# Mary Somerville's Diophantine Equations

Diana Mocanu

THE UNIVERSITY OF
WARWICK

# Mary Somerville

Mary Somerville (born Mary Fairfax 1780 - 1872)

Figure: Painting by Thomas Phillips, 1834

# Equation 1

**I. QUESTION 311**, by Mr. John Hynes, Dublin.
To divide a given square number $n^2$, into two such parts that the sum of their squares and the sum of their cubes may both be rational squares.

# Equation 1

**I. QUESTION 311**, by Mr. John Hynes, Dublin.
To divide a given square number $n^2$, into two such parts that the sum of their squares and the sum of their cubes may both be rational squares.

Solution published under the pseudonym "a Lady".

# Mary Somerville's Solution

Somerville begins her solution by denoting the first part by $x$. Hence, in her notation, the problem asks to find such $x, n$ that make

$$\begin{cases} x^2 + (n^2 - x)^2 = \text{square} \\ x^3 + (n^2 - x)^3 = \text{square} \end{cases}$$

# Mary Somerville's Solution

Somerville begins her solution by denoting the first part by $x$. Hence, in her notation, the problem asks to find such $x, n$ that make

$$\begin{cases} x^2 + (n^2 - x)^2 = \text{square} \\ x^3 + (n^2 - x)^3 = \text{square} \end{cases}$$

Expanding she gets that $x^2 + (n^2 - x)^2 = n^4 - 2n^2x + 2x^2$ and $x^3 + (n^2 - x)^3 = n^2(n^4 - 3n^2x + 3x^2)$ must be squares and notices that the later reduces to $n^4 - 3n^2x + 3x^2$ being a square.

# Mary Somerville's Solution

Consequently, she assumes that

$$\begin{cases} -3n^2 + 3x = -2n^2px + p^2x^2 \\ -2n^2 + 2x = -2n^2q + q^2x \end{cases} \tag{1}$$

which will give $n^4 - 2n^2x + 2x^2 = (n^2 - qx)^2$ and $n^4 - 3n^2x + 3x^2 = (n^2 - px)^2$.

# Mary Somerville's Solution

Consequently, she assumes that

$$\begin{cases} -3n^2 + 3x = -2n^2px + p^2x^2 \\ -2n^2 + 2x = -2n^2q + q^2x \end{cases} \tag{1}$$

which will give $n^4 - 2n^2x + 2x^2 = (n^2 - qx)^2$ and $n^4 - 3n^2x + 3x^2 = (n^2 - px)^2$. Then she solves both equations in (1) for $x$ and equalizes them, and hence getting

$$\frac{3n^2 - 2n^2p}{3 - p^2} = \frac{2n^2 - 2n^2q}{2 - q^2}.$$

# Mary Somerville's Solution

Consequently, she assumes that

$$\begin{cases} -3n^2 + 3x = -2n^2px + p^2x^2 \\ -2n^2 + 2x = -2n^2q + q^2x \end{cases} \tag{1}$$

which will give $n^4 - 2n^2x + 2x^2 = (n^2 - qx)^2$ and $n^4 - 3n^2x + 3x^2 = (n^2 - px)^2$. Then she solves both equations in (1) for $x$ and equalizes them, and hence getting

$$\frac{3n^2 - 2n^2p}{3 - p^2} = \frac{2n^2 - 2n^2q}{2 - q^2}.$$

Here, she makes the strict assumptions that $3 - 2p = 2 - 2q$ and $3 - p^2 = 2 - q^2$, which gives her $q = \frac{3}{4}$ and $p = \frac{5}{4}$. Finally, these values give the desired values $x = \frac{8n^2}{23}$ and $n^2 - x = \frac{15n^2}{23}$.

# Equation 2

**XX. PRIZE QUESTION 310**, by Mr. W. Wallace.
Find such integer values of $x, y, z$ as shall render the three expressions $x^2 + axy + y^2$, $x^2 + a'xz + z^2$, $y^2 + a''yz + z^2$ squares, $a, a', a''$ being given numbers.

# Mary's solution

She starts her solution by assuming that $x, y$ and $z$ are parameterized by two new variables $m, n$ in the following way:

$$\begin{cases} x = an^2 + 2mn, \\ y = m^2 - n^2, \\ z = a''n^2 + 2mn. \end{cases} \tag{2}$$

These make the first and third expression into a square as Somerville writes:

$$\begin{cases} x^2 + axy + y^2 = (m^2 + amn + n^2)^2, \\ y^2 + a''yz + z^2 = (m^2 + a''mn + n^2)^2. \end{cases} \tag{3}$$

# Mary's Solution

Next, in order to make the middle expression into a square, Somerville reparameterizes $an + 2m = p^2 - q^2$, $a''n + 2m = a'q^2 + 2pq$ in order to get

$$x^2 + a'xz + z^2 = n^2(p^2 + a'pq + q^2)^2.$$

The rest of her solution consists in writing $m, n$ in terms of the parameters $p, q$ which after several simplifications leads to the following formulae:
Recall $x = an^2 + 2mn$

$$\begin{cases} m = a''p^2 - 2apq - (a'a + a'')q^2, \\ n = 2(a' + 1)q^2 + 4pq - 2p^2. \end{cases} \tag{4}$$

# Diophantine Equations

= polynomial equation in two or more unknowns with integer coefficients, such that the only solutions of interest are the integer ones.

# Diophantine Equations

= polynomial equation in two or more unknowns with integer coefficients, such that the only solutions of interest are the integer ones.

## Examples

- Linear Diophantine equation
$$ax + by = c$$
- Pell's equations
$$x^2 - ny^2 = \pm 1$$
- Elliptic Curves
$$y^2 = x^3 + ax + b$$
- Generalized Fermat Equation
$$x^n + y^m = z^r$$

# Algebraic Varieties

Let $k$ be an algebraically closed field.

- **Affine n-space** $\mathbb{A}^n := k^n$ (vector space)

# Algebraic Varieties

Let $k$ be an algebraically closed field.

- **Affine n-space** $\mathbb{A}^n := k^n$ (vector space)
- $R := k[x_1, ..., x_n]$ polynomial ring over $k$ in $n$ variables. Let $f_i \in R$ for $i \in \{1, ..., n\}$.

# Algebraic Varieties

Let $k$ be an algebraically closed field.

- **Affine n-space** $\mathbb{A}^n := k^n$ (vector space)
- $R := k[x_1, ..., x_n]$ polynomial ring over $k$ in $n$ variables. Let $f_i \in R$ for $i \in \{1, ..., n\}$.
- **Algebraic (affine) variety over** $k$
  $V(f_1, f_2, ..., f_n) := \{\mathbf{a} \in \mathbb{A}^n | f_i(\mathbf{a}) = 0, \text{ for } i \in \{1, ..., n\}\}$.

# Algebraic Varieties

Let $k$ be an algebraically closed field.

- **Affine n-space** $\mathbb{A}^n := k^n$ (vector space)
- $R := k[x_1, ..., x_n]$ polynomial ring over $k$ in $n$ variables. Let $f_i \in R$ for $i \in \{1, ..., n\}$.
- **Algebraic (affine) variety over** $k$
  $V(f_1, f_2, ..., f_n) := \{\mathbf{a} \in \mathbb{A}^n | f_i(\mathbf{a}) = 0, \text{ for } i \in \{1, ..., n\}\}$.

## Examples

- $V(0) = k^n$

# Algebraic Varieties

Let $k$ be an algebraically closed field.

- **Affine n-space** $\mathbb{A}^n := k^n$ (vector space)
- $R := k[x_1, ..., x_n]$ polynomial ring over $k$ in $n$ variables. Let $f_i \in R$ for $i \in \{1, ..., n\}$.
- **Algebraic (affine) variety over** $k$
  $V(f_1, f_2, ..., f_n) := \{\mathbf{a} \in \mathbb{A}^n | f_i(\mathbf{a}) = 0, \text{ for } i \in \{1, ..., n\}\}$.

## Examples

- $V(0) = k^n$
- $V(1) = \emptyset$

# Algebraic Varieties

Let $k$ be an algebraically closed field.

- **Affine n-space** $\mathbb{A}^n := k^n$ (vector space)
- $R := k[x_1, ..., x_n]$ polynomial ring over $k$ in $n$ variables. Let $f_i \in R$ for $i \in \{1, ..., n\}$.
- **Algebraic (affine) variety over** $k$
  $V(f_1, f_2, ..., f_n) := \{\mathbf{a} \in \mathbb{A}^n | f_i(\mathbf{a}) = 0, \text{ for } i \in \{1, ..., n\}\}$.

## Examples

- $V(0) = k^n$
- $V(1) = \emptyset$
- $V(x - a_1, x - a_2, ..., x - a_n) = \{(a_1, ...., a_n)\}$.

# Algebraic Varieties

Let $k$ be an algebraically closed field.

- **Affine n-space** $\mathbb{A}^n := k^n$ (vector space)
- $R := k[x_1, ..., x_n]$ polynomial ring over $k$ in $n$ variables. Let $f_i \in R$ for $i \in \{1, ..., n\}$.
- **Algebraic (affine) variety over** $k$
  $V(f_1, f_2, ..., f_n) := \{\mathbf{a} \in \mathbb{A}^n | f_i(\mathbf{a}) = 0, \text{ for } i \in \{1, ..., n\}\}$.

## Examples

- $V(0) = k^n$
- $V(1) = \emptyset$
- $V(x - a_1, x - a_2, ..., x - a_n) = \{(a_1, ...., a_n)\}$.
- $n = 2, V(xy) =$ the two axis $V(x^2 + y^2 - 1) =$ unit circle , $V(y^2 - x^3 - x - 1) =$ elliptic curve

# Algebraic Varieties

Let $k$ be an algebraically closed field.

- **Affine n-space** $\mathbb{A}^n := k^n$ (vector space)
- $R := k[x_1, ..., x_n]$ polynomial ring over $k$ in $n$ variables. Let $f_i \in R$ for $i \in \{1, ..., n\}$.
- **Algebraic (affine) variety over** $k$
  $V(f_1, f_2, ..., f_n) := \{\mathbf{a} \in \mathbb{A}^n | f_i(\mathbf{a}) = 0, \text{ for } i \in \{1, ..., n\}\}$.

## Examples

- $V(0) = k^n$
- $V(1) = \emptyset$
- $V(x - a_1, x - a_2, ..., x - a_n) = \{(a_1, ...., a_n)\}$.
- $n = 2, V(xy) =$ the two axis $V(x^2 + y^2 - 1) =$ unit circle , $V(y^2 - x^3 - x - 1) =$ elliptic curve
- $n = 3, V(a_1x_1 + ... + a_3x_3) =$ hyperplane, $V(x^2 + y^2 - z^2) =$ cone .

# Dimensions

- A variety $X := V(f_1, f_2, ..., f_n)$ is **reducible** if $X = X_1 \cup X_2$ and **irreducible** otherwise.

# Dimensions

- A variety $X := V(f_1, f_2, ..., f_n)$ is **reducible** if $X = X_1 \cup X_2$ and **irreducible** otherwise.
  **FACT**: irreducible $\Leftrightarrow$ the **vanishing ideal** $I(X) := \{f \in R : f(x) = 0,\ \forall x \in X\}$ is a prime ideal.

# Dimensions

- A variety $X := V(f_1, f_2, ..., f_n)$ is **reducible** if $X = X_1 \cup X_2$ and **irreducible** otherwise.
  **FACT**: irreducible $\Leftrightarrow$ the **vanishing ideal** $I(X) := \{f \in R : f(x) = 0,\ \forall x \in X\}$ is a prime ideal.
- **Chain of length m** is a chain of strict inclusions: $\emptyset \neq X_0 \subsetneq X_1 ... \subsetneq X_m$

# Dimensions

- A variety $X := V(f_1, f_2, ..., f_n)$ is **reducible** if $X = X_1 \cup X_2$ and **irreducible** otherwise.
  **FACT**: irreducible $\Leftrightarrow$ the **vanishing ideal** $I(X) := \{f \in R : f(x) = 0,\ \forall x \in X\}$ is a prime ideal.
- **Chain of length m** is a chain of strict inclusions: $\emptyset \neq X_0 \subsetneq X_1 ... \subsetneq X_m$
- The **local dimension** $\dim_p X$ of $X$ at a point $p \in X$ is the maximum over all lengths of chains starting with $X_0 = \{p\}$. The **dimension** of $X$ is

$$\textbf{dim} X := \max_{p \in X} \textbf{dim}_p X.$$

# Dimensions

## Examples

- $V(0) = k^n$

# Dimensions

**Examples**

- $V(0) = k^n$
- $V(1) = \emptyset$

# Dimensions

## Examples

- $V(0) = k^n$
- $V(1) = \emptyset$
- $V(x - a_1, x - a_2, ..., x - a_n) = \{(a_1, ...., a_n)\}$.

# Dimensions

## Examples

- $V(0) = k^n$
- $V(1) = \emptyset$
- $V(x - a_1, x - a_2, ..., x - a_n) = \{(a_1, ...., a_n)\}$.
- $n = 2, V(xy) =$ the two cartesian axes , $V(x^2 + y^2 - 1) =$ unit circle , $V(y^2 - x^3 - x - 1) =$ elliptic curve

# Dimensions

## Examples

- $V(0) = k^n$
- $V(1) = \emptyset$
- $V(x - a_1, x - a_2, ..., x - a_n) = \{(a_1, ...., a_n)\}$.
- $n = 2, V(xy) =$ the two cartesian axes , $V(x^2 + y^2 - 1) =$ unit circle , $V(y^2 - x^3 - x - 1) =$ elliptic curve
- $n = 3, V(a_1x_1 + ... + a_3x_3) =$ hyperplane, $V(x^2 + y^2 - z^2) =$ cone .

# Singularities

- A **tangent space** to an affine variety $X$ at a point $p$:
  $T_pX := \cup$(lines tangent to $X$ at $p$)

# Singularities

- A **tangent space** to an affine variety $X$ at a point $p$:
  $T_pX := \cup$(lines tangent to $X$at $p$)
- A point $p \in X$ is a **smooth point** if $\dim_k T_pX = \dim_p X$. A point $p \in X$ is a **singular point** if $\dim_k T_pX > \dim_p X$.

# Singularities

- A **tangent space** to an affine variety $X$ at a point $p$:
  $T_pX := \cup(\text{lines tangent to } X \text{at } p)$
- A point $p \in X$ is a **smooth point** if $\dim_k T_pX = \dim_p X$. A point $p \in X$ is a **singular point** if $\dim_k T_pX > \dim_p X$.
  **FACT:** $\text{Sing}(X) := \{\text{all singular points}\} \subset X$ is a subvariety when $X$ is irreducible.

# Singularities

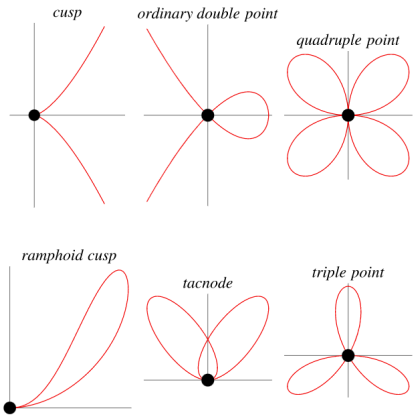
- A **tangent space** to an affine variety $X$ at a point $p$:
  $T_pX := \cup$(lines tangent to $X$at $p$)
- A point $p \in X$ is a **smooth point** if $\dim_k T_pX = \dim_p X$. A point $p \in X$ is a **singular point** if $\dim_k T_pX > \dim_p X$.
  **FACT:** Sing$(X) := \{$all singular points$\} \subset X$ is a subvariety when $X$ is irreducible.

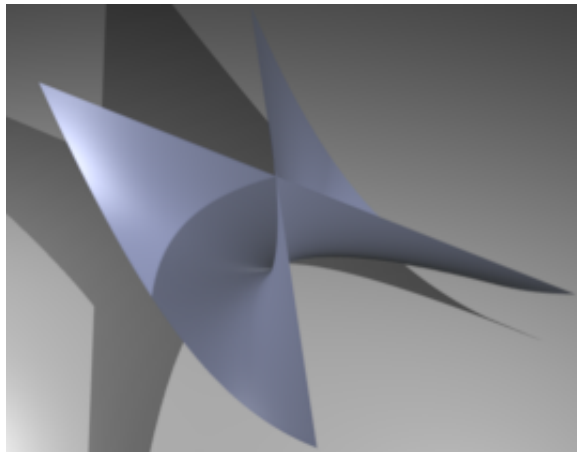
**Theorem**

*Let $X \subset \mathbb{A}^n$ be an irreducible aff. var. of dimension $d$ with $I(X) =< f_1, f_2, ..., f_n >$. Then Sing($X$) $\subset X$ is a subvariety given by the vanishing in $X$ of all $(n-d) \times (n-d)$ minors of the Jacobian matrix*

$$Jac = \left( \frac{\partial f_i}{\partial x_j} \right)$$

# Singularities



# Maps

- $F\colon \mathbb{A}^n \to \mathbb{A}^m$ is **a morphism (or polynomial map)** if it is defined by polynomials: $F(a) = (f_1(a), ..., f_m(a))$ for some $f_1, ..., f_m \in R := k[x_1, ..., x_n]$.
- $F\colon X \to Y$ is a **morphism of affine varieties** if it is the restriction of a morphism $\mathbb{A}^n \to \mathbb{A}^m$ (here $X \subset \mathbb{A}^n$ and $Y \subset \mathbb{A}^m$).
  $F(a) = (f_1(a), ..., f_m(a))$ for some $f_1, ..., f_m \in k[X] := R/I(X)$.
- **isomorphism** = morphism which has an inverse which is a morphism

# Projective Space

- **Zariski topology** on $\mathbb{A}^n$: declare the basic open sets to be for any $f \in R$:

$$D(f) = \mathbb{A}^n \setminus V(f) := \{a \in k^n : f(a) \neq 0\}$$

$\implies$ induces a topology on an algebraic variety $X \subset \mathbb{A}^n$
**PROBLEM**: not compact

# Projective Space

- **Zariski topology** on $\mathbb{A}^n$: declare the basic open sets to be for any $f \in R$:

$$D(f) = \mathbb{A}^n \setminus V(f) := \{a \in k^n : f(a) \neq 0\}$$

  $\Longrightarrow$ induces a topology on an algebraic variety $X \subset \mathbb{A}^n$
  **PROBLEM**: not compact
  **SOLUTION**: "compactifying" $\mathbb{A}^n$ by hyperplanes, planes, and points at infinity
- The **projective space** is $\mathbb{P}^n_k :=$(space of straight lines in $k^{(n+1)}$ through $0$)

# Projective Space

- **Zariski topology** on $\mathbb{A}^n$: declare the basic open sets to be for any $f \in R$:

$$D(f) = \mathbb{A}^n \setminus V(f) := \{a \in k^n : f(a) \neq 0\}$$

$\Longrightarrow$ induces a topology on an algebraic variety $X \subset \mathbb{A}^n$
**PROBLEM**: not compact
**SOLUTION**: "compactifying" $\mathbb{A}^n$ by hyperplanes, planes, and points at infinity

- The **projective space** is $\mathbb{P}^n_k$ :=(space of straight lines in $k^{(n+1)}$ through $0$)

$$\text{affine variety} \xrightarrow{\text{homogenization}} \text{projective variety}$$

# Projective Space

- **Zariski topology** on $\mathbb{A}^n$: declare the basic open sets to be for any $f \in R$:

$$D(f) = \mathbb{A}^n \setminus V(f) := \{a \in k^n : f(a) \neq 0\}$$

$\implies$ induces a topology on an algebraic variety $X \subset \mathbb{A}^n$
**PROBLEM**: not compact
**SOLUTION**: "compactifying" $\mathbb{A}^n$ by hyperplanes, planes, and points at infinity

- The **projective space** is $\mathbb{P}^n_k$ :=(space of straight lines in $k^{(n+1)}$ through $0$)

$$\text{affine variety} \xrightarrow{\text{homogenization}} \text{projective variety}$$

- **Birational map** between two (affine/projective) varieties is "an isomorphism between open dense subsets"

# Resolution of Singularities

Let $k$ be an algebraically closed field.

- The problem of **resolution of singularities** asks whether every algebraic variety $X$ has a resolution, a non-singular variety $Y$ with a proper birational map $Y \to X$.
- Hironaka (1964): proved it for varieties over $k$, of characteristic $0$
- Open for characteristic $p$ and dimension $> 4$.

**TODAY:** characteristic $0$: dimension $1$ (curves), dimension $2$ (surfaces).

# Dimension 1: Curves

Let $k$ be an algebraically closed field.

- Let $C$ be a variety of dimension $1$, then we call $C$ an **algebraic curve**.

# Dimension 1: Curves

Let $k$ be an algebraically closed field.

- Let $C$ be a variety of dimension $1$, then we call $C$ an **algebraic curve**.
- Every algebraic curve has a unique nonsingular projective resolution.

# Dimension 1: Curves

Let $k$ be an algebraically closed field.

- Let $C$ be a variety of dimension $1$, then we call $C$ an **algebraic curve**.
- Every algebraic curve has a unique nonsingular projective resolution.
- The **genus** of a smooth complete algebraic curve $C$ is a numerical invariant under birational maps. If $k = \mathbb{C}$, then an algebraic curve $C$ is the same as a Riemann surface. In this case, the smooth complex curve $X$ of genus $g$ is homeomorphic to the sphere with $g$ handles.

# Examples

Let $k$ be an algebraically closed field.

- **genus 0** : $\mathbb{P}^1$, "rational curves" .
  Every smooth conic over $k$ is birational to $\mathbb{P}^1$.

# Examples

Let $k$ be an algebraically closed field.

- **genus 0** : $\mathbb{P}^1$, "rational curves" .
  Every smooth conic over $k$ is birational to $\mathbb{P}^1$.
- **genus 1**: elliptic curves
  Every smooth curve of genus 1 is birationally isomorphic to smooth cubic curves in $\mathbb{P}^2$. In characteristic $0$ they have an affine model:

$$E/k : y^2 = x^3 + Ax + B \text{ with } \Delta = 4A^3 + 27B^2 \neq 0$$

# Examples

Let $k$ be an algebraically closed field.

- **genus 0** : $\mathbb{P}^1$, "rational curves" .
  Every smooth conic over $k$ is birational to $\mathbb{P}^1$.
- **genus 1**: elliptic curves
  Every smooth curve of genus 1 is birationally isomorphic to smooth cubic curves in $\mathbb{P}^2$. In characteristic $0$ they have an affine model:

$$E/k : y^2 = x^3 + Ax + B \text{ with } \Delta = 4A^3 + 27B^2 \neq 0$$

- **genus $\geq 2$**: Every smooth curve of genus $\geq 2$ is birationally isomorphic to hyper-elliptic curves and non-hyper-elliptic curves.
  Example: hyperelliptic curves:

$$C/k : y^2 = f(x), \deg(f) \geq 5$$

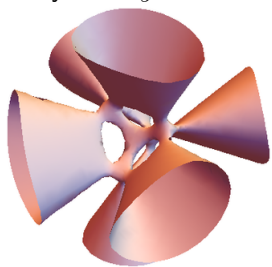
# Dimension 2: Surfaces

Let $k$ be an algebraically closed field.

- Let $S$ be a variety of dimension $2$, then we call $S$ an **algebraic surface**.
- Surfaces have many different nonsingular projective resolutions (unlike the case of curves). However, a surface still has a unique minimal resolution.
- $\kappa$ is the **Kodaira dimension**, an arithmetic invariant which classifies algebraic surfaces.

# Examples

- $\kappa = -\infty$: rational surfaces, ruled surface
  Any rational surface is birational to $\mathbb{P}^2$. A ruled surface: every point lies on a line.
- $\kappa = 0$: abelian surfaces, hyperelliptic surface, K3 surface, Enriques surface
  For example the K3 surface given by $x^4 + y^4 + z^4 + w^4 = 0$:



- $\kappa = 1$: elliptic surface
  For example, $E \times C$ where $E$ is an elliptic curve and $C$ is any curve.
- $\kappa = 2$: surface of general type

# Diophantine Equation 1

**I. QUESTION 311**, by Mr. John Hynes, Dublin.
To divide a given square number $n^2$, into two such parts that the sum of their squares and the sum of their cubes may both be rational squares.

# Diophantine Equation 1

**I. QUESTION 311**, by Mr. John Hynes, Dublin.
To divide a given square number $n^2$, into two such parts that the sum of their squares and the sum of their cubes may both be rational squares.

Somerville rewrites the problem such that one needs to find such $x, n$ that make $x^2 + (n^2 - x)^2$ and $x^3 + (n^2 - x)^3$ into squares. Expanding she gets that $x^2 + (n^2 - x)^2 = n^4 - 2n^2x + 2x^2$ and $x^3 + (n^2 - x)^3 = n^2(n^4 - 3n^2x + 3x^2)$ must be squares and notices that the later reduces to $n^4 - 3n^2x + 3x^2$ being a square.

# Diophantine Equation 1

**I. QUESTION 311**, by Mr. John Hynes, Dublin.
To divide a given square number $n^2$, into two such parts that the sum of their squares and the sum of their cubes may both be rational squares.

Somerville rewrites the problem such that one needs to find such $x, n$ that make $x^2 + (n^2 - x)^2$ and $x^3 + (n^2 - x)^3$ into squares. Expanding she gets that $x^2 + (n^2 - x)^2 = n^4 - 2n^2x + 2x^2$ and $x^3 + (n^2 - x)^3 = n^2(n^4 - 3n^2x + 3x^2)$ must be squares and notices that the later reduces to $n^4 - 3n^2x + 3x^2$ being a square.

We denote by $y = n^2$.

# Diophantine Equation 1

- We can rewrite the problem as finding the common zeros of the following two equations:

$$\begin{cases} y^2 - 2yx + 2x^2 = w^2 \\ y^2 - 3yx + 3x^2 = w'^2. \end{cases}$$

# Diophantine Equation 1

- We can rewrite the problem as finding the common zeros of the following two equations:

$$\begin{cases} y^2 - 2yx + 2x^2 = w^2 \\ y^2 - 3yx + 3x^2 = w'^2. \end{cases} \tag{5}$$

- Let's denote by $C$ the vanishing set of these two equations in $\mathbb{P}^3$ of coordinates $[x : y : w : w']$. We note that Somerville's solution corresponds to the point $S = [8 : 23 : 17 : 13]$.
  Let's examine $C(\mathbb{Q})$ which are the points in $\mathbb{P}^3$ with rational coordinates.

# Diophantine Equation 1

- We can rewrite the problem as finding the common zeros of the following two equations:

$$\begin{cases} y^2 - 2yx + 2x^2 = w^2 \\ y^2 - 3yx + 3x^2 = w'^2. \end{cases} \tag{5}$$

- Let's denote by $C$ the vanishing set of these two equations in $\mathbb{P}^3$ of coordinates $[x : y : w : w']$. We note that Somerville's solution corresponds to the point $S = [8 : 23 : 17 : 13]$.
  Let's examine $C(\mathbb{Q})$ which are the points in $\mathbb{P}^3$ with rational coordinates.

- Dimension of $C$ is $1$ and genus of $C$ is $1$ and has an obvious rational point $[0 : 1 : 1 : 1] \Longrightarrow C$ is birational to an elliptic curve.

# Diophantine Equation 1: An Elliptic Curve

- Since $C$ is birational to an elliptic curve, it has an model which can be computed to be:

$$E : y^2 = x^3 + 8x^2 + 12x$$

where $[0 : 1 : 1 : 1]$ is the point at infinity.

# Diophantine Equation 1: An Elliptic Curve

- Since $C$ is birational to an elliptic curve, it has an model which can be computed to be:
$$E : y^2 = x^3 + 8x^2 + 12x$$
where $[0 : 1 : 1 : 1]$ is the point at infinity.
- Somerville's point $S = [8 : 23 : 17 : 13]$ corresponds to the affine point $S_E = (48, 360)$ on $E$.

Hence, a modern algebraic geometer would say that Mary Somerville constructed a point on an elliptic curve.

# Other rational points?

Recall that elliptic curves come with a group law.

**Theorem (Mordell-Weil)**

*Let $E/\mathbb{Q}$ be an elliptic curve. Then,*

$$E(\mathbb{Q}) \cong \mathit{Tors} + \mathbb{Z}^r,$$

*where $r$ is called the rank of $E$.*

# Other rational points?

- In our case, $E : y^2 = x^3 + 8x^2 + 12x$ and

$$E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}$$

with generators $S_1 = (-6, 0), \quad S_2 = (-2, 0), \quad S_3 = (6, -24).$

# Other rational points?

- In our case, $E : y^2 = x^3 + 8x^2 + 12x$ and

$$E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}$$

  with generators $S_1 = (-6, 0), \quad S_2 = (-2, 0), \quad S_3 = (6, -24)$.
- They correspond to the points $S_1 = [1 : 1 : 1 : -1]$, $S_2 = [1 : 1 : -1 : 1]$, $S_3 = [1 : 1 : -1 : -1]$ on the initial curve $C$, which all lead to the rather uninteresting pair of solutions. Somerville's point turns out to be $S = S_3 + S_3 = [2]S_3$, which has infinite order.

# Other rational points?

- In our case, $E : y^2 = x^3 + 8x^2 + 12x$ and

$$E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}$$

  with generators $S_1 = (-6, 0), \quad S_2 = (-2, 0), \quad S_3 = (6, -24)$.
- They correspond to the points $S_1 = [1 : 1 : 1 : -1]$, $S_2 = [1 : 1 : -1 : 1]$, $S_3 = [1 : 1 : -1 : -1]$ on the initial curve $C$, which all lead to the rather uninteresting pair of solutions. Somerville's point turns out to be $S = S_3 + S_3 = [2]S_3$, which has infinite order.
- In conclusion, Somerville's point gives rise to infinitely many solutions. For example,

$$S + S = (36481/3600, 9620479/216000)$$

  which gives rise to the solution: $[10130640, 18240049, 12976609, 9286489]$.

# Diophantine equation 2

A present-day mathematician would rewrite the statement in the following way. Find such integer values of $x, y, z$ such that:

$$\begin{cases} x^2 + axy + y^2 = w^2 \\ x^2 + a'xz + z^2 = w'^2 \\ y^2 + a''yz + z^2 = w''^2. \end{cases} \tag{6}$$

# Diophantine equation 2

A present-day mathematician would rewrite the statement in the following way. Find such integer values of $x, y, z$ such that:

$$\begin{cases} x^2 + axy + y^2 = w^2 \\ x^2 + a'xz + z^2 = w'^2 \\ y^2 + a''yz + z^2 = w''^2. \end{cases} \tag{6}$$

As the above equations are homogeneous, a natural way to view their common solutions is as a projective variety in $\mathbb{P}^5$. More concretely, consider the following homogeneous polynomials of degree 2:

$$\begin{cases} f_1(x, y, z, w, w', w'') = x^2 + axy + y^2 - w^2 \\ f_2(x, y, z, w, w', w'') = x^2 + a'xz + z^2 - w'^2 \\ f_3(x, y, z, w, w', w'') = y^2 + a''yz + z^2 - w''^2. \end{cases} \tag{7}$$

# Diophantine equation 2

- Define the projective variety:

$$S_{a,a',a''} := \{\mathbf{p} = [x : y : z : w : w' : w''] \in \mathbb{P}^5 : f_1(\mathbf{p}) = 0, f_2(\mathbf{p}) = 0, f_3(\mathbf{p}) = 0\}.$$

# Diophantine equation 2

- Define the projective variety:

$$S_{a,a',a''} := \{\mathbf{p} = [x : y : z : w : w' : w''] \in \mathbb{P}^5 : f_1(\mathbf{p}) = 0, f_2(\mathbf{p}) = 0, f_3(\mathbf{p}) = 0\}.$$

- We can show that $S_{a,a',a''}$ has dimension $2$ so it is a surface.

# Diophantine equation 2

- Define the projective variety:

$$S_{a,a',a''} := \{\mathbf{p} = [x : y : z : w : w' : w''] \in \mathbb{P}^5 : f_1(\mathbf{p}) = 0, f_2(\mathbf{p}) = 0, f_3(\mathbf{p}) = 0\}.$$

- We can show that $S_{a,a',a''}$ has dimension $2$ so it is a surface.
- If $a \notin \{\pm 2\}$, $a' \notin \{\pm 2\}$ and $a'' \notin \{\pm 2\}$, then the singularities of $S_{a,a',a''}$ consist in $12$ isolated singularities, and $S_{a,a',a''}$ is irreducible. These singularities are double points ("not too bad").

# Diophantine equation 2

- Define the projective variety:

$$S_{a,a',a''} := \{\mathbf{p} = [x : y : z : w : w' : w''] \in \mathbb{P}^5 : f_1(\mathbf{p}) = 0, f_2(\mathbf{p}) = 0, f_3(\mathbf{p}) = 0\}.$$

- We can show that $S_{a,a',a''}$ has dimension $2$ so it is a surface.
- If $a \notin \{\pm 2\}$, $a' \notin \{\pm 2\}$ and $a'' \notin \{\pm 2\}$, then the singularities of $S_{a,a',a''}$ consist in $12$ isolated singularities, and $S_{a,a',a''}$ is irreducible. These singularities are double points ("not too bad").
- The resolution of singularities theorem tells us that $S_{a,a',a''}$ has a minimal resolution belonging to the classification of surfaces.Which one?

# Diophantine equation 2: a K3 surface

**Theorem**

*Let $k$ be a field of characteristic $0$. Assume that $X$ is a surface over $k$ of one of the following three types:*

1. *a quartic surface in $\mathbb{P}^3_k$,*
2. *an intersection of a cubic and a quadric hypersurface in $\mathbb{P}^4_k$,*
3. *an intersection of three quadrics in $\mathbb{P}^5_k$.*

*Furthermore, assume that all singularities of $X$ are rational double points. Then the minimal regular model of $X$ is a K3-surface.*

# Back to Somerville's Solution

- We will work in the general case (i.e. when $a \notin \{\pm 2\}$, $a' \notin \{\pm 2\}$ and $a'' \notin \{\pm 2\}$) and moreover we assume that $a, a'$ and $a''$ are all distinct. In the language of Algebraic Geometry, Somerville's solution proposes a birational map

$$F \colon \mathbb{P}^1 \dashrightarrow S_{a,a',a''}$$

defined over $\mathbb{Q}$, given as a composition of a couple of explicit rational maps. More precisely, $F = f \circ g$, where $f$ is given by (2) and $g$ is given by (4).

# Back to Somerville's Solution

- We will work in the general case (i.e. when $a \notin \{\pm 2\}$, $a' \notin \{\pm 2\}$ and $a'' \notin \{\pm 2\}$) and moreover we assume that $a, a'$ and $a''$ are all distinct. In the language of Algebraic Geometry, Somerville's solution proposes a birational map

$$F \colon \mathbb{P}^1 \dashrightarrow S_{a,a',a''}$$

  defined over $\mathbb{Q}$, given as a composition of a couple of explicit rational maps. More precisely, $F = f \circ g$, where $f$ is given by (2) and $g$ is given by (4).
- Hence, Somerville's solution $Im(F) \subset S_{a,a',a''}$ is birational to $\mathbb{P}^1$ and it can be shown that it misses the singularities.

# Back to Somerville's Solution

- We will work in the general case (i.e. when $a \notin \{\pm 2\}$, $a' \notin \{\pm 2\}$ and $a'' \notin \{\pm 2\}$) and moreover we assume that $a, a'$ and $a''$ are all distinct. In the language of Algebraic Geometry, Somerville's solution proposes a birational map

$$F \colon \mathbb{P}^1 \dashrightarrow S_{a,a',a''}$$

  defined over $\mathbb{Q}$, given as a composition of a couple of explicit rational maps. More precisely, $F = f \circ g$, where $f$ is given by (2) and $g$ is given by (4).
- Hence, Somerville's solution $Im(F) \subset S_{a,a',a''}$ is birational to $\mathbb{P}^1$ and it can be shown that it misses the singularities.
- Hence, in modern language, Somerville constructs a rational curve on a $K3$ surface.

# Thank you!