The generalized Fermat equation : a progress report

Michael Bennett (with Imin Chen, Sander Dahmen and Soroosh Yazdani)

University of British Columbia

Hawaii-Manoa : March, 2012

A Diophantine equation : Generalized Fermat

We consider the equation

$$x^p + y^q = z^r$$

where x, y and z are relatively prime integers, and p, q and r are positive integers with

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1.$$

- $(p, q, r) = (n, n, n)$: Fermat's equation
- $y = 1$: Catalan's equation
- considered by Beukers, Granville, Tijdeman, Zagier, Beal (and many others)

A simple case

$$x^p + y^q = z^r$$

where x, y and z are relatively prime integers, and p, q and r are positive integers with

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} = 1.$$

- $(p, q, r) = (2, 6, 3), (2, 4, 4), (4, 4, 2), (3, 3, 3), (2, 3, 6)$
- each case corresponds to an elliptic curve of rank 0
- the only coprime nonzero solutions is with $(p, q, r) = (2, 3, 6)$ – corresponding to $3^2 - 2^3 = 1$

For example : $x^3 + y^3 = z^3$

We write

$$Y = \frac{36(x-y)}{x+y} \text{ and } X = \frac{12z}{x+y},$$

so that

$$Y^2 = X^3 - 432.$$

For example : $x^3 + y^3 = z^3$

We write

$$Y = \frac{36(x-y)}{x+y} \quad \text{and} \quad X = \frac{12z}{x+y},$$

so that

$$Y^2 = X^3 - 432.$$

This is 27A in Cremona's tables – it has rank zero and

$$E(\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}.$$

A less simple case

$$x^p + y^q = z^r$$

where x, y and z are relatively prime integers, and p, q and r are positive integers with

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} > 1.$$

- $(2,2,r), (2,q,2), (2,3,3), (2,3,4), (2,4,3), (2,3,5)$
- in each case, the coprime integer solutions come in finitely many two parameter families (the canonical model is that of Pythagorean triples)
- in the $(2,3,5)$ case, there are precisely 27 such families (as proved by J. Edwards, 2004)

Back to

$$x^p + y^q = z^r$$

where x, y and z are relatively prime integers, and p, q and r are positive integers with

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1.$$

Some solutions

$$1^n + 2^3 = 3^2,$$

$$2^5 + 7^2 = 3^4,$$

$$3^5 + 11^4 = 122^2,$$

$$2^7 + 17^3 = 71^2,$$

$$7^3 + 13^2 = 2^9,$$

$$43^8 + 96222^3 = 30042907^2,$$

$$33^8 + 1549034^2 = 15613^3,$$

$$17^7 + 76271^3 = 21063928^2,$$

$$1414^3 + 2213459^2 = 65^7,$$

$$9262^3 + 15312283^2 = 113^7.$$

Conjecture (weak version $0)

There are at most finitely many other solutions.

Conjecture (weak version $0)

There are at most finitely many other solutions.

Conjecture (Beal prize problem $100,000)

Every such solution has $\min\{p, q, r\} = 2$.

Conjecture (weak version \$0)

There are at most finitely many other solutions.

Conjecture (Beal prize problem \$100,000)

Every such solution has $\min\{p, q, r\} = 2$.

Conjecture (strong version $\geq$ \$100,000)

There are no additional solutions.

What we know

Theorem (Darmon and Granville) If A, B, C, p, q and r are fixed positive integers with

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1,$$

then the equation

$$Ax^p + By^q = Cz^r$$

has at most finitely many solutions in coprime nonzero integers x, y and z.

The state of the art (?)

(p, q, r)	reference(s)
(n, n, n)	Wiles, Taylor-Wiles
$(n, n, k), k \in \{2, 3\}$	Darmon-Merel, Poonen
$(2n, 2n, 5)$	B.
$(2, 4, n)$	Ellenberg, B-Ellenberg-Ng, Bruin
$(2, 6, n)$	B-Chen, Bruin
$(2, n, 4)$	B-Skinner, Bruin
$(2, n, 6)$	BCDY
$(3j, 3k, n),\ j, k \geq 2$	immediate from Kraus
$(3, 3, 2n)$	BCDY
$(3, 6, n)$	BCDY
$(2, 2n, k),\ k \in \{9, 10, 15\}$	BCDY
$(4, 2n, 3)$	BCDY

The state of the art : continued

(p, q, r)	reference(s)
$(3, 3, n)^*$	Chen-Siksek, Kraus, Bruin, Dahmen
$(2, 2n, 3)^*$	Chen, Dahmen, Siksek
$(2, 2n, 5)^*$	Chen
$(2m, 2n, 3)^*$	BCDY
$(2, 4n, 3)^*$	BCDY
$(3, 3n, 2)^*$	BCDY
$(2, 3, n),\ 6 \le n \le 10$	PSS, Bruin, Brown, Siksek
$(3, 4, 5)$	Siksek-Stoll
$(5, 5, 7),\ (7, 7, 5)$	Dahmen-Siksek

The state of the art : continued

The * here refers to conditional results. For instance, in case $(p, q, r) = (3, 3, n)$, we have no solutions if either $3 \leq n \leq 10^4$, or $n \equiv \pm 2$ modulo 5, or $n \equiv \pm 17$ modulo 78, or

$$n \equiv 51, 103, 105 \text{ modulo } 106,$$

or for n (modulo 1296) one of

$$43, 49, 61, 79, 97, 151, 157, 169, 187, 205, 259, 265, 277, 295, 313, 367, 373, 385, 403, 421, 475, 481, 493, 511, 529, 583, 601, 619, 637, 691, 697, 709, 727, 745, 799, 805, 817, 835, 853, 907, 913, 925, 943, 961, 1015, 1021, 1033, 1051, 1069, 1123, 1129, 1141, 1159, 1177, 1231, 1237, 1249, 1267, 1285.$$

Methods of proof

These results have primarily followed from either

- Chabauty-type techniques, or
- Methods based upon the modularity of certain Galois representations

Methods of proof

These results have primarily followed from either

- Chabauty-type techniques, or
- Methods based upon the modularity of certain Galois representations

We will discuss the latter – the former is a p-adic method for (potentially) determining the rational points on curves of positive genus.

Elliptic curves

Consider a cubic curve of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

or, more simply, if we avoid characteristic 2 and 3,

$$E \quad : \quad y^2 = x^3 + ax + b$$

with discriminant

$$\Delta = -16\left(4a^3 + 27b^2\right) \neq 0.$$

Let us suppose that a and b are rational integers.

Elliptic curves (continued)

For prime p not dividing $\Delta = \Delta_E$, we define

$$a_p = p + 1 - \#E(\mathbb{F}_p)$$

so that, by a theorem of Hasse,

$$|a_p| \leq 2\sqrt{p}.$$

An L-function

Define

$$L(E,s) = \prod_p \left(1 - a_p\, p^{-s} + \epsilon(p) p^{1-2s}\right)^{-1}.$$

Since we can write

$$L(E,s) = \sum_n a_n n^{-s},$$

this suggests considering the generating series

$$f_E(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}.$$

Note that we have $f_E(z+1) = f_E(z)$.

Modular forms

Definition : A *modular form* (of weight 2 and level N) is a holomorphic function f on the upper half-plane satisfying

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 f(z)$$

for all

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N),$$

i.e. for $a, b, c, d \in \mathbb{Z}$, $ad - bc = 1$ and $N \mid c$.

Modular forms (continued)

Fourier expansion : Since $f(z+1) = f(z)$, we have

$$f(z) = \sum_{n=0}^{\infty} c_n q^n, \quad q = e^{2\pi i z}.$$

The Modularity Conjecture / Wiles' Theorem

If E is an elliptic curve over $\mathbb{Q}$, then the corresponding generating series $f_E(z)$ is a modular form of weight 2 and level N, where N is the *conductor* of the curve E.

The conductor is an arithmetic invariant of the curve E, measuring the primes for which E has bad reduction (i.e. those primes p dividing Δ_E).

The conductor : Szpiro's conjecture

As an aside, let me remark that N_E divides Δ_E. In the other direction, Szpiro conjectures that for $\epsilon > 0$, there exists $c(\epsilon)$ such that

$$|\Delta_E| < c(\epsilon) N_E^{6+\epsilon}.$$

In particular, the ratio

$$S(E) = \frac{\log |\Delta_E|}{\log N_E}$$

should be absolutely bounded.

The conductor : Szpiro's conjecture continued

The example we know with $S(E)$ largest corresponds to

$$E \; : \; y^2 + xy = x^3 - Ax - B,$$

where $A = 424151762667003358518$ and

$$B = 6292273164116612928531204122716,$$

which has minimal discriminant

$$\Delta_E = -2^{33} \cdot 7^{18} \cdot 13^{27} \cdot 19^3 \cdot 29^2 \cdot 127,$$

conductor

$$N_E = 2 \cdot 7 \cdot 13 \cdot 19 \cdot 29 \cdot 127$$

and hence $S(E) = 9.01996 \ldots$.

Back to modularity : an example

$$E \; : \; y^2 + y = x^3 - x^2 - 10x - 20.$$

We compute that, setting $q = e^{2\pi i z}$,

$$f_E(z) = q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - \cdots$$

On the other hand, defining

$$\begin{aligned} f(z) &= (\eta(z)\eta(11z))^2 \\ &= q\left(\prod_{n=1}^{\infty}(1-q^n)(1-q^{11n})\right)^2, \end{aligned}$$

we find that $f(z) = f_E(z)$ is the (unique) weight 2 modular form of level 11.

Ribet's theorem : level lowering

For our purposes, we are especially interested in modular forms of relatively low level.

In a number of cases, a fundamental result of Ribet enables us to move from consideration of a form $f(z) = \sum_m c_m q^m$ of level N, to a modular form $g(z) = \sum_m d_m q^m$ of level N/l satisfying

$$c_p \equiv d_p \text{ modulo } n$$

for all primes p coprime to Nn, where $l \mid N$ and n are primes.

Ribet's theorem : an example

For example, the elliptic curve

$$E : y^2 = x^3 - 228813x + 42127856$$

has discriminant

$$\Delta = -2^6 \cdot 3^3 \cdot 17^7$$

and conductor

$$N = 2^5 \cdot 3^3 \cdot 17.$$

The corresponding cuspidal newform f has Fourier coefficients

c_5	c_{11}	c_{13}	c_{19}	c_{23}	c_{29}	c_{31}	c_{37}
-1	4	-7	-1	-1	5	2	-2

Ribet's theorem : an example (continued)

Our curve E has conductor $2^5 \cdot 3^3 \cdot 17$ (it's Cremona's 14688r)

c_5	c_{11}	c_{13}	c_{19}	c_{23}	c_{29}	c_{31}	c_{37}
-1	4	-7	-1	-1	5	2	-2

Lurking at level $864 = 2^5 \cdot 3^3$, we find a newform g corresponding to (in the notation of Cremona) the elliptic curve $864d1$:

$$E_1 : y^2 = x^3 - 3x - 6.$$

This form has Fourier coefficients

d_5	d_{11}	d_{13}	d_{19}	d_{23}	d_{29}	d_{31}	d_{37}
-1	-3	0	6	6	-2	9	-2

Fermat's Last Theorem

If $a^n + b^n = c^n$ is a nontrivial solution of the Fermat equation, then the elliptic curve

$$E : y^2 = x(x - a^n)(x + b^n)$$

has minimal discriminant $(abc)^{2n}/2^8$ and conductor $N = \prod_{p|abc} p$.

After a short calculation, one finds that, for prime $n \geq 5$, the aforementioned theorems of Ribet and Wiles guarantee the existence of a weight 2, cuspidal newform of level 2. The nonexistence of such a form completes the proof of Fermat's Last Theorem.

A program for attacking certain $x^p + y^q = z^r$

Given a solution to

$$x^p + y^q = z^r,$$

we would like to

1. Construct a "Frey-Hellegouarch" curve $E_{x,y,z}$ with conductor $N_{x,y,z}$

A program for attacking certain $x^p + y^q = z^r$

Given a solution to

$$x^p + y^q = z^r,$$

we would like to

1. Construct a "Frey-Hellegouarch" curve $E_{x,y,z}$ with conductor $N_{x,y,z}$
2. Consider a corresponding mod "n" Galois representation ρ_E with Artin conductor N

A program for attacking certain $x^p + y^q = z^r$

Given a solution to

$$x^p + y^q = z^r,$$

we would like to

1. Construct a "Frey-Hellegouarch" curve $E_{x,y,z}$ with conductor $N_{x,y,z}$
2. Consider a corresponding mod "n" Galois representation ρ_E with Artin conductor N
3. Show that this is connected to a weight 2 cuspidal newform of level N

A program for attacking certain $x^p + y^q = z^r$

Given a solution to

$$x^p + y^q = z^r,$$

we would like to

1. Construct a "Frey-Hellegouarch" curve $E_{x,y,z}$ with conductor $N_{x,y,z}$
2. Consider a corresponding mod "n" Galois representation ρ_E with Artin conductor N
3. Show that this is connected to a weight 2 cuspidal newform of level N
4. Use properties of $E_{x,y,z}$ and the newforms at level N to derive arithmetic information

Potential difficulties

1. We are (at present) quite limited in the signatures (p, q, r) for which such a program can be implemented.

Potential difficulties

1. We are (at present) quite limited in the signatures (p, q, r) for which such a program can be implemented.
2. Small values of exponents may present problems.

Potential difficulties

1. We are (at present) quite limited in the signatures (p, q, r) for which such a program can be implemented.
2. Small values of exponents may present problems.
3. We might not derive much (or even any) information!

Possible signatures

Work of Darmon and Granville suggests that restricting attention to Frey-Hellegouarch curves over $\mathbb{Q}$ (or, for that matter, to $\mathbb{Q}$-curves) might enable us to treat only signatures which can be related via descent to one of

$$(p, q, r) \in \{(n, n, n), (n, n, 2), (n, n, 3), (2, 3, n), (3, 3, n)\}.$$

Possible signatures

Work of Darmon and Granville suggests that restricting attention to Frey-Hellegouarch curves over $\mathbb{Q}$ (or, for that matter, to $\mathbb{Q}$-curves) might enable us to treat only signatures which can be related via descent to one of

$$(p,q,r) \in \{(n,n,n),(n,n,2),(n,n,3),(2,3,n),(3,3,n)\}.$$

Of course, as demonstrated by, for example, striking work of Ellenberg, there are some quite nontrivial examples of ternary equations which may be reduced to the study of the form $Aa^p + Bb^q = Cc^r$ for one of these signatures.

Signature $(n, n, 2)$

Given $Aa^n + Bb^n = Cc^2$, we consider the Frey-Hellegouarch curve

$$E_{a,b,c} \; : \; y^2 = x^3 + 2cCx^2 + BCb^n x,$$

of discriminant $\Delta_E = 64AB^2C^3 \left(ab^2\right)^n$.

Signature $(n, n, 2)$

Given $Aa^n + Bb^n = Cc^2$, we consider the Frey-Hellegouarch curve

$$E_{a,b,c} \; : \; y^2 = x^3 + 2cCx^2 + BCb^n x,$$

of discriminant $\Delta_E = 64AB^2C^3 \left(ab^2\right)^n$.

Darmon and Merel use this with $A = B = C = 1$ and derive a correspondence between E and an elliptic curve of conductor 32 with complex multiplication.

A new equation via descent

Suppose we have coprime integers a, b and c with

$$a^4 - b^2 = c^n,$$

with $n \geq 7$, say, prime. Then either

$$a^2 - b = r^n \text{ and } a^2 + b = s^n,$$

or

$$a^2 - b = 2^\delta r^n \text{ and } a^2 + b = 2^{n-\delta} s^n,$$

for some integers r and s, and $\delta \in \{1, n-1\}$.

It follows that

$$r^n + s^n = 2a^2 \text{ or } r^n + 2^{n-\delta-1}s^n = a^2,$$

both of which are shown to have no solutions with $|rs| > 1$ in a paper of B-Skinner (for $n \geq 7$). For $n = 5$, the first of these has the solution $(r, s, a) = (3, -1, 11)$.

It follows that

$$r^n + s^n = 2a^2 \text{ or } r^n + 2^{n-\delta-1}s^n = a^2,$$

both of which are shown to have no solutions with $|rs| > 1$ in a paper of B-Skinner (for $n \geq 7$). For $n = 5$, the first of these has the solution $(r, s, a) = (3, -1, 11)$.

The solution $r = s = 1$ to the first equation shows up as a modular form of level 256 (with, again, complex multiplication).

More equations via descent

If, instead, we consider

$$a^4 + b^2 = c^n,$$

factoring over $\mathbb{Q}(i)$ leads to a Frey-Hellegouarch $\mathbb{Q}$-curve.

More equations via descent

If, instead, we consider

$$a^4 + b^2 = c^n,$$

factoring over $\mathbb{Q}(i)$ leads to a Frey-Hellegouarch $\mathbb{Q}$-curve.

Ellenberg uses this approach to show that the above equation has no nontrivial solutions for prime $n \geq 211$ (subsequently reduced to $n \geq 4$ by B-Ellenberg-Ng).

What can go wrong

If we suppose we have a solution to

$$x^3 + y^3 = z^n,$$

then, in general, all we can prove is that a corresponding Frey curve E is congruent modulo n to a particular elliptic curve F of conductor 72.

What can go wrong

If we suppose we have a solution to

$$x^3 + y^3 = z^n,$$

then, in general, all we can prove is that a corresponding Frey curve E is congruent modulo n to a particular elliptic curve F of conductor 72.

This does enable us to conclude that

- $z \equiv 3$ modulo 6, and
- $n > 10^4$, and
- $n \equiv \pm 1$ modulo 5, etc.

The equation $x^3 + y^6 = z^n$

In this case, we can use Frey-Hellegouarch curves to attack both

$$a^2 + b^3 = c^n \text{ and } a^3 + b^3 = c^n.$$

The equation $x^3 + y^6 = z^n$

In this case, we can use Frey-Hellegouarch curves to attack both

$$a^2 + b^3 = c^n \text{ and } a^3 + b^3 = c^n.$$

These *multi-Frey* methods can sometimes work well!

The equation $x^3 + y^6 = z^n$

In this case, we can use Frey-Hellegouarch curves to attack both

$$a^2 + b^3 = c^n \text{ and } a^3 + b^3 = c^n.$$

These *multi-Frey* methods can sometimes work well!

In this case, careful examination modulo 7 yields the desired result. From the first Frey-Hellegouarch curve, we are able to show that $7 \mid y$. After some work, we find that the second such curve E necessarily has $a_7(E) = \pm 4$, while $a_7(F) = 0$.

The equation $x^2 + y^4 = z^3$

Coprime integer solutions to this equation necessarily have one of

$$y = \pm(s^2 + 3t^2)\left(s^4 - 18s^2t^2 + 9t^4\right), \text{ or}$$

$$y = 6ts(4s^4 - 3t^4), \text{ or}$$

$$y = 6ts(s^4 - 12t^4), \text{ or}$$

$$y = 3(s-t)(s+t)(s^4 + 8ts^3 + 6t^2s^2 + 8t^3s + t^4),$$

for s and t coprime integers satisfying certain conditions modulo 6.

The equation $a^2 + b^{4n} = c^3$

We may conclude that

$$b^n = 3(s-t)(s+t)(s^4 + 8s^3t + 6s^2t^2 + 8st^3 + t^4),$$

where

$$s \not\equiv t \text{ modulo } 2 \quad \text{and} \quad s \not\equiv t \text{ modulo } 3.$$

The equation $a^2 + b^{4n} = c^3$

We may conclude that

$$b^n = 3(s-t)(s+t)(s^4 + 8s^3t + 6s^2t^2 + 8st^3 + t^4),$$

where

$$s \not\equiv t \text{ modulo } 2 \quad \text{and} \quad s \not\equiv t \text{ modulo } 3.$$

We thus deduce the existence of integers A, B and C for which

$$s-t = A^n, \quad s+t = \frac{1}{3}B^n, \quad s^4+8s^3t+6s^2t^2+8st^3+t^4 = -C^n.$$

It follows that

$$A^{4n} - \frac{1}{27} B^{4n} = 2C^n,$$

with ABC odd and $3 \mid B$. There are (at least) three Frey-Hellegouarch curves we can attach to this Diophantine equation:

$$\begin{array}{rcl} E_1 : Y^2 & = & X(X - A^{4n}) \left(X - \frac{B^{4n}}{27} \right), \\ E_2 : Y^2 & = & X^3 + 2A^{2n} X^2 + 2C^n X, \\ E_3 : Y^2 & = & X^3 - \frac{2B^{2n}}{27} X^2 - \frac{2C^n}{27} X. \end{array}$$

The equation $A^{4n} - \frac{1}{27}B^{4n} = 2C^n$

Adding $2B^{4n}$ to both sides of the equation, we find that

$$A^{4n} + \frac{53}{27}B^{4n} = 2(C^n + B^{4n}),$$

and, after some work, that $C + B^4$ is a quadratic non residue modulo 53.

The equation $A^{4n} - \frac{1}{27}B^{4n} = 2C^n$

Adding $2B^{4n}$ to both sides of the equation, we find that

$$A^{4n} + \frac{53}{27}B^{4n} = 2(C^n + B^{4n}),$$

and, after some work, that $C + B^4$ is a quadratic non residue modulo 53.

On the other hand, considering $a_{53}(E_1)$, we find that necessarily

$$(C/B^4)^n \equiv 17 \text{ modulo } 53.$$

The equation $A^{4n} - \frac{1}{27}B^{4n} = 2C^n$

Adding $2B^{4n}$ to both sides of the equation, we find that

$$A^{4n} + \frac{53}{27}B^{4n} = 2(C^n + B^{4n}),$$

and, after some work, that $C + B^4$ is a quadratic non residue modulo 53.

On the other hand, considering $a_{53}(E_1)$, we find that necessarily

$$(C/B^4)^n \equiv 17 \text{ modulo } 53.$$

This is a contradiction for $n \equiv \pm 2, \pm 4 \mod 13$.

Proposition

(BCDY) If n is a positive integer with

$$n \equiv \pm 2 \text{ modulo } 5 \quad \text{or} \quad n \equiv \pm 2, \pm 4 \text{ modulo } 13,$$

then the equation $a^2 + b^{4n} = c^3$ has only the solution $(a, b, c, n) = (1549034, 33, 15613, 2)$ in positive coprime integers.

A final example : the equation $x^3 + y^{3n} = z^2$

This is a much more subtle case, where we appeal to both parametrizations to $a^3 + b^3 = c^2$ as well as Frey curves attached to $a^2 = b^3 + c^n$

A final example : the equation $x^3 + y^{3n} = z^2$

This is a much more subtle case, where we appeal to both parametrizations to $a^3 + b^3 = c^2$ as well as Frey curves attached to $a^2 = b^3 + c^n$

If, for example, z is odd, the parametrizations imply that

$$b^n = s^4 - 4ts^3 - 6t^2s^2 - 4t^3s + t^4$$

and so

$$b^n = (s-t)^4 - 12(st)^2 = U^4 - 12V^2,$$

to which we attach the $\mathbb{Q}$-curve

$$E_{U,V} : y^2 = x^3 + 2(\sqrt{3}-1)Ux^2 + (2-\sqrt{3})(U^2 - 2\sqrt{3}V)x.$$

The equation $x^3 + y^{3n} = z^2$

After much work, one arrives at . . .

Theorem

If $n \equiv 1 \mod 8$ is prime, then the only solution in nonzero integers to the equation

$$x^3 + y^{3n} = z^2$$

is with $x = 2, y = 1$ and $z = \pm 2$.

Darmon's program

Darmon generalizes the notion of *Frey curve* to that of *Frey abelian variety* to provided a framework for analyzing solutions to

$$x^p + y^p = z^r.$$

Darmon's program

Darmon generalizes the notion of *Frey curve* to that of *Frey abelian variety* to provided a framework for analyzing solutions to

$$x^p + y^p = z^r.$$

The technical machinery required to carry out this program for given prime $r > 3$ and arbitrary p is still under development.