Introduction Szpiro's Conjecture Computations Local Szpiro's Conjecture

Szpiro's Conjecture

Soroosh Yazdani

McMaster University

Workshop on Discovery and Experimentation in Number Theory

Introduction

Elliptic Curves

Minimal Discriminant

Conductor

Szpiro's Conjecture

Statement

What is known

Evidence For

Evidence Against

Computations

Cremona's Table

Stein-Watkins's Table

Curves with Torsion points

Local Szpiro's Conjecture

Motivation

Statement

Evidence for

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, a_i \in \mathbb{Q}$$

be a Weierstrass equation for E/\mathbb{Q}

By simple changes of variable we can find a simpler Weierstrass equation

$$y^2 = x^3 + Ax + B.$$

$$\Delta(E) = -16(4A^3 - 27B^2)$$

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, a_i \in \mathbb{Q}$$

be a Weierstrass equation for E/\mathbb{Q} .

By simple changes of variable we can find a simpler Weierstrass equation

$$y^2 = x^3 + Ax + B.$$

$$\Delta(E) = -16(4A^3 - 27B^2)$$

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, a_i \in \mathbb{Q}$$

be a Weierstrass equation for E/\mathbb{Q} .

By simple changes of variable we can find a simpler Weierstrass equation

$$y^2 = x^3 + Ax + B.$$

$$\Delta(E) = -16(4A^3 - 27B^2).$$

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, a_i \in \mathbb{Q}$$

be a Weierstrass equation for E/\mathbb{Q} .

By simple changes of variable we can find a simpler Weierstrass equation

$$y^2 = x^3 + Ax + B.$$

$$\Delta(E) = -16(4A^3 - 27B^2).$$

Let $X = u^2x$ and $Y = u^3y$, then

$$E': Y^2 = X^3 + Au^{-4}X + Bu^{-6},$$

and we get

$$\Delta' = u^{-12} \Delta.$$

Let $X = u^2x$ and $Y = u^3y$, then

$$E': Y^2 = X^3 + Au^{-4}X + Bu^{-6},$$

and we get

$$\Delta' = u^{-12} \Delta.$$

Let $X = u^2x$ and $Y = u^3y$, then

$$E': Y^2 = X^3 + Au^{-4}X + Bu^{-6},$$

and we get

$$\Delta'=u^{-12}\Delta.$$

Let $X = u^2x$ and $Y = u^3y$, then

$$E': Y^2 = X^3 + Au^{-4}X + Bu^{-6},$$

and we get

$$\Delta'=u^{-12}\Delta.$$

Definition

If the Weierstrass equation

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

is such that $a_i \in \mathbb{Z}$ and for any other Weierstrass equation of E with $a_i' \in \mathbb{Z}$ we have

$$|\Delta'| \ge |\Delta|,$$

we say that it is a minimal Weierstrass equation.

The discriminant of this minimal model is an invariant of E/\mathbb{Q} . We call this discriminant the minimal discriminant of E, and we denote it by Δ_E .

Definition

If the Weierstrass equation

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

is such that $a_i \in \mathbb{Z}$ and for any other Weierstrass equation of E with $a_i' \in \mathbb{Z}$ we have

$$|\Delta'| \ge |\Delta|,$$

we say that it is a minimal Weierstrass equation.

The discriminant of this minimal model is an invariant of E/\mathbb{Q} .

We call this discriminant the minimal discriminant of E, and we denote it by Δ_E .

Definition

If the Weierstrass equation

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

is such that $a_i \in \mathbb{Z}$ and for any other Weierstrass equation of E with $a_i' \in \mathbb{Z}$ we have

$$|\Delta'| \ge |\Delta|$$
,

we say that it is a minimal Weierstrass equation.

The discriminant of this minimal model is an invariant of E/\mathbb{Q} . We call this discriminant the minimal discriminant of E, and we denote it by Δ_E .

$$X_0(N) \rightarrow E$$
.

$$N_E = \prod_{p|\Delta_E} p^{\nu_p}$$

$$\nu_p = \begin{cases} 1 & \text{if } p \text{ is a prime of multiplicative reduction,} \\ 2 & \text{if } p > 3 \text{ and is a prime of additive reduction,} \\ \leq 8 & \text{in general.} \end{cases}$$

That means, there is an integer N and a rational surjective morphism

$$X_0(N) \rightarrow E$$
.

The conductor of E is the smallest N such that such a map exist. For E/\mathbb{Q} , let Δ_E be the minimal discriminant of E. Then

$$N_E = \prod_{p|\Delta_E} p^{\nu_p}$$

where

$$u_p = \begin{cases}
1 & \text{if } p \text{ is a prime of multiplicative reduction,} \\
2 & \text{if } p > 3 \text{ and is a prime of additive reduction} \\
\leq 8 & \text{in general.}
\end{cases}$$

That means, there is an integer N and a rational surjective morphism

$$X_0(N) \rightarrow E$$
.

The conductor of E is the smallest N such that such a map exist.

For E/\mathbb{Q} , let Δ_E be the minimal discriminant of E. Then

$$N_E = \prod_{p|\Delta_E} p^{\nu_p}$$

where

$$u_p = \begin{cases}
1 & \text{if } p \text{ is a prime of multiplicative reduction,} \\
2 & \text{if } p > 3 \text{ and is a prime of additive reduction} \\
\leq 8 & \text{in general.}
\end{cases}$$

That means, there is an integer N and a rational surjective morphism

$$X_0(N) \rightarrow E$$
.

The conductor of E is the smallest N such that such a map exist. For E/\mathbb{Q} , let Δ_E be the minimal discriminant of E. Then

$$N_E = \prod_{p \mid \Delta_E} p^{
u_p}$$

where

$$\nu_p = \begin{cases} 1 & \text{if } p \text{ is a prime of multiplicative reduction,} \\ 2 & \text{if } p > 3 \text{ and is a prime of additive reduction,} \\ \leq 8 & \text{in general.} \end{cases}$$

Szpiro's Conjecture

Conjecture

For any $\varepsilon>0$ there exists a positive number C_{ε} such that for any elliptic curve E/\mathbb{Q} we have

$$|\Delta_E| \leq C_{\varepsilon} (N_E)^{6+\varepsilon},$$

where Δ_E is the minimal discriminant of E, and N_E is the conductor of E.

The above conjecture generalizes to any number field, and in general global fields in obvious way.

Szpiro's Conjecture

Conjecture

For any $\varepsilon>0$ there exists a positive number C_{ε} such that for any elliptic curve E/\mathbb{Q} we have

$$|\Delta_E| \leq C_{\varepsilon} (N_E)^{6+\varepsilon},$$

where Δ_E is the minimal discriminant of E, and N_E is the conductor of E.

The above conjecture generalizes to any number field, and in general global fields in obvious way.

- ▶ Szpiro's conjecture is true for function field case with $\varepsilon = 0$.
- Stewart and Yu's result for ABC conjecture shows that

$$|\Delta_E| < K^{(N_E)^{1/3+\varepsilon}},$$

- ► There are few families where we can prove Szpiro uncoditionally:
 - Szpiro's conjecture is true for elliptic curves with prime conductor
 - Szpiro's conjecture is true for semistable elliptic curves with perfect power discriminant $\Delta_E = D^I$.

- ▶ Szpiro's conjecture is true for function field case with $\varepsilon = 0$.
- Stewart and Yu's result for ABC conjecture shows that

$$|\Delta_E| < K^{(N_E)^{1/3+\varepsilon}},$$

- ► There are few families where we can prove Szpiro uncoditionally:
 - Szpiro's conjecture is true for elliptic curves with prime conductor
 - Szpiro's conjecture is true for semistable elliptic curves with perfect power discriminant $\Delta_F = D^I$.

- ▶ Szpiro's conjecture is true for function field case with $\varepsilon = 0$.
- Stewart and Yu's result for ABC conjecture shows that

$$|\Delta_E| < K^{(N_E)^{1/3+\epsilon}},$$

- ► There are few families where we can prove Szpiro uncoditionally:
 - Szpiro's conjecture is true for elliptic curves with prime conductor.
 - Szpiro's conjecture is true for semistable elliptic curves with perfect power discriminant $\Delta_E = D^I$.

- ▶ Szpiro's conjecture is true for function field case with $\varepsilon = 0$.
- Stewart and Yu's result for ABC conjecture shows that

$$|\Delta_E| < K^{(N_E)^{1/3+\epsilon}},$$

- ► There are few families where we can prove Szpiro uncoditionally:
 - Szpiro's conjecture is true for elliptic curves with prime conductor.
 - Szpiro's conjecture is true for semistable elliptic curves with perfect power discriminant $\Delta_E = D^I$.

- ▶ Szpiro's conjecture is true for function field case with $\varepsilon = 0$.
- Stewart and Yu's result for ABC conjecture shows that

$$|\Delta_E| < K^{(N_E)^{1/3+\epsilon}},$$

- There are few families where we can prove Szpiro uncoditionally:
 - Szpiro's conjecture is true for elliptic curves with prime conductor.
 - Szpiro's conjecture is true for semistable elliptic curves with perfect power discriminant $\Delta_E = D^I$.

- ► The ABC conjecture for number fields implies Szpiro's conjecture.
- Vojta's conjecture implies Szpiro's Conjecture
- ▶ It is true for function field case with $\varepsilon = 0$.
- ▶ For families of elliptic curves E_t , one gets that

$$\liminf \frac{\log |\Delta_{E_t}|}{\log N_{E_t}} \le 6.$$

► It is such a simple conjecture with such wonderful consequences (a lot of them proven). It will be a shame if it's not true.

- ► The *ABC* conjecture for number fields implies Szpiro's conjecture.
- Vojta's conjecture implies Szpiro's Conjecture
- lt is true for function field case with $\varepsilon = 0$.
- ▶ For families of elliptic curves E_t , one gets that

$$\liminf \frac{\log |\Delta_{E_t}|}{\log N_{E_t}} \le 6.$$

It is such a simple conjecture with such wonderful consequences (a lot of them proven). It will be a shame if it's not true.

- ► The *ABC* conjecture for number fields implies Szpiro's conjecture.
- Vojta's conjecture implies Szpiro's Conjecture
- ▶ It is true for function field case with $\varepsilon = 0$.
- \triangleright For families of elliptic curves E_t , one gets that

$$\liminf \frac{\log |\Delta_{E_t}|}{\log N_{E_t}} \le 6.$$

It is such a simple conjecture with such wonderful consequences (a lot of them proven). It will be a shame if it's not true.

- ► The ABC conjecture for number fields implies Szpiro's conjecture.
- Vojta's conjecture implies Szpiro's Conjecture
- ▶ It is true for function field case with $\varepsilon = 0$.
- ▶ For families of elliptic curves E_t , one gets that

$$\liminf \frac{\log |\Delta_{E_t}|}{\log N_{E_t}} \le 6.$$

It is such a simple conjecture with such wonderful consequences (a lot of them proven). It will be a shame if it's not true.

- ► The *ABC* conjecture for number fields implies Szpiro's conjecture.
- Vojta's conjecture implies Szpiro's Conjecture
- ▶ It is true for function field case with $\varepsilon = 0$.
- ▶ For families of elliptic curves E_t , one gets that

$$\liminf \frac{\log |\Delta_{E_t}|}{\log N_{E_t}} \le 6.$$

▶ It is such a simple conjecture with such wonderful consequences (a lot of them proven). It will be a shame if it's not true.

- ▶ Szpiro's conjecture for \mathbb{Q} implies the ABC conjecture (with slightly different constants) for \mathbb{Q} .
- ▶ One can construct elliptic curves *E* such that

$$\frac{\log |\Delta_E|}{\log N_E}$$

- ➤ To make things worst, many of the above examples happen for elliptic curves with large conductor.
- Szpiro's conjecture implies so many results, that it can't possibly be true.

- ▶ Szpiro's conjecture for ℚ implies the *ABC* conjecture (with slightly different constants) for ℚ.
- ▶ One can construct elliptic curves *E* such that

$$\frac{\log |\Delta_E|}{\log N_E}$$

- ➤ To make things worst, many of the above examples happen for elliptic curves with large conductor.
- Szpiro's conjecture implies so many results, that it can't possibly be true.

- ▶ Szpiro's conjecture for ℚ implies the *ABC* conjecture (with slightly different constants) for ℚ.
- ▶ One can construct elliptic curves *E* such that

$$\frac{\log |\Delta_E|}{\log N_E}$$

- ➤ To make things worst, many of the above examples happen for elliptic curves with large conductor.
- Szpiro's conjecture implies so many results, that it can't possibly be true.

- ▶ Szpiro's conjecture for ℚ implies the *ABC* conjecture (with slightly different constants) for ℚ.
- ▶ One can construct elliptic curves *E* such that

$$\frac{\log |\Delta_E|}{\log N_E}$$

- ➤ To make things worst, many of the above examples happen for elliptic curves with large conductor.
- Szpiro's conjecture implies so many results, that it can't possibly be true.

Searching through Cremona's table of elliptic curves, we find the following elliptic curves.

Szpiro Ratio	
8.90370022	
8.801596	
8.75731615	
8.16352289	
8.11481288	
7.88245679	
7.67049417	
7.55196781	
7.53394369	
7.44459994	

Cremona's Table Stein-Watkins's Table Curves with Torsion points

Well, there aren't any good examples in this table, since these are searched by bounding the discriminant.

Elliptic curves with 7 torsion points are parametrized by

$$E_7: y^2 + (s^2 - st - t^2)xy - s^2t^3y = x^3 - s^2t(s - t)x^2,$$

and it has discriminant

$$\Delta_7 = s^7 t^7 (s-t)^7 (s^3 - 8s^2 t + 5st^2 + t^3).$$

Quotiening by the 7 torsion pint we get E_7' with discriminant $\Delta_7' = st(s-t)(s^3 - 8s^2t + 5st^2 + t^3)^7$.

Choosing s and t really powerful numbers, one expects to get elliptic curves with high Szpiro ratio.

Elliptic curves with 7 torsion points are parametrized by

$$E_7: y^2 + (s^2 - st - t^2)xy - s^2t^3y = x^3 - s^2t(s - t)x^2,$$

and it has discriminant

$$\Delta_7 = s^7 t^7 (s-t)^7 (s^3 - 8s^2 t + 5st^2 + t^3).$$

Quotiening by the 7 torsion pint we get E_7' with discriminant $\Delta_7' = st(s-t)(s^3 - 8s^2t + 5st^2 + t^3)^7$.

Choosing s and t really powerful numbers, one expects to get elliptic curves with high Szpiro ratio.

Elliptic curves with 7 torsion points are parametrized by

$$E_7: y^2 + (s^2 - st - t^2)xy - s^2t^3y = x^3 - s^2t(s - t)x^2,$$

and it has discriminant

$$\Delta_7 = s^7 t^7 (s-t)^7 (s^3 - 8s^2 t + 5st^2 + t^3).$$

Quotiening by the 7 torsion pint we get E_7' with discriminant $\Delta_7' = st(s-t)(s^3 - 8s^2t + 5st^2 + t^3)^7$.

Choosing s and t really powerful numbers, one expects to get elliptic curves with high Szpiro ratio.

7-Torsion Search

S	t	N	σ
11	2	858	8.75731614557112
312500	49221	50476302089404230	7.92756011861372
312500	49221	50476302089404230	7.53984409257145
486	487	202824786	7.44460382021831
425984	369285	175354399584002730	7.36245698593439
304	21	120369522	7.32780268502485
707281	10935	9246380170145557110	7.31803486329741
:	:	:	:
1712421	868096	1363130725497912232710	7.11870486158338
147392	127223	13911787389465294	7.10618688719188

Good Szpiro Ratio and non-trivial Torsion

N	T	σ
2526810	4	8.811944
9690	2	8.801596
858	7	8.75731615
167490523410	4	8.688968
610537970	3	8.596580
29070	2	8.502119
391491534	5	8.48609917
91910	2	8.485421
33641790	3	8.245590

Here is a typical application of Szpiro's Conjecture to Diophantine equations.

Proposition

Assume for some $\varepsilon > 0$ and some constant C_{ε} , Szpiro's conjecture is true. Then there are only finitely many solutions to

$$A^a + B^b = C^c,$$

with A, B, C coprime integers, and 1/a + 1/b + 1/c < 1.

Here is a typical application of Szpiro's Conjecture to Diophantine equations.

Proposition

Assume for some $\varepsilon > 0$ and some constant C_{ε} , Szpiro's conjecture is true. Then there are only finitely many solutions to

$$A^a + B^b = C^c,$$

with A, B, C coprime integers, and 1/a + 1/b + 1/c < 1.

Proof.

For any such triple (a, b, c), Darmon and Granville have showed that the above equation has only finitely many solutions.

So assume that $\max(a, b, c)$ is really really large. For simplicity, assume that $\min(a, b, c) > 6 + \varepsilon$. Construct the Frey elliptic curve

$$y^2 = x(x - A^a)(x + B^b),$$

which has minimal discriminant and conductor

$$\Delta_E = 2^r A^a B^b C^c, N_E = \prod_{p|ABC} p < ABC$$

Then Szpiro's conjecture says

$$|2^r A^a B^b C^c| < C_{\varepsilon} (ABC)^{6+\varepsilon}$$



Proof.

For any such triple (a,b,c), Darmon and Granville have showed that the above equation has only finitely many solutions. So assume that $\max(a,b,c)$ is really really large. For simplicity, assume that $\min(a,b,c)>6+\varepsilon$. Construct the Frey elliptic curve

$$y^2 = x(x - A^a)(x + B^b),$$

which has minimal discriminant and conductor

$$\Delta_E = 2^r A^a B^b C^c, N_E = \prod_{p \mid ABC} p < ABC$$

Then Szpiro's conjecture says

$$|2^r A^a B^b C^c| < C_{\varepsilon} (ABC)^{6+\varepsilon}$$



Proof.

For any such triple (a,b,c), Darmon and Granville have showed that the above equation has only finitely many solutions. So assume that $\max(a,b,c)$ is really really large. For simplicity, assume that $\min(a,b,c)>6+\varepsilon$. Construct the Frey elliptic curve

$$y^2 = x(x - A^a)(x + B^b),$$

which has minimal discriminant and conductor

$$\Delta_E = 2^r A^a B^b C^c, N_E = \prod_{p \mid ABC} p < ABC$$

Then Szpiro's conjecture says

$$|2^r A^a B^b C^c| < C_{\varepsilon} (ABC)^{6+\varepsilon}$$
.



Note that Szpiro was used to prove that not all powers of primes in the discriminant can be large.

Conjecture

Let E/\mathbb{Q} be a semistable elliptic curve with conductor N_E and minimal discriminant Δ_E . Then there exists a prime number $p|N_E$ such that

$$v_p(\Delta_E) \leq 6.$$

Note that Szpiro was used to prove that not all powers of primes in the discriminant can be large.

Conjecture

Let E/\mathbb{Q} be a semistable elliptic curve with conductor N_E and minimal discriminant Δ_E . Then there exists a prime number $p|N_E$ such that

$$v_p(\Delta_E) \leq 6.$$

Note that Szpiro was used to prove that not all powers of primes in the discriminant can be large.

Conjecture

Let E/\mathbb{Q} be a semistable elliptic curve with conductor N_E and minimal discriminant Δ_E . Then there exists a prime number $p|N_E$ such that

$$v_p(\Delta_E) \leq 6.$$



Note that Szpiro was used to prove that not all powers of primes in the discriminant can be large.

Conjecture

Let E/\mathbb{Q} be a semistable elliptic curve with conductor N_E and minimal discriminant Δ_E . Then there exists a prime number $p|N_E$ such that

$$v_p(\Delta_E) \leq 6.$$

- ▶ Szpiro's conjecture implies it (at least asymptotically.)
- It seems to be strictly weaker than Szpiro's conjecture
- ► (Naive) computer search.
- ▶ It is closely related to Frey-Mazur's conjecture.

- Szpiro's conjecture implies it (at least asymptotically.)
- ▶ It seems to be strictly weaker than Szpiro's conjecture.
- ► (Naive) computer search.
- ▶ It is closely related to Frey-Mazur's conjecture.

- Szpiro's conjecture implies it (at least asymptotically.)
- ▶ It seems to be strictly weaker than Szpiro's conjecture.
- ► (Naive) computer search.
- ▶ It is closely related to Frey-Mazur's conjecture.

- Szpiro's conjecture implies it (at least asymptotically.)
- ▶ It seems to be strictly weaker than Szpiro's conjecture.
- ► (Naive) computer search.
- ▶ It is closely related to Frey-Mazur's conjecture.

We have the following (very) partial result in this direction:

Theorem

For any integer M, there exist a constant C(M) such that for any p>C(M) and any elliptic curve E/\mathbb{Q} of conductor Mp and a non-trivial rational isogeny we have

$$v_p(\Delta_E) \leq 6.$$

Conjecture

Let l>6 be a prime. Let E/\mathbb{Q} be a semistable elliptic curve with minimal discriminant $\Delta_E=p^rM^l$ for some integer M coprime to p. Then $r\leq 6$.

This is closely related to the following Diophantine problem:

Conjecture

Conjecture

Let l>6 be a prime. Let E/\mathbb{Q} be a semistable elliptic curve with minimal discriminant $\Delta_E=p^rM^l$ for some integer M coprime to p. Then $r\leq 6$.

This is closely related to the following Diophantine problem:

Conjecture

Conjecture

Let l>6 be a prime. Let E/\mathbb{Q} be a semistable elliptic curve with minimal discriminant $\Delta_E=p^rM^l$ for some integer M coprime to p. Then $r\leq 6$.

This is closely related to the following Diophantine problem:

Conjecture

Conjecture

Let l>6 be a prime. Let E/\mathbb{Q} be a semistable elliptic curve with minimal discriminant $\Delta_E=p^rM^l$ for some integer M coprime to p. Then $r\leq 6$.

This is closely related to the following Diophantine problem:

Conjecture