N-Congruences Between Quadratic Twists of Elliptic Curves

Sam Frengley

University of Cambridge

18 August 2021

Congruences of Elliptic Curves

Definition

Let K be a field of characteristic 0. Let E/K and E'/K be elliptic curves and $N \geq 2$. We say that E and E' are N-congruent if $E[N] \cong E'[N]$ as Galois modules.

Examples

- Let E be given by a Weierstrass equation $y^2 = f(x)$. Then the quadratic twist E^d given by $dy^2 = f(x)$ is 2-congruent to E.
- Let E be given by a Weierstrass equation $F(X, Y, Z) = 0$. Then the family given by $F + \lambda H(F) = 0$ are 3-congruent to E (where H is the Hessian).
- Let $\phi : E \to E'$ be an isogeny of degree coprime to N, defined over K. Then ϕ induces an N-congruence (such congruences are said to be trivial).

The Big Conjecture

Conjecture (Frey-Mazur)

There are no non-trivial N-congruences over $\mathbb{Q}$ for $N >?$ for some ?.

In fact when $N = p$ is a prime number, this has been refined by Fisher who has conjectured that there are no non-trivial p-congruences for $p > 17$.

How to Construct Examples of Congruences?

- Searching through the LMFDB database of elliptic curves (see Cremona-Freitas).
- Fix an elliptic curve $E/\mathbb{Q}$, then the elliptic curves $E'/\mathbb{Q}$ which are (N, r)-congruent to E correspond to rational points on a twist, $X_E^r(N)$, of the modular curve $X(N)$.
- There exists a surface, $Z(N, r)/\mathbb{Q}$, which parametrises pairs (E, E') of (N, r)-congruent elliptic curves.
- The "quadratic twists" construction of Halberstadt and Cremona-Freitas.

The State of Things

N	Known non-trivial N-congruences over $\mathbb{Q}$	Notes
≤ 13	∞-many pairs with distinct j-invariants	Due to Rubin-Silverberg, Halberstadt-Kraus, Kumar, Poonen-Schaefer-Stoll, Chen, Fisher, and Papadopulos.
14	∞-many pairs	Due to Halberstadt, all pairs are quadratic twists (i.e., (E, E^d)).
17	2 pairs	Due to Fisher, conjectured to be the only 17-congruences.
22	∞-many pairs	Due to Halberstadt, all pairs are quadratic twists
Primes ≥ 19	Fisher has conjectured there are no pairs	

Infinite Families of Congruences Between Quadratic Twists

Theorem (F.)

There are infinitely many j-invariants of elliptic curves $E/\mathbb{Q}$ which admit a (non-trivial) N-congruence with a non-trivial quadratic twist if and only if either $N \leq 12$, $N \leq 24$ is even, $N = 28$ or $N = 36$.

Examples of N-Congruences for Large N

Theorem (F.)

We have

1. *The elliptic curve with Weierstrass equation*

$$y^2 + y = x^3 + 46824073615289101\,0x - 1483745866244648762473169 57$$

is 48*-congruent (over* $\mathbb{Q}$*) to its quadratic twist by its discriminant.*

2. *The elliptic curve with Weierstrass equation*

$$y^2 + xy = x^3 - x^2 - 273176601587417x - 174181879994890510962 0$$

is 30*-congruent (over* $\mathbb{Q}$*) to its quadratic twist by* -214663*.*

The Idea for p-Congruences

Theorem (Halberstadt, Cremona-Freitas)

Let p be an odd prime. Then the non-cuspidal K-points on the modular curves $X_{ns}^{+}(p)$ and $X_{s}^{+}(p)$ parametrise elliptic curves which admit a p-congruence (over K) with a quadratic twist.

Halberstadt's results for $N = 14$ and $N = 22$ follow from the theorem. The curve $X_{ns}^{+}(7)$ (respectively $X_{ns}^{+}(11)$) has infinitely many rational points - hence give us infinitely many (j-invariants of) elliptic curves, $E/\mathbb{Q}$ admitting a 7 (respectively 11) congruence with a quadratic twist. But quadratic twists are also 2-congruent.
The following lemma shows that infinitely many of these congruences are non-trivial.

Lemma

An elliptic curve E admits an isogeny with a quadratic twist if and only if E has complex multiplication.

Aside: The Class Number 1 Problem

Recall there is a bijection

$$\left\{\begin{array}{l}\text{Orders } \mathcal{O} \text{ in imaginary} \\ \text{quadratic fields } K/\mathbb{Q} \text{ with} \\ \text{class number, } h(\mathcal{O}) = 1\end{array}\right\} \leftrightarrow \left\{\begin{array}{l} j\text{-invariants of elliptic} \\ \text{curves } E/\mathbb{Q} \text{ with CM}\end{array}\right\}$$

In fact, every elliptic curve with CM by an order of discriminant $d > 4p$ give rise to a point on $X_{ns}^{+}(p)$ (see Serre's *Lectures on the MW Theorem*). In particular, solving the Frey-Mazur conjecture for p-congruences between quadratic twists is in itself very difficult!

The Idea of Our Construction for 15-Congruences

Consider the fibre product

$$\begin{array}{ccc} X_{ns}^{+}(3) \times_{X(1)} X_{ns}^{+}(5) & \longrightarrow & X_{ns}^{+}(5) \\ \downarrow & & \downarrow \\ X_{ns}^{+}(3) & \longrightarrow & X(1) \end{array}$$

Then $X_{ns}^{+}(15) = X_{ns}^{+}(3) \times_{X(1)} X_{ns}^{+}(5)$ parametrises elliptic curves E/K admitting a 3-congruence with a quadratic twist E^{d}, and a 5-congruence with a (possibly different) quadratic twist $E^{d'}$. We the construct a double cover C of $X_{ns}^{+}(15)$ which corresponds to requiring that these quadratic twists are in fact *isomorphic* - i.e., dd' is a square in K.

The Idea of Our Construction for 15-Congruences

It turns out in this case that C is a genus 2 curve, and by searching for points, we find that there is a 15-congruence (over $\mathbb{Q}$) between the elliptic curve

$$E : y^2 + xy = x^3 - x^2 - 273176601587417x \\ - 1741818799948905109620$$

and its quadratic twist by -214663.

But then E is 30-congruent to this quadratic twist (since all quadratic twists are trivially 2-congruent).

In fact, we can prove that the only rational points on C are either cusps, CM points (i.e., correspond to trivial 15-congruences), or give rise to the 15-congruence above.