The Diophantine Equation $x^p + L^r y^p + z^p = 0$

Mike Bennett

11 July 2016

Recap: The Modularity Theorem

We call a newform **rational** if all its coefficients are in $\mathbb{Q}$, otherwise it is **irrational**.

Theorem (Modularity Theorem)

There is a bijection

$$\text{rational newforms } f \text{ of level } N \longleftrightarrow \text{isogeny classes of elliptic curves of conductor } N.$$

If $f = q + \sum_{n \geq 2} c_n q^n$ *corresponds to* $E/\mathbb{Q}$ *then for all* $\ell \nmid N$

$$c_\ell = a_\ell(E), \qquad a_\ell(E) = \ell + 1 - \#E(\mathbb{F}_\ell).$$

Recap: 'arises from'

Definition

Let

- E be an elliptic curve of conductor N,
- $f = q + \sum_{n \geq 2} c_n q^n$ be a newform of level N',
- $K = \mathbb{Q}(c_2, c_3, \ldots)$,
- $\mathcal{O}_K$ the ring of integers of K,
- p a prime.

We say that E **arises from** f **mod** p and write $E \sim_p f$ if there is some prime ideal $\mathfrak{P} \mid p$ of $\mathcal{O}_K$ such that for all primes ℓ

(i) if $\ell \nmid pNN'$ then $a_\ell(E) \equiv c_\ell \pmod{\mathfrak{P}}$, and

(ii) if $\ell \nmid pN'$ and $\ell \mid\mid N$ then $\ell + 1 \equiv \pm c_\ell \pmod{\mathfrak{P}}$.

Recap: Ribet's Level Lowering Theorem

Let

1. $E/\mathbb{Q}$ be an elliptic curve,
2. $\Delta = \Delta_{\min}$ be the discriminant of a minimal model of E,
3. N be the conductor of E,
4. for a prime p let
$$N_p = N \Bigg/ \prod_{\substack{q \| N, \\ p \mid \mathrm{ord}_q(\Delta)}} q.$$

Theorem (Ribet's Theorem)

- *Let $p \geq 3$ be a prime.*
- *Suppose E does not have any p-isogenies.*
- *Suppose E is modular.*

Then there exists a newform f of level N_p such that $E \sim_p f$.

Frey Curves

Given a Diophantine equation, suppose it has a solution, and associate with it an elliptic curve E called a **Frey curve**, if possible. The key properties of the Frey curve are

- The coefficients of the elliptic curve somehow depend on the solution to the Diophantine equation.
- The minimal discriminant can be written in the form $\Delta = C \cdot D^p$ where D depends on the solution. The factor C **does not depend on the solutions but only on the Diophantine equation**.
- E has multiplicative reduction at the primes dividing D. (i.e. if $p \mid D$ then $p \mid\mid N$).

We conclude

1. The conductor N of E is divisible by primes dividing C and D (depends on the equation and the solution).
2. The primes dividing D can be removed when we write down N_p (depends only on the equation).
3. There are only finitely many possibilities for N_p.
4. For each N_p, there are only finitely many newforms f of level N_p.

Frey Curve

1. The conductor N of E is divisible by primes dividing C and D (depends on the equation and the solution).
2. The primes dividing D can be removed when we write down N_p (depends only on the equation).
3. There are only finitely many possibilities for N_p.
4. For each N_p, there are only finitely many newforms f of level N_p.

Applying Wiles, Ribet and Mazur, we have $E \sim_p f$ for one of finitely many f.

What can we learn about the solution to the Diophantine equation from knowing the finitely many f?

Some Frey Curves

The Frey curves for equations like $Aa^p + Bb^p + Cc^p = 0$ arise from the fact that an elliptic curve with rational torsion containing $\mathbb{Z}_2 \times \mathbb{Z}_2$ may be parametrized in the shape

$$E_{r,s} \ : \ y^2 = x(x+r)(x+s)$$

with discriminant

$$\Delta_{r,s} = 16r^2s^2(r-s)^2.$$

Some Frey Curves

The Frey curves for equations like $Aa^p + Bb^p + Cc^p = 0$ arise from the fact that an elliptic curve with rational torsion containing $\mathbb{Z}_2 \times \mathbb{Z}_2$ may be parametrized in the shape

$$E_{r,s} \ : \ y^2 = x(x+r)(x+s)$$

with discriminant

$$\Delta_{r,s} = 16r^2s^2(r-s)^2.$$

Similarly, elliptic curves with at least one rational 2-torsion point may be parametrized as

$$E_{r,s} \ : \ y^2 = x^3 + rx^2 + sx$$

with discriminant

$$\Delta_{r,s} = 16s^2(r^2 - 4s).$$

Some Frey Curves

Similarly, elliptic curves with at least one rational 2-torsion point may be parametrized as

$$E_{r,s} \; : \; y^2 = x^3 + rx^2 + sx$$

with discriminant

$$\Delta_{r,s} = 16s^2(r^2 - 4s).$$

Some Frey Curves

Similarly, elliptic curves with at least one rational 2-torsion point may be parametrized as

$$E_{r,s} \;:\; y^2 = x^3 + rx^2 + sx$$

with discriminant

$$\Delta_{r,s} = 16s^2(r^2 - 4s).$$

If we want to try to prove something about, for example, the equation

$$a^p + b^p = c^2,$$

we can consider E_{2c,b^p} which has discriminant

$$16b^{2p}(4c^2 - 4b^p) = 64b^{2p}a^p.$$

Some Frey Curves

We can use such an approach to "write down" Frey curves corresponding to equations like

1. $Aa^p + Bb^p = Cc^p$
2. $Aa^p + Bb^p = Cc^2$
3. $Aa^p + Bb^p = Cc^3$
4. $a^q + b^q = Cc^p$, $q = 3, 5$, etc

Some Frey Curves

We can use such an approach to "write down" Frey curves corresponding to equations like

1. $Aa^p + Bb^p = Cc^p$
2. $Aa^p + Bb^p = Cc^2$
3. $Aa^p + Bb^p = Cc^3$
4. $a^q + b^q = Cc^p$, $q = 3, 5$, etc

These lead to further equations like

$$a^2 + b^4 = c^p$$

considered by Ellenberg and others.

The Diophantine Equation $a^p + L^r b^p + c^p = 0$

Let L be an odd prime number. Consider

$$a^p + L^r b^p + c^p = 0, \qquad abc \neq 0, \qquad p \geq 5 \text{ is prime.}$$

We assume that

$$a,\ b,\ c \text{ are coprime}, \qquad 0 < r < p.$$

Let A, B, C be a permutation of a^p, $L^r b^p$, c^p such that

$$2 \mid B, \qquad A \equiv -1 \pmod 4.$$

Let E be the elliptic curve

$$E \ : \ y^2 = x(x - A)(x + B).$$

Then

$$\Delta_{\min} = \frac{L^{2r}(abc)^{2p}}{2^8}, \qquad N = \prod_{\ell \mid Labc} \ell.$$

$$\Delta_{\min} = \frac{L^{2r}(abc)^{2p}}{2^8}, \qquad N = \prod_{q|Labc} q.$$

$$N_p = N \Big/ \prod_{\substack{q||N, \\ p \,|\, \mathrm{ord}_q(\Delta)}} q = 2L.$$

Ribet's Theorem $\implies$ there is a newform f of level $N_p = 2L$ such that $E \sim_p f$.

Theorem

There are no newforms at levels

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 22, 25, 28, 60\,.$$

Therefore the equation

$$a^p + L^r b^p + c^p = 0, \qquad abc \neq 0, \qquad p \geq 5 \text{ is prime.}$$

has no solutions for $L = 3$, 5, 11.
What can we do for other values of L? Say $L = 19$, so $N_p = 38$.
There are two newforms of level 38:

$$f_1 = q - q^2 + q^3 + q^4 - q^6 - q^7 + \cdots$$
$$f_2 = q + q^2 - q^3 + q^4 - 4q^5 - q^6 + 3q^7 + \cdots$$

No contradiction yet.

Bounding the Exponent

$$E \ : \ y^2 = x(x-A)(x+B).$$

$$N = \prod_{\ell \mid 19abc} \ell, \qquad N_p = 38.$$

$$f_1 = q - q^2 + q^3 + q^4 - q^6 - q^7 + \cdots$$
$$f_2 = q + q^2 - q^3 + q^4 - 4q^5 - q^6 + 3q^7 + \cdots$$

$E \sim_p f = q + \sum_{n \geq 2} c_n q^n$, where f is one of f_1, f_2. Suppose $\ell \nmid 38$.

(i) If $\ell \nmid abc$ then $a_\ell(E) \equiv c_\ell \pmod{p}$.

(ii) If $\ell \mid abc$ then $\ell + 1 \equiv \pm c_\ell \pmod{p}$.

What do we know about $a_\ell(E)$?

$$E \ : \ y^2 = x(x-A)(x+B)$$

has conductor N. Suppose $\ell \nmid N$. Then

$$-2\sqrt{\ell} \le a_\ell(E) \le 2\sqrt{\ell} \qquad \textbf{Hasse–Weil Bound}.$$

Also, $4 \mid \#E(\mathbb{F}_\ell)$. But

$$\ell + 1 - a_\ell(E) = \#E(\mathbb{F}_\ell) \equiv 0 \pmod 4.$$

So

$$\ell + 1 \equiv a_\ell(E) \pmod 4.$$

Conclusion: If $\ell \nmid N$ then

$$a_\ell(E) \in S_\ell := \{a \in \mathbb{Z} \ : \ -2\sqrt{\ell} \le a \le 2\sqrt{\ell}, \qquad \ell + 1 \equiv a \pmod 4\}.$$

$$N = \prod_{\ell \mid 19abc} \ell, \qquad N_p = 38.$$

$E \sim_p f = q + \sum_{n \geq 2} c_n q^n$, where f is one of f_1, f_2. Suppose $\ell \nmid 38$.

(i) If $\ell \nmid abc$ then $a_\ell(E) \equiv c_\ell \pmod{p}$.

(ii) If $\ell \mid abc$ then $\ell + 1 \equiv \pm c_\ell \pmod{p}$.

If $\ell \nmid abc$ then

$$a_\ell(E) \in S_\ell := \{a \in \mathbb{Z} \,:\, -2\sqrt{\ell} \leq a \leq 2\sqrt{\ell}, \qquad \ell + 1 \equiv a \pmod{4}\}.$$

So $p \mid B_\ell(f)$ where

$$B_\ell(f) = (\ell + 1 - c_\ell)(\ell + 1 + c_\ell) \cdot \prod_{a \in S_\ell} (a - c_\ell).$$

$$S_\ell := \{a \in \mathbb{Z} \ : \ -2\sqrt{\ell} \le a \le 2\sqrt{\ell}, \qquad \ell + 1 \equiv a \pmod 4\}.$$

So $p \mid B_\ell(f)$ where

$$B_\ell(f) = (\ell + 1 - c_\ell)(\ell + 1 + c_\ell) \cdot \prod_{a \in S_\ell} (a - c_\ell),$$

and $f = f_1$ or f_2.

$$f_1 = q - q^2 + q^3 + q^4 - q^6 - q^7 + \cdots$$
$$f_2 = q + q^2 - q^3 + q^4 - 4q^5 - q^6 + 3q^7 + \cdots$$

Letting $\ell = 3$, we have

$$B_3(f_1) = -15, \qquad B_3(f_2) = 15.$$

So $p = 5$.

So $p \leq 5$. Is that all?

Well, if we go ahead and compute $B_5(f_1)$, we find that $B_5(f_1) = -144$ and

$$\gcd(B_3(f_1), B_5(f_1)) = \gcd(-15, -144) = 3,$$

so $E \not\sim_p f_1 \qquad\qquad (p \geq 5)$.

So $p \leq 5$. Is that all?

Well, if we go ahead and compute $B_5(f_1)$, we find that $B_5(f_1) = -144$ and

$$\gcd(B_3(f_1), B_5(f_1)) = \gcd(-15, -144) = 3,$$

so $E \not\sim_p f_1 \qquad\qquad (p \geq 5)$.

Eliminated f_1.

A Variant of the Fermat Equation

Suppose

$$x^p + 19^r y^p + z^p = 0, \qquad xyz \neq 0, \quad p \geq 5 \text{ is prime},$$

has a non-trivial solution. Then $E \sim_p f_2$. But

$$B_3(f_2) = 15, \quad B_5(f_2) = 240, \quad B_7(f_2) = 1155, \quad B_{11}(f_2) = 3360$$
$$\implies p = 5.$$

A Variant of the Fermat Equation

Suppose

$$x^p + 19^r y^p + z^p = 0, \qquad xyz \neq 0, \quad p \geq 5 \text{ is prime},$$

has a non-trivial solution. Then $E \sim_p f_2$. But

$$B_3(f_2) = 15, \quad B_5(f_2) = 240, \quad B_7(f_2) = 1155, \quad B_{11}(f_2) = 3360$$
$$\implies p = 5.$$

Is $B_\ell(f_2)$ always divisible by 5?

A Variant of the Fermat Equation

Suppose

$$x^p + 19^r y^p + z^p = 0, \qquad xyz \neq 0, \quad p \geq 5 \text{ is prime},$$

has a non-trivial solution. Then $E \sim_p f_2$. But

$$B_3(f_2) = 15, \quad B_5(f_2) = 240, \quad B_7(f_2) = 1155, \quad B_{11}(f_2) = 3360$$
$$\implies p = 5.$$

Is $B_\ell(f_2)$ always divisible by 5?

$$\text{newform } f_2 \longleftrightarrow \text{elliptic curve } F = 38B1.$$

A Variant of the Fermat Equation

Suppose

$$x^p + 19^r y^p + z^p = 0, \qquad xyz \neq 0, \quad p \geq 5 \text{ is prime},$$

has a non-trivial solution. Then $E \sim_p f_2$. But

$$B_3(f_2) = 15, \quad B_5(f_2) = 240, \quad B_7(f_2) = 1155, \quad B_{11}(f_2) = 3360$$
$$\Longrightarrow p = 5.$$

Is $B_\ell(f_2)$ always divisible by 5?

newform $f_2 \longleftrightarrow$ elliptic curve $F = 38B1$.

$$\#F(\mathbb{Q})_{\text{tors}} = 5 \Longrightarrow 5 \mid (\ell + 1 - c_\ell)$$
$$\Longrightarrow 5 \mid B_\ell(f_2) := (\ell + 1 - c_\ell)(\ell + 1 + c_\ell) \prod_{a \in S_\ell} (a - c_\ell).$$

Eliminating $p = 5$

Suppose $p = 5$. Want a contradiction.

Eliminating $p = 5$

Suppose $p = 5$. Want a contradiction.

$$\ell \nmid NN' \implies a_\ell(E) \equiv c_\ell \pmod{5}.$$

Eliminating $p = 5$

Suppose $p = 5$. Want a contradiction.

$$\ell \nmid NN' \implies a_\ell(E) \equiv c_\ell \pmod{5}.$$

$$\#E(\mathbb{F}_\ell) = \ell + 1 - a_\ell(E) \equiv \ell + 1 - c_\ell \equiv 0 \pmod{5}.$$

Eliminating $p = 5$

Suppose $p = 5$. Want a contradiction.

$$\ell \nmid NN' \Longrightarrow a_\ell(E) \equiv c_\ell \pmod{5}.$$

$$\#E(\mathbb{F}_\ell) = \ell + 1 - a_\ell(E) \equiv \ell + 1 - c_\ell \equiv 0 \pmod{5}.$$

Čebotarev Density Theorem $\Longrightarrow$ E has a 5-isogeny.

Eliminating $p = 5$

Suppose $p = 5$. Want a contradiction.

$$\ell \nmid NN' \implies a_\ell(E) \equiv c_\ell \pmod 5.$$

$$\#E(\mathbb{F}_\ell) = \ell + 1 - a_\ell(E) \equiv \ell + 1 - c_\ell \equiv 0 \pmod 5.$$

Čebotarev Density Theorem $\implies$ E has a 5-isogeny.

But E is semi-stable and has full 2-torsion. **Mazur's Theorem gives contradiction.**

Eliminating $p = 5$

Suppose $p = 5$. Want a contradiction.

$$\ell \nmid NN' \implies a_\ell(E) \equiv c_\ell \pmod{5}.$$

$$\#E(\mathbb{F}_\ell) = \ell + 1 - a_\ell(E) \equiv \ell + 1 - c_\ell \equiv 0 \pmod{5}.$$

Čebotarev Density Theorem $\implies$ E has a 5-isogeny.

But E is semi-stable and has full 2-torsion. **Mazur's Theorem gives contradiction.**

The equation

$$x^p + 19^r y^p + z^p = 0, \qquad xyz \neq 0, \quad p \geq 5 \text{ is prime},$$

has no solutions.

$p = 3$?

Note that we cannot extend this to the case $p = 3$.

$p = 3$?

Note that we cannot extend this to the case $p = 3$.

We have

$$8^3 + 19 \cdot (-3)^3 + 1^3 = 0.$$

$p = 3$?

Note that we cannot extend this to the case $p = 3$.

We have

$$8^3 + 19 \cdot (-3)^3 + 1^3 = 0.$$

In fact, the elliptic curve corresponding to

$$x^p + 19^r y^p + z^p = 0$$

has rank 2 if $r = 1$ (and rank 0 for $r = 2$).

Mazur

Using similar ideas, Mazur proved the following.

Theorem (Mazur)

Let L be an odd prime that is neither a Fermat prime nor a Mersenne prime. Then there is a positive C_L such that the following holds: the only solutions to the equation

$$a^p + L^r b^p + c^p = 0$$

with $p > C_L$ satisfy $abc = 0$.

For details of the proof, see the notes.

How did we "know" this would work?

We had that

$$p \mid B_\ell(f) := (\ell + 1 - c_\ell)(\ell + 1 + c_\ell) \prod_{a \in S_\ell} (a - c_\ell),$$

for some f from a finite set and ℓ "nice". The S_ℓ is the set of "possible" Fourier coefficients of our Frey curve.

How did we "know" this would work?

We had that

$$p \mid B_\ell(f) := (\ell + 1 - c_\ell)(\ell + 1 + c_\ell) \prod_{a \in S_\ell} (a - c_\ell),$$

for some f from a finite set and ℓ "nice". The S_ℓ is the set of "possible" Fourier coefficients of our Frey curve.

The only way this can fail to bound p is if we have $B_\ell(f) = 0$ for *every* suitable ℓ.

How did we "know" this would work?

We had that

$$p \mid B_\ell(f) := (\ell + 1 - c_\ell)(\ell + 1 + c_\ell) \prod_{a \in S_\ell} (a - c_\ell),$$

for some f from a finite set and ℓ "nice". The S_ℓ is the set of "possible" Fourier coefficients of our Frey curve.

The only way this can fail to bound p is if we have $B_\ell(f) = 0$ for *every* suitable ℓ.

We claim that this can never happen if f is an *irrational* form, if our Frey curve is defined over $\mathbb{Q}$ (Sturm bounds!).

How did we “know” this would work?

We had that

$$p \mid B_\ell(f) := (\ell + 1 - c_\ell)(\ell + 1 + c_\ell) \prod_{a \in S_\ell} (a - c_\ell),$$

for some f from a finite set and ℓ “nice”. The S_ℓ is the set of “possible” Fourier coefficients of our Frey curve.

The only way this can fail to bound p is if we have $B_\ell(f) = 0$ for *every* suitable ℓ.

We claim that this can never happen if f is an *irrational* form, if our Frey curve is defined over $\mathbb{Q}$ (Sturm bounds!).

It can also never happen if, say, our Frey curve (defined over $\mathbb{Q}$) has a rational 2-torsion point and f is a *rational* form, corresponding to and elliptic curve without rational 2-torsion.