Geometry Controls Arithmetic: Rational Points and Beyond

James Rawson

AGQ Conference: 05/11/25

A very brief history by examples

Diophantus (c. 250AD) gave some of the earliest recorded examples of algebraic methods to solve arithmetic problems.

A very brief history by examples

Diophantus (c. 250AD) gave some of the earliest recorded examples of algebraic methods to solve arithmetic problems.

Theorem (Fermat's Last Theorem (conjectured 1637), Wiles 1994)

For any integer $n \geq 3$, there are no non-trivial integer solutions to $a^n + b^n = c^n$. Equivalently, there are no non-trivial rational solutions to $x^n + y^n = 1$.

A very brief history by examples

Diophantus (c. 250AD) gave some of the earliest recorded examples of algebraic methods to solve arithmetic problems.

Theorem (Fermat's Last Theorem (conjectured 1637), Wiles 1994)

For any integer $n \geq 3$, there are no non-trivial integer solutions to $a^n + b^n = c^n$. Equivalently, there are no non-trivial rational solutions to $x^n + y^n = 1$.

Theorem (Balakrishnan–Dogra–Müller–Tuitman–Vonk 2019)

The equation $y^4 + 5x^4 - 6x^2y^2 + 6x^3 + 26x^2y + 10xy^2 - 10y^3 - 32x^2 - 40xy + 24y^2 + 32x - 16 = 0$ has only 5 rational solutions, $(1,1)$, $(\frac{1}{2}, \frac{1}{2})$, $(0,0)$, $(\frac{-3}{2}, \frac{3}{2})$, $(0,2)$.

Why is this so hard? I

Theorem (Frye 1988)

The smallest integer solution to $x^4 + y^4 + z^4 = w^4$ *is* $(95800, 217519, 414560, 422481)$.

Why is this so hard? I

Theorem (Frye 1988)

The smallest integer solution to $x^4 + y^4 + z^4 = w^4$ *is* $(95800, 217519, 414560, 422481)$.

Theorem (Booker–Sutherland 2020)

The three smallest integer solutions to $x^3 + y^3 + z^3 = 3$ *are* $(1, 1, 1)$, $(4, 4, -5)$ *and*

$$(569936821221962380720, -569936821113563493509, \\ -472715493453327032).$$

Why is this so hard? II

Example

The positive integer solutions to $y^2 - 2x^2 = 1$ are $(2,3), (12,17), (70,99), (408,577), \ldots$.

Why is this so hard? II

Example

The positive integer solutions to $y^2 - 2x^2 = 1$ are $(2,3),(12,17),(70,99),(408,577),\ldots$.

Explicitly, $\left(\frac{(3+2\sqrt{2})^n-(3-2\sqrt{2})^n}{\sqrt{2}}, \frac{(3+2\sqrt{2})^n+(3-2\sqrt{2})^n}{2}\right)$

Why is this so hard? II

Example

The positive integer solutions to $y^2 - 2x^2 = 1$ are $(2,3), (12,17), (70,99), (408,577), \ldots$.
Explicitly, $\left(\frac{(3+2\sqrt{2})^n - (3-2\sqrt{2})^n}{\sqrt{2}}, \frac{(3+2\sqrt{2})^n + (3-2\sqrt{2})^n}{2}\right)$

Example

Which right-angled triangles with rational side lengths have area 6?

$$(3,4,5), \left(\frac{7}{10}, \frac{120}{7}, \frac{1201}{70}\right), \left(\frac{3404}{1551}, \frac{4653}{851}, \frac{7776485}{1319901}\right), \ldots.$$

Why is this so hard? III

Theorem (Hilbert's 10th Problem (1900), Matiyasevich (1970), Robinson, Davis, Putnam)

Does there exist an algorithm to determine if a polynomial equation has a solution in the integers? No!

Why is this so hard? III

Theorem (Hilbert's 10th Problem (1900), Matiyasevich (1970), Robinson, Davis, Putnam)

Does there exist an algorithm to determine if a polynomial equation has a solution in the integers? No!

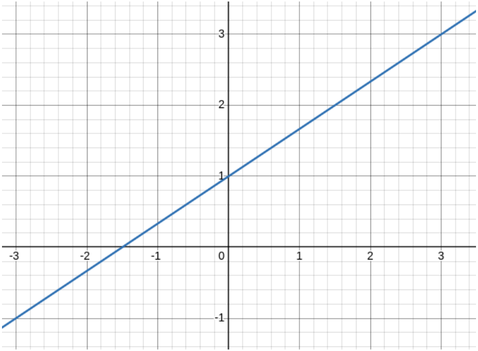
Question

Does there exist an algorithm to determine if a polynomial equation has a solution in the rationals?

Degree 1 Curves

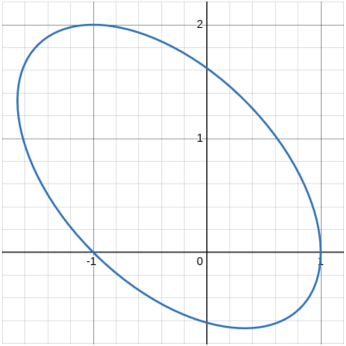
A general equation of degree 1 (in two variables) has the form $ax + by = c$, $a, b, c \in \mathbb{Q}$.

These equations have infinitely many solutions, one for each (rational) value of x.



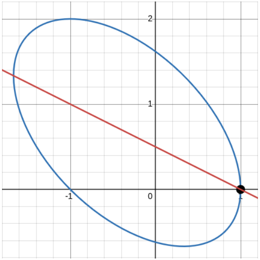
Degree 2 Curves

A general degree 2 equation is a conic;
$a_1x^2 + a_2xy + a_3y^2 + a_4x + a_5y + a_6 = 0, \ a_i \in \mathbb{Q}.$



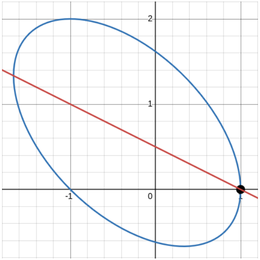
Degree 2 Curves

If it has a rational solution, then there are infinitely many solutions by projection from the rational point.



Degree 2 Curves

If it has a rational solution, then there are infinitely many solutions by projection from the rational point.



For example, $x^2 + y^2 = 1$, has a rational point at $(0, 1)$. Write $y = tx + 1$, then this is the same as $x^2 + t^2x^2 + 2tx + 1 = 1$. There are two solutions for each t, $x = 0$ or $x = \frac{-2t}{1+t^2}$. This gives the paramterisation $\left(\frac{-2t}{1+t^2}, \frac{1-t^2}{1+t^2}\right)$

Degree 2 Curves

Can you (easily) tell if such an equation has a point?

Degree 2 Curves

Can you (easily) tell if such an equation has a point?
The equation $x^2 + 2y^2 = -1$ has no solutions as the lefthand side is always positive.

Degree 2 Curves

Can you (easily) tell if such an equation has a point?
The equation $x^2 + 2y^2 = -1$ has no solutions as the lefthand side is always positive.
$y^2 - 3x^2 = 6x - 1$ has no solutions, by considering values modulo 3.

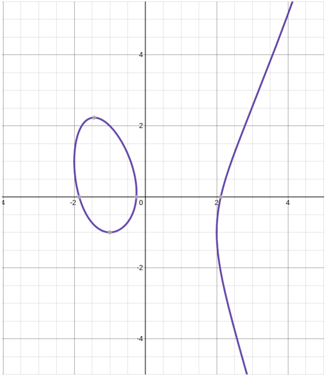
Degree 2 Curves

Can you (easily) tell if such an equation has a point?
The equation $x^2 + 2y^2 = -1$ has no solutions as the lefthand side is always positive.
$y^2 - 3x^2 = 6x - 1$ has no solutions, by considering values modulo 3.

Theorem (Hasse–Minkowski)

A degree 2 equation has rational solutions if and only if it has solutions modulo p for every p, and real solutions.

Degree 3 Curves



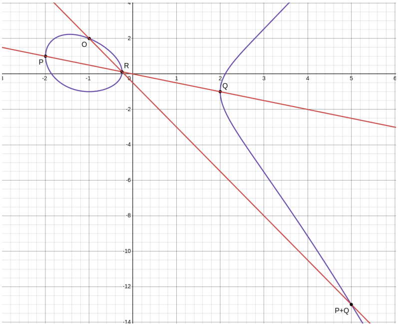
Degree 3 Curves

If a cubic curve has a rational point, $\mathcal{O}$, the rational points form a group (with identity $\mathcal{O}$).

1. Let P, Q be rational points. Take the line through them, if $P \neq Q$, and the tangent line if $P = Q$.
2. Let R be the third point of intersection (counting multiplicities).
3. Take the line through $\mathcal{O}$ and R. The third point of intersection is $P + Q$.

Degree 3 Curves

If a cubic curve has a rational point, $\mathcal{O}$, the rational points form a group (with identity $\mathcal{O}$).



Degree 3 Curves

If a cubic curve has a rational point, $\mathcal{O}$, the rational points form a group (with identity $\mathcal{O}$).

Theorem (Mordell–Weil)

The group of rational points is a finitely generated abelian group, that is, isomorphic to $\mathbb{Z}^r \oplus T$ for some $r \in \mathbb{Z}_{\geq 0}$ and T a finite abelian group.

Degree 3 Curves

Do reductions control the behaviour of degree 3 curves?

Degree 3 Curves

Do reductions control the behaviour of degree 3 curves?
The curve $3x^3 + 4y^3 = 5$ has solutions modulo every prime and over $\mathbb{R}$.

Degree 3 Curves

Do reductions control the behaviour of degree 3 curves?
The curve $3x^3 + 4y^3 = 5$ has solutions modulo every prime and over $\mathbb{R}$. But this curve has no rational points (Selmer 1951)!

Degree 3 Curves

Do reductions control the behaviour of degree 3 curves?
The curve $3x^3 + 4y^3 = 5$ has solutions modulo every prime and over $\mathbb{R}$. But this curve has no rational points (Selmer 1951)!

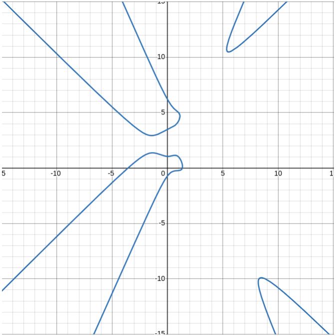
Conjecture (Birch–Swinnerton-Dyer)

Fix a cubic curve C, with rational solutions forming a finitely generated abelian group $\mathbb{Z}^r \oplus T$. Let the number of solutions modulo p be N_p, then $\prod_{p \leq x} \frac{N_p}{p} \sim \log(x)^r$.

Degree 4 Curves

Already seen two examples:

- Fermat's Last Theorem: $x^4 + y^4 = 1$ only has 4 solutions.
- The curve $y^4 + 5x^4 - 6x^2y^2 + 6x^3 + 26x^2y + 10xy^2 - 10y^3 - 32x^2 - 40xy + 24y^2 + 32x - 16 = 0$ only has 5 solutions



Degree 4 Curves

Already seen two examples:

- Fermat's Last Theorem: $x^4 + y^4 = 1$ only has 4 solutions.
- The curve $y^4 + 5x^4 - 6x^2y^2 + 6x^3 + 26x^2y + 10xy^2 - 10y^3 - 32x^2 - 40xy + 24y^2 + 32x - 16 = 0$ only has 5 solutions

For any $a \in \mathbb{Z}$, the equation $x^4 - y^4 = a$ has only finitely many integer solutions, as $x^4 - y^4 = (x^2 - y^2)(x^2 + y^2)$.

Degree Is Not A Good Invariant

- Changing variables does not preserve degree: substituting $y = z + x^{100}$ in $y = x$ gives $z = x - x^{100}$.

Degree Is Not A Good Invariant

- Changing variables does not preserve degree: substituting $y = z + x^{100}$ in $y = x$ gives $z = x - x^{100}$.
- Some equations do not behave as expected, e.g. $y^2 = x^3 + x^2$, has solutions parameterised by $\frac{y}{x}$.

Degree Is Not A Good Invariant

- Changing variables does not preserve degree: substituting $y = z + x^{100}$ in $y = x$ gives $z = x - x^{100}$.
- Some equations do not behave as expected, e.g. $y^2 = x^3 + x^2$, has solutions parameterised by $\frac{y}{x}$.
- When there are more variables, things are not always as expected. The equations $y = x^2, z = xy$ have solutions parameterised by x, but $a^2 + b^2 = c^2, ab = 2 \times 6$ can be converted to $v^2 = u^3 - 36u$.

Genus

Complex solutions to an equation come with a complex manifold structure.

Genus

Complex solutions to an equation come with a complex manifold structure.
Complex curves (real surfaces) are parameterised by their genus (# holes).

Genus

Complex solutions to an equation come with a complex manifold structure.
Complex curves (real surfaces) are parameterised by their genus (# holes).
This can also be defined in terms of the dimension of the space of differential forms.

Genus

Complex solutions to an equation come with a complex manifold structure.

Complex curves (real surfaces) are parameterised by their genus (# holes).

This can also be defined in terms of the dimension of the space of differential forms.

Definition

The genus of an equation is the genus of the complex solution set.

Genus Of Small Degree Curves

- Degrees 1 and 2: the complex solutions are parameterised by $\mathbb{C}$. This compactifies to a sphere, so the genus is zero.
- Degree 3: genus one. Can be transformed to $y^2 = f(x)$ with f degree 3.
- Degree 4: genus three.
- Degree d: genus $\frac{(d-1)(d-2)}{2}$.

Geometry Controls Arithmetic

Theorem

A genus zero curve either has infinitely many solutions (parameterised by $\mathbb{Q}$), or no solutions. Moreover, this can be checked efficiently.

Geometry Controls Arithmetic

Theorem

A genus zero curve either has infinitely many solutions (parameterised by $\mathbb{Q}$), or no solutions. Moreover, this can be checked efficiently.

Theorem (Mordell–Weil)

A genus one curve either has a rational solution (and the solutions form a finitely generated abelian group), or no solutions.

Geometry Controls Arithmetic

Theorem

A genus zero curve either has infinitely many solutions (parameterised by $\mathbb{Q}$), or no solutions. Moreover, this can be checked efficiently.

Theorem (Mordell–Weil)

A genus one curve either has a rational solution (and the solutions form a finitely generated abelian group), or no solutions.

Theorem (Faltings 1983)

A curve of genus at least 2 has only finitely many solutions (in $\mathbb{Q}$).

Limits To Rational Solutions

As rational points on high genus curves are finite, many very different curves have the same rational points.

Limits To Rational Solutions

As rational points on high genus curves are finite, many very different curves have the same rational points.
What if we allow more complicated solutions? For example, those expressible in terms of $\sqrt{2}$? Or $\sqrt{-1}$? Or the real root of $x^5 - x + 1$?

Limits To Rational Solutions

As rational points on high genus curves are finite, many very different curves have the same rational points.

What if we allow more complicated solutions? For example, those expressible in terms of $\sqrt{2}$? Or $\sqrt{-1}$? Or the real root of $x^5 - x + 1$?

The three theorems still hold! Solutions in "small" fields do not see all of the curve.

Low Degree Points

Definition

A degree d solution to an equation is a solution whose values lie in a degree d extension of $\mathbb{Q}$ – they can be expressed in terms of a root of a degree d polynomial.

Low Degree Points

Definition

A degree d solution to an equation is a solution whose values lie in a degree d extension of $\mathbb{Q}$ – they can be expressed in terms of a root of a degree d polynomial.

Degree 2 solutions are also called quadratic points, and can always be expressed in terms of a square root.

Low Degree Points

Definition

A degree d solution to an equation is a solution whose values lie in a degree d extension of $\mathbb{Q}$ – they can be expressed in terms of a root of a degree d polynomial.

Degree 2 solutions are also called quadratic points, and can always be expressed in terms of a square root.
Degree 3 solutions are also called cubic points. Some of them can be expressed in terms of a cube root.

Quadratic Points On Small Degree Curves

- Degree 1 curves (lines) have infinitely many quadratic points

Quadratic Points On Small Degree Curves

- Degree 1 curves (lines) have infinitely many quadratic points
- Degree 2 curves (conics) also have infintiely many quadratic points

Quadratic Points On Small Degree Curves

- Degree 1 curves (lines) have infinitely many quadratic points
- Degree 2 curves (conics) also have infintiely many quadratic points
- Degree 3 curves have infinitely many quadratic points, if they have a rational point.

Quadratic Points On Small Degree Curves

- Degree 1 curves (lines) have infinitely many quadratic points
- Degree 2 curves (conics) also have infintiely many quadratic points
- Degree 3 curves have infinitely many quadratic points, if they have a rational point.
- Degree 4 curves can have infinitely many quadratic points, e.g. $y^4 = x^3 - 36x$.

Quadratic Points On Small Degree Curves

- Degree 1 curves (lines) have infinitely many quadratic points
- Degree 2 curves (conics) also have infintiely many quadratic points
- Degree 3 curves have infinitely many quadratic points, if they have a rational point.
- Degree 4 curves can have infinitely many quadratic points, e.g. $y^4 = x^3 - 36x$.
- Degree 5 curves have only finitely many quadratic points.

Genus Is Not Enough

Example

For a (squarefree) degree d polynomial, f, the curve $y^2 = f(x)$ has genus $\lceil \frac{d}{2} \rceil - 1$.

Genus Is Not Enough

Example

For a (squarefree) degree d polynomial, f, the curve $y^2 = f(x)$ has genus $\lceil \frac{d}{2} \rceil - 1$. But it always has infinitely many quadratic points.

Genus Is Not Enough

Example

For a (squarefree) degree d polynomial, f, the curve $y^2 = f(x)$ has genus $\lceil \frac{d}{2} \rceil - 1$. But it always has infinitely many quadratic points.

Example

For any integer n, the pair of equations $y^2 = x^3 - 36x$, $z^2 = x^n y - 1$, define a genus $n + 3$ curve. But it still has infinitely many quadratic points.

Geometry Controls Arithmetic Again

Theorem (Harris–Silverman 1991)

If an equation has infinitely many quadratic points, then the associated Riemann surface is a double cover of a sphere ($\mathbb{P}^1$) or a torus (an elliptic curve).

Geometry Controls Arithmetic Again

Theorem (Harris–Silverman 1991)

If an equation has infinitely many quadratic points, then the associated Riemann surface is a double cover of a sphere ($\mathbb{P}^1$) or a torus (an elliptic curve).

Theorem (Kadets–Vogt 2025)

If an equation of genus $g \gtrsim \frac{d^2}{2}$ has infinitely many degree d points, then the associated Riemann surface has a degree d' map to a Riemann surface whose equation has infinitely many degree e solutions, where $d = ed'$.

Plane Curves

Theorem (Debarre–Klassen 1994)

Let $d \geq 7$, then a degree d equation has only finitely many solutions of degree at most $d - 2$.

Plane Curves

Theorem (Debarre–Klassen 1994)

Let $d \geq 7$, then a degree d equation has only finitely many solutions of degree at most $d - 2$.

Example

The Fermat equation, $x^n + y^n = 1$, has only finitely many degree $\leq n - 2$ solutions, for any $n \geq 7$.

Directions of Current Research

- Classify the curves with infinitely many degree d points below the genus threshold.
- Which curves have infinitely many cubic points that *can* be expressed in terms of cube roots? What about in higher degrees?
- What if the complex solutions describe a complex surface (real 4-fold)?
- How do degree d solutions behave under mappings?
- For "interesting" equations, can you describe all of their degree d points?

Thank you! Any Questions?