On the generalized Fermat equation

Imin Chen

Simon Fraser University

March 19, 2017

Fermat's Last Theorem and Beyond

Recall the usual Fermat's Last Theorem proven by Wiles' et al.

Theorem

The equation $x^p + y^p = z^p$ *has no solutions in non-zero integers* x, y, z *for* $p \geq 3$.

Sometime in the 1990's several people (Beal, Granville, Tijdeman-Zagier, ...) noted and made a conjecture regarding the following generalization.

Conjecture

The equation $x^p + y^q = z^r$ *has no solutions in non-zero mutually coprime integers* x, y, z *for* $p, q, r \geq 3$.

It is not clear who was the first to make the conjecture. Beal has funded a \$1 million USD prize for its resolution.

Galois representations and Modular Forms are useful ...

The proof of Fermat's Last Theorem used the following idea:

1. *Find a Frey curve*: Given a 'non-trivial primitive solution' to $x^p + y^p = z^p$, attach a 'Frey curve' E.
2. *Establish modularity and level lowering*: Show that $\rho_{E,p} \cong \rho_{f,\mathfrak{p}}$ where f is a modular form of level N bounded independently of the solution and exponent p, which we refer to as the *Serre level*.
3. *Eliminate forms*: Show that $\rho_{E,p} \cong \rho_{f,\mathfrak{p}}$ is not possible.

The overall strategy, which we now refer to as 'the modular method', was discovered by Frey, Serre, Ribet, et al. but it was not until Wiles' that we had the crucial ingredient of modularity.

It is useful to make the following definitions and comments:

A solution to a generalized Fermat equation $x^p + y^q = z^r$ is a triple $(a, b, c) \in \mathbb{Z}^3$. A solution (a, b, c) is non-trivial iff $abc \neq 0$. A solution (a, b, c) is primitive iff $(a, b, c) = 1$.

The hypothesis that $(x, y, z) = 1$ ensures the problem is 1-dimensional, rather than 2-dimensional.

Without it, there are many solutions. For instance, for the equation $x^5 + y^5 = z^p$, we have the solution $2^5 + 2^5 = 2^6$.

It is also the case that if we have one solution (x_0, y_0, z_0), we can produce infinitely many imprimitive solutions from it.

The hypothesis that $p, q, r \geq 3$ ensures $\chi < 0$ (except for $p = q = r = 3$) and we avoid all known solutions.

When $\frac{1}{p}+\frac{1}{q}+\frac{1}{r}<1$, all known non-trivial primitive solutions have $\min\{p,q,r\}$ equal to 2. They result from the identities

$$1^p+2^3=3^2,$$
$$2^5+7^2=3^4,$$
$$7^3+13^2=2^9,$$
$$2^7+17^3=71^2,$$
$$3^5+11^4=122^2,$$
$$17^7+76271^3=21063928^2,$$
$$1414^3+2213459^2=65^7,$$
$$9262^3+15312283^2=113^7,$$
$$43^8+96222^3=30042907^2,$$
$$\text{and}\quad 33^8+1549034^2=15613^3.$$

The Modular Method works ... sometimes.

Natural question: Can the modular method used to tackle the generalized Fermat equation $x^p + y^q = z^r$?

Short Answer: Sometimes.

For example:

- $x^p + y^p = z^p$ for $p \geq 3$ (Wiles)
- $x^p + y^p = z^2$ for $p \geq 5$ (Darmon-Merel)
- $x^p + y^p = z^3$ for $p \geq 5$ (Darmon-Merel)
- $x^2 + y^4 = z^p$ for $p \geq 5$ (Ellenberg, Bennett-Ellenberg-Ng)
- $x^2 + y^6 = z^p$ for $p \geq 3$ (Bennett-Chen)

- $x^3 + y^3 = z^p$ for 84.4% of prime exponents p:

  $3 \le p \le 10^9, p \equiv 2 \pmod 3, p \equiv 2, 3 \pmod 5,$
  $p \equiv 61 \pmod{78}, p \equiv 51, 103, 105 \pmod{106},$ or
  $p \equiv 43, 49, 61, 79, 97, 151, 157, 169, 187, 205, 259, 265, 277,$
  $295, 313, 367, 373, 385, 403, 421, 475, 481, 493, 511, 529, 583, 601,$
  $619, 637, 691, 697, 709, 727, 745, 799, 805, 817, 835, 853, 907, 913,$
  $925, 943, 961, 1015, 1021, 1033, 1051, 1069, 1123, 1129, 1141, 1159,$
  $1177, 1231, 1237, 1249, 1267, 1285 \pmod{1296}$

  (Kraus, Chen-Siksek, Freitas)
- $x^3 + y^{3p} = z^2$ for $p \equiv 1 \pmod 8$
  (Bennett-Chen-Dahmen-Yazdani)

Where the obstructions lie ...

1. We can't find a suitable Frey curve.
2. Modularity is not yet established.
3. We can't eliminate some modular forms.

Construction of Frey curves

Definition

Let K be a number field. A Frey representation over K of signature (p, q, r) is a representation $\rho : G_{K(t)} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ such that

- $\rho^{\mathrm{geom}} = \rho\,|_{G_{\overline{K}(t)}}$ has trivial determinant and is irreducible.
- ρ^{geom} is unramified outside $\{0, 1, \infty\}$.
- The inertia groups at $0, 1, \infty$ have order p, q, r, respectively.

The original modular method used Frey elliptic curves over $\mathbb{Q}$. Darmon-Granville classified the Frey representations which give rise to Frey elliptic curves over $\mathbb{Q}$.

The prime non-compact signatures which have Frey elliptic curves over $\mathbb{Q}$ are: $(2, 3, \infty)$, $(\infty, \infty, 2)$, $(\infty, \infty, 3)$, $(3, 3, \infty)$, (∞, ∞, ∞).

We can expand the list to include non-compact signatures which arise from arithmetic triangle groups (which were classified by Takeuchi).

This adds signatures $(2, 4, \infty)$ and $(2, 6, \infty)$, which require using Frey $\mathbb{Q}$-curves (which are elliptic curves over a number field whose isogeny class is defined over $\mathbb{Q}$).

To tackle more signatures, we need Frey curves which are not necessary defined over $\mathbb{Q}$ nor restricted to being elliptic curves.

Darmon's program: Frey curves

Darmon proposed a strategy to resolve a one parameter family of generalized Fermat equations, i.e., signature (p, p, r), (r, r, p), or (r, q, p), where the aim is to resolve these generalized Fermat equations for p sufficiently large compared to fixed r, q.

In particular, he constructed:

- explicit Frey hyperelliptic curves for signature (p, p, r),
- described Frey hypergeometric abelian varieties for signatures (r, r, p) and (r, q, p).

For example, for the equation $x^p + y^p = z^5$, we have the Frey hyperelliptic curves,

$$\begin{aligned} y^2 &= x^5 - 5c^2x^2 + 5c^4x - 2(a^p - b^p) \\ \Delta &= 2^8 5^5 a^{2p} b^{2p} \\ y^2 &= (x + 2c)(x^5 - 5c^2x^2 + 5c^4x - 2(a^p - b^p)) \\ \Delta &= 2^{12} 5^5 a^{4p} b^{2p}. \end{aligned}$$

which we attach to a non-trivial primitive solution $(a, b, c) \in \mathbb{Z}^3$. The jacobians J of these hyperelliptic curves (genus 2) have real multiplication by $\mathbb{Q}(\sqrt{5})$.

In the modular method, the following gets generalized:

- $\rho_{E,p}$ gets replaced by $\rho_{J,\mathfrak{p}}$
- the classical modular form f gets replaced by a Hilbert modular form f over $\mathbb{Q}(\sqrt{5})$.

Freitas' elliptic curves over totally real fields

Theorem (Darmon)

Let $\rho : G_{K(t)} \to GL_2(\overline{\mathbb{F}}_p)$ be a Frey representation over K of signature (p, p, r) or (r, r, p) (resp. (r, q, p)). Then

- *K contains $\mathbb{Q}(\zeta_r + \zeta_r^{-1})$ (resp. $\mathbb{Q}(\zeta_r + \zeta_r^{-1}, \zeta_q + \zeta_q^{-1})$)*
- *the traces of ρ contain the residue field of $\mathbb{Q}(\zeta_r + \zeta_r^{-1})$ (resp. $\mathbb{Q}(\zeta_r + \zeta_r^{-1}, \zeta_q + \zeta_q^{-1})$) at a prime $\mathfrak{p}$ above p.*

Darmon in fact gives a classification of Frey representations of these signatures. This result may appear to suggest we require more general curves.

In fact, this is not entirely the case.

Freitas constructed Frey elliptic curves over totally real fields for signature (r, r, p).

For example, for $a^5 + b^5 = c^p$:

$$y^2 = x^3 - 5(a^2 + b^2)x^2 + 5\phi_5(a, b)x,$$
$$\Delta = 2^4 5^3 (a + b)^2 (a^5 + b^5)^2$$
$$y^2 = x^3 + 2(a + b)x^2 - \bar{\omega}\psi_5(a, b)x$$
$$\Delta = 2^6 \bar{\omega}\phi_5(a, b)\psi_5(a, b)$$
$$y^2 = x^3 + 2(a - b)x^2 + (-3(\omega - \bar{\omega})/10 + 1/2)\,\psi_5(a, b)x$$
$$\Delta = 2^6 \left(-3(\omega - \bar{\omega})/10 + 1/2\right)^2 \left((\omega - \bar{\omega})/10 + 1/2\right) \phi_5(a, b)\psi_5(a, b).$$

where

$$\omega = (-1 + \sqrt{5})/2$$
$$X^5 + Y^5 = (X + Y)\phi_5(X, Y)\bar{\phi}_5(X, Y)$$
$$\phi_5(X, Y) = \psi_5(X, Y)\bar{\psi}_5(X, Y).$$

There is no inconsistency because Freitas' Frey elliptic curves are Frey representations of multiplicity ∞ on some subset of the 5-th roots over unity.

Darmon's description of Frey hypergeometric abelian varieties is somewhat less explicit. For small q, r, it is still possible to describe the curve in hyperelliptic form.

For example, for the equation $a^3 - b^5 = c^p$, we have the Frey hyperelliptic curve

$$y^2 = x^6 - 10bx^3 + 12ax + 5b^2, \Delta = 2^{12}3^6 5^5 (a^3 - b^5)^2.$$

On the other hand, hypergeometric abelian varieties have a rich structure. An approach of current interest is to try to make the modular method work for hypergeometric abelian varieties.

Modularity and level lowering:

Fermat's Last Theorem has historically inspired a lot of deep mathematics, and its eventual proof was no different.

Wiles' breakthrough paved the road for proving modularity results of greater and greater generality, in particular results which are valid over totally real fields.

Some highlights include:

- A proof of Serre's conjectures (i.e. every odd continuous Galois representation $G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ is modular) by Khare-Wintenberger.
- Every elliptic curve over a real quadratic field is modular (Freitas-Le Hung-Siksek).

Both rely on the deep machinery in the form of modularity lifting theorems, developed by a long list of mathematicians.

For level lowering we have results from Fujiwara, Jarvis, and Rajaei, which usually suffice.

Given the rapid developments on the Galois representation side, modularity and level lowering no longer pose an essential obstruction, at least in comparison to the other ones we discuss.

There is one important technical point however for level lowering: one needs to have irreducibility of the Galois representation $\rho_{E,p}$ or more generally, $\rho_{J,\mathfrak{p}}$.

In the elliptic curve case, this is usually provided by a version of Mazur's Theorem.

Theorem

Let E be an elliptic curve over $\mathbb{Q}$. Then $\rho_{E,p}$ is irreducible for $p > 163$.

For Frey elliptic curves over $\mathbb{Q}$, the bound is often $p \geq 5$ due to the fact that Frey elliptic curves are semi-stable outside a small set of primes.

For Frey elliptic curves over a totally real field, one can use more general Mazur-type results, such as the uniform bound boundedness theorems by Merel and Parent.

For more general Frey curves, no Mazur-type result is known.

Let K be a totally real number field and fix a prime $\mathfrak{q}$ of K. Let $c, f \geq 1$ be integers with c even. Consider a finite set $S_f(\mathfrak{q})$ of elements of the form $\alpha_1 + \alpha_2$ where $\alpha_i \in \overline{\mathbb{Z}}$ are (for every embedding $\overline{\mathbb{Z}} \hookrightarrow \mathbb{C}$) of complex absolute value $N(\mathfrak{q})^{f/2}$ and $\alpha_1\alpha_2 = N(\mathfrak{q})^f$.

Theorem (Billerey-Chen-Dieulefait-Freitas)

There exists a constant $c_1 = c_1(K, c, f, S_f(\mathfrak{q}))$ such that the following holds. Suppose that $p > c_1$ and A/K is an abelian variety satisfying

(i) *A is semistable at the primes of K above p,*

(ii) *A is of GL_2-type with multiplications by some totally real field F,*

(iii) *all endomorphisms of A are defined over K, that is $End_K(A) = End_{\overline{K}}(A)$,*

(iv) *A over K has inertial exponent c,*

(v) *A has potentially good reduction at $\mathfrak{q}$ with residual degree f,*

(vi) *the trace of $Frob_{\mathfrak{q}}^f$ acting on $V_{\mathfrak{p}}(A)$ lies in $S_f(\mathfrak{q})$, where $\mathfrak{p}$ is a prime of F above p.*

Then the representation $\rho_{A,\mathfrak{p}}$ is irreducible.

We say that an abelian variety A/K has inertial exponent $c \in \mathbb{N}$ if for every finite prime v of the number field K, there exists a finite Galois extension M/K such that A/M is semistable at all primes of M lying over v, and the exponent of the inertia subgroup at v of $\mathrm{Gal}(M/K)$ divides c.

Let A/K be an abelian variety with potentially good reduction at a prime $\mathfrak{q}$ of a number field K. We say that A has residual degree f at $\mathfrak{q}$ if f is minimal among the degrees of the residual extensions corresponding to all extensions $L/K_{\mathfrak{q}}$ such that A/L has good reduction.

Methods to eliminate forms

We come to what is perhaps the most serious obstruction, which is showing that $\rho_{E,p} \cong \rho_{f,\mathfrak{p}}$ cannot occur.

The methods used can be divided into local and global methods.

Local methods

1. Check if $\rho_{E,p}(F) \equiv \rho_{f,\mathfrak{p}}(F) \pmod{\mathfrak{p}}$ at a Frobenius element F.
2. Check if $\rho_{E,p}\,|_I \cong \rho_{f,\mathfrak{p}}\,|_I$ by comparing the size of the image of inertia, fixed fields of inertia, or conductors.

Some examples of global methods.

Theorem (Darmon-Merel)

Let $r = 2, 3$ and p be a prime. Suppose E is an elliptic curve over $\mathbb{Q}$ such that $\rho_{E,r}$ is reducible and $\rho_{E,p}$ lies in the normalizer of a Cartan subgroup of $GL_2(\mathbb{F}_p)$. If $p \geq 5$, then E has potentially good at all primes, except possibly p.

In particular, if f has complex multiplication, then we cannot have $\rho_{E,p} \cong \rho_{f,\mathfrak{p}}$ if E satisfies the conditions above. This was used to resolve the equations $x^p + y^p = z^r$ for $r = 2, 3$.

The trivial solution $\pm(1, -1)$ gives rise to a Frey curve E with complex multiplication.

Theorem (Ellenberg)

Let K be an imaginary quadratic field and d a square-free integer. There exists an effective constant $M_{k,d}$ such that, for all primes $p > M_{K,d}$, and all $\mathbb{Q}$-curves E over K of degree d, either

- *the representation $\mathbb{P}\rho_{E,p}$ is surjective, or*
- *E has potentially good reduction at all primes not dividing 6.*

This result was used to resolve the equation $x^2 + y^4 = z^p$.

The trivial solutions $\pm(1, 0)$ and $\pm(0, 1)$ give rise to Frey $\mathbb{Q}$-curves with complex multiplication.

Types of trivial solutions

We distinguish between two types of 'trivial' solutions.

1. Trivial solutions that persist for every exponent p: For example, $(1)^p + (-1)^p = 0^r$ for the equation $x^p + y^p = z^r$.
2. Trivial solutions that do not persist for every exponent p: For example, $1^3 + 2^3 = 3^2$ for the equation $x^3 + y^3 = z^p$.

In addition, a trivial solution may behaved in the following two ways with respect to a Frey curve E:

- a The trivial solution gives rise to a valid Frey curve E at the Serre level of $\rho_{E,p}$.
- b The trivial solution does not give rise to a valid Frey curve E at the Serre level of $\rho_{E,p}$.

Case 1a presents the biggest obstacle because it requires a global method to distinguish Galois representations which is uniform in p.

Aside from the elliptic curve case, no such global methods are known.

This is due to the lack of efficient but conceptual methods to determine rational points on curves, of which Mazur's method is the only known example.

The curves of interest in Darmon's program are almost always associated to non-congruence subgroups.

Even in the elliptic curve case, we do not have a complete answer.

Conjecture (Serre)

There is a absolute constant c such that if $p > c$ and E is an elliptic curve over $\mathbb{Q}$ without CM, then $\rho_{E,p}$ does not have image contained in the normalizer of a non-split Cartan subgroup.

Conjecture (Frey-Mazur)

There is a absolute constant c such that if $p > c$ and E, E' are elliptic curves over $\mathbb{Q}$, such that $\rho_{E,p} \cong \rho_{E',p}$, then E and E' are isogenous over $\mathbb{Q}$.

Before we eliminate a form, we need to compute it ...

Currently, the modular method requires a computation of all modular forms at the Serre level N.

The implemented algorithms of Stein, Dembélé, and Voight have allowed such computations to be made for classical and Hilbert modular forms.

However, in the case of Hilbert modular forms, one quickly reaches computational limits.

For example, in considering the equation $x^7 + y^7 = 3z^p$, Freitas encountered the need for computations of spaces of Hilbert modular forms of dimension 10753.

The Multi-Frey approach

In the early days, it was noted that some Fermat type equations had more than one Frey curve for which one could apply the modular method.

Siksek coined the term 'multi-Frey' to mean using more than one Frey curve in the modular method simultaneously.

For example, in the local method that compares traces, we can impose the condition $a_{\mathfrak{q}}(E_i) \equiv a_{\mathfrak{q}}(f) \pmod{\mathfrak{p}}$ for every Frey curve E_i that we have available.

There is growing evidence that the multi-Frey technique is quite powerful, provided we have a sufficiently 'rich' set of Frey curves at our disposal.

We illustrate the multi-Frey approach by considering the equation

$$x^5 + y^5 = 3z^p. \tag{1}$$

As we saw, there are three Frey elliptic curves for this equation which we can attach to a non-trivial primitive solution (a, b, c).

$$W = W_{a,b} : y^2 = x^3 - 5(a^2 + b^2)x^2 + 5\phi_5(a, b)x,$$
$$E = E_{a,b} : y^2 = x^3 + 2(a + b)x^2 - \bar{\omega}\psi_5(a, b)x$$
$$F = F_{a,b} : y^2 = x^3 + 2(a - b)x^2 + (-3(\omega - \bar{\omega})/10 + 1/2)\,\psi_5(a, b)x$$

(a, b, c) is non-trivial iff $abc \neq 0$.

(a, b, c) is primitive iff $(a, b, c) = 1$.

The multi-Frey technique in action ...

1. W is used to prove $v_2(a) = 1$ and the result for $p \leq 10^7$.
2. E is used to prove $5 \mid a + b$.
3. We now assume $v_2(a) = 1$, $p > 10^7$ and $5 \mid a + b$.
4. Under these assumptions, $\rho_{F,p} \cong \rho_{F_{1,-1},p} \otimes \chi$.
5. However, we know $v_2(a) = 1$, but this is not satisfied by the trivial solution $(1, -1)$.
6. An image of inertia argument is used to distinguish $\rho_{F,p}$ and $\rho_{F_{1,-1},p} \otimes \chi$.

Theorem (Billerey-Chen-Dieulefait-Freitas)

For every integer $n \geq 2$, the equation $x^5 + y^5 = 3z^n$ has no non-trivial primitive solutions.

The multi-Frey method is used several times in the proof to refine the bounds on p (irreducibility and elimination steps) and reduce the Serre levels (modularity step).

For the exponents $p = 2, 3, 5$, we regard (1) as an equation of signature $(p, p, 2)$, $(p, p, 3)$, (p, p, p), respectively.

The case $x^5 + y^5 = 3z^5$ is due to L. Dirichlet.

Current approaches

Generalize the modular method to work with hypergeometric abelian varieties

$$C_\lambda^{[N;i,j,k]} : y^N = x^i(1-x)^j(1-\lambda x)^k,$$

which can be used to realize Frey representations explicitly.

This would enlarge the library of Frey abelian varieties at our disposal.

The modular method has so far as remained within the realm of abelian varieties of GL_2-type. But now we have the tantalizing:

Theorem (Scholze)

Let p be a prime and let g be a Hecke eigenclass in

$$H^j(\Gamma\backslash\mathscr{H}_n, \mathbb{Z}/p\mathbb{Z}).$$

Then there exists a continuous semi-simple Galois representation

$$\rho_g : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_n(\overline{\mathbb{F}}_p)$$

which is associated to g in the sense that the characteristic polynomial of $\rho_g(Frob_\ell)$ has coefficients $a_{\ell,i}$ given by the eigenvalues of the Hecke operators $T_{\ell,i}$ on g.

Fundamental challenges

1. Find a universal Frey mechanism for $x^p + y^q = z^r$ to deal with three varying exponents.
2. Eliminate the elimination step so no computation of automorphic forms is needed.
3. Prove a Mazur-type result applicable to Frey abelian varieties or provide a trick to avoid having to prove it in full generality.