Modular Approach to Diophantine Equations

Samir Siksek

University of Warwick

June 13, 2012

Objectives

Galois representations and modularity led to Wiles' proof of Fermat's Last Theorem. A similar strategy can be used to study many other Diophantine equations. To understand the ideas behind this method properly you need to know:

Objectives

Galois representations and modularity led to Wiles' proof of Fermat's Last Theorem. A similar strategy can be used to study many other Diophantine equations. To understand the ideas behind this method properly you need to know:

1. a lot about elliptic curves,
2. a lot about modular forms,
3. a lot about Galois representations.

Objectives

Galois representations and modularity led to Wiles' proof of Fermat's Last Theorem. A similar strategy can be used to study many other Diophantine equations. To understand the ideas behind this method properly you need to know:

1. a lot about elliptic curves,
2. a lot about modular forms,
3. a lot about Galois representations.

Instead, we want to see how to **use** the method with:

Objectives

Galois representations and modularity led to Wiles' proof of Fermat's Last Theorem. A similar strategy can be used to study many other Diophantine equations. To understand the ideas behind this method properly you need to know:

1. a lot about elliptic curves,
2. a lot about modular forms,
3. a lot about Galois representations.

Instead, we want to see how to **use** the method with:

1. knowing only a few things about elliptic curves,
2. knowing even less about modular forms,
3. knowing nothing about Galois representations.

Facts About Newforms I

Definition for the cognescenti. By the newforms of level N I mean a normalized eigenbasis for $S_2^{\mathrm{new}}(N)$.

Facts About Newforms I

Definition for the cognescenti. By the newforms of level N I mean a normalized eigenbasis for $S_2^{\mathrm{new}}(N)$.

For everyone else.

1. $N \geq 1$ is an integer called the level.

Facts About Newforms I

Definition for the cognescenti. By the newforms of level N I mean a normalized eigenbasis for $S_2^{\mathrm{new}}(N)$.

For everyone else.

1. $N \geq 1$ is an integer called the level.
2. There are finitely many newforms of level N.

Facts About Newforms I

Definition for the cognescenti. By the newforms of level N I mean a normalized eigenbasis for $S_2^{\mathrm{new}}(N)$.

For everyone else.

1. $N \geq 1$ is an integer called the level.
2. There are finitely many newforms of level N.
3. There are algorithms implemented in `SAGE` and `MAGMA` for computing the newforms of level N.

Facts About Newforms I

Definition for the cognescenti. By the newforms of level N I mean a normalized eigenbasis for $S_2^{\mathrm{new}}(N)$.
For everyone else.

1. $N \geq 1$ is an integer called the level.
2. There are finitely many newforms of level N.
3. There are algorithms implemented in `SAGE` and `MAGMA` for computing the newforms of level N.
4. A newform is normally given in terms of its q-expansion

$$f = q + \sum_{n \geq 2} c_n q^n.$$

Facts About Newforms II

1. A newform is normally given in terms of its q-expansion

$$f = q + \sum_{n \geq 2} c_n q^n.$$

Facts About Newforms II

1. A newform is normally given in terms of its q-expansion

$$f = q + \sum_{n \geq 2} c_n q^n.$$

2. $K = \mathbb{Q}(c_2, c_3, \ldots)$ is a totally real **finite** extension of $\mathbb{Q}$.

Facts About Newforms II

1. A newform is normally given in terms of its q-expansion
$$f = q + \sum_{n \geq 2} c_n q^n.$$
2. $K = \mathbb{Q}(c_2, c_3, \ldots)$ is a totally real **finite** extension of $\mathbb{Q}$.
3. $c_i \in \mathcal{O}_K$.

Facts About Newforms II

1. A newform is normally given in terms of its q-expansion
$$f = q + \sum_{n \geq 2} c_n q^n.$$
2. $K = \mathbb{Q}(c_2, c_3, \ldots)$ is a totally real **finite** extension of $\mathbb{Q}$.
3. $c_i \in \mathcal{O}_K$.
4. If ℓ is a prime then
$$|c_\ell^\sigma| \leq 2\sqrt{\ell} \qquad \text{for all embeddings } \sigma : K \hookrightarrow \mathbb{R}.$$

Facts About Newforms II

1. A newform is normally given in terms of its q-expansion
$$f = q + \sum_{n \geq 2} c_n q^n.$$
2. $K = \mathbb{Q}(c_2, c_3, \dots)$ is a totally real **finite** extension of $\mathbb{Q}$.
3. $c_i \in \mathcal{O}_K$.
4. If ℓ is a prime then
$$|c_\ell^\sigma| \leq 2\sqrt{\ell} \qquad \text{for all embeddings } \sigma : K \hookrightarrow \mathbb{R}.$$

Theorem

There are no newforms at levels

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

Example

The newforms at a fixed level N can be computed using the modular symbols algorithm implemented in `MAGMA` and `SAGE`. For example, the newforms at level 110 are

$$f_1 = q - q^2 + q^3 + q^4 - q^5 - q^6 + 5q^7 + \cdots,$$
$$f_2 = q + q^2 + q^3 + q^4 - q^5 + q^6 - q^7 + \cdots,$$
$$f_3 = q + q^2 - q^3 + q^4 + q^5 - q^6 + 3q^7 + \cdots,$$
$$f_4 = q - q^2 + \theta q^3 + q^4 + q^5 - \theta q^6 - \theta q^7 + \cdots.$$

Example

The newforms at a fixed level N can be computed using the modular symbols algorithm implemented in `MAGMA` and `SAGE`. For example, the newforms at level 110 are

$$\begin{aligned} f_1 &= q - q^2 + q^3 + q^4 - q^5 - q^6 + 5q^7 + \cdots, \\ f_2 &= q + q^2 + q^3 + q^4 - q^5 + q^6 - q^7 + \cdots, \\ f_3 &= q + q^2 - q^3 + q^4 + q^5 - q^6 + 3q^7 + \cdots, \\ f_4 &= q - q^2 + \theta q^3 + q^4 + q^5 - \theta q^6 - \theta q^7 + \cdots. \end{aligned}$$

f_1, f_2, f_3 have coefficients in $\mathbb{Z}$

Example

The newforms at a fixed level N can be computed using the modular symbols algorithm implemented in `MAGMA` and `SAGE`. For example, the newforms at level 110 are

$$\begin{aligned}
f_1 &= q - q^2 + q^3 + q^4 - q^5 - q^6 + 5q^7 + \cdots, \\
f_2 &= q + q^2 + q^3 + q^4 - q^5 + q^6 - q^7 + \cdots, \\
f_3 &= q + q^2 - q^3 + q^4 + q^5 - q^6 + 3q^7 + \cdots, \\
f_4 &= q - q^2 + \theta q^3 + q^4 + q^5 - \theta q^6 - \theta q^7 + \cdots.
\end{aligned}$$

f_1, f_2, f_3 have coefficients in $\mathbb{Z}$
f_4 has coefficients in $\mathbb{Z}[\theta]$ where $\theta = (-1 + \sqrt{33})/2$.

Example

The newforms at a fixed level N can be computed using the modular symbols algorithm implemented in `MAGMA` and `SAGE`. For example, the newforms at level 110 are

$$f_1 = q - q^2 + q^3 + q^4 - q^5 - q^6 + 5q^7 + \cdots,$$
$$f_2 = q + q^2 + q^3 + q^4 - q^5 + q^6 - q^7 + \cdots,$$
$$f_3 = q + q^2 - q^3 + q^4 + q^5 - q^6 + 3q^7 + \cdots,$$
$$f_4 = q - q^2 + \theta q^3 + q^4 + q^5 - \theta q^6 - \theta q^7 + \cdots.$$

f_1, f_2, f_3 have coefficients in $\mathbb{Z}$
f_4 has coefficients in $\mathbb{Z}[\theta]$ where $\theta = (-1 + \sqrt{33})/2$.
there is a fifth newform at level 110 which is the conjugate of f_4.

Correspondence between rational newforms and elliptic curves

We call a newform *rational* if its coefficients are all in $\mathbb{Q}$, otherwise we call it *irrational*.

Correspondence between rational newforms and elliptic curves

We call a newform *rational* if its coefficients are all in $\mathbb{Q}$, otherwise we call it *irrational*.

The Modularity Theorem for Elliptic Curves (Wiles and many others). There is a bijection

$$\text{rational newforms of level } N \longleftrightarrow \begin{array}{l}\text{isogeny classes of elliptic curves}\\ \text{of conductor } N\end{array}$$

$$f = q + \sum c_n q^n \mapsto E_f/\mathbb{Q},$$

Correspondence between rational newforms and elliptic curves

We call a newform *rational* if its coefficients are all in $\mathbb{Q}$, otherwise we call it *irrational*.

The Modularity Theorem for Elliptic Curves (Wiles and many others). There is a bijection

$$\text{rational newforms of level } N \longleftrightarrow \text{isogeny classes of elliptic curves of conductor } N$$

$$f = q + \sum c_n q^n \mapsto E_f/\mathbb{Q},$$

such that for all primes $\ell \nmid N$

$$c_\ell = a_\ell(E_f) \qquad a_\ell(E_f) := \ell + 1 - \#E(\mathbb{F}_\ell).$$

'arises from'

Definition

Let E/Q be an elliptic curve and

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

a newform.

'arises from'

Definition

Let E/Q be an elliptic curve and

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

a newform. We say that the curve E **arises modulo p from the newform** f if there is some prime ideal $\mathfrak{P} \mid p$ of $\mathcal{O}_K$ such that

‘arises from’

Definition

Let E/Q be an elliptic curve and

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

a newform. We say that the curve E **arises modulo** p **from the newform** f if there is some prime ideal $\mathfrak{P} \mid p$ of $\mathcal{O}_K$ such that

$$a_\ell(E) \equiv c_\ell \pmod{\mathfrak{P}} \qquad \text{for almost all primes } \ell.$$

'arises from'

Definition

Let E/Q be an elliptic curve and

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

a newform. We say that the curve E **arises modulo** p **from the newform** f if there is some prime ideal $\mathfrak{P} \mid p$ of $\mathcal{O}_K$ such that

$$a_\ell(E) \equiv c_\ell \pmod{\mathfrak{P}} \qquad \text{for almost all primes } \ell.$$

Notation: $E \sim_p f$.

More Precise 'Arises From'

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 $\ell + 1 \equiv \pm c_\ell \pmod{\mathfrak{P}}$.*

More Precise 'Arises From'

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 $E \sim_p E_f$.

More Precise 'Arises From'

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 $\ell + 1 \equiv \pm a_\ell(F) \pmod{p}$.*

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

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

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

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

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 $E \sim_p f$.

Example

Let

$$E \quad : \quad y^2 = x^3 - x^2 - 77x + 330 \qquad (132B1).$$

Then

$$\Delta_{\min} = 2^4 \times 3^{10} \times 11, \qquad N = 132 = 2^2 \times 3 \times 11.$$

The only isogeny the curve E has is a 2-isogeny. Recall

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

So

$$N_5 = \frac{2^2 \times 3 \times 11}{3} = 44, \qquad N_p = 132 \text{ for } p \geq 7.$$

Example Continued

Apply Ribet Theorem with $p = 5$. Then $E \sim_5 f$ for some newform of level $N_5 = 44$. There is only one newform at level 44 which corresponds to the elliptic curve

$$F \;:\quad y^2 = x^3 + x^2 + 3x - 1 \qquad (44A1).$$

Thus $E \sim_5 F$.

ℓ	2	3	5	7	11	13	17	19
$a_\ell(E)$	0	-1	2	2	-1	6	-4	-2
$a_\ell(F)$	0	1	-3	2	-1	-4	6	8

Example Continued

Apply Ribet Theorem with $p = 5$. Then $E \sim_5 f$ for some newform of level $N_5 = 44$. There is only one newform at level 44 which corresponds to the elliptic curve

$$F \;:\quad y^2 = x^3 + x^2 + 3x - 1 \qquad (44A1).$$

Thus $E \sim_5 F$.

ℓ	2	3	5	7	11	13	17	19
$a_\ell(E)$	0	-1	2	2	-1	6	-4	-2
$a_\ell(F)$	0	1	-3	2	-1	-4	6	8

For $p \geq 7$, we have $N_p = N$, and Ribet's Theorem tells us the $E \sim_p E$ which is not interesting.

Absence of Isogenies

Theorem

(Mazur) Let $E/\mathbb{Q}$ be an elliptic curve satisfying **at least one** *of the following conditions holds.*

- $p \geq 17$ *and* $j(E) \notin \mathbb{Z}[\frac{1}{2}]$,
- *or* $p \geq 11$ *and* E *is a semi-stable elliptic curve,*
- *or* $p \geq 5$, $\#E(\mathbb{Q})[2] = 4$, *and* E *is a semi-stable elliptic curve,*

Then E *does not have any* p*-isogenies.*

Absence of Isogenies

Theorem

(Mazur) Let $E/\mathbb{Q}$ be an elliptic curve satisfying **at least one** *of the following conditions holds.*

- $p \geq 17$ *and* $j(E) \notin \mathbb{Z}[\frac{1}{2}]$,
- *or* $p \geq 11$ *and E is a semi-stable elliptic curve,*
- *or* $p \geq 5$, $\#E(\mathbb{Q})[2] = 4$, *and E is a semi-stable elliptic curve,*

Then E does not have any p-isogenies.

Theorem

(Diamond and Kramer) If $\mathrm{ord}_2(N) = 3, 5, 7$ *then E does not have any isogenies of odd degree.*

Absence of Isogenies

Theorem

(Mazur) Let $E/\mathbb{Q}$ be an elliptic curve satisfying **at least one** *of the following conditions holds.*

- $p \geq 17$ *and* $j(E) \notin \mathbb{Z}[\frac{1}{2}]$,
- *or* $p \geq 11$ *and* E *is a semi-stable elliptic curve,*
- *or* $p \geq 5$, $\#E(\mathbb{Q})[2] = 4$, *and* E *is a semi-stable elliptic curve,*

Then E *does not have any* p*-isogenies.*

Theorem

(Diamond and Kramer) If $\mathrm{ord}_2(N) = 3, 5, 7$ *then* E *does not have any isogenies of odd degree.*

If all else fails,

$$E \text{ has no } p\text{-isogenies} \iff p\text{-th division poly is irreducible.}$$

Fermat's Last Theorem

Theorem

(Wiles) Suppose $p \geq 5$ is prime. The equation

$$x^p + y^p + z^p = 0 \tag{1}$$

has no solutions with $xyz \neq 0$.

Proof. Suppose $xyz \neq 0$. Without loss of generality: x, y, z are coprime, and

$$2 \mid y, \qquad x^p \equiv -1 \pmod 4, \qquad z^p \equiv 1 \pmod 4.$$

Associate to this solution the elliptic curve (called a Frey curve)

$$E \ : \quad Y^2 = X(X - x^p)(X + y^p).$$

Proof of FLT (continued)

Without loss of generality: x, y, z are coprime, and

$$2 \mid y, \qquad x^p \equiv -1 \pmod 4, \qquad z^p \equiv 1 \pmod 4.$$

Associate to this solution the elliptic curve (called a Frey curve)

$$E \quad : \quad Y^2 = X(X - x^p)(X + y^p).$$

Proof of FLT (continued)

Without loss of generality: x, y, z are coprime, and

$$2 \mid y, \qquad x^p \equiv -1 \pmod 4, \qquad z^p \equiv 1 \pmod 4.$$

Associate to this solution the elliptic curve (called a Frey curve)

$$E \ : \quad Y^2 = X(X - x^p)(X + y^p).$$

(For $Y^2 = X(X+a)(X+b)$, the discriminant is $16a^2b^2(a-b)^2$.)

Proof of FLT (continued)

Without loss of generality: x, y, z are coprime, and

$$2 \mid y, \qquad x^p \equiv -1 \pmod 4, \qquad z^p \equiv 1 \pmod 4.$$

Associate to this solution the elliptic curve (called a Frey curve)

$$E \ : \quad Y^2 = X(X - x^p)(X + y^p).$$

(For $Y^2 = X(X + a)(X + b)$, the discriminant is $16a^2b^2(a - b)^2$.)
So

$$\Delta = 16x^{2p}y^{2p}(x^p + y^p)^2 = 16x^{2p}y^{2p}z^{2p}$$

using $x^p + y^p + z^p = 0$.

Proof of FLT (continued)

Without loss of generality: x, y, z are coprime, and

$$2 \mid y, \qquad x^p \equiv -1 \pmod 4, \qquad z^p \equiv 1 \pmod 4.$$

Associate to this solution the elliptic curve (called a Frey curve)

$$E \ : \quad Y^2 = X(X - x^p)(X + y^p).$$

(For $Y^2 = X(X+a)(X+b)$, the discriminant is $16a^2b^2(a-b)^2$.)
So

$$\Delta = 16x^{2p}y^{2p}(x^p + y^p)^2 = 16x^{2p}y^{2p}z^{2p}$$

using $x^p + y^p + z^p = 0$.
Also

$$c_4 = 16(z^{2p} - x^p y^p), \qquad \gcd(c_4, \Delta) = 16.$$

FLT continued

Applying Tate's algorithm to compute the minimal discriminant and conductor:

$$\Delta_{\min} = 2^{-8}(xyz)^{2p}, \qquad N = \prod_{\ell \mid xyz} \ell.$$

FLT continued

Applying Tate's algorithm to compute the minimal discriminant and conductor:

$$\Delta_{\min} = 2^{-8}(xyz)^{2p}, \qquad N = \prod_{\ell \mid xyz} \ell.$$

$$N_p = N \Big/ \prod_{\substack{\ell \| N, \\ p \,\mid\, \mathrm{ord}_\ell(\Delta)}} \ell \implies N_2 = 2.$$

FLT continued

Applying Tate's algorithm to compute the minimal discriminant and conductor:

$$\Delta_{\min} = 2^{-8}(xyz)^{2p}, \qquad N = \prod_{\ell \mid xyz} \ell.$$

$$N_p = N \Big/ \prod_{\substack{\ell \| N, \\ p \,\mid\, \mathrm{ord}_\ell(\Delta)}} \ell \Longrightarrow N_2 = 2.$$

$$E(\mathbb{Q})[2] = 4 \text{ and } N \text{ squarefree } \underbrace{\Longrightarrow}_{\text{Mazur}} \text{ no } p\text{-isogenies.}$$

FLT continued

Applying Tate's algorithm to compute the minimal discriminant and conductor:

$$\Delta_{\min} = 2^{-8}(xyz)^{2p}, \qquad N = \prod_{\ell \mid xyz} \ell.$$

$$N_p = N \Big/ \prod_{\substack{\ell \| N, \\ p \,\mid\, \mathrm{ord}_\ell(\Delta)}} \ell \Longrightarrow N_2 = 2.$$

$$E(\mathbb{Q})[2] = 4 \text{ and } N \text{ squarefree} \underbrace{\Longrightarrow}_{\text{Mazur}} \text{no } p\text{-isogenies.}$$

By Ribet, there is a newform f of level $N_p = 2$ such that $E \sim_p f$.

FLT continued

Applying Tate's algorithm to compute the minimal discriminant and conductor:

$$\Delta_{\min} = 2^{-8}(xyz)^{2p}, \qquad N = \prod_{\ell \mid xyz} \ell.$$

$$N_p = N \Bigg/ \prod_{\substack{\ell \| N, \\ p \mid \mathrm{ord}_\ell(\Delta)}} \ell \Longrightarrow N_2 = 2.$$

$$E(\mathbb{Q})[2] = 4 \text{ and } N \text{ squarefree} \underbrace{\Longrightarrow}_{\text{Mazur}} \text{no } p\text{-isogenies.}$$

By Ribet, there is a newform f of level $N_p = 2$ such that $E \sim_p f$. CONTRADICTION.

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 $E \sim_p f$.