Twisted Extensions of Fermat's Last Theorem

Carmen Bruni

University of British Columbia

June 7th, 2014

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

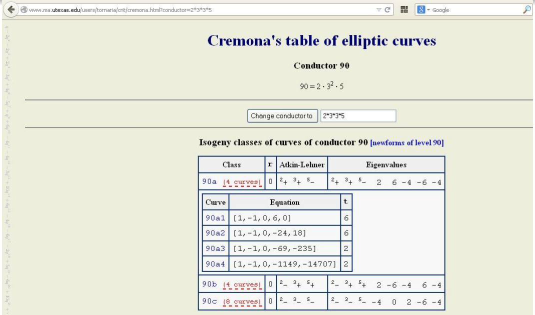
Let S be the set of primes $p \geq 5$ for which there exists an elliptic curve E with conductor $N_E \in \{18p, 36p, 72p\}$ with at least one non-trivial rational 2-torsion point.

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.


www.ma.utexas.edu/users/tornaria/cnt/cremona.html?conductor=2*3*3*5

Cremona's table of elliptic curves

Conductor 90

$90 = 2 \cdot 3^2 \cdot 5$

Change conductor to 2*3*3*5

Isogeny classes of curves of conductor 90 [newforms of level 90]

Class	r	Atkin-Lehner	Eigenvalues
90a (4 curves)	0	$2_+ \ 3_+ \ 5_-$	$2_+ \ 3_+ \ 5_-$ 2 6 -4 -6 -4
90b (4 curves)	0	$2_- \ 3_+ \ 5_+$	$2_- \ 3_+ \ 5_+$ 2 -6 -4 6 -4
90c (8 curves)	0	$2_- \ 3_- \ 5_-$	$2_- \ 3_- \ 5_-$ -4 0 2 -6 -4

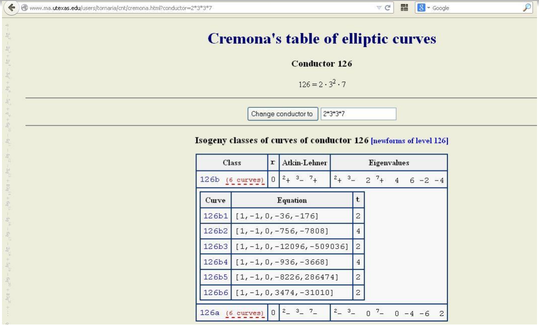
Curve	Equation	t
90a1	[1,-1,0,6,0]	6
90a2	[1,-1,0,-24,18]	6
90a3	[1,-1,0,-69,-235]	2
90a4	[1,-1,0,-1149,-14707]	2

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.



www.ma.utexas.edu/users/tornaria/cnt/cremona.html?conductor=2*3*3*7

Cremona's table of elliptic curves

Conductor 126

$126 = 2 \cdot 3^2 \cdot 7$

Change conductor to 2*3*3*7

Isogeny classes of curves of conductor 126 [newforms of level 126]

Class	r	Atkin-Lehner	Eigenvalues
126b (6 curves)	0	$^2+$ $^3-$ $^7+$	$^2+$ $^3-$ 2 $^7+$ 4 6 -2 -4

Curve	Equation	t
126b1	[1,-1,0,-36,-176]	2
126b2	[1,-1,0,-756,-7808]	4
126b3	[1,-1,0,-12096,-509036]	2
126b4	[1,-1,0,-936,-3668]	4
126b5	[1,-1,0,-8226,286474]	2
126b6	[1,-1,0,3474,-31010]	2

Class	r	Atkin-Lehner	Eigenvalues
126a (6 curves)	0	$^2-$ $^3-$ $^7-$	$^2-$ $^3-$ 0 $^7-$ 0 -4 -6 2

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.

Isogeny classes of curves of conductor 3546 [newforms of level 3546]

No elliptic curves of conductor 3546

Isogeny classes of curves of conductor 7092 [newforms of level 7092]

Class	r	Atkin-Lehner	Eigenvalues
7092a (1 curve)	0	2_- 3_- 197_-	2_- 3_- 0 3 -2 4 -4 -1
7092b (1 curve)	0	2_- 3_- 197_-	2_- 3_- 4 -1 -4 -2 0 3

Isogeny classes of curves of conductor 14184 [newforms of level 14184]

Class	r	Atkin-Lehner	Eigenvalues
14184a (1 curve)	1	2_+ 3_- 197_-	2_+ 3_- -4 3 -4 -2 4 -1
14184b (1 curve)	1	2_- 3_- 197_+	2_- 3_- 2 -5 2 -4 0 -5
14184c (1 curve)	0	2_- 3_- 197_-	2_- 3_- 0 3 6 4 0 -1

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

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

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 $\ell \le p^2$ 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 $\mathcal{P}_b \subset S$.

For $p = 53$,

954b (2 curves)	0	$^2+$ $^3+$ $^{53}-$	$^2+$ $^3+$ -2 4 2 2 0 -4

Curve	Equation	t
954b1	[1,-1,0,12,-100]	2
954b2	[1,-1,0,-258,-1450]	2

954g (2 curves)	0	$^2-$ $^3+$ $^{53}+$	$^2-$ $^3+$ 2 4 -2 2 0 -4

Curve	Equation	t
954g1	[1,-1,1,1,3]	2
954g2	[1,-1,1,-29,63]	2

Hecke Eigenvalues for elliptic curve 954b1

a2	a3	a5	a7	a11	a13	a17	a19	a23	a29	a31	a37	a41	a43	a47	a53	a59	a61	a67	a71	a73	a79	a83	a89	a97
+	+	-2	4	2	2	0	-4	0	6	-2	6	2	4	4	-	10	8	4	0	6	-10	-8	-4	6

Hecke Eigenvalues for elliptic curve 954g1

a2	a3	a5	a7	a11	a13	a17	a19	a23	a29	a31	a37	a41	a43	a47	a53	a59	a61	a67	a71	a73	a79	a83	a89	a97
-	+	2	4	-2	2	0	-4	0	-6	-2	6	-2	4	-4	+	-10	8	4	0	6	-10	8	4	6

Hecke Eigenvalues for elliptic curve 1908b1

a2	a3	a5	a7	a11	a13	a17	a19	a23	a29	a31	a37	a41	a43	a47	a53	a59	a61	a67	a71	a73	a79	a83	a89	a97
-	-	-2	0	4	-2	-2	2	2	-2	2	10	-2	-4	12	-	12	10	-2	-6	10	10	6	10	14

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

New Result

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.

New Result

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 $\mathcal{P}_b$.

New Result

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

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 $\mathcal{P}_b$

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

$$E : y^2 = x(x^2 + a_2 x + a_4)$$

- 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

$$E : y^2 = x(x^2 + a_2 x + a_4)$$

- 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.

Generalizing the previous slides

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

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

$$\begin{aligned} y^2 &= (x+b-a)(x^2+(a-b)x+(a^2+ab+b^2)) \\ &= x^3+3ab+b^3-a^3. \end{aligned}$$

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

$$\begin{aligned} y^2 &= (x+b-a)(x^2+(a-b)x+(a^2+ab+b^2)) \\ &= x^3+3ab+b^3-a^3. \end{aligned}$$

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

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

$$\begin{aligned} y^2 &= (x+b-a)(x^2+(a-b)x+(a^2+ab+b^2)) \\ &= x^3+3ab+b^3-a^3. \end{aligned}$$

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

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

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

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

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

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

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

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

- 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.

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).

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.

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.

Comparing $(3, 3, p)$ and $(5, 5, p)$

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

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 $n \geq p^{13p}$.

- 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 ℓ whenever $\left(\frac{5}{\ell}\right) = 1$ so when $\ell \equiv \pm 1 \pmod 5$.

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

- 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 ℓ whenever $\left(\frac{5}{\ell}\right) = 1$ so when $\ell \equiv \pm 1 \pmod{5}$.
- For such an ℓ, we have

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

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 $4 \nmid \#E_{\text{tor}}(\mathbb{Q})$ 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 $\mathcal{P}_{b,5} \subset S_5$.

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 $4 \nmid \#E_{\text{tor}}(\mathbb{Q})$ 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 $\mathcal{P}_{b,5} \subset S_5$.

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

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 $4 \nmid \#E_{\text{tor}}(\mathbb{Q})$ 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 $\mathcal{P}_{b,5} \subset S_5$.

Primes in $\mathcal{P}_{b,5}$ include
$23, 53, 71, 73, 83, 97, 107, 137, 151, 173, 181, 191, 193, 197, \ldots.$
Classifying these points gives the following theorem.

New Result

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.

New Result

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 $\mathcal{P}_{b,5}$.

New Result

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 $n \geq p^{13p}$.

Future Directions

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?

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.