ is a square modulo ℓ.

If E and F have mult. reduction at two primes p and q, then

$$\frac{\nu_p(\Delta_{\min}(E))\nu_q(\Delta_{\min}(E))}{\nu_p(\Delta_{\min}(F))\nu_q(\Delta_{\min}(F))}$$

must always be a square modulo ℓ.

An example

Theorem

Let $\ell \geqslant 5$ be a prime such that $12 \nmid \ell - 1$. Then any integers (x, y, z) satisfying

$$x^\ell + 3y^\ell + 5z^\ell = 0$$

for which y is even, must satisfy $x = y = z = 0$.

- Given a non-trivial solution, consider

$$E\colon Y^2 = X(X - x^\ell)(X + 3y^\ell) \text{ with } \Delta_{\min}(E) = (15)^2(xyz)^{2\ell}/2^8.$$

An example

Theorem

Let $\ell \geqslant 5$ be a prime such that $12 \nmid \ell - 1$. Then any integers (x, y, z) satisfying

$$x^\ell + 3y^\ell + 5z^\ell = 0$$

for which y is even, must satisfy $x = y = z = 0$.

- Given a non-trivial solution, consider

$$E\colon Y^2 = X(X - x^\ell)(X + 3y^\ell) \quad \text{with} \quad \Delta_{\min}(E) = (15)^2 (xyz)^{2\ell} / 2^8.$$

- Level lowering result: we find $N_\ell = 30$, with

$$F\colon Y^2 + XY + Y = X^3 + X + 2 \quad \text{with} \quad \Delta(F) = -2160 = -2^4 \cdot 3^3 \cdot 5.$$

An example

Theorem

Let $\ell \geqslant 5$ be a prime such that $12 \nmid \ell - 1$. Then any integers (x, y, z) satisfying

$$x^\ell + 3y^\ell + 5z^\ell = 0$$

for which y is even, must satisfy $x = y = z = 0$.

- Given a non-trivial solution, consider

$$\mathsf{E}\colon \mathsf{Y}^2 = \mathsf{X}(\mathsf{X} - x^\ell)(\mathsf{X} + 3y^\ell) \;\text{ with }\; \Delta_{\text{min}}(\mathsf{E}) = (15)^2(xyz)^{2\ell}/2^8.$$

- Level lowering result: we find $N_\ell = 30$, with

$$\mathsf{F}\colon \mathsf{Y}^2 + \mathsf{XY} + \mathsf{Y} = \mathsf{X}^3 + \mathsf{X} + 2 \;\text{ with }\; \Delta(\mathsf{F}) = -2160 = -2^4 \cdot 3^3 \cdot 5.$$

- Both E and F have multiplicative reduction at the primes 2, 3 and 5.

An example

Theorem

Let $\ell \geqslant 5$ be a prime such that $12 \nmid \ell - 1$. Then any integers (x, y, z) satisfying

$$x^{\ell} + 3y^{\ell} + 5z^{\ell} = 0$$

for which y is even, must satisfy $x = y = z = 0$.

- Then all of

$$\frac{-8 \cdot 2}{4 \cdot 3}, \quad \frac{-8 \cdot 2}{4 \cdot 1} \quad \text{and} \quad \frac{2 \cdot 2}{3 \cdot 1}$$

must be squares modulo ℓ.

An example

Theorem

Let $\ell \geqslant 5$ be a prime such that $12 \nmid \ell - 1$. Then any integers (x, y, z) satisfying

$$x^\ell + 3y^\ell + 5z^\ell = 0$$

for which y is even, must satisfy $x = y = z = 0$.

- Then all of

$$\frac{-8 \cdot 2}{4 \cdot 3}, \quad \frac{-8 \cdot 2}{4 \cdot 1} \quad \text{and} \quad \frac{2 \cdot 2}{3 \cdot 1}$$

  must be squares modulo ℓ.
- Hence -1 and 3 must be squares, so $\ell \equiv 1 \pmod{12}$. $\square$

Example of a theorem (D., 2020)

Let $k, \alpha \geqslant 0$ be integers and $\ell \geqslant 5$ a prime. Then the equation

$$x^\ell + 2^\alpha y^\ell + 3^k z^\ell = 0$$

has no nontrivial solutions if

- $\alpha = 0$ or $\alpha > 3$.
- $k = 0$ and $\alpha \neq 1$, where the exceptional case only has the non-trivial solutions $(\pm n, \mp n, \pm n)$.
- $\alpha \in \{1, 2, 3\}$ and y is even.
- $\alpha \in \{1, 2\}$ and ℓ is such that k is not a square modulo ℓ.
- $\alpha = 3$ and ℓ is such that $2k$ is not a square modulo ℓ.