Twisted Extensions of Fermat's Last Theorem

Carmen Bruni

University of British Columbia

December 7th, 2012

Why Study Diophantine Equations?

Why Study Diophantine Equations?

- It's a fun challenge.

Why Study Diophantine Equations?

- It's a fun challenge.
- It gives justification for other studying subjects (for example algebraic number theory or algebraic geometry).

Why Study Diophantine Equations?

- It's a fun challenge.
- It gives justification for other studying subjects (for example algebraic number theory or algebraic geometry).
- It leads to other interesting questions.

Why Study Diophantine Equations?

- It's a fun challenge.
- It gives justification for other studying subjects (for example algebraic number theory or algebraic geometry).
- It leads to other interesting questions. For example
  - Pell equations, $x^2 - dy^2 = 1$, lead to questions about continued fractions and fundamental units.

Why Study Diophantine Equations?

- It's a fun challenge.
- It gives justification for other studying subjects (for example algebraic number theory or algebraic geometry).
- It leads to other interesting questions. For example
  - Pell equations, $x^2 - dy^2 = 1$, lead to questions about continued fractions and fundamental units.
  - Fermat's Last Theorem $x^n + y^n = z^n$ lead to questions about unique factorization domains, cyclotomic fields, elliptic curves and modular forms.

The set S and the work of Bennett, Luca and Mulholland

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.

The set S and the work of Bennett, Luca and Mulholland

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 and the work of Bennett, Luca and Mulholland

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).

The set S and the work of Bennett, Luca and Mulholland

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.

The set S and the work of Bennett, Luca and Mulholland

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 $p \notin S$.

The set S and the work of Bennett, Luca and Mulholland

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.

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.

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 $n \geq p^{2p}$.

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 $n \geq p^{2p}$.

What about primes in S?

An extension of the approach of Bennett, Luca and Mulholland

- Suppose we have a solution to our Diophantine equation, say $a^3 + b^3 = p^\alpha c^n$.

An extension of the approach of Bennett, Luca and Mulholland

- 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

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

An extension of the approach of Bennett, Luca and Mulholland

- 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 $\ell \equiv 1 \pmod 6$.

An extension of the approach of Bennett, Luca and Mulholland

- 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, $4 \mid \#E_{a,b}(\mathbb{F}_l)$ and thus

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

An extension of the approach of Bennett, Luca and Mulholland

- 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, $4 \mid \#E_{a,b}(\mathbb{F}_l)$ 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 $n \leq p^{2p}$.

An extension of the approach of Bennett, Luca and Mulholland

- 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 $\ell \equiv 1 \pmod 6$.

An extension of the approach of Bennett, Luca and Mulholland

- 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 ℓ.

An extension of the approach of Bennett, Luca and Mulholland

- 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 ℓ.
- 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 ℓ is small compared to p^{2p}.

An extension of the approach of Bennett, Luca and Mulholland

- 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 ℓ.
- 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 ℓ 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 $\mathcal{P}_b \subset S$.

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 $\mathcal{P}_b \subset S$.

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

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 $\mathcal{P}_b \subset S$.

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

New Result

Theorem (B. 2013?)

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.

New Result

Theorem (B. 2013?)

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 $\mathcal{P}_b$.

New Result

Theorem (B. 2013?)

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. 2013?)

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

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 in $\mathcal{P}_b$

- $p = 5, 7, 11, 13, 17, 19, 23, 29, 31, 47, 67, 73, 193, 1153$
- $p = 2^a 3^b \pm 1$
- $p = |3^b \pm 2^a|$
- $p^n = \pm(t^2 - 2^a 3^b)$, $n = 1$, 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 $a = 2, 4, 5$

Proof Outline

- First, suppose that $p \in \mathcal{P}_b \subset S$ and assume towards a contradiction that $\Delta_E = -3m^2$.

Proof Outline

- 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

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

Proof Outline

- 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 $4 \nmid \#E(\mathbb{F}_\ell)$.

Proof Outline

- 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 $k \mid m$.

Proof Outline

- 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.

Proof Outline

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

Proof Outline

- 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 $\mathbb{F}_\ell$.

Proof Outline

- 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 ℓ where a_4 is a non-quadratic residue modulo ℓ (this gives the 2 torsion criteria) , Δ_E is a non-quadratic residue modulo ℓ (this prevents the original elliptic curve from splitting) and -3 is a quadratic residue modulo ℓ (this is $\ell \equiv 1 \pmod 6$).

Proof Outline

- 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 ℓ where a_4 is a non-quadratic residue modulo ℓ (this gives the 2 torsion criteria) , Δ_E is a non-quadratic residue modulo ℓ (this prevents the original elliptic curve from splitting) and -3 is a quadratic residue modulo ℓ (this is $\ell \equiv 1 \pmod 6$). This can be accomplished.

"The Truth"

- How far can this technique extend?

"The Truth"

- 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?

"The Truth"

- 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.

"The Truth"

- 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.

Thank you.