Elliptic Curves, Modular Forms and the Modularity Theorem

Michael Bennett

University of British Columbia

Bilecik : September, 2014

Elliptic Curves : motivation

According to Hilbert....
A *Diophantine equation* is an equation of the form

$$D(x_1, \ldots, x_m) = 0,$$

where D is a polynomial with integer coefficients.

Hilbert's 10th problem : Determination of the solvability of a Diophantine equation. Given a diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers.

Elliptic Curves : motivation

Unfortunately (?), no such process exists in general....

Elliptic Curves : motivation

Unfortunately (?), no such process exists in general....

On the other hand, Matiyasevich showed that it is possible to construct equations of the shape

$$D(x_1, \ldots, x_m) = 0$$

which have solutions in integers precisely when one of the following is true

- Goldbach's Conjecture
- the Riemann Hypothesis
- the Four Colour Theorem

Elliptic Curves : motivation

On the other hand, the only examples known of equations which are non-solvable have either a fairly large number of variables or a high degree, or both.

Elliptic Curves : motivation

On the other hand, the only examples known of equations which are non-solvable have either a fairly large number of variables or a high degree, or both.

Perhaps we can still hope for an algorithmic resolution of Diophantine equations in "simple" cases!

Simple cases

- Polynomials in one variable :

$$a_n x^n + \cdots + a_1 x + a_0 = 0 \text{ with } a_i \in \mathbb{Z}.$$

- Linear equations in two variables :

$$ax + by = c.$$

- Quadratic equations in two variables (conics) :

$$ax^2 + bxy + cy^2 + dx + ey + f = 0.$$

The next case

Cubic equations :

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0.$$

The next case

Cubic equations :

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0.$$

Such equations can have

The next case

Cubic equations :

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0.$$

Such equations can have

- No rational solutions,

The next case

Cubic equations :

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0.$$

Such equations can have

- No rational solutions,
- Finitely many rational solutions, or

The next case

Cubic equations :

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0.$$

Such equations can have

- No rational solutions,
- Finitely many rational solutions, or
- Infinitely many rational solutions.

The next case

Cubic equations :

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0.$$

Such equations can have

- No rational solutions,
- Finitely many rational solutions, or
- Infinitely many rational solutions.

We have no algorithm for determining all rational solutions to such equations (though, conjecturally, we do).

Elliptic curves : definition

Definition An elliptic curve over $\mathbb{Q}$ is a smooth cubic projective curve E defined over $\mathbb{Q}$, with at least one rational point that we call the origin.

Elliptic curves

Via change of variable, we may consider a cubic curve of the form

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

or, more simply, if we avoid characteristic 2 and 3,

$$E \quad : \quad y^2 = x^3 + ax + b$$

with discriminant

$$\Delta = \Delta_E = -16\left(4a^3 + 27b^2\right) \neq 0.$$

Let us suppose that a and b are rational integers.

Elliptic curves

Given

$$E \quad : \quad y^2 = x^3 + ax + b,$$

the projective closure of E is a smooth plane projective curve with a single (flex) point at infinity, $\mathcal{O}_E = [0 : 1 : 0]$.

Elliptic curves

Given

$$E \quad : \quad y^2 = x^3 + ax + b,$$

the projective closure of E is a smooth plane projective curve with a single (flex) point at infinity, $\mathcal{O}_E = [0 : 1 : 0]$.

If K is a number field, the rational points $E(K)$ form an abelian group with identity $\mathcal{O}_E$, where $P + Q + R = \mathcal{O}_E$ iff $P; Q; R$ are the intersection points of E with a line.

The Mordell-Weil Theorem

Theorem (Mordell-Weil) Under chord-tangent addition, $E(K)$ forms a finitely generated abelian group.

The Mordell-Weil Theorem

Theorem (Mordell-Weil) Under chord-tangent addition, $E(K)$ forms a finitely generated abelian group.

In particular, we have

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tors}}$$

where r is a nonnegative integer, called the *rank* of E over $\mathbb{Q}$, and $E(\mathbb{Q})_{\text{tors}}$ is a finite abelian group.

What are the possibilities for the rank r?

What are the possibilities for the rank r?

We know examples of rank exactly 19 and at least 28.

What are the possibilities for the rank r?

We know examples of rank exactly 19 and at least 28.

It has been conjectured that r can be arbitrarily large.

What are the possibilities for the rank r?

We know examples of rank exactly 19 and at least 28.

It has been conjectured that r can be arbitrarily large.

It has been conjectured that r can not be arbitrarily large.

What are the possibilities for the rank r?

We know examples of rank exactly 19 and at least 28.

It has been conjectured that r can be arbitrarily large.

It has been conjectured that r can not be arbitrarily large.

Remarkable recent work of Bhargava and his coauthors lends support to the belief that "typically" we have $r \in \{0, 1\}$.

Mazur's Theorem : take 1

Question : What are the possibilities for $E(\mathbb{Q})_{\mathsf{tors}}$?

Mazur's Theorem : take 1

Question : What are the possibilities for $E(\mathbb{Q})_{\text{tors}}$?

Theorem (Oggs conjecture; Mazur's theorem 1977) Let E be an elliptic curve defined over $\mathbb{Q}$. Then, $E(\mathbb{Q})_{\text{tors}}$ is isomorphic to exactly one of the following groups :

$$\mathbb{Z}/N\mathbb{Z} \text{ with } 1 \leq N \leq 10 \text{ or } N = 12; \text{ or}$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/M\mathbb{Z} \text{ with } 1 \leq M \leq 4.$$

Isogenies

Given two elliptic curves E and E', an *isogeny* $\phi : E \to E'$ is a rational morphism that maps $\mathcal{O}_E$ to $\mathcal{O}_{E'}$.
If not constant an isogeny is (geometrically) surjective, and of finite degree

$$d = \deg(\phi) = \#\ker(\phi).$$

The isogeny ϕ is defined over K if $\ker(\phi)$ is stable under the action of $\mathrm{Gal}(\overline{K}/K)$.

Mazur's Theorem : take 2

Over $K = \mathbb{Q}$, the possible isogenies of prime degree may be classified by a result of Mazur (1972) :

Theorem : The primes p which occur as degrees of isogenies between elliptic curves defined over $\mathbb{Q}$ are

$$p \in \{2, 3, 5, 7, 13\} \cup \{11, 17, 19, 37, 43, 67, 163\}.$$

Mazur's Theorem : take 2

Over $K = \mathbb{Q}$, the possible isogenies of prime degree may be classified by a result of Mazur (1972) :

Theorem : The primes p which occur as degrees of isogenies between elliptic curves defined over $\mathbb{Q}$ are

$$p \in \{2, 3, 5, 7, 13\} \cup \{11, 17, 19, 37, 43, 67, 163\}.$$

The $p \in \{2, 3, 5, 7, 13\}$ each occur infinitely often, while the remaining ones occur for a finite number of j-invariants.

Zeta and L-functions

An L-function is a function $L(s)$, usually given as an infinite series of the form :

$$L(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

where the coefficients $a_n \in \mathbb{C}$. These are analytic objects whose primary interest to Number Theorists lies in their ability to capture arithmetic information.

An example

Take $a_n = 1$ for all n :

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1-p^{-s}}$$

$$= \left(\frac{1}{1-2^{-s}}\right)\left(\frac{1}{1-3^{-s}}\right)\left(\frac{1}{1-5^{-s}}\right)\cdots$$

This *Euler product* was used (by Euler) to give a new proof that there exist infinitely many primes.

Elliptic curves over $\mathbb{F}_p$

How big would we expect $E(\mathbb{F}_p)$ to be?

Elliptic curves over $\mathbb{F}_p$

How big would we expect $E(\mathbb{F}_p)$ to be?

For prime p not dividing $\Delta = \Delta_E$, we define

$$a_p = p + 1 - \#E\left(\mathbb{F}_p\right).$$

Elliptic curves over $\mathbb{F}_p$

How big would we expect $E(\mathbb{F}_p)$ to be?

For prime p not dividing $\Delta = \Delta_E$, we define

$$a_p = p + 1 - \#E\left(\mathbb{F}_p\right).$$

Then, by a theorem of Hasse, we have

$$|a_p| \leq 2\sqrt{p}.$$

An L-function

Define the Hasse-Weil L-function of an elliptic curve E over $\mathbb{Q}$ via

$$L(E,s) = \prod_p \left(1 - a_p\, p^{-s} + \epsilon(p) p^{1-2s}\right)^{-1},$$

so that we can write

$$L(E,s) = \sum_{n=1}^{\infty} a_n n^{-s}.$$

An L-function

Define the Hasse-Weil L-function of an elliptic curve E over $\mathbb{Q}$ via

$$L(E,s) = \prod_p \left(1 - a_p\, p^{-s} + \epsilon(p) p^{1-2s}\right)^{-1},$$

so that we can write

$$L(E,s) = \sum_{n=1}^{\infty} a_n n^{-s}.$$

From Hasse's bound, $L(E,s)$ converges for s with real part $> 3/2$.

An L-function continued

Indeed, mathematicians conjectured that $L(E, s)$ should have an analytic continuation to the whole complex plane and that it must satisfy a functional equation relating the values of $L(E, s)$ and $L(E, 2 - s)$.

The Conjecture of Birch and Swinnerton-Dyer (simplest form)

$L(E, s)$ has a zero at $s = 1$ of order r, where r is the rank of $E(\mathbb{Q})$. The full conjecture describes the residue at $s = 1$.

The Conjecture of Birch and Swinnerton-Dyer (simplest form)

$L(E, s)$ has a zero at $s = 1$ of order r, where r is the rank of $E(\mathbb{Q})$. The full conjecture describes the residue at $s = 1$.

Speaking on this conjecture, John Tate noted that : "This remarkable conjecture relates the behavior of a function L at a point where it is not at present known to be defined $(s = 1)$ to the order of a group $Ш$ which is not known to be finite!"

From L-functions to Fourier series

Starting from

$$L(E,s) = \sum_{n=1}^{\infty} a_n n^{-s},$$

we might consider the generating series

$$f_E(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}.$$

Note that we have $f_E(z+1) = f_E(z)$.

Modular forms

Definition : A *modular form* (of weight 2 and level N) is a holomorphic function f on the upper half-plane satisfying

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 f(z)$$

for all

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N),$$

i.e. for $a, b, c, d \in \mathbb{Z}$, $ad - bc = 1$ and $N \mid c$.

Modular forms (continued)

Fourier expansion : Since $f(z+1) = f(z)$, we have

$$f(z) = \sum_{n=0}^{\infty} c_n q^n, \quad q = e^{2\pi i z}.$$

The Modularity Conjecture / Wiles' Theorem

If E is an elliptic curve over $\mathbb{Q}$, then the corresponding generating series $f_E(z)$ is a modular form of weight 2 and level N, where N is the *conductor* of the curve E.

The conductor is an arithmetic invariant of the curve E, measuring the primes for which E has bad reduction (i.e. those primes p dividing Δ_E).

The conductor : Szpiro's conjecture

As an aside, let me remark that N_E divides Δ_E. In the other direction, Szpiro conjectures that for $\epsilon > 0$, there exists $c(\epsilon)$ such that

$$|\Delta_E| < c(\epsilon) N_E^{6+\epsilon}.$$

In particular, the ratio

$$S(E) = \frac{\log |\Delta_E|}{\log N_E}$$

should be absolutely bounded.

The conductor : Szpiro's conjecture continued

The example we know with $S(E)$ largest corresponds to

$$E \ : \ y^2 + xy = x^3 - Ax - B,$$

where $A = 4241517626670033585 18$ and

$$B = 6292273164116612928531204122716,$$

which has minimal discriminant

$$\Delta_E = -2^{33} \cdot 7^{18} \cdot 13^{27} \cdot 19^3 \cdot 29^2 \cdot 127,$$

conductor

$$N_E = 2 \cdot 7 \cdot 13 \cdot 19 \cdot 29 \cdot 127$$

and hence $S(E) = 9.01996\ldots$.

Back to modularity : an example

$$E \ : \ y^2 + y = x^3 - x^2 - 10x - 20.$$

We compute that, setting $q = e^{2\pi iz}$,

$$f_E(z) = q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - \cdots$$

On the other hand, defining

$$\begin{aligned} f(z) &= (\eta(z)\eta(11z))^2 \\ &= q\left(\prod_{n=1}^{\infty}(1-q^n)(1-q^{11n})\right)^2, \end{aligned}$$

we find that $f(z) = f_E(z)$ is the (unique) weight 2 modular form of level 11.

Ribet's theorem : level lowering

For our purposes, we are especially interested in modular forms of relatively low level.

In a number of cases, a fundamental result of Ribet enables us to move from consideration of a form $f(z) = \sum_m c_m q^m$ of level N, to a modular form $g(z) = \sum_m d_m q^m$ of level N/l satisfying

$$c_p \equiv d_p \text{ modulo } n$$

for all primes p coprime to Nn, where $l \mid N$ and n are primes.

Ribet's theorem : an example

For example, the elliptic curve

$$E \ : \ y^2 = x^3 - 228813x + 42127856$$

has discriminant

$$\Delta = -2^6 \cdot 3^3 \cdot 17^7$$

and conductor

$$N = 2^5 \cdot 3^3 \cdot 17.$$

The corresponding cuspidal newform f has Fourier coefficients

c_5	c_{11}	c_{13}	c_{19}	c_{23}	c_{29}	c_{31}	c_{37}
-1	4	-7	-1	-1	5	2	-2

Ribet's theorem : an example (continued)

Our curve E has conductor $2^5 \cdot 3^3 \cdot 17$ (it's Cremona's 14688r)

c_5	c_{11}	c_{13}	c_{19}	c_{23}	c_{29}	c_{31}	c_{37}
-1	4	-7	-1	-1	5	2	-2

Lurking at level $864 = 2^5 \cdot 3^3$, we find a newform g corresponding to (in the notation of Cremona) the elliptic curve $864d1$:

$$E_1 \ : \ y^2 = x^3 - 3x - 6.$$

This form has Fourier coefficients

d_5	d_{11}	d_{13}	d_{19}	d_{23}	d_{29}	d_{31}	d_{37}
-1	-3	0	6	6	-2	9	-2