Modular Approach to Diophantine Equations II

Samir Siksek

University of Warwick

June 15, 2012

Recap: Ribet's Level-Lowering Theorem

Let

- $E/\mathbb{Q}$ an elliptic curve,
- $\Delta = \Delta_{\min}$ be the discriminant for a minimal model of E,
- N be the conductor of E,
- for a prime p let

$$N_p = N \Bigg/ \prod_{\substack{q \| N, \\ p \mid \operatorname{ord}_q(\Delta)}} q.$$

Recap: Ribet's Level-Lowering Theorem

Let

- $E/\mathbb{Q}$ an elliptic curve,
- $\Delta = \Delta_{\min}$ be the discriminant for a minimal model of E,
- N be the conductor of E,
- for a prime p let

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

Theorem

(A simplified special case of Ribet's Level-Lowering Theorem) Let $p \geq 5$ be a prime such that E does not have any p-isogenies. Let N_p be as defined above. Then there exists a newform f of level N_p such that $E \sim_p f$.

Recap

Proposition

Let $E/\mathbb{Q}$ have conductor N, and f have level N'. Suppose $E \sim_p f$. Then there is some prime ideal $\mathfrak{P} \mid p$ of $\mathcal{O}_K$ such that for all primes ℓ

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

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

Recap

Proposition

Let $E/\mathbb{Q}$ have conductor N, and f have level N'. Suppose $E \sim_p f$. Then there is some prime ideal $\mathfrak{P} \mid p$ of $\mathcal{O}_K$ such that for all primes ℓ

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

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

If $E \sim_p f$ and f is rational then we write $E \sim_p E_f$.

Recap

Proposition

Let $E/\mathbb{Q}$ have conductor N, and f have level N'. Suppose $E \sim_p f$. Then there is some prime ideal $\mathfrak{P} \mid p$ of $\mathcal{O}_K$ such that for all primes ℓ

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

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

If $E \sim_p f$ and f is rational then we write $E \sim_p E_f$.

Proposition

Let E, F have conductors N and N' respectively. If $E \sim_p F$ then for all primes ℓ

(i) *if $\ell \nmid NN'$ then $a_\ell(E) \equiv a_\ell(F) \pmod{p}$, and*

(ii) *if $\ell \nmid N'$ and $\ell \mid\mid N$ then $\ell + 1 \equiv \pm a_\ell(F) \pmod{p}$.*

Frey Curves

Given a Diophantine equation, suppose that it has a solution

Frey Curves

Given a Diophantine equation, suppose that it has a solution and associate the solution somehow to an elliptic curve E called a *Frey curve*, **if possible**.

Frey Curves

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

Frey Curves

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

- the coefficients of E depend on the solution to the Diophantine equation;

Frey Curves

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

- the coefficients of E depend on the solution to the Diophantine equation;
- the minimal discriminant of the elliptic curve can be written in the form $\Delta = C \cdot D^p$ where D is an expression that depends on the solution of the Diophantine equation. The factor C **does not depend on the solutions but only on the equation itself**.

Frey Curves

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

- the coefficients of E depend on the solution to the Diophantine equation;
- the minimal discriminant of the elliptic curve can be written in the form $\Delta = C \cdot D^p$ where D is an expression that depends on the solution of the Diophantine equation. The factor C **does not depend on the solutions but only on the equation itself**.
- E has multiplicative reduction at primes dividing D.

Frey Curves II

- the coefficients of E depend on the solution to the Diophantine equation;
- the minimal discriminant of the elliptic curve can be written in the form $\Delta = C \cdot D^p$ where D is an expression that depends on the solution of the Diophantine equation. The factor C **does not depend on the solutions but only on the equation itself**.
- E has multiplicative reduction at primes dividing D.

The conductor N of E will be divisible by the primes dividing C and D, and those dividing D will be removed when we write down N_p. In other words we can make a finite list of possibilities for N_p that depend on the equation. Thus we are able to list a finite set of newforms f such that $E \sim_p f$.

A Variant of the Fermat Equation

Let L be an odd prime number. Consider

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

A Variant of the Fermat Equation

Let L be an odd prime number. Consider

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

We assume that

$$x,\ y,\ z \text{ are pairwise coprime}, \qquad 0 < r < p.$$

A Variant of the Fermat Equation

Let L be an odd prime number. Consider

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

We assume that

$$x,\ y,\ z \text{ are pairwise coprime}, \qquad 0 < r < p.$$

Let A, B, C be some permutation of x^p, $L^r y^p$ and z^p such that $A \equiv -1 \pmod 4$ and $2 \mid B$, and let E be the elliptic curve

$$E \ : \quad Y^2 = X(X-A)(X+B).$$

The minimal discriminant and conductor of E are

$$\Delta_{\min} = 2^{-8} L^{2r} (xyz)^{2p}, \qquad N = \mathrm{Rad}(Lxyz).$$

A Variant of the Fermat Equation

Let L be an odd prime number. Consider

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

We assume that

$$x,\ y,\ z \text{ are pairwise coprime}, \qquad 0 < r < p.$$

Let A, B, C be some permutation of x^p, $L^r y^p$ and z^p such that $A \equiv -1 \pmod 4$ and $2 \mid B$, and let E be the elliptic curve

$$E \quad : \quad Y^2 = X(X-A)(X+B).$$

The minimal discriminant and conductor of E are

$$\Delta_{\min} = 2^{-8} L^{2r} (xyz)^{2p}, \qquad N = \mathrm{Rad}(Lxyz).$$

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

A Variant of the Fermat Equation

Let L be an odd prime number. Consider

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

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

A Variant of the Fermat Equation

Let L be an odd prime number. Consider

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

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

Fact: there are no newforms at levels

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

A Variant of the Fermat Equation

Let L be an odd prime number. Consider

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

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

Fact: there are no newforms at levels

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

Equation has no non-trivial solutions for $L = 3,\ 5,\ 11$.

A Variant of the Fermat Equation

Let L be an odd prime number. Consider

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

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

Fact: there are no newforms at levels

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

Equation has no non-trivial solutions for $L = 3,\ 5,\ 11$.

Can we do anything for other values of L? e.g. $L = 19$.

A Variant of the Fermat Equation

Let L be an odd prime number. Consider

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

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

Fact: there are no newforms at levels

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

Equation has no non-trivial solutions for $L = 3$, 5, 11.

Can we do anything for other values of L? e.g. $L = 19$.

From the above we know that $E \sim_p f$ for some newform at level $N_p = 38$. There are two newforms at level 38:

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

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

A Variant of the Fermat Equation

Let L be an odd prime number. Consider

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

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

Fact: there are no newforms at levels

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

Equation has no non-trivial solutions for $L = 3,\ 5,\ 11$.

Can we do anything for other values of L? e.g. $L = 19$.

From the above we know that $E \sim_p f$ for some newform at level $N_p = 38$. There are two newforms at level 38:

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

No contradiction yet.

Bounding the Exponent

Notation:

Bounding the Exponent

Notation:

- $E/\mathbb{Q}$ elliptic curve of conductor N,

Bounding the Exponent

Notation:

- $E/\mathbb{Q}$ elliptic curve of conductor N,
- $t \mid \#E(\mathbb{Q})_{\text{tors}}$,

Bounding the Exponent

Notation:

- $E/\mathbb{Q}$ elliptic curve of conductor N,
- $t \mid \#E(\mathbb{Q})_{\mathrm{tors}}$,
- f is a newform of level N':

Bounding the Exponent

Notation:

- $E/\mathbb{Q}$ elliptic curve of conductor N,
- $t \mid \#E(\mathbb{Q})_{\mathrm{tors}}$,
- f is a newform of level N':

$$f = q + \sum_{n \geq 2} c_n q^n, \qquad K = \mathbb{Q}(c_2, c_3, \dots).$$

- Suppose $E \sim_p f$.

Bounding the Exponent

Notation:

- $E/\mathbb{Q}$ elliptic curve of conductor N,
- $t \mid \#E(\mathbb{Q})_{\mathrm{tors}}$,
- f is a newform of level N':

$$f = q + \sum_{n \geq 2} c_n q^n, \qquad K = \mathbb{Q}(c_2, c_3, \dots).$$

- Suppose $E \sim_p f$.
- Let ℓ be a prime such that

$$\ell \nmid N', \qquad \ell^2 \nmid N.$$

We know, for some $\mathfrak{P} \mid p$,

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

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

Bounding the Exponent

- $t \mid \#E(\mathbb{Q})_{\mathrm{tors}}$,
- Let ℓ be a prime such that

$$\ell \nmid N', \qquad \ell^2 \nmid N.$$

We know, for some $\mathfrak{P} \mid p$,

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

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

Bounding the Exponent

- $t \mid \#E(\mathbb{Q})_{\text{tors}}$,
- Let ℓ be a prime such that

$$\ell \nmid N', \qquad \ell^2 \nmid N.$$

We know, for some $\mathfrak{P} \mid p$,

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

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

- Either $p = \ell$,
- or $p \mid \text{Norm}(a_\ell(E) - c_\ell) \qquad$ (case $\ell \nmid N$),
- or $p \mid \text{Norm}((\ell+1)^2 - c_\ell^2) \qquad$ (case $\ell \mid N$).

Bounding the Exponent

- $t \mid \#E(\mathbb{Q})_{\mathrm{tors}}$,
- Either $p = \ell$,
- or $p \mid \mathrm{Norm}(a_\ell(E) - c_\ell)$ (case $\ell \nmid N$),
- or $p \mid \mathrm{Norm}((\ell+1)^2 - c_\ell^2)$ (case $\ell \mid N$).

Bounding the Exponent

- $t \mid \#E(\mathbb{Q})_{\mathrm{tors}}$,

- Either $p = \ell$,
- or $p \mid \mathrm{Norm}(a_\ell(E) - c_\ell)$ (case $\ell \nmid N$),
- or $p \mid \mathrm{Norm}((\ell+1)^2 - c_\ell^2)$ (case $\ell \mid N$).

Suppose $\ell \nmid N$.

$$-2\sqrt{\ell} \leq a_\ell(E) \leq \sqrt{\ell}.$$

Bounding the Exponent

- $t \mid \#E(\mathbb{Q})_{\mathrm{tors}}$,

- Either $p = \ell$,
- or $p \mid \mathrm{Norm}(a_\ell(E) - c_\ell)$ (case $\ell \nmid N$),
- or $p \mid \mathrm{Norm}((\ell+1)^2 - c_\ell^2)$ (case $\ell \mid N$).

Suppose $\ell \nmid N$.

$$-2\sqrt{\ell} \leq a_\ell(E) \leq \sqrt{\ell}.$$

Also

$$t \mid \#E(\mathbb{F}_\ell), \qquad \text{since } E(\mathbb{Q})_{\mathrm{tors}} \hookrightarrow E(\mathbb{F}_\ell).$$

Bounding the Exponent

- $t \mid \#E(\mathbb{Q})_{\mathrm{tors}}$,

- Either $p = \ell$,
- or $p \mid \mathrm{Norm}(a_\ell(E) - c_\ell)$ (case $\ell \nmid N$),
- or $p \mid \mathrm{Norm}((\ell+1)^2 - c_\ell^2)$ (case $\ell \mid N$).

Suppose $\ell \nmid N$.

$$-2\sqrt{\ell} \le a_\ell(E) \le \sqrt{\ell}.$$

Also

$$t \mid \#E(\mathbb{F}_\ell), \qquad \text{since } E(\mathbb{Q})_{\mathrm{tors}} \hookrightarrow E(\mathbb{F}_\ell).$$

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

Bounding the Exponent

- $t \mid \#E(\mathbb{Q})_{\mathrm{tors}}$,

- Either $p = \ell$,
- or $p \mid \mathrm{Norm}(a_\ell(E) - c_\ell)$ (case $\ell \nmid N$),
- or $p \mid \mathrm{Norm}((\ell+1)^2 - c_\ell^2)$ (case $\ell \mid N$).

Suppose $\ell \nmid N$.

$$-2\sqrt{\ell} \le a_\ell(E) \le \sqrt{\ell}.$$

Also

$$t \mid \#E(\mathbb{F}_\ell), \qquad \text{since } E(\mathbb{Q})_{\mathrm{tors}} \hookrightarrow E(\mathbb{F}_\ell).$$

But $\#E(\mathbb{F}_\ell) = \ell + 1 - a_\ell(E)$. So

$$p \mid \mathrm{Norm}(a - c_\ell) \qquad -2\sqrt{\ell} \le a \le \sqrt{\ell}, \qquad \ell + 1 \equiv a \pmod{t}.$$

Bounding the Exponent

Proposition

Let ℓ be a prime such that $\ell \nmid N'$ and $\ell^2 \nmid N$. Let

$$S_\ell = \left\{ a \in \mathbb{Z} \ : \quad -2\sqrt{\ell} \le a \le 2\sqrt{\ell}, \quad a \equiv \ell + 1 \pmod{t} \right\}.$$

Let c_ℓ be the ℓ-th coefficient of f and define

$$B'_\ell(f) = \mathrm{Norm}_{K/\mathbb{Q}}((\ell+1)^2 - c_l^2) \prod_{a \in S_\ell} \mathrm{Norm}_{K/\mathbb{Q}}(a - c_\ell)$$

and

$$B_\ell(f) = \begin{cases} \ell \cdot B'_\ell(f) & \text{if } f \text{ is irrational,} \\ B'_\ell(f) & \text{if } f \text{ is rational.} \end{cases}$$

If $E \sim_p f$ then $p \mid B_\ell(f)$.

A Variant of the Fermat Equation

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

We know that $E \sim_p f$ for some newform at level $N_p = 38$. There are two newforms at level 38:

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

A Variant of the Fermat Equation

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

We know that $E \sim_p f$ for some newform at level $N_p = 38$. There are two newforms at level 38:

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

Apply the Proposition with $t = 4$:

$$B_3(f_1) = -15, \qquad B_5(f_1) = -144,$$
$$\gcd(-15, 144) = 3 \Longrightarrow E \not\sim_p f_1 \qquad\qquad (p \geq 5).$$

A Variant of the Fermat Equation

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

We know that $E \sim_p f$ for some newform at level $N_p = 38$. There are two newforms at level 38:

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

Apply the Proposition with $t = 4$:

$$B_3(f_1) = -15, \qquad B_5(f_1) = -144,$$
$$\gcd(-15, 144) = 3 \Longrightarrow E \not\sim_p f_1 \qquad (p \geq 5).$$

Eliminated f_1.

A Variant of the Fermat Equation

Suppose

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

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

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

A Variant of the Fermat Equation

Suppose

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

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

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

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

A Variant of the Fermat Equation

Suppose

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

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

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

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

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

A Variant of the Fermat Equation

Suppose

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

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

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

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

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

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

Eliminating $p = 5$

Suppose $p = 5$. Want a contradiction.

Eliminating $p = 5$

Suppose $p = 5$. Want a contradiction.

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

Eliminating $p = 5$

Suppose $p = 5$. Want a contradiction.

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

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

Eliminating $p = 5$

Suppose $p = 5$. Want a contradiction.

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

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

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

Eliminating $p = 5$

Suppose $p = 5$. Want a contradiction.

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

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

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

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

Eliminating $p = 5$

Suppose $p = 5$. Want a contradiction.

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

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

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

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

The equation

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

has no solutions.

Bounding the Exponent $x^2 - 2 = y^p$?

$$x^2 - 2 = y^p, \qquad p \geq 5 \text{ prime.}$$

Bounding the Exponent $x^2 - 2 = y^p$?

$$x^2 - 2 = y^p, \qquad p \geq 5 \text{ prime.}$$

Frey curve: $\quad E_{(x,y)} \;:\quad Y^2 = X^3 + 2xX^2 + 2X, \qquad\qquad t = 2.$

Bounding the Exponent $x^2 - 2 = y^p$?

$$x^2 - 2 = y^p, \qquad p \geq 5 \text{ prime.}$$

Frey curve: $\quad E_{(x,y)} \; : \quad Y^2 = X^3 + 2xX^2 + 2X, \qquad\qquad t = 2.$

$$\Delta_{\min} = 2^8 y^p, \qquad N = 2^7 \operatorname{Rad}(y), \qquad N_p = 128.$$

Bounding the Exponent $x^2 - 2 = y^p$?

$$x^2 - 2 = y^p, \qquad p \geq 5 \text{ prime}.$$

Frey curve: $\quad E_{(x,y)} \; : \quad Y^2 = X^3 + 2xX^2 + 2X, \qquad t = 2.$

$$\Delta_{\min} = 2^8 y^p, \qquad N = 2^7 \operatorname{Rad}(y), \qquad N_p = 128.$$

By Ribet, $E_{(x,y)} \sim_p F$ where F is one of

$$F_1 = 128A1, \quad F_2 = 128B1, \quad F_3 = 128C1, \quad F_4 = 128D1.$$

Bounding the Exponent $x^2 - 2 = y^p$?

$$x^2 - 2 = y^p, \qquad p \geq 5 \text{ prime.}$$

Frey curve: $\quad E_{(x,y)} \ : \quad Y^2 = X^3 + 2xX^2 + 2X, \qquad t = 2.$

$$\Delta_{\min} = 2^8 y^p, \qquad N = 2^7 \,\mathrm{Rad}(y), \qquad N_p = 128.$$

By Ribet, $E_{(x,y)} \sim_p F$ where F is one of

$$F_1 = 128A1, \quad F_2 = 128B1, \quad F_3 = 128C1, \quad F_4 = 128D1.$$

Exercise: Show that $B_\ell(F_i) = 0$ for all ℓ and $i = 1, 2, 3, 4$.

Bounding the Exponent $x^2 - 2 = y^p$?

$$x^2 - 2 = y^p, \qquad p \geq 5 \text{ prime.}$$

Frey curve: $\quad E_{(x,y)} \; : \quad Y^2 = X^3 + 2xX^2 + 2X, \qquad\qquad t = 2.$

$$\Delta_{\min} = 2^8 y^p, \qquad N = 2^7 \operatorname{Rad}(y), \qquad N_p = 128.$$

By Ribet, $E_{(x,y)} \sim_p F$ where F is one of

$$F_1 = 128A1, \quad F_2 = 128B1, \quad F_3 = 128C1, \quad F_4 = 128D1.$$

Exercise: Show that $B_\ell(F_i) = 0$ for all ℓ and $i = 1, 2, 3, 4$.
No bound on p from the modular method. Note $E_{(-1,-1)} = F_1$ and $E_{(1,-1)} = F_3$.

Bounding the Exponent $x^2 - 2 = y^p$?

$$x^2 - 2 = y^p, \qquad p \geq 5 \text{ prime.}$$

Frey curve: $\quad E_{(x,y)} \ : \quad Y^2 = X^3 + 2xX^2 + 2X, \qquad t = 2.$

$$\Delta_{\min} = 2^8 y^p, \qquad N = 2^7 \operatorname{Rad}(y), \qquad N_p = 128.$$

By Ribet, $E_{(x,y)} \sim_p F$ where F is one of

$$F_1 = 128A1, \quad F_2 = 128B1, \quad F_3 = 128C1, \quad F_4 = 128D1.$$

Exercise: Show that $B_\ell(F_i) = 0$ for all ℓ and $i = 1, 2, 3, 4$.
No bound on p from the modular method. Note $E_{(-1,-1)} = F_1$ and $E_{(1,-1)} = F_3$.
Note equation has solutions $(x, y, p) = (\pm 1, -1, p)$.

Bounding the Exponent

$$B_\ell(f) \neq 0 \implies p \text{ is bounded.}$$

Bounding the Exponent

$$B_\ell(f) \neq 0 \Longrightarrow p \text{ is bounded.}$$

We are guaranteed to succeed in two cases:

(a) **If f is irrational**, then $c_\ell \notin \mathbb{Q}$ for infinitely many of the coefficients ℓ, and so $B_\ell(f) \neq 0$.

Bounding the Exponent

$$B_\ell(f) \neq 0 \Longrightarrow p \text{ is bounded.}$$

We are guaranteed to succeed in two cases:

(a) **If f is irrational**, then $c_\ell \notin \mathbb{Q}$ for infinitely many of the coefficients ℓ, and so $B_\ell(f) \neq 0$.

(b) Suppose
- f is rational,
- t is prime or $t = 4$,
- every elliptic curve F in the isogeny class corresponding to f we have $t \nmid \#F(\mathbb{Q})_{\mathrm{tors}}$.

Then there are infinitely many primes ℓ such that $B_\ell(f) \neq 0$.

Method of Kraus

$$x^2 + 7 = y^m, \qquad m \geq 3.$$

Method of Kraus

$$x^2 + 7 = y^m, \qquad m \geq 3.$$

Easy exercise: Show there are no solutions with y odd.

Method of Kraus

$$x^2 + 7 = y^m, \qquad m \geq 3.$$

Easy exercise: Show there are no solutions with y odd.

- Hint: just like $x^2 + 1 = y^p$.

Method of Kraus

$$x^2 + 7 = y^m, \qquad m \geq 3.$$

Easy exercise: Show there are no solutions with y odd.

- Hint: just like $x^2 + 1 = y^p$.
- Don't bother doing the exercise!

Method of Kraus

$$x^2 + 7 = y^m, \qquad m \geq 3.$$

Easy exercise: Show there are no solutions with y odd.

- Hint: just like $x^2 + 1 = y^p$.
- Don't bother doing the exercise!

Plenty of solutions with y even.

m	x	y	m	x	y	m	x	y
3	± 1	2	3	± 181	32	4	± 3	± 2
5	± 5	2	5	± 181	8	7	± 11	2
15	± 181	2						

The Method of Kraus

$$x^2 + 7 = y^p, \qquad p \geq 11.$$

The Method of Kraus

$$x^2 + 7 = y^p, \qquad p \geq 11.$$

WLOG

$$x \equiv 1 \pmod 4 \qquad \text{and} \qquad y \text{ is even.}$$

The Method of Kraus

$$x^2 + 7 = y^p, \qquad p \geq 11.$$

WLOG

$$x \equiv 1 \pmod 4 \qquad \text{and} \qquad y \text{ is even.}$$

$$E_x : \qquad Y^2 = X^3 + xX^2 + \frac{(x^2+7)}{4} X$$

$$\Delta = \frac{-7y^p}{2^{12}}, \qquad N = 14 \prod_{\ell \mid y,\ \ell \nmid 14} \ell.$$

The Method of Kraus

$$x^2 + 7 = y^p, \qquad p \geq 11.$$

WLOG

$$x \equiv 1 \pmod 4 \qquad \text{and} \qquad y \text{ is even.}$$

$$E_x: \qquad Y^2 = X^3 + xX^2 + \frac{(x^2+7)}{4} X$$

$$\Delta = \frac{-7y^p}{2^{12}}, \qquad N = 14 \prod_{\ell \mid y,\ \ell \nmid 14} \ell.$$

$E_x \sim_p F$ where $F = 14A$. Note $E_{-11} = 14A4$.

Fix $p \geq 11$. We choose ℓ satisfying certain conditions so that we obtain a contradiction.

- **Condition 1:** $\ell \nmid 14, \qquad \left(\frac{-7}{\ell}\right) = 1.$

Fix $p \geq 11$. We choose ℓ satisfying certain conditions so that we obtain a contradiction.

- **Condition 1:** $\ell \nmid 14$, $\quad \left(\frac{-7}{\ell}\right) = 1$.

So $\ell \nmid (x^2 + 7)$. Hence $\ell \nmid NN'$.

Fix $p \geq 11$. We choose ℓ satisfying certain conditions so that we obtain a contradiction.

- **Condition 1:** $\ell \nmid 14, \qquad \left(\frac{-7}{\ell}\right) = 1.$

So $\ell \nmid (x^2 + 7)$. Hence $\ell \nmid NN'$.

$$a_\ell(E_x) \equiv a_\ell(F) \pmod{p}.$$

Fix $p \geq 11$. We choose ℓ satisfying certain conditions so that we obtain a contradiction.

- **Condition 1:** $\ell \nmid 14, \qquad \left(\frac{-7}{\ell}\right) = 1.$

So $\ell \nmid (x^2+7)$. Hence $\ell \nmid NN'$.

$$a_\ell(E_x) \equiv a_\ell(F) \pmod{p}.$$

Let

$$T(\ell, p) = \{\alpha \in \mathbb{F}_\ell : a_\ell(E_\alpha) \equiv a_\ell(F) \pmod{p}\}.$$

Fix $p \geq 11$. We choose ℓ satisfying certain conditions so that we obtain a contradiction.

- **Condition 1:** $\ell \nmid 14, \qquad \left(\frac{-7}{\ell}\right) = 1.$

So $\ell \nmid (x^2 + 7)$. Hence $\ell \nmid NN'$.

$$a_\ell(E_x) \equiv a_\ell(F) \pmod{p}.$$

Let

$$T(\ell, p) = \{\alpha \in \mathbb{F}_\ell : a_\ell(E_\alpha) \equiv a_\ell(F) \pmod{p}\}.$$

So $x \equiv \alpha \pmod{\ell}$ for some $\alpha \in T(\ell, p)$.
Let

$$R(\ell, p) = \{\beta \in \mathbb{F}_\ell : \beta^2 + 7 \in (\mathbb{F}_\ell^\times)^p\}.$$

Also $x \equiv \beta \pmod{\ell}$ for some $\beta \in R(\ell, p)$.

The Method of Kraus

Lemma

If ℓ satisfies Condition 1 and $T(\ell, p) \cap R(\ell, p) = \emptyset$ then $x^2 + 7 = y^p$ has no solutions.

The Method of Kraus

Lemma

If ℓ satisfies Condition 1 and $T(\ell, p) \cap R(\ell, p) = \emptyset$ then $x^2 + 7 = y^p$ has no solutions.

$$T(\ell, p) = \{\alpha \in \mathbb{F}_\ell : a_\ell(E_\alpha) \equiv a_\ell(F) \pmod{p}\}.$$

$$R(\ell, p) = \{\beta \in \mathbb{F}_\ell : \beta^2 + 7 \in (\mathbb{F}_\ell^\times)^p\}.$$

The Method of Kraus

Lemma

If ℓ satisfies Condition 1 and $T(\ell, p) \cap R(\ell, p) = \emptyset$ then $x^2 + 7 = y^p$ has no solutions.

$$T(\ell, p) = \{\alpha \in \mathbb{F}_\ell : a_\ell(E_\alpha) \equiv a_\ell(F) \pmod{p}\}.$$

$$R(\ell, p) = \{\beta \in \mathbb{F}_\ell : \beta^2 + 7 \in (\mathbb{F}_\ell^\times)^p\}.$$

Note $T(\ell, p) \neq \emptyset$. e.g. $\overline{-11} \in T(\ell, p)$.

The Method of Kraus

Lemma

If ℓ satisfies Condition 1 and $T(\ell,p) \cap R(\ell,p) = \emptyset$ then $x^2 + 7 = y^p$ has no solutions.

$$T(\ell,p) = \{\alpha \in \mathbb{F}_\ell : a_\ell(E_\alpha) \equiv a_\ell(F) \pmod{p}\}.$$

$$R(\ell,p) = \{\beta \in \mathbb{F}_\ell : \beta^2 + 7 \in (\mathbb{F}_\ell^\times)^p\}.$$

Note $T(\ell,p) \neq \emptyset$. e.g. $\overline{-11} \in T(\ell,p)$.
If $p \nmid (\ell - 1)$ then

$$(\mathbb{F}_\ell^\times)^p = \mathbb{F}_\ell^\times \implies R(\ell,p) = \mathbb{F}_\ell \implies T(\ell,p) \cap R(\ell,p) \neq \emptyset.$$

The Method of Kraus

Lemma

If ℓ satisfies Condition 1 and $T(\ell, p) \cap R(\ell, p) = \emptyset$ then $x^2 + 7 = y^p$ has no solutions.

$$T(\ell, p) = \{\alpha \in \mathbb{F}_\ell : a_\ell(E_\alpha) \equiv a_\ell(F) \pmod{p}\}.$$

$$R(\ell, p) = \{\beta \in \mathbb{F}_\ell : \beta^2 + 7 \in (\mathbb{F}_\ell^\times)^p\}.$$

Note $T(\ell, p) \neq \emptyset$. e.g. $\overline{-11} \in T(\ell, p)$.

If $p \nmid (\ell - 1)$ then

$$(\mathbb{F}_\ell^\times)^p = \mathbb{F}_\ell^\times \implies R(\ell, p) = \mathbb{F}_\ell \implies T(\ell, p) \cap R(\ell, p) \neq \emptyset.$$

However, if $p \mid (\ell - 1)$, then

$$\#(\mathbb{F}_\ell^\times)^p = \frac{\ell - 1}{p}. \implies \text{good chance that } T(\ell, p) = R(\ell, p).$$

Proposition

There are no solutions to $x^2 + 7 = y^p$ *with* $11 \leq p \leq 10^8$.

Proof.

By computer. For each p find $\ell \equiv 1 \pmod{p}$ satisfying condition 1, so that $T(\ell, p) \cap R(\ell, p) = \emptyset$. □

Theorem

The only solutions to $x^2 + 7 = y^m$, *with* $m \geq 3$ *are*

m	x	y	m	x	y	m	x	y
3	± 1	2	3	± 181	32	4	± 3	± 2
5	± 5	2	5	± 181	8	7	± 11	2
15	± 181	2						

Proof.

Linear forms in logs tell us $p \leq 10^8$. For small m reduce to Thue equations and solve by computer algebra. □