Twisted Extensions of Fermat’s Last Theorem

Carmen Bruni

University of British Columbia

June 7th, 2014
Today, I will present known solutions of $x^3 + y^3 = p^\alpha z^n$ with $p$ a given prime and $\alpha \geq 1$ an integer.

**Definition**

Let $S$ be the set of primes $p \geq 5$ for which there exists an elliptic curve $E$ with conductor $N_E \in \{18p, 36p, 72p\}$ with at least one non-trivial rational 2-torsion point.
Today, I will present known solutions of $x^3 + y^3 = p^\alpha z^n$ with $p$ a given prime and $\alpha \geq 1$ an integer.

**Definition**

Let $S$ be the set of primes $p \geq 5$ for which there exists an elliptic curve $E$ with conductor $N_E \in \{18p, 36p, 72p\}$ with at least one non-trivial rational 2-torsion point.
Today, I will present known solutions of $x^3 + y^3 = p^\alpha z^n$ with $p$ a given prime and $\alpha \geq 1$ an integer.

**Definition**

Let $S$ be the set of primes $p \geq 5$ for which there exists an elliptic curve $E$ with conductor $N_E \in \{18p, 36p, 72p\}$ with at least one non-trivial rational 2-torsion point.
Today, I will present known solutions of \( x^3 + y^3 = p^\alpha z^n \) with \( p \) a given prime and \( \alpha \geq 1 \) an integer.

**Definition**

Let \( S \) be the set of primes \( p \geq 5 \) for which there exists an elliptic curve \( E \) with conductor \( N_E \in \{18p, 36p, 72p\} \) with at least one non-trivial rational 2-torsion point.
Today, I will present known solutions of \( x^3 + y^3 = p^\alpha z^n \) with \( p \) a given prime and \( \alpha \geq 1 \) an integer.

**Definition**

Let \( S \) be the set of primes \( p \geq 5 \) for which there exists an elliptic curve \( E \) with conductor \( N_E \in \{18p, 36p, 72p\} \) with at least one non-trivial rational 2-torsion point.

- The set \( S \) contains the primes between 5 and 193 (the first exception is 197).
Today, I will present known solutions of $x^3 + y^3 = p^\alpha z^n$ with $p$ a given prime and $\alpha \geq 1$ an integer.

**Definition**

Let $S$ be the set of primes $p \geq 5$ for which there exists an elliptic curve $E$ with conductor $N_E \in \{18p, 36p, 72p\}$ with at least one non-trivial rational 2-torsion point.

- The set $S$ contains the primes between 5 and 193 (the first exception is 197).
- It is not known if $S$ is infinite.
Today, I will present known solutions of $x^3 + y^3 = p^\alpha z^n$ with $p$ a given prime and $\alpha \geq 1$ an integer.

**Definition**

Let $S$ be the set of primes $p \geq 5$ for which there exists an elliptic curve $E$ with conductor $N_E \in \{18p, 36p, 72p\}$ with at least one non-trivial rational 2-torsion point.

- The set $S$ contains the primes between 5 and 193 (the first exception is 197).
- It is not known if $S$ is infinite.
- It is known that the complement is infinite. It can be shown that if $p \equiv 317, 1757 \pmod{2040}$ then $p \notin S$. 
Today, I will present known solutions of \( x^3 + y^3 = p^\alpha z^n \) with \( p \) a given prime and \( \alpha \geq 1 \) an integer.

**Definition**

Let \( S \) be the set of primes \( p \geq 5 \) for which there exists an elliptic curve \( E \) with conductor \( N_E \in \{18p, 36p, 72p\} \) with at least one non-trivial rational 2-torsion point.

- The set \( S \) contains the primes between 5 and 193 (the first exception is 197).
- It is not known if \( S \) is infinite.
- It is known that the complement is infinite. It can be shown that if \( p \equiv 317, 1757 \pmod{2040} \) then \( p \notin S \).
- In fact, the complement of \( S \) forms a set of density one in the primes.
<table>
<thead>
<tr>
<th>Reminder</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Definition</strong></td>
</tr>
<tr>
<td>Let $S$ be the set of primes $p \geq 5$ for which there exists an elliptic curve $E$ with conductor $N_E \in {18p, 36p, 72p}$ with at least one non-trivial rational 2-torsion point.</td>
</tr>
</tbody>
</table>
Reminder

Definition

Let $S$ be the set of primes $p \geq 5$ for which there exists an elliptic curve $E$ with conductor $N_E \in \{18p, 36p, 72p\}$ with at least one non-trivial rational 2-torsion point.

Theorem (Bennett, Luca, Mulholland - 2011)

Suppose $p \geq 5$ is prime and $p \notin S$. Let $\alpha \geq 1, \alpha \in \mathbb{Z}$. Then the equation

$$x^3 + y^3 = p^\alpha z^n$$

has no solution in coprime nonzero $x, y, z \in \mathbb{Z}$ and prime $n$ with $n \geq p^{2p}$. 

Carmen Bruni
Twisted Extensions of Fermat's Last Theorem
Reminder

Definition
Let $S$ be the set of primes $p \geq 5$ for which there exists an elliptic curve $E$ with conductor $N_E \in \{18p, 36p, 72p\}$ with at least one non-trivial rational 2-torsion point.

Theorem (Bennett, Luca, Mulholland - 2011)

Suppose $p \geq 5$ is prime and $p \not\in S$. Let $\alpha \geq 1$, $\alpha \in \mathbb{Z}$. Then the equation

$$x^3 + y^3 = p^\alpha z^n$$

has no solution in coprime nonzero $x, y, z \in \mathbb{Z}$ and prime $n$ with $n \geq p^{2p}$.

What about primes in $S$?
Suppose we have a solution to our Diophantine equation, say 
\[ a^3 + b^3 = p^\alpha c^n. \]
Suppose we have a solution to our Diophantine equation, say \( a^3 + b^3 = p^\alpha c^n \).

Associate to this solution a Frey curve \( E_{a,b} : y^2 = f(x) \) where

\[
f(x) := (x + b - a)(x^2 + (a - b)x + (a^2 + ab + b^2))
\]
Suppose we have a solution to our Diophantine equation, say \( a^3 + b^3 = p^\alpha c^n \).

Associate to this solution a Frey curve \( E_{a,b} : y^2 = f(x) \) where

\[
    f(x) := (x + b - a)(x^2 + (a - b)x + (a^2 + ab + b^2))
\]

This last quadratic has discriminant \(-3(a + b)^2\) and hence splits completely over \( \mathbb{F}_\ell \) when \( \left( \frac{-3}{\ell} \right) = 1 \), that is when \( \ell \equiv 1 \pmod{6} \).
Suppose we have a solution to our Diophantine equation, say $a^3 + b^3 = p^\alpha c^n$.

Associate to this solution a Frey curve $E_{a,b} : y^2 = f(x)$ where

$$f(x) := (x + b - a)(x^2 + (a - b)x + (a^2 + ab + b^2))$$

This last quadratic has discriminant $-3(a + b)^2$ and hence splits completely over $\mathbb{F}_\ell$ when $\left(\frac{-3}{\ell}\right) = 1$, that is when $\ell \equiv 1 \pmod{6}$.

Hence, $4 \mid \#E_{a,b}(\mathbb{F}_\ell)$ and thus

$$a_\ell(E_{a,b}) := \ell + 1 - \#E_{a,b}(\mathbb{F}_\ell) \equiv \ell + 1 \pmod{4}.$$
Suppose we have a solution to our Diophantine equation, say \( a^3 + b^3 = p^\alpha c^n \).

Associate to this solution a Frey curve \( E_{a,b} : y^2 = f(x) \) where

\[
f(x) := (x + b - a)(x^2 + (a - b)x + (a^2 + ab + b^2))
\]

This last quadratic has discriminant \(-3(a + b)^2\) and hence splits completely over \( \mathbb{F}_\ell \) when \(( \frac{-3}{\ell} ) = 1\), that is when \( \ell \equiv 1 \pmod{6} \).

Hence, \( 4 \mid \#E_{a,b}(\mathbb{F}_\ell) \) and thus

\[
a_\ell(E_{a,b}) := \ell + 1 - \#E_{a,b}(\mathbb{F}_\ell) \equiv \ell + 1 \pmod{4}.
\]

Ribet’s level lowering applied to \( E_{a,b} \) gives us a newform \( f \) of level \( 18p, 36p \) or \( 72p \). When the newform is irrational or if the newform is rational and does not have two torsion, we can show that \( n \leq p^{2p} \).
For rational newforms with two torsion, suppose that the associated elliptic curve $F$ has the property that $a_\ell(F) \not\equiv \ell + 1 \pmod{4}$ for some prime $\ell \equiv 1 \pmod{6}$. 

Ribet's level lowering gives us that $n \mid (a_\ell(E_{a,b}) - a_\ell(F))$ for all but finitely many primes $\ell$. We already know that $a_\ell(E_{a,b}) \equiv \ell + 1 \not\equiv a_\ell(F) \pmod{4}$. A result of Kraus states that a prime where they differ must occur at some value of $\ell \leq p^2$ and thus the Hasse bound says that this difference at $\ell$ is small compared to $p^2$. Hence in this case we get an additional restriction on $n$. Our goal is thus to classify the following set.
For rational newforms with two torsion, suppose that the associated elliptic curve $F$ has the property that $a_\ell(F) \not\equiv \ell + 1 \pmod{4}$ for some prime $\ell \equiv 1 \pmod{6}$.

Ribet’s level lowering gives us that $n \mid (a_\ell(E_{a,b}) - a_\ell(F))$ for all but finitely many primes $\ell$. 
For rational newforms with two torsion, suppose that the associated elliptic curve $F$ has the property that $a_\ell(F) \not\equiv \ell + 1 \pmod{4}$ for some prime $\ell \equiv 1 \pmod{6}$.

Ribet’s level lowering gives us that $n | (a_\ell(E_{a,b}) - a_\ell(F))$ for all but finitely many primes $\ell$.

We already know that $a_\ell(E_{a,b}) \equiv \ell + 1 \not\equiv a_\ell(F) \pmod{4}$. A result of Kraus states that a prime where they differ must occur at some value of $\ell \leq p^2$ and thus the Hasse bound says that this difference at $\ell$ is small compared to $p^{2p}$.
For rational newforms with two torsion, suppose that the associated elliptic curve $F$ has the property that $a_\ell(F) \not\equiv \ell + 1 \pmod{4}$ for some prime $\ell \equiv 1 \pmod{6}$.

Ribet’s level lowering gives us that $n \mid (a_\ell(E_{a,b}) - a_\ell(F))$ for all but finitely many primes $\ell$.

We already know that $a_\ell(E_{a,b}) \equiv \ell + 1 \not\equiv a_\ell(F) \pmod{4}$. A result of Kraus states that a prime where they differ must occur at some value of $\ell \leq p^2$ and thus the Hasse bound says that this difference at $\ell$ is small compared to $p^{2p}$.

Hence in this case we get an additional restriction on $n$. Our goal is thus to classify the following set.
The set $\mathcal{P}_b$

**Definition**

Let $\mathcal{P}_b$ be the set of primes $p \geq 5$ such that for every elliptic curve $E$ with conductor $N_E \in \{18p, 36p, 72p\}$ we have that $4 \nmid \#E_{\text{tor}}(\mathbb{Q})$ and at least one curve having a non-trivial rational 2-torsion point. Also, at all curves $F$ with non-trivial rational 2-torsion, we require that there exists a prime $\ell \equiv 1 \pmod{6}$ such that $a_\ell(F) \not\equiv \ell + 1 \pmod{4}$. Note $\mathcal{P}_b \subset S$. 

Carmen Bruni  
Twisted Extensions of Fermat’s Last Theorem
The set \( \mathcal{P}_b \)

**Definition**

Let \( \mathcal{P}_b \) be the set of primes \( p \geq 5 \) such that for every elliptic curve \( E \) with conductor \( N_E \in \{18p, 36p, 72p\} \) we have that \( 4 \nmid \#E_{\text{tor}}(\mathbb{Q}) \) and at least one curve having a non-trivial rational 2-torsion point. Also, at all curves \( F \) with non-trivial rational 2-torsion, we require that there exists a prime \( \ell \equiv 1 \pmod{6} \) such that \( a_\ell(F) \not\equiv \ell + 1 \pmod{4} \). Note \( \mathcal{P}_b \subset S \).

For \( p = 53 \),

<table>
<thead>
<tr>
<th>Curve</th>
<th>Equation</th>
<th>( t )</th>
</tr>
</thead>
<tbody>
<tr>
<td>954b1</td>
<td>([1,-1,0,12,-100])</td>
<td>2</td>
</tr>
<tr>
<td>954b2</td>
<td>([1,-1,0,-258,-1450])</td>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Curve</th>
<th>Equation</th>
<th>( t )</th>
</tr>
</thead>
<tbody>
<tr>
<td>954g1</td>
<td>([1,-1,1,1,3])</td>
<td>2</td>
</tr>
<tr>
<td>954g2</td>
<td>([1,-1,1,-29,63])</td>
<td>2</td>
</tr>
</tbody>
</table>

**Hecke Eigenvalues**

**Hecke Eigenvalues for elliptic curve 954b1**

| \(-2\) | \(-3\) | \(-5\) | \(-7\) | \(-9\) | \(-11\) | \(-13\) | \(-17\) | \(-19\) | \(-23\) | \(-29\) | \(-31\) | \(-37\) | \(-41\) | \(-43\) | \(-47\) | \(-53\) | \(-59\) | \(-61\) | \(-67\) | \(-71\) | \(-73\) | \(-79\) | \(-83\) | \(-89\) | \(-97\) |
|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|

**Hecke Eigenvalues for elliptic curve 954g1**

| \(-2\) | \(-3\) | \(-5\) | \(-7\) | \(-9\) | \(-11\) | \(-13\) | \(-17\) | \(-19\) | \(-23\) | \(-29\) | \(-31\) | \(-37\) | \(-41\) | \(-43\) | \(-47\) | \(-53\) | \(-59\) | \(-61\) | \(-67\) | \(-71\) | \(-73\) | \(-79\) | \(-83\) | \(-89\) | \(-97\) |
|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|
| + 2    | + 2    | + 2    | + 2    | + 2    | + 2    | + 2    | + 2    | + 2    | + 2    | + 2    | + 2    | + 2    | + 2    | + 2    | + 2    | + 2    | + 2    | + 2    | + 2    | + 2    | + 2    | + 2    | + 2    | + 2    | + 2    |

**Hecke Eigenvalues for elliptic curve 1908b1**

| \(-2\) | \(-3\) | \(-5\) | \(-7\) | \(-9\) | \(-11\) | \(-13\) | \(-17\) | \(-19\) | \(-23\) | \(-29\) | \(-31\) | \(-37\) | \(-41\) | \(-43\) | \(-47\) | \(-53\) | \(-59\) | \(-61\) | \(-67\) | \(-71\) | \(-73\) | \(-79\) | \(-83\) | \(-89\) | \(-97\) |
|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|
| + 0    | + 0    | + 0    | + 0    | + 0    | + 0    | + 0    | + 0    | + 0    | + 0    | + 0    | + 0    | + 0    | + 0    | + 0    | + 0    | + 0    | + 0    | + 0    | + 0    | + 0    | + 0    | + 0    | + 0    | + 0    | + 0    |
The set $\mathcal{P}_b$

**Definition**

Let $\mathcal{P}_b$ be the set of primes $p \geq 5$ such that for every elliptic curve $E$ with conductor $N_E \in \{18p, 36p, 72p\}$ we have that $4 \nmid \#E_{tor}(\mathbb{Q})$ and at least one curve having a non-trivial rational 2-torsion point. Also, at all curves $F$ with non-trivial rational 2-torsion, we require that there exists a prime $\ell \equiv 1 \pmod{6}$ such that $a_\ell(F) \not\equiv \ell + 1 \pmod{4}$. Note $\mathcal{P}_b \subset S$.

- Primes in $\mathcal{P}_b$ include 53, 83, 149, 167, 173, 199, ... (sequence A212420 in OEIS).
Definition

Let $\mathcal{P}_b$ be the set of primes $p \geq 5$ such that for every elliptic curve $E$ with conductor $N_E \in \{18p, 36p, 72p\}$ we have that $4 \nmid \#E_{tor}(\mathbb{Q})$ and at least one curve having a non-trivial rational 2-torsion point. Also, at all curves $F$ with non-trivial rational 2-torsion, we require that there exists a prime $\ell \equiv 1 \pmod{6}$ such that $a_\ell(F) \not\equiv \ell + 1 \pmod{4}$. Note $\mathcal{P}_b \subset S$.

- Primes in $\mathcal{P}_b$ include 53, 83, 149, 167, 173, 199, ... (sequence A212420 in OEIS).
- Classifying these points gives the following theorem.
New Result

Carmen Bruni

Twisted Extensions of Fermat’s Last Theorem
**Theorem (B. 2014?)**

Suppose that \( p \in S \) and that for each curve of conductor \( \{18p, 36p, 72p\} \), we have that the rational torsion subgroup is not divisible by 4. Then \( p \in \mathcal{P}_b \) if and only if every elliptic curve with conductor in \( \{18p, 36p, 72p\} \) and non-trivial rational two torsion has discriminant not of the form \(-3m^2\) for any integer \( m \).
Theorem (B. 2014?)

Suppose that $p \in S$ and that for each curve of conductor $\{18p, 36p, 72p\}$, we have that the rational torsion subgroup is not divisible by 4. Then $p \in P_b$ if and only if every elliptic curve with conductor in $\{18p, 36p, 72p\}$ and non-trivial rational two torsion has discriminant not of the form $-3m^2$ for any integer $m$. In fact, we can also give the type of such primes that are in $S$ but not in $P_b$. 

Carmen Bruni
Twisted Extensions of Fermat’s Last Theorem
Theorem (B. 2014?)

Suppose that \( p \in S \) and that for each curve of conductor \( \{18p, 36p, 72p\} \), we have that the rational torsion subgroup is not divisible by 4. Then \( p \in \mathcal{P}_b \) if and only if every elliptic curve with conductor in \( \{18p, 36p, 72p\} \) and non-trivial rational two torsion has discriminant not of the form \(-3m^2\) for any integer \( m \). In fact, we can also give the type of such primes that are in \( S \) but not in \( \mathcal{P}_b \).

Hence, we have

Theorem (B. 2014?)

Suppose \( p \geq 5 \) is prime and \( p \in \mathcal{P}_b \subset S \). Let \( \alpha \geq 1, \alpha \in \mathbb{Z} \). Then the equation \( x^3 + y^3 = p^\alpha z^n \) has no solution in coprime nonzero \( x, y, z \in \mathbb{Z} \) and prime \( n \) with \( n \geq p^{2p} \).
Primes in $S$

$p = 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 47, 67, 73, 193, 1153$

$p = 3^a3^b \pm 1$,

$p = |3^t2^a \pm 2^a|$, $n = 1$ or the least prime divisor of $n$ is 7.

$p = 3^t2^a \pm 2^a$, $n = 3$ and $p \equiv 1 \pmod 4$, $n = 1$ or the least prime divisor of $n$ is 7.
Primes in $S$

- $p = 5, 7, 11, 13, 17, 19, 23, 29, 31, 47, 67, 73, 193, 1153$
- $p = 2^a 3^b \pm 1$
- $p = |3^b \pm 2^a|$ 
- $p^n = |t^2 \pm 2^a 3^b|, \ n = 1$ or the least prime divisor of $n$ is 7.
- $3^b p = t^2 + 2^a$
- $p = |3t^2 \pm 2^a|$
- $p = t^2 + 4 \cdot 3^b$
- $p = |t^2 - 4 \cdot 3^{2b+1}|$
- $4p = t^2 + 3^{2b+1}$
- $4p^n = 3t^2 + 1$ and $p \equiv 1 \pmod{4}, \ n = 1, 2$
- $p = 3t^2 - 2^a$ with $a = 2, 4, 5$
- $3^b p^n = t^2 + 32, \ n = 1$ or the least prime divisor of $n$ is 7.
- $p = 3t^2 + 2^a$ and $a = 2, 4, 5$
Primes to avoid to be in $\mathcal{P}_b$

- $p = 5, 7, 11, 13, 17, 19, 23, 29, 31, 47, 67, 73, 193, 1153$
- $p = 2^a3^b \pm 1$
- $p = |3^b \pm 2^a|$
- $p^n = \pm (t^2 - 2^a3^b)$, $n = 1$, and $a, b$ not both even, $a \neq 4$.
- $3^b p = t^2 + 2^a$, $t \neq \pm 1$
- $p = |3t^2 \pm 2^a|$
- $p = t^2 + 4 \cdot 3^b$, $b$ even
- $p = |t^2 - 4 \cdot 3^{2b+1}|$
- $4p = t^2 + 3^{2b+1}$
- $4p^n = 3t^2 + 1$ and $p \equiv 1 \pmod{4}$, $n = 1, 2$
- $p = 3t^2 - 2^a$ with $a = 2, 4, 5$
- $3^b p^n = t^2 + 32$, $n = 1$ or the least prime divisor of $n$ is 7.
- $p = 3t^2 + 2^a$ and $a = 2, 4, 5$
First, suppose that $p \in \mathcal{P}_b \subset S$ and assume towards a contradiction that $\Delta_E = -3m^2$. 

We may assume that any $E$ with conductor in \{18p, 36p, 72p\} and with a non-trivial 2 torsion point has the form $E: y^2 = x(x^2 + a^2x + a^4)$. 

By definition, there exists a prime $\ell \equiv 1 \pmod{6}$ such that $4 \nmid \# E(F_\ell)$. 

The discriminant of the quadratic above has the form $\Delta_q = -3k^2$ for some $k | m$. 

Since $\ell \equiv 1 \pmod{6}$, this quadratic splits in $F_\ell$ and thus $4 \nmid \# E(F_\ell)$, a contradiction.
First, suppose that $p \in \mathcal{P}_b \subset S$ and assume towards a contradiction that $\Delta_E = -3m^2$.

We may assume that any $E$ with conductor in \{18p, 36p, 72p\} and with a non-trivial 2 torsion point has the form

$$E : y^2 = x(x^2 + a_2x + a_4)$$
First, suppose that $p \in \mathcal{P}_b \subset S$ and assume towards a contradiction that $\Delta_E = -3m^2$.

We may assume that any $E$ with conductor in $\{18p, 36p, 72p\}$ and with a non-trivial 2 torsion point has the form

$$E : y^2 = x(x^2 + a_2x + a_4)$$

By definition, there exists a prime $\ell \equiv 1 \pmod{6}$ such that $4 \nmid \#E(\mathbb{F}_\ell)$. 

Carmen Bruni
Twisted Extensions of Fermat’s Last Theorem
First, suppose that $p \in \mathcal{P}_b \subset S$ and assume towards a contradiction that $\Delta_E = -3m^2$.

We may assume that any $E$ with conductor in $\{18p, 36p, 72p\}$ and with a non-trivial 2 torsion point has the form

$$E : y^2 = x(x^2 + a_2x + a_4)$$

By definition, there exists a prime $\ell \equiv 1 \pmod{6}$ such that $4 \nmid \#E(\mathbb{F}_\ell)$.

The discriminant of the quadratic above has the form $\Delta_q = -3k^2$ for some $k \mid m$. 

Carmen Bruni
Twisted Extensions of Fermat’s Last Theorem
First, suppose that $p \in \mathcal{P}_b \subset S$ and assume towards a contradiction that $\Delta_E = -3m^2$.

We may assume that any $E$ with conductor in $\{18p, 36p, 72p\}$ and with a non-trivial 2 torsion point has the form

$$E : y^2 = x(x^2 + a_2x + a_4)$$

By definition, there exists a prime $\ell \equiv 1 \pmod{6}$ such that $4 \nmid \#E(\mathbb{F}_\ell)$.

The discriminant of the quadratic above has the form $\Delta_q = -3k^2$ for some $k \mid m$.

Since $\ell \equiv 1 \pmod{6}$, this quadratic splits in $\mathbb{F}_\ell$ and thus $4 \mid \#E(\mathbb{F}_\ell)$, a contradiction.
For the opposite direction, suppose that $\Delta_E = -3m^2$. We want that $p \in \mathcal{P}_b$. 

This can be accomplished.
For the opposite direction, suppose that $\Delta_E = -3m^2$. We want that $p \in \mathcal{P}_b$.

To show this, we are looking for a prime $\ell \equiv 1 \pmod{6}$ so that the curve does not split and does not contain a point of order 4 in $\mathbb{F}_\ell$. 

Look at the numerator of $x(2P)$, which is $(x^2 - a^4)^2$. We want an $\ell$ where $a^4$ is a non-quadratic residue modulo $\ell$ (this gives the 2 torsion criteria), $\Delta_E$ is a non-quadratic residue modulo $\ell$ (this prevents the original elliptic curve from splitting) and $-3$ is a quadratic residue modulo $\ell$ (this is $\ell \equiv 1 \pmod{6}$). 

This can be accomplished.
For the opposite direction, suppose that $\Delta_E = -3m^2$. We want that $p \in \mathcal{P}_b$.

To show this, we are looking for a prime $\ell \equiv 1 \pmod{6}$ so that the curve does not split and does not contain a point of order 4 in $\mathbb{F}_\ell$.

Look at the numerator of $x(2P)$, which is $(x^2 - a_4)^2$. We want an $\ell$ where $a_4$ is a non-quadratic residue modulo $\ell$ (this gives the 2 torsion criteria), $\Delta_E$ is a non-quadratic residue modulo $\ell$ (this prevents the original elliptic curve from splitting) and $-3$ is a quadratic residue modulo $\ell$ (this is $\ell \equiv 1 \pmod{6}$).
For the opposite direction, suppose that $\Delta_E = -3m^2$. We want that $p \in \mathcal{P}_b$.

To show this, we are looking for a prime $\ell \equiv 1 \pmod{6}$ so that the curve does not split and does not contain a point of order 4 in $\mathbb{F}_\ell$.

Look at the numerator of $x(2P)$, which is $(x^2 - a_4)^2$. We want an $\ell$ where $a_4$ is a non-quadratic residue modulo $\ell$ (this gives the 2 torsion criteria), $\Delta_E$ is a non-quadratic residue modulo $\ell$ (this prevents the original elliptic curve from splitting) and $-3$ is a quadratic residue modulo $\ell$ (this is $\ell \equiv 1 \pmod{6}$). This can be accomplished.
How far can this technique extend?
How far can this technique extend?

So far we can show $x^3 + y^3 = p^\alpha z^n$ has no solution if $n \geq p^{2p}$ provided that $p \not\in S$ or when $p \in \mathcal{P}_b \subseteq S$. Can we extend this to all of $S$?
How far can this technique extend?

So far we can show $x^3 + y^3 = p^\alpha z^n$ has no solution if $n \geq p^{2p}$ provided that $p \not\in S$ or when $p \in \mathcal{P}_b \subseteq S$. Can we extend this to all of $S$?

Suppose that $p = x^3 + y^3$. Factoring (in one case) gives $p = 3x^2 - 3x + 1$, where the right hand side is irreducible. Hence, Schinzel’s hypothesis H suggests that this should be prime infinitely often.
How far can this technique extend?

So far we can show $x^3 + y^3 = p^\alpha z^n$ has no solution if $n \geq p^{2p}$ provided that $p \notin S$ or when $p \in \mathcal{P}_b \subseteq S$. Can we extend this to all of $S$?

Suppose that $p = x^3 + y^3$. Factoring (in one case) gives $p = 3x^2 - 3x + 1$, where the right hand side is irreducible. Hence, Schinzel’s hypothesis H suggests that this should be prime infinitely often.

Hence, whenever $p = x^3 + y^3$, we should always have a solution, namely when $\alpha = 1$, $z = 1$ and $n$ is any natural number. Thus any primes in $S$ that are a sum of two cubes will not have a theorem statement like the above.
Generalizing the previous slides

Let’s try to break down the key ingredients of the previous slides.

First and foremost, we need a Frey curve with rational two torsion. In our previous case, the Frey curve was:

\[ y^2 = (x+b-a)(x^2 + (a-b)x + (a^2 + ab + b^2)) = x^3 + 3ab + b^3 - a^3. \]

We needed a classification of the elliptic curves of conductor \( \alpha \beta \gamma \) and non-trivial rational two torsion. We needed some solved cases of Diophantine equations to help simplify the classification.
Let’s try to break down the key ingredients of the previous slides.

- First and foremost, we need a Frey curve with rational two torsion. In our previous case, the Frey curve was

\[
y^2 = (x + b - a)(x^2 + (a - b)x + (a^2 + ab + b^2))
= x^3 + 3ab + b^3 - a^3.
\]
Generalizing the previous slides

Let’s try to break down the key ingredients of the previous slides.

- First and foremost, we need a Frey curve with rational two torsion. In our previous case, the Frey curve was

\[
y^2 = (x + b - a)(x^2 + (a - b)x + (a^2 + ab + b^2)) = x^3 + 3ab + b^3 - a^3.
\]

- We needed a classification of the elliptic curves of conductor \(2^\alpha 3^\beta p^\gamma\) and non-trivial rational two torsion.
Let’s try to break down the key ingredients of the previous slides.

- First and foremost, we need a Frey curve with rational two torsion. In our previous case, the Frey curve was

\[ y^2 = (x + b - a)(x^2 + (a - b)x + (a^2 + ab + b^2)) = x^3 + 3ab + b^3 - a^3. \]

- We needed a classification of the elliptic curves of conductor \(2^{\alpha}3^{\beta}p^{\gamma}\) and non-trivial rational two torsion.

- We needed some solved cases of Diophantine equations to help simplify the classification.
Generalizing the previous slides

Here are the aspects that extend to the situation $x^5 + y^5 = p^\alpha z^n$. 

We have a Frey curve with rational two torsion. In our new case, the Frey curve is $E_{5, a, b}$:

$$y^2 = x^3 - 5(a^2 + b^2)x^2 + 5(a^5 + b^5)a + b.$$ 

We can compute a classification of the elliptic curves of conductor $2^{\alpha}5^{\beta}p^{\gamma}$ and non-trivial rational two torsion. We have some solved cases of Diophantine equations to help simplify the classification, but the classification is not as neat as in the previous case.
Here are the aspects that extend to the situation $x^5 + y^5 = p^\alpha z^n$.

- We have a Frey curve with rational two torsion. In our new case, the Frey curve is

$$E_{5,a,b} : y^2 = x^3 - 5(a^2 + b^2)x^2 + 5 \left( \frac{a^5 + b^5}{a + b} \right) x.$$
Here are the aspects that extend to the situation $x^5 + y^5 = p^\alpha z^n$.

- We have a Frey curve with rational two torsion. In our new case, the Frey curve is

$$E_{5,a,b} : y^2 = x^3 - 5(a^2 + b^2)x^2 + 5 \left( \frac{a^5 + b^5}{a + b} \right) x.$$ 

- We can compute a classification of the elliptic curves of conductor $2^\alpha 5^\beta p^\gamma$ and non-trivial rational two torsion.
Here are the aspects that extend to the situation $x^5 + y^5 = p^\alpha z^n$.

- We have a Frey curve with rational two torsion. In our new case, the Frey curve is

$$E_{5,a,b} : y^2 = x^3 - 5(a^2 + b^2)x^2 + 5\left(\frac{a^5 + b^5}{a + b}\right)x.$$  

- We can compute a classification of the elliptic curves of conductor $2^\alpha 5^\beta p^\gamma$ and non-trivial rational two torsion.

- We have some solved cases of Diophantine equations to help simplify the classification, but the classification is not as neat as in the previous case.
Extending to $(5, 5, p)$

**Definition**

Let $S_5$ be the set of primes $p \geq 5$ for which there exists an elliptic curve $E$ with conductor $N_E \in \{50p, 200p, 400p\}$ with at least one non-trivial rational 2-torsion point.

The set $S_5$ contains the primes between 7 and 41 (the first exception is 43).

As before it is not known if $S_5$ is infinite.

As before the complement of $S_5$ forms a set of density one in the primes.
Extending to $(5, 5, \, \ell)$

**Definition**

Let $S_5$ be the set of primes $p \geq 5$ for which there exists an elliptic curve $E$ with conductor $N_E \in \{50\ell, 200\ell, 400\ell\}$ with at least one non-trivial rational 2-torsion point.

- The set $S_5$ contains the primes between 7 and 41 (the first exception is 43).
Extending to $(5, 5, p)$

**Definition**

Let $S_5$ be the set of primes $p \geq 5$ for which there exists an elliptic curve $E$ with conductor $N_E \in \{50p, 200p, 400p\}$ with at least one non-trivial rational 2-torsion point.

- The set $S_5$ contains the primes between 7 and 41 (the first exception is 43).
- As before it is not known if $S_5$ is infinite.
Definition

Let $S_5$ be the set of primes $p \geq 5$ for which there exists an elliptic curve $E$ with conductor $N_E \in \{50p, 200p, 400p\}$ with at least one non-trivial rational 2-torsion point.

- The set $S_5$ contains the primes between 7 and 41 (the first exception is 43).
- As before it is not known if $S_5$ is infinite.
- As before the complement of $S_5$ forms a set of density one in the primes.
Comparing $\left( 3, 3, p \right)$ and $\left( 5, 5, p \right)$

**Definition**

Let $S$ be the set of primes $p \geq 5$ for which there exists an elliptic curve $E$ with conductor $N_E \in \{18p, 36p, 72p\}$ with at least one non-trivial rational 2-torsion point.

**Theorem (Bennett, Luca, Mulholland - 2011)**

Suppose $p \geq 5$ is prime and $p \notin S$. Let $\alpha \geq 1$, $\alpha \in \mathbb{Z}$. Then the equation

$$x^3 + y^3 = p^\alpha z^n$$

has no solution in coprime nonzero $x, y, z \in \mathbb{Z}$ and prime $n$ with $n \geq p^{2p}$. 

Carmen Bruni  
Twisted Extensions of Fermat’s Last Theorem
Comparing $(3, 3, p)$ and $(5, 5, p)$

**Definition**
Let $S_5$ be the set of primes $p \geq 7$ for which there exists an elliptic curve $E$ with conductor $N_E \in \{50p, 200p, 400p\}$ with at least one non-trivial rational 2-torsion point.

**Theorem (B. - 2014?)**
Suppose $p \geq 7$ is prime and $p \notin S_5$. Let $\alpha \geq 1$, $\alpha \in \mathbb{Z}$. Then the equation

$$x^5 + y^5 = p^\alpha z^n$$

has no solution in coprime nonzero $x, y, z \in \mathbb{Z}$ and prime $n$ with $n \geq p^{13p}$. 

Carmen Bruni
Twisted Extensions of Fermat’s Last Theorem
The methods involving the sets $S$ and $\mathcal{P}_b$ will also extend over. The set $S_5$ now consists of primes $p \geq 5$ such that the elliptic curves with at least one non-trivial two torsion and conductor in the set $\{50p, 200p, 400p\}$. The associated quadratic polynomial for our Frey curve

$$E_{a,b} : y^2 = x \left( x^2 - 5(a^2 + b^2)x + 5 \left( \frac{a^5 + b^5}{a + b} \right) \right)$$

has discriminant $5(a + b)^4$ and so splits modulo $\ell$ whenever $(\frac{5}{\ell}) = 1$ so when $\ell \equiv \pm 1 \pmod{5}$.
The methods involving the sets $S$ and $\mathcal{P}_b$ will also extend over. The set $S_5$ now consists of primes $p \geq 5$ such that the elliptic curves with at least one non-trivial two torsion and conductor in the set $\{50p, 200p, 400p\}$. The associated quadratic polynomial for our Frey curve

$$E_{a,b} : y^2 = x \left( x^2 - 5(a^2 + b^2)x + 5 \left( \frac{a^5 + b^5}{a + b} \right) \right)$$

has discriminant $5(a + b)^4$ and so splits modulo $\ell$ whenever $\left( \frac{5}{\ell} \right) = 1$ so when $\ell \equiv \pm 1 \pmod{5}$.

For such an $\ell$, we have

$$a_\ell(E_{a,b}) = \ell + 1 - \#E_{a,b}(\mathbb{Q})_{\text{tor}} \equiv \ell + 1 \pmod{4}$$
The set $P_{b,5}$

Definition

Let $P_{b,5}$ be the set of primes $p \geq 7$ such that for every elliptic curve $E$ with conductor $N_E \in \{50p, 200p, 400p\}$ we have that $4 \nmid \#E_{tor}(\mathbb{Q})$ and at least one curve having a non-trivial rational 2-torsion point. Also, at all curves $F$ with non-trivial rational 2-torsion, we require that there exists a prime $\ell \equiv \pm 1 \pmod{5}$ such that $a_\ell(F) \not\equiv \ell + 1 \pmod{4}$. Note $P_{b,5} \subset S_5$. 

Primes in $P_{b,5}$ include $23, 53, 71, 73, 83, 97, 107, 137, 151, 173, 181, 191, 193, 197, \ldots$. 

Classifying these points gives the following theorem.
The set $P_{b,5}$

Definition

Let $P_{b,5}$ be the set of primes $p \geq 7$ such that for every elliptic curve $E$ with conductor $N_E \in \{50p, 200p, 400p\}$ we have that $4 \nmid \#E_{\text{tor}}(\mathbb{Q})$ and at least one curve having a non-trivial rational 2-torsion point. Also, at all curves $F$ with non-trivial rational 2-torsion, we require that there exists a prime $\ell \equiv \pm 1 \pmod{5}$ such that $a_\ell(F) \not\equiv \ell + 1 \pmod{4}$. Note $P_{b,5} \subset S_5$.

Primes in $P_{b,5}$ include
23, 53, 71, 73, 83, 97, 107, 137, 151, 173, 181, 191, 193, 197, ....
The set $\mathcal{P}_{b,5}$

**Definition**

Let $\mathcal{P}_{b,5}$ be the set of primes $p \geq 7$ such that for every elliptic curve $E$ with conductor $N_E \in \{50p, 200p, 400p\}$ we have that $4 \nmid \#E_{tor}(\mathbb{Q})$ and at least one curve having a non-trivial rational 2-torsion point. Also, at all curves $F$ with non-trivial rational 2-torsion, we require that there exists a prime $\ell \equiv \pm 1 \pmod{5}$ such that $a_{\ell}(F) \not\equiv \ell + 1 \pmod{4}$. Note $\mathcal{P}_{b,5} \subset S_5$.

Primes in $\mathcal{P}_{b,5}$ include

23, 53, 71, 73, 83, 97, 107, 137, 151, 173, 181, 191, 193, 197, ....

Classifying these points gives the following theorem.
Theorem (B. 2014?)

Suppose that \( p \in S_5 \) and that for each curve of conductor \( \{50p, 200p, 400p\} \), we have that the rational torsion subgroup is not divisible by 4. Then \( p \in \mathcal{P}_{b,5} \) if and only if every elliptic curve with conductor in \( \{50p, 200p, 400p\} \) and non-trivial rational two torsion has discriminant not of the form \( 5m^2 \) for any integer \( m \).
Theorem (B. 2014?)

Suppose that \( p \in S_5 \) and that for each curve of conductor \( \{50p, 200p, 400p\} \), we have that the rational torsion subgroup is not divisible by 4. Then \( p \in P_{b,5} \) if and only if every elliptic curve with conductor in \( \{50p, 200p, 400p\} \) and non-trivial rational two torsion has discriminant not of the form \( 5m^2 \) for any integer \( m \). In fact, we can also give the type of such primes that are in \( S_5 \) but not in \( P_{b,5} \).
Theorem (B. 2014?)

Suppose that \( p \in S_5 \) and that for each curve of conductor \( \{50p, 200p, 400p\} \), we have that the rational torsion subgroup is not divisible by 4. Then \( p \in \mathcal{P}_{b,5} \) if and only if every elliptic curve with conductor in \( \{50p, 200p, 400p\} \) and non-trivial rational two torsion has discriminant not of the form \( 5m^2 \) for any integer \( m \). In fact, we can also give the type of such primes that are in \( S_5 \) but not in \( \mathcal{P}_{b,5} \).

Hence, we have

Theorem (B. 2014?)

Suppose \( p \geq 7 \) is prime and \( p \in \mathcal{P}_{b,5} \subset S_5 \). Let \( \alpha \geq 1, \alpha \in \mathbb{Z} \). Then the equation \( x^5 + y^5 = p^\alpha z^n \) has no solution in coprime nonzero \( x, y, z \in \mathbb{Z} \) and prime \( n \) with \( n \geq p^{13p} \).
Can we continue to push the envelope and use this technique to solve $x^7 + y^7 = p^\alpha z^n$ and higher? Answer: Sadly no. The above techniques cannot immediately be extended to $x^7 + y^7 = p^\alpha z^n$ as of yet. There is no Frey curve with rational two torsion known. However, Freitas has work on cyclotomic polynomials that have lead to advances for the curves $x^7 + y^7 = dz^p$ and for $x^{13} + y^{13} = dz^p$. For the later, a higher form of modularity (to Hilbert modular forms) was needed.
Future Directions

- Can we continue to push the envelope and use this technique to solve $x^7 + y^7 = p^\alpha z^n$ and higher?

Answer: Sadly no. The above techniques cannot immediately be extended to $x^7 + y^7 = p^\alpha z^n$ as of yet. There is no Frey curve with rational two torsion known. However, Freitas has work on cyclotomic polynomials that have lead to advances for the curves $x^7 + y^7 = dz^p$ and for $x^{13} + y^{13} = dz^p$. For the later, a higher form of modularity (to Hilbert modular forms) was needed.
Future Directions

- Can we continue to push the envelope and use this technique to solve $x^7 + y^7 = p^\alpha z^n$ and higher?
- Answer: Sadly no. The above techniques cannot immediately be extended to $x^7 + y^7 = p^\alpha z^n$ as of yet. There is no Frey curve with rational two torsion known.
Future Directions

- Can we continue to push the envelope and use this technique to solve $x^7 + y^7 = p^\alpha z^n$ and higher?

- Answer: Sadly no. The above techniques cannot immediately be extended to $x^7 + y^7 = p^\alpha z^n$ as of yet. There is no Frey curve with rational two torsion known.

- However, Freitas has work on cyclotomic polynomials that have lead to advances for the curves $x^7 + y^7 = dz^p$ and for $x^{13} + y^{13} = dz^p$. For the later, a higher form of modularity (to Hilbert modular forms) was needed.
Thank you.