The symplectic type of congruences between elliptic curves

John Cremona

University of Warwick

—

joint work with Nuno Freitas (Warwick)

AGC^{2}T Luminy, 10 June 2019

EPSRC
Engineering and Physical Sciences
Research Council

WARWICK
THE UNIVERSITY OF WARWICK

Overview

1. Elliptic curves, mod p Galois representations, Weil pairing.
2. Congruences between curves, symplectic types. The isogeny criterion.
3. The Frey–Mazur Conjecture over $\mathbb{Q}$.
4. Finding all congruences in the LMFDB database.
5. Determining the symplectic type using modular curves.
6. Congruences between twists.

Elliptic Curves

In this talk we consider elliptic curves over a number field K, for example $K = \mathbb{Q}$.
If we need explicit equations we'll use short Weierstrass models

$$E_{a,b}: \quad Y^2 = X^3 + aX + b$$

with $a, b \in K$ such that $4a^3 + 27b^2 \neq 0$.

Elliptic Curves

In this talk we consider elliptic curves over a number field K, for example $K = \mathbb{Q}$.
If we need explicit equations we'll use short Weierstrass models

$$E_{a,b} : \quad Y^2 = X^3 + aX + b$$

with $a, b \in K$ such that $4a^3 + 27b^2 \neq 0$.
The set of K-rational points $E(K)$ forms an abelian group.
For $m \geq 2$ we denote by $E[m]$ the *m-torsion subgroup*:

$$E[m] = \{P \in E(\overline{K}) \mid mP = 0\}.$$

Elliptic Curves

In this talk we consider elliptic curves over a number field K, for example $K = \mathbb{Q}$.
If we need explicit equations we'll use short Weierstrass models

$$E_{a,b} : \quad Y^2 = X^3 + aX + b$$

with $a, b \in K$ such that $4a^3 + 27b^2 \neq 0$.
The set of K-rational points $E(K)$ forms an abelian group.
For $m \geq 2$ we denote by $E[m]$ the *m-torsion subgroup*:

$$E[m] = \{P \in E(\overline{K}) \mid mP = 0\}.$$

We have $E[m] \cong (\mathbb{Z}/mZ)^2$ as abelian groups.

But $E[m]$ carries additional structure. . . .

Mod p Galois representations

Let $G_K = \mathrm{Gal}(\overline{K}/K)$, the *absolute Galois group* of K. This acts on $E(\overline{K})$ by acting on coordinates:

$$P = (x, y) \in E(\overline{K}), \quad \sigma \in G_K : \qquad \sigma(P) = (\sigma(x), \sigma(y)) \in E(\overline{K}).$$

Mod p Galois representations

Let $G_K = \mathrm{Gal}(\overline{K}/K)$, the *absolute Galois group* of K. This acts on $E(\overline{K})$ by acting on coordinates:

$$P = (x, y) \in E(\overline{K}), \quad \sigma \in G_K : \qquad \sigma(P) = (\sigma(x), \sigma(y)) \in E(\overline{K}).$$

The Galois action preserves the group structure:

$$\sigma(P + Q) = \sigma(P) + \sigma(Q).$$

Hence each $E[m]$ is a *G_K-module*.

Mod p Galois representations

Let $G_K = \mathrm{Gal}(\overline{K}/K)$, the *absolute Galois group* of K. This acts on $E(\overline{K})$ by acting on coordinates:

$$P = (x, y) \in E(\overline{K}), \quad \sigma \in G_K : \qquad \sigma(P) = (\sigma(x), \sigma(y)) \in E(\overline{K}).$$

The Galois action preserves the group structure:

$$\sigma(P + Q) = \sigma(P) + \sigma(Q).$$

Hence each $E[m]$ is a *G_K-module*.

Taking $m = p$ prime, $E[p]$ is a 2-dimensional vector space over $\mathbb{F}_p$. Fixing a basis of $E[p]$ we obtain the *mod p Galois representation*

$$\overline{\rho}_{E,p} : G_K \to \mathrm{GL}_2(\mathbb{F}_p).$$

The Weil pairing

As well as being a vector space, $E[p]$ admits a *symplectic structure*: there is a non-degenerate alternating bilinear pairing, the *Weil pairing*

$$e_p = e_{E,p} : \quad E[p] \times E[p] \to \mu_p$$

where μ_p denotes the group of pth roots of unity in $\overline{\mathbb{Q}}^*$.

The Weil pairing

As well as being a vector space, $E[p]$ admits a *symplectic structure*: there is a non-degenerate alternating bilinear pairing, the *Weil pairing*

$$e_p = e_{E,p} : \quad E[p] \times E[p] \to \mu_p$$

where μ_p denotes the group of pth roots of unity in $\overline{\mathbb{Q}}^*$.

The Weil pairing is *Galois equivariant*:

$$e_p(\sigma(P), \sigma(Q)) = \sigma(e_p(P, Q)) = e_p(P, Q)^{\chi_p(\sigma)}$$

where $\chi_p : G_K \to \mathbb{F}_p^*$ is the cyclotomic character.

The Weil pairing

As well as being a vector space, $E[p]$ admits a *symplectic structure*: there is a non-degenerate alternating bilinear pairing, the *Weil pairing*

$$e_p = e_{E,p} : \quad E[p] \times E[p] \to \mu_p$$

where μ_p denotes the group of pth roots of unity in $\overline{\mathbb{Q}}^*$.

The Weil pairing is *Galois equivariant*:

$$e_p(\sigma(P), \sigma(Q)) = \sigma(e_p(P, Q)) = e_p(P, Q)^{\chi_p(\sigma)}$$

where $\chi_p : G_K \to \mathbb{F}_p^*$ is the cyclotomic character.

This Galois-equivariant symplectic structure on $E[p]$ is what we are interested in.

Congruences and their symplectic types

We are interested in the situation where two *different* curves have *isomorphic* p-torsion modules.

Congruences and their symplectic types

We are interested in the situation where two *different* curves have *isomorphic* p-torsion modules.

E_1 and E_2 are said to satisfy a *mod p congruence* if there is a bijective map

$$\phi : \quad E_1[p] \to E_2[p]$$

which is both $\mathbb{F}_p$-linear and G_K-equivariant, *i.e.*, is an isomorphism of G_K-modules.

Congruences and their symplectic types

We are interested in the situation where two *different* curves have *isomorphic* p-torsion modules.

E_1 and E_2 are said to satisfy a *mod p congruence* if there is a bijective map

$$\phi : \quad E_1[p] \to E_2[p]$$

which is both $\mathbb{F}_p$-linear and G_K-equivariant, *i.e.*, is an isomorphism of G_K-modules.

To each such ϕ there is a constant $d_\phi \in \mathbb{F}_p^*$ such that

$$e_{E_2,p}(\phi(P), \phi(Q)) = e_{E_1,p}(P, Q)^{d_\phi}.$$

We say that ϕ is *symplectic* if d_ϕ is a *square* mod p and *anti-symplectic* otherwise.

Isogenies

Isogenies between curves provide one source of congruences.

Isogenies

Isogenies between curves provide one source of congruences.

Let $\phi : E_1 \to E_2$ be an isogeny$/K$ of degree $\deg(\phi)$ *coprime to p*, defined over K. Then ϕ induces an $\mathbb{F}_p G_K$-isomorphism $E_1[p] \to E_2[p]$. The *isogeny criterion* says that ϕ is symplectic if and only if the Legendre symbol $(\deg(\phi)/p) = +1$.

Isogenies

Isogenies between curves provide one source of congruences.

Let $\phi : E_1 \to E_2$ be an isogeny$/K$ of degree $\deg(\phi)$ *coprime to p*, defined over K. Then ϕ induces an $\mathbb{F}_p G_K$-isomorphism $E_1[p] \to E_2[p]$. The *isogeny criterion* says that ϕ is symplectic if and only if the Legendre symbol $(\deg(\phi)/p) = +1$.

Proof.

Using Weil reciprocity, for $P, Q \in E_1[p]$,

$$\begin{aligned} e_{E_2,p}(\phi(P), \phi(Q)) &= e_{E_1,p}(P, \hat{\phi}\phi(Q)) \\ &= e_{E_1,p}(P, \deg(\phi)(Q)) \\ &= e_{E_1,p}(P, Q)^{\deg(\phi)}, \end{aligned}$$

where $\hat{\phi}$ denotes the dual isogeny, since $\hat{\phi}\phi = \deg(\phi)$. □

Isogenies

Isogenies between curves provide one source of congruences.

Let $\phi : E_1 \to E_2$ be an isogeny$/K$ of degree $\deg(\phi)$ *coprime to p*, defined over K. Then ϕ induces an $\mathbb{F}_p G_K$-isomorphism $E_1[p] \to E_2[p]$. The *isogeny criterion* says that ϕ is symplectic if and only if the Legendre symbol $(\deg(\phi)/p) = +1$.

Proof.

Using Weil reciprocity, for $P, Q \in E_1[p]$,

$$\begin{aligned} e_{E_2,p}(\phi(P), \phi(Q)) &= e_{E_1,p}(P, \hat{\phi}\phi(Q)) \\ &= e_{E_1,p}(P, \deg(\phi)(Q)) \\ &= e_{E_1,p}(P, Q)^{\deg(\phi)}, \end{aligned}$$

where $\hat{\phi}$ denotes the dual isogeny, since $\hat{\phi}\phi = \deg(\phi)$. □

Do any other mod p congruences exist?

The Frey-Mazur conjecture

The *Uniform Frey–Mazur conjecture* (over $\mathbb{Q}$) states:

> *There is a constant $C = C_{\mathbb{Q}}$ such that, if $E_1/\mathbb{Q}$ and $E_2/\mathbb{Q}$ satisfy $E_1[p] \simeq E_2[p]$ as $G_{\mathbb{Q}}$-modules for some prime $p > C$, then E_1 and E_2 are $\mathbb{Q}$-isogenous.*

The Frey-Mazur conjecture

The *Uniform Frey–Mazur conjecture* (over $\mathbb{Q}$) states:

> *There is a constant $C = C_{\mathbb{Q}}$ such that, if $E_1/\mathbb{Q}$ and $E_2/\mathbb{Q}$ satisfy $E_1[p] \simeq E_2[p]$ as $G_{\mathbb{Q}}$-modules for some prime $p > C$, then E_1 and E_2 are $\mathbb{Q}$-isogenous.*

Theorem (C. & Freitas)

If $E_1/\mathbb{Q}$ and $E_2/\mathbb{Q}$ both have conductor $\leq 400\,000$ are not isogenous, and satisfy $E_1[p] \simeq E_2[p]$ as $G_{\mathbb{Q}}$-modules for some prime p, then $p \leq 17$.

The Frey-Mazur conjecture

The *Uniform Frey–Mazur conjecture* (over $\mathbb{Q}$) states:

> *There is a constant $C = C_{\mathbb{Q}}$ such that, if $E_1/\mathbb{Q}$ and $E_2/\mathbb{Q}$ satisfy $E_1[p] \simeq E_2[p]$ as $G_{\mathbb{Q}}$-modules for some prime $p > C$, then E_1 and E_2 are $\mathbb{Q}$-isogenous.*

Theorem (C. & Freitas)

If $E_1/\mathbb{Q}$ and $E_2/\mathbb{Q}$ both have conductor $\leq 400\,000$ are not isogenous, and satisfy $E_1[p] \simeq E_2[p]$ as $G_{\mathbb{Q}}$-modules for some prime p, then $p \leq 17$.

- A stronger version of the Frey–Mazur conjecture states that it is holds with $C = 23$.
- Congruences for small p are common; for $p = 17$ there is essentially only one known, between 47775be1 and 3675b1.

Finding congruences in the LMFDB database

The LMFDB database contains all elliptic curves defined over $\mathbb{Q}$ of conductor up to $400\,000$: that is $2\,483\,649$ curves in $1\,741\,002$ isogeny classes.

What congruences are there between (non-isogenous) curves, and how do we find them?

Two representations have isomorphic semisimplifications if and only if they have the same traces. We can test this condition by testing whether

$$a_\ell(E_1) \equiv a_\ell(E_2) \pmod{p} \quad \text{for all primes } \ell \nmid pN_1N_2,$$

where N_1 and N_2 are the conductors of E_1 and E_2.

But there are infinitely many primes ℓ. And for each curve we need to ignore a different bad set!

Sieving

To get around these issues we use a *sieve* with a hash function, and only test $\ell > 400\,000$.

Let $\mathcal{L}_B = \{\ell_0, \ldots, \ell_{B-1}\}$ be the set of the B smallest primes greater than $400\,000$. For each p we define the hash of E to be

$$\sum_{i=0}^{B-1} \overline{a}_{\ell_i}(E) p^i \in \mathbb{Z}.$$

Any two p-congruent curves (up to semisimplification) have the same hash value. If B is not too small then we will get few (if any) “false positive” clashes.

We can also parallelise this with respect to p, so that we only need to compute each $a_\ell(E)$ once. Against each hash value, we store lists of curves which have that p-hash (processing the curves one at a time, one from each isogeny class). At the end we extract the lists of size at least 2, to give us sets of curves which are likely to all be p-congruent.

Sieving in practice

This works well in practice with $B = 40$. Not quite with $B = 35$!

Sieving in practice

This works well in practice with $B = 40$. Not quite with $B = 35$!

The curves with labels 25921a1 and 78400gw1 have traces a_ℓ which are *equal for all* $\ell \in \mathcal{L}_{35}$, that is, for all ℓ with $400000 \leq \ell < 400457$ (though not for the 36th $\ell = 400457$).

Sieving in practice

This works well in practice with $B = 40$. Not quite with $B = 35$!

The curves with labels $25921a1$ and $78400gw1$ have traces a_ℓ which are *equal for all* $\ell \in \mathcal{L}_{35}$, that is, for all ℓ with $400000 \leq \ell < 400457$ (though not for the 36th $\ell = 400457$).

Note on reducibility: here we are testing for p-congruence only up to semisimplification. For curves with $E[p]$ reducible (*i.e.*, which have a rational p-isogeny) this is a weaker condition than p-congruence, and we need to carry out further tests.

Sieving in practice

This works well in practice with $B = 40$. Not quite with $B = 35$!

The curves with labels 25921a1 and 78400gw1 have traces a_ℓ which are *equal for all* $\ell \in \mathcal{L}_{35}$, that is, for all ℓ with $400000 \le \ell < 400457$ (though not for the 36th $\ell = 400457$).

Note on reducibility: here we are testing for p-congruence only up to semisimplification. For curves with $E[p]$ reducible (*i.e.*, which have a rational p-isogeny) this is a weaker condition than p-congruence, and we need to carry out further tests.

We also need to test whether curves which appear to be p-congruent after sieving actually are. With $B = 40$ this is always the case.

Sieving results

For $5 \leq p \leq 97$ we find the following number of sets of more than one mutually p-congruent curves (up to semisimplification, ignoring isogenies):

p	#sets	# irred.	max.irred.	# red.	max. red.
5	102043	101717	18	326	430
7	20138	19883	5	255	76
11	635	635	2	0	-
13	150	150	2	0	-
17	8	8	2	0	-
19$\leq p \leq$ 97	0	0	-	0	-

After eliminating reducibles which are not isomorphic, for $p = 7$ we find 337 non-trivial sets, of size up to 4.

Distinguishing symplectic from anti-symplectic

Freitas and Kraus have a long paper (to appear) which gives many different *local criteria* for determining whether a congruence $E_1[p] \cong E_2[p]$ is symplectic or anti-symplectic. These criteria are not guaranteed to apply in all cases, but usually do, and are usually fast. They depend on knowing in advance that a congruence does hold.

Distinguishing symplectic from anti-symplectic

Freitas and Kraus have a long paper (to appear) which gives many different *local criteria* for determining whether a congruence $E_1[p] \cong E_2[p]$ is symplectic or anti-symplectic. These criteria are not guaranteed to apply in all cases, but usually do, and are usually fast. They depend on knowing in advance that a congruence does hold.

There are several tests involving the structure of $E[p]$ at primes of bad reduction; these are all fast. Then there are two tests involving primes of good reduction, one of which is slow.

Distinguishing symplectic from anti-symplectic

Freitas and Kraus have a long paper (to appear) which gives many different *local criteria* for determining whether a congruence $E_1[p] \cong E_2[p]$ is symplectic or anti-symplectic. These criteria are not guaranteed to apply in all cases, but usually do, and are usually fast. They depend on knowing in advance that a congruence does hold.

There are several tests involving the structure of $E[p]$ at primes of bad reduction; these are all fast. Then there are two tests involving primes of good reduction, one of which is slow.

This test suite has now been implemented, and the tests are powerful enough to handle *all* the congruences in the database.

Distinguishing symplectic from anti-symplectic

Freitas and Kraus have a long paper (to appear) which gives many different *local criteria* for determining whether a congruence $E_1[p] \cong E_2[p]$ is symplectic or anti-symplectic. These criteria are not guaranteed to apply in all cases, but usually do, and are usually fast. They depend on knowing in advance that a congruence does hold.

There are several tests involving the structure of $E[p]$ at primes of bad reduction; these are all fast. Then there are two tests involving primes of good reduction, one of which is slow.

This test suite has now been implemented, and the tests are powerful enough to handle *all* the congruences in the database. There are congruences (outside the database) for which none of the local criteria apply; we developed some new global methods to handle these.

Using modular curves

For $p = 7$ we use a method based on *modular curves* to establish congruences and their symplectic type.

Using modular curves

For $p = 7$ we use a method based on *modular curves* to establish congruences and their symplectic type.

For each prime p there is a modular curve $X(p)$ defined over $\mathbb{Q}$ which parametrises elliptic curves together with a level p structure (essentially, a marked basis for $E[p]$).

Using modular curves

For $p = 7$ we use a method based on *modular curves* to establish congruences and their symplectic type.

For each prime p there is a modular curve $X(p)$ defined over $\mathbb{Q}$ which parametrises elliptic curves together with a level p structure (essentially, a marked basis for $E[p]$).

For $p \leq 5$, this curve has genus 0, and p-congruences are very common.

$X(7)$ has genus 3, and the Klein quartic is one model for it.

$X(11)$ has genus 26.

Using modular curves

For $p = 7$ we use a method based on *modular curves* to establish congruences and their symplectic type.
For each prime p there is a modular curve $X(p)$ defined over $\mathbb{Q}$ which parametrises elliptic curves together with a level p structure (essentially, a marked basis for $E[p]$).
For $p \leq 5$, this curve has genus 0, and p-congruences are very common.
$X(7)$ has genus 3, and the Klein quartic is one model for it.
$X(11)$ has genus 26.

Fix one elliptic curve E over $\mathbb{Q}$. Then there exists a curve $X_E^+(p)$ (or simply $X_E(p)$), which is a twist of $X(p)$, whose (non-cuspidal) points correspond to curves E' with $E[p] \cong E'[p]$ symplectically. (Strictly, to pairs (E', α) where $\alpha : E[p] \to E'[p]$ is a symplectic isomorphism, up to scaling.)

The modular curves $X_E^{\pm}(p)$

As well as $X_E^{+}(p)$, there is another twist $X_E^{-}(p)$ parametrizing curves E' which are anti-symplectically isomorphic to E.

The modular curves $X_E^{\pm}(p)$

As well as $X_E^+(p)$, there is another twist $X_E^-(p)$ parametrizing curves E' which are anti-symplectically isomorphic to E.

An explicit model for $X_E^+(7)$ was found by Kraus and Halberstadt (2003) together with the degree 168 map $j : X_E^+(7) \to X(1) = \mathbb{P}^1$ (giving the j-invariant of the congruent curve E'), and incomplete formulas for the coefficients of E'. A model for $X_E^-(7)$ was given by Poonen and Stoll.

The modular curves $X_E^{\pm}(p)$

As well as $X_E^+(p)$, there is another twist $X_E^-(p)$ parametrizing curves E' which are anti-symplectically isomorphic to E.

An explicit model for $X_E^+(7)$ was found by Kraus and Halberstadt (2003) together with the degree 168 map $j : X_E^+(7) \to X(1) = \mathbb{P}^1$ (giving the j-invariant of the congruent curve E'), and incomplete formulas for the coefficients of E'. A model for $X_E^-(7)$ was given by Poonen and Stoll.

More complete formulas were provided by Fisher (2014), who also gave all the formulas for $X_E^-(7)$ parametrizing anti-symplectic congruences, and $X_E^{\pm}(11)$ (which has genus 26).

The modular curves $X_E^{\pm}(p)$

As well as $X_E^{+}(p)$, there is another twist $X_E^{-}(p)$ parametrizing curves E' which are anti-symplectically isomorphic to E.

An explicit model for $X_E^{+}(7)$ was found by Kraus and Halberstadt (2003) together with the degree 168 map $j : X_E^{+}(7) \to X(1) = \mathbb{P}^1$ (giving the j-invariant of the congruent curve E'), and incomplete formulas for the coefficients of E'. A model for $X_E^{-}(7)$ was given by Poonen and Stoll.

More complete formulas were provided by Fisher (2014), who also gave all the formulas for $X_E^{-}(7)$ parametrizing anti-symplectic congruences, and $X_E^{\pm}(11)$ (which has genus 26).

For $p = 7$ we implemented these formulas and apply them as follows.

Using $X_E^{\pm}(7)$: the algorithm

1. Given two elliptic curves E, E' defined over a field K of characteristic 0. We do not need to assume anything about them. Compute $j(E')$, and the curves $X_E^{\pm}(7)$.
2. Use the explicit map $j : X_E^{+}(7) \to \mathbb{P}^1$ to find the preimages (if any) of $j(E')$ in $X_E^{+}(7)(K)$. If none then E, E' are not symplectically p-congruent over K.
3. For any $P \in X_E^{+}(7)(K)$ use Fisher's formulas to find a model for the associated congruent curve E''.
4. If $E' \cong E''$ for any of these, then E, E' are symplectically p-congruent over K, otherwise not.
5. repeat steps 3–5 with $X_E^{-}(7)$.

Using $X_E^{\pm}(7)$: the algorithm

1. Given two elliptic curves E, E' defined over a field K of characteristic 0. We do not need to assume anything about them. Compute $j(E')$, and the curves $X_E^{\pm}(7)$.
2. Use the explicit map $j : X_E^{+}(7) \to \mathbb{P}^1$ to find the preimages (if any) of $j(E')$ in $X_E^{+}(7)(K)$. If none then E, E' are not symplectically p-congruent over K.
3. For any $P \in X_E^{+}(7)(K)$ use Fisher's formulas to find a model for the associated congruent curve E''.
4. If $E' \cong E''$ for any of these, then E, E' are symplectically p-congruent over K, otherwise not.
5. repeat steps 3–5 with $X_E^{-}(7)$.

It would be possible to implement a similar algorithm for $p = 11$ using Fisher's formulas.

Using $X_E^{\pm}(7)$: results

Of the $19\,883$ non-trivial sets of isogeny classes with mutually isomorphic irreducible mod 7 representations, we find that in $12\,394$ cases all the isomorphisms are symplectic, while in the remaining $7\,489$ cases anti-symplectic isomorphisms occur.

Using $X_E^{\pm}(7)$: results

Of the $19\,883$ non-trivial sets of isogeny classes with mutually isomorphic irreducible mod 7 representations, we find that in $12\,394$ cases all the isomorphisms are symplectic, while in the remaining $7\,489$ cases anti-symplectic isomorphisms occur.

We successfully checked that in all these cases, the results of applying the local criteria are consistent. At the same time we found that for all pairs of 7-congruent curves in the database, at least one of the local criteria are able to decide whether the congruence was symplectic or not.

Results for $p > 7$

For $p \geq 11$ we used the local criteria only to test congruences. It would be possible to implement Fisher's formulas for $X_E^{\pm}(11)$, but we have not yet done so.

For $11 \leq p \leq 17$ we only find congruences with $E[p]$ irreducible and we never find sets of more than two congruent curves (excluding isogenies).

p	# congruent pairs	# symplectic	# anti-symplectic
11	635	446	189
13	150	88	62
17	8	0	8

The Frey–Mazur conjecture

For $17 < p < 100$ we found no congruences in the database.

We also *proved* that there are no congruences (in the database) for $p > 100$.

This would be possible, though time-consuming, by considering all pairs of curves (one from each isogeny class). Instead:

The Frey–Mazur conjecture

For $17 < p < 100$ we found no congruences in the database.
We also *proved* that there are no congruences (in the database) for $p > 100$.
This would be possible, though time-consuming, by considering all pairs of curves (one from each isogeny class). Instead:

First: compare non-isogenous curves of the same conductor, by computing $\gcd_{\ell \le B, \ell \nmid N}(a_\ell(E_1) - a_\ell(E_2))$ for increasing B.

The Frey–Mazur conjecture

For $17 < p < 100$ we found no congruences in the database.
We also *proved* that there are no congruences (in the database) for $p > 100$.
This would be possible, though time-consuming, by considering all pairs of curves (one from each isogeny class). Instead:

First: compare non-isogenous curves of the same conductor, by computing $\gcd_{\ell \leq B, \ell \nmid N}(a_\ell(E_1) - a_\ell(E_2))$ for increasing B.

Lemma

If E_1 and E_2 have different conductors N_1 and N_2 and are p-congruent for some $p \geq 5$, then for $i = 1$ or $i = 2$ there exists a prime $q \mid\mid N_i$ such that $p \mid \operatorname{ord}_q(\Delta_i)$, where Δ_i is the minimal discriminant of E_i.

Lemma

If $N_E \leq 400000$ and $q \mid\mid N_E$ and $p \mid \operatorname{ord}_q(\Delta_E)$ then $p \leq 97$.

Twists

As well as computational results, we also have some results of a more theoretical nature. Many of these involve *twists*.

Twists

As well as computational results, we also have some results of a more theoretical nature. Many of these involve *twists*.

First, it is easy to show that when we have a congruence $E_1[p] \cong E_2[p]$ then for any quadratic twist (associated to a quadratic extension $K(\sqrt{d})/K$), the twisted curves also satisfy a p-congruence: $E_1^d[p] \cong E_2^d[p]$. Moreover the symplectic type is preserved.

Twists

As well as computational results, we also have some results of a more theoretical nature. Many of these involve *twists*.

First, it is easy to show that when we have a congruence $E_1[p] \cong E_2[p]$ then for any quadratic twist (associated to a quadratic extension $K(\sqrt{d})/K$), the twisted curves also satisfy a p-congruence: $E_1^d[p] \cong E_2^d[p]$. Moreover the symplectic type is preserved.

So the previous tables could have only shown the number of congruences “up to twist”. (But twisting changes the conductor in general.) However, we can count the total number of curves, up to twist, appearing in any of the congruences we found.

Congruences up to twist

For $p = 7$ there are $10\,348$ distinct j-invariants of curves with irreducible mod 7 representations which are congruent to at least one non-isogenous curve, and 358 distinct j-invariants in the reducible case.

Congruences up to twist

For $p = 7$ there are $10\,348$ distinct j-invariants of curves with irreducible mod 7 representations which are congruent to at least one non-isogenous curve, and 358 distinct j-invariants in the reducible case. (There are $1\,012\,376$ different j in all.)

Congruences up to twist

For $p = 7$ there are $10\,348$ distinct j-invariants of curves with irreducible mod 7 representations which are congruent to at least one non-isogenous curve, and 358 distinct j-invariants in the reducible case. (There are $1\,012\,376$ different j in all.)

For $p = 11$ there are 191 distinct j-invariants.
For $p = 13$ there are 39.
For $p = 17$ there are just 2:

Congruences up to twist

For $p = 7$ there are $10\,348$ distinct j-invariants of curves with irreducible mod 7 representations which are congruent to at least one non-isogenous curve, and 358 distinct j-invariants in the reducible case. (There are $1\,012\,376$ different j in all.)

For $p = 11$ there are 191 distinct j-invariants.
For $p = 13$ there are 39.
For $p = 17$ there are just 2: all eight 17-congruent isogeny classes consist of single curves, the eight pairs are quadratic twists, and the j-invariants of the curves in each pair are $48412981936758748562855/7785374327443204139 7$ and $-46585/243$. One such pair of 17-congruent curves consists of 47775b1 and 3675b1.

Congruences between twists I

With some mild conditions to exclude very small images we have a correspondence between the following situations, for odd p over any number field K:

- the projective image in $\mathrm{PGL}_2(\mathbb{F}_p)$ being dihedral;
- the image being contained in the normaliser N of a Cartan subgroup C, but not contained in C;
- a p-congruence between quadratic twists: $E[p] \cong E^d[p]$.

Congruences between twists I

With some mild conditions to exclude very small images we have a correspondence between the following situations, for odd p over any number field K:

- the projective image in $\mathrm{PGL}_2(\mathbb{F}_p)$ being dihedral;
- the image being contained in the normaliser N of a Cartan subgroup C, but not contained in C;
- a p-congruence between quadratic twists: $E[p] \cong E^d[p]$.

- in the second situation, C cuts out a quadratic extension $K(\sqrt{d})/K$ and $\overline{\rho}_{E,p}(\sigma) \equiv 0 \pmod{p}$ whenever $\sigma(\sqrt{d}) = -\sqrt{d}$. Hence $\overline{\rho}_{E,p}$ and $\overline{\rho}_{E^d,p}$ have the same traces, so are equivalent (if irreducible).

Congruences between twists I

With some mild conditions to exclude very small images we have a correspondence between the following situations, for odd p over any number field K:

- the projective image in $\mathrm{PGL}_2(\mathbb{F}_p)$ being dihedral;
- the image being contained in the normaliser N of a Cartan subgroup C, but not contained in C;
- a p-congruence between quadratic twists: $E[p] \cong E^d[p]$.

- in the second situation, C cuts out a quadratic extension $K(\sqrt{d})/K$ and $\overline{\rho}_{E,p}(\sigma) \equiv 0 \pmod{p}$ whenever $\sigma(\sqrt{d}) = -\sqrt{d}$. Hence $\overline{\rho}_{E,p}$ and $\overline{\rho}_{E^d,p}$ have the same traces, so are equivalent (if irreducible).

- the converse is similar.

Congruences between twists II

In this situation we can easily determine whether the congruence is symplectic:

Congruences between twists II

In this situation we can easily determine whether the congruence is symplectic:

Proposition

If $\phi :\ E[p] \cong E^d[p]$ with image contained in $N \supseteq C$ a Cartan normaliser, then

1. *ϕ is symplectic if C is split and $p \equiv 1 \pmod 4$ or if C is nonsplit and $p \equiv 3 \pmod 4$;*
2. *ϕ is anti-symplectic if C is split and $p \equiv 3 \pmod 4$ or if C is nonsplit and $p \equiv 1 \pmod 4$.*

Congruences between twists III

Normally there can be no more than one congruence between E and a quadratic twist. The exception is when the projective image is $C_2 \times C_2$.

Congruences between twists III

Normally there can be no more than one congruence between E and a quadratic twist. The exception is when the projective image is $C_2 \times C_2$.

Proposition

Suppose that $\overline{\rho}_{E,p}$ has projective image $C_2 \times C_2$. Then there are three quadratic twists E^{d_i} which are p-congruent to E.

- *If $\sqrt{p^*} \in K$ then all three congruences are symplectic;*
- *Otherwise one is the symplectic congruence $E[p] \cong E^{p^*}[p]$, and the other two are anti-symplectic.*

$p^* = \pm p \equiv 1 \pmod 4$, and $\sqrt{p^*} \in K$ iff $\mathbb{P}\overline{\rho}_{E,p}(G_K) \subseteq \mathrm{PSL}_2(\mathbb{F}_p)$.

Congruences between twists III

Normally there can be no more than one congruence between E and a quadratic twist. The exception is when the projective image is $C_2 \times C_2$.

Proposition

Suppose that $\overline{\rho}_{E,p}$ has projective image $C_2 \times C_2$. Then there are three quadratic twists E^{d_i} which are p-congruent to E.

- *If $\sqrt{p^*} \in K$ then all three congruences are symplectic;*
- *Otherwise one is the symplectic congruence $E[p] \cong E^{p^*}[p]$, and the other two are anti-symplectic.*

$p^* = \pm p \equiv 1 \pmod 4$, and $\sqrt{p^*} \in K$ iff $\mathbb{P}\overline{\rho}_{E,p}(G_K) \subseteq \mathrm{PSL}_2(\mathbb{F}_p)$.

Example

$E = 6534a1$, of conductor $6534 = 2 \cdot 3^3 \cdot 11^2$ is symplectically 3-congruent to $E^{-3} = 6534v1$, and anti-symplectically to $E^{-11} = 6534p1$ and $E^{33} = 6534h1$.

Quartic twists

Curves of the form $E_a: \; Y^2 = X^3 + aX$ have $j(E_a) = 1728$ and CM by $\sqrt{-1}$, and admit *quartic twists* $E_a \sim E_{ta}$, parametrized by $t \in K^*/(K^*)^4$.

Quartic twists

Curves of the form $E_a : \ Y^2 = X^3 + aX$ have $j(E_a) = 1728$ and CM by $\sqrt{-1}$, and admit *quartic twists* $E_a \sim E_{ta}$, parametrized by $t \in K^*/(K^*)^4$.

Proposition

The only p-congruence between these curves is the one induced by the 2-isogeny: $E_a[p] \cong E_{-4a}[p]$.

Quartic twists

Curves of the form $E_a : \; Y^2 = X^3 + aX$ have $j(E_a) = 1728$ and CM by $\sqrt{-1}$, and admit *quartic twists* $E_a \sim E_{ta}$, parametrized by $t \in K^*/(K^*)^4$.

Proposition

The only p-congruence between these curves is the one induced by the 2-isogeny: $E_a[p] \cong E_{-4a}[p]$.

This is only non-trivial when $\sqrt{-1} \notin K$, as otherwise the curves themselves are isomorphic (since $-4 = (1 + \sqrt{-1})^4$).

Sextic twists

Curves of the form $E_b:\ Y^2 = X^3 + b$ have $j(E_b) = 0$ and CM by $\sqrt{-3}$, and admit *sextic twists* $E_b \sim E_{tb}$, parametrized by $t \in K^*/(K^*)^6$.

Sextic twists

Curves of the form $E_b: \ Y^2 = X^3 + b$ have $j(E_b) = 0$ and CM by $\sqrt{-3}$, and admit *sextic twists* $E_b \sim E_{tb}$, parametrized by $t \in K^*/(K^*)^6$.

During our computations with $p = 7$ we noticed something which led to the following.

Sextic twists

Curves of the form $E_b: \ Y^2 = X^3 + b$ have $j(E_b) = 0$ and CM by $\sqrt{-3}$, and admit *sextic twists* $E_b \sim E_{tb}$, parametrized by $t \in K^*/(K^*)^6$.

During our computations with $p = 7$ we noticed something which led to the following.

Proposition

Assume $\sqrt{-3} \notin K$. The only 7-congruences between these are:

- $E_b[7] \cong E_{-27b}[7]$*, anti-symplectic (induced by a 3-isogeny);*
- $E_b[7] \cong E_{-28/b}[7]$*, symplectic;*
- $E_b[7] \cong E_{27\cdot 28/b}[7]$*, anti-symplectic (composite of previous).*

Sextic twists

Curves of the form $E_b : \; Y^2 = X^3 + b$ have $j(E_b) = 0$ and CM by $\sqrt{-3}$, and admit *sextic twists* $E_b \sim E_{tb}$, parametrized by $t \in K^*/(K^*)^6$.

During our computations with $p = 7$ we noticed something which led to the following.

Proposition

Assume $\sqrt{-3} \notin K$. The only 7-congruences between these are:

- $E_b[7] \cong E_{-27b}[7]$, *anti-symplectic (induced by a 3-isogeny);*
- $E_b[7] \cong E_{-28/b}[7]$, *symplectic;*
- $E_b[7] \cong E_{27\cdot 28/b}[7]$, *anti-symplectic (composite of previous).*

We hope to generalise this to other primes p.