The quadratic formula

You may recall the quadratic formula for roots of quadratic polynomials $ax^2 + bx + c$. It says that the solutions to this polynomial are

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

The quadratic formula

You may recall the quadratic formula for roots of quadratic polynomials $ax^2 + bx + c$. It says that the solutions to this polynomial are

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

For example, when we take the polynomial $f(x) = x^2 - 3x - 4$, we obtain

$$\frac{3 \pm \sqrt{9 + 16}}{2}$$

which gives 4 and -1.

The quadratic formula

You may recall the quadratic formula for roots of quadratic polynomials $ax^2 + bx + c$. It says that the solutions to this polynomial are

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

For example, when we take the polynomial $f(x) = x^2 - 3x - 4$, we obtain

$$\frac{3 \pm \sqrt{9 + 16}}{2}$$

which gives 4 and -1.

Some quick terminology

- We say that 4 and -1 are *roots* of the polynomial $x^2 - 3x - 4$ or *solutions* to the polynomial equation $x^2 - 3x - 4 = 0$.

The quadratic formula

You may recall the quadratic formula for roots of quadratic polynomials $ax^2 + bx + c$. It says that the solutions to this polynomial are

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

For example, when we take the polynomial $f(x) = x^2 - 3x - 4$, we obtain

$$\frac{3 \pm \sqrt{9 + 16}}{2}$$

which gives 4 and -1.

Some quick terminology

- We say that 4 and -1 are *roots* of the polynomial $x^2 - 3x - 4$ or *solutions* to the polynomial equation $x^2 - 3x - 4 = 0$.
- We may *factor* $x^2 - 3x - 4$ as $(x - 4)(x + 1)$.

The quadratic formula

You may recall the quadratic formula for roots of quadratic polynomials $ax^2 + bx + c$. It says that the solutions to this polynomial are

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

For example, when we take the polynomial $f(x) = x^2 - 3x - 4$, we obtain

$$\frac{3 \pm \sqrt{9 + 16}}{2}$$

which gives 4 and -1.

Some quick terminology

- We say that 4 and -1 are *roots* of the polynomial $x^2 - 3x - 4$ or *solutions* to the polynomial equation $x^2 - 3x - 4 = 0$.
- We may *factor* $x^2 - 3x - 4$ as $(x - 4)(x + 1)$.
- If we denote $x^2 - 3x - 4$ as $f(x)$, we have $f(4) = 0$ and $f(-1) = 0$.

Note that in the example both roots are integers, but other times it may give numbers are not integers or even rational numbers, such as with $x^2 - 5$, which gives $\pm\sqrt{5}$, which is a real number that is not rational.

Note that in the example both roots are integers, but other times it may give numbers are not integers or even rational numbers, such as with $x^2 - 5$, which gives $\pm\sqrt{5}$, which is a real number that is not rational.

Other times it may even give complex numbers that are not real, such as with $x^2 + 1$, which gives $\pm i$.

Higher degree polynomials

If you look at a cubic polynomial $a_3x^3 + a_2x^2 + a_1x + a_0$ or a quartic $a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ (where the a_i are all integers) there are similar (but more complicated) formulas.

Higher degree polynomials

If you look at a cubic polynomial $a_3x^3 + a_2x^2 + a_1x + a_0$ or a quartic $a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ (where the a_i are all integers) there are similar (but more complicated) formulas.

For degree 5, there are no such formulas. This is called the *insolubility of the quintic* and it is a famous result proved by Abel and Galois in the early 19th century.

Higher degree polynomials

If you look at a cubic polynomial $a_3x^3 + a_2x^2 + a_1x + a_0$ or a quartic $a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ (where the a_i are all integers) there are similar (but more complicated) formulas.

For degree 5, there are no such formulas. This is called the *insolubility of the quintic* and it is a famous result proved by Abel and Galois in the early 19th century.

However, we will be interested in something a bit more simple to begin with: *rational number* solutions to polynomials with integer coefficients.

Higher degree polynomials

If you look at a cubic polynomial $a_3x^3 + a_2x^2 + a_1x + a_0$ or a quartic $a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ (where the a_i are all integers) there are similar (but more complicated) formulas.

For degree 5, there are no such formulas. This is called the *insolubility of the quintic* and it is a famous result proved by Abel and Galois in the early 19th century.

However, we will be interested in something a bit more simple to begin with: *rational number* solutions to polynomials with integer coefficients.

That is, we will consider polynomials of the form

$$f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$$

Higher degree polynomials

If you look at a cubic polynomial $a_3x^3 + a_2x^2 + a_1x + a_0$ or a quartic $a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ (where the a_i are all integers) there are similar (but more complicated) formulas.

For degree 5, there are no such formulas. This is called the *insolubility of the quintic* and it is a famous result proved by Abel and Galois in the early 19th century.

However, we will be interested in something a bit more simple to begin with: *rational number* solutions to polynomials with integer coefficients.

That is, we will consider polynomials of the form

$$f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$$

and look for *rational numbers* b/c such that

$$f(b/c) = 0.$$

Rational solutions to polynomials

Note that if we have $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ and

$$f(b/c) = 0,$$

(where b/c is in lowest terms, i.e. b and c have no common factors) then we have

$$a_0 = \frac{b}{c}\left(a_n\left(\frac{b}{c}\right)^{n-1} + \ldots x_1\right)$$

so b must divide a_0.

Rational solutions to polynomials

Note that if we have $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ and

$$f(b/c) = 0,$$

(where b/c is in lowest terms, i.e. b and c have no common factors) then we have

$$a_0 = \frac{b}{c}\left(a_n\left(\frac{b}{c}\right)^{n-1} + \ldots x_1\right)$$

so b must divide a_0.

Similarly, after multiplying through by $(c/b)^n$ we obtain

$$a_n = \frac{c}{b}\left(a_0\left(\frac{c}{b}\right)^{n-1} + \cdots + a_{n-1}\right)$$

so c must divide a_n.

Rational solutions to polynomials

Note that if we have $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ and

$$f(b/c) = 0,$$

(where b/c is in lowest terms, i.e. b and c have no common factors) then we have

$$a_0 = \frac{b}{c}\left(a_n\left(\frac{b}{c}\right)^{n-1} + \ldots x_1\right)$$

so b must divide a_0.

Similarly, after multiplying through by $(c/b)^n$ we obtain

$$a_n = \frac{c}{b}\left(a_0\left(\frac{c}{b}\right)^{n-1} + \cdots + a_{n-1}\right)$$

so c must divide a_n.

Since there are finitely many rational b/c such that b divides a_n and c divides a_0, this reduces finding all the rational solutions to $f(x) = 0$ to a simple search problem.

Polynomials in two variables

What if we look instead at polynomials in two variables? Those are polynomials like $x^4y^2 + 5xy^3 + 7x + y + 10$ and $y^2 - x^3 - 2x + 1$.

Polynomials in two variables

What if we look instead at polynomials in two variables? Those are polynomials like $x^4y^2 + 5xy^3 + 7x + y + 10$ and $y^2 - x^3 - 2x + 1$.

Example

Fermat's last theorem (first considered by Fermat in 1637, proved by Wiles in 1994) says that for $n \geq 3$, there are no positive integers A, B, and C such that

$$A^n + B^n = C^n.$$

Polynomials in two variables

What if we look instead at polynomials in two variables? Those are polynomials like $x^4y^2 + 5xy^3 + 7x + y + 10$ and $y^2 - x^3 - 2x + 1$.

Example

Fermat's last theorem (first considered by Fermat in 1637, proved by Wiles in 1994) says that for $n \geq 3$, there are no positive integers A, B, and C such that

$$A^n + B^n = C^n.$$

Dividing by C, we get

$$\left(\frac{A}{C}\right)^n + \left(\frac{B}{C}\right)^n = 1.$$

Thus, integer solutions to Fermat's equation are the same as rational solutions to the two-variable equation

$$x^n + y^n - 1 = 0.$$

Even older polynomial equations in two variable

Example

Pythagorean triples $A^2 + B^2 = C^2$, e.g. $3^2 + 4^2 = 5^2$, become solutions to

$$x^2 + y^2 - 1 = 0$$

after dividing by C (that is, letting $x = A/C$ and $y = B/C$).

Even older polynomial equations in two variable

Example

Pythagorean triples $A^2 + B^2 = C^2$, e.g. $3^2 + 4^2 = 5^2$, become solutions to

$$x^2 + y^2 - 1 = 0$$

after dividing by C (that is, letting $x = A/C$ and $y = B/C$).

Example

Take the polynomial equation

$$y^2 = x^8 + x^4 + x^2.$$

Diophantus of Alexandria found that $x = 1/4, y = 9/16$ was a solution in the third century AD.

Even older polynomial equations in two variable

Example

Pythagorean triples $A^2 + B^2 = C^2$, e.g. $3^2 + 4^2 = 5^2$, become solutions to

$$x^2 + y^2 - 1 = 0$$

after dividing by C (that is, letting $x = A/C$ and $y = B/C$).

Example

Take the polynomial equation

$$y^2 = x^8 + x^4 + x^2.$$

Diophantus of Alexandria found that $x = 1/4, y = 9/16$ was a solution in the third century AD. In 1997, Wetherell showed that was the *only* nonzero solution, up to sign (of course $x = \pm 1/4, y = \pm 9/16$ are solutions as well).

Questions about two-variable polynomials

Based on what we have seen so far, it seems that questions about rational solutions to two-variable polynomial equations are much harder than for one variable. So here's some questions:

Questions about two-variable polynomials

Based on what we have seen so far, it seems that questions about rational solutions to two-variable polynomial equations are much harder than for one variable. So here's some questions:

- Can you tell when a two-variable polynomial has infinitely many rational solutions?

Questions about two-variable polynomials

Based on what we have seen so far, it seems that questions about rational solutions to two-variable polynomial equations are much harder than for one variable. So here's some questions:

- Can you tell when a two-variable polynomial has infinitely many rational solutions?
- Is there a method for finding all the solutions when the number is finite?

Questions about two-variable polynomials

Based on what we have seen so far, it seems that questions about rational solutions to two-variable polynomial equations are much harder than for one variable. So here's some questions:

- Can you tell when a two-variable polynomial has infinitely many rational solutions?
- Is there a method for finding all the solutions when the number is finite?
- Does the number of rational solutions depend only on the degree of the polynomial (when that number is finite)?

Questions about two-variable polynomials

Based on what we have seen so far, it seems that questions about rational solutions to two-variable polynomial equations are much harder than for one variable. So here's some questions:

- Can you tell when a two-variable polynomial has infinitely many rational solutions?
- Is there a method for finding all the solutions when the number is finite?
- Does the number of rational solutions depend only on the degree of the polynomial (when that number is finite)?

Since we will be talking about degree a lot I should define it with an example:

Questions about two-variable polynomials

Based on what we have seen so far, it seems that questions about rational solutions to two-variable polynomial equations are much harder than for one variable. So here's some questions:

- Can you tell when a two-variable polynomial has infinitely many rational solutions?
- Is there a method for finding all the solutions when the number is finite?
- Does the number of rational solutions depend only on the degree of the polynomial (when that number is finite)?

Since we will be talking about degree a lot I should define it with an example:

The degree of $y^2 - x^8 + x^4 + x^2$ is 8, the degree of $y^2x^9 + 7x^5y^3 + x + 3y$ is 11. The degree is the total degree – x-degree plus y-degree – of the term of highest total degree. We'll begin by considering polynomials of various degrees.

Two-variable polynomials of degree 2

Two-variable polynomials of degree 2 may have infinitely many solutions. You may recall that there are infinitely many Pythagorean triples $A^2 + B^2 = C^2$. Dividing through as we saw before gives infinitely many solutions to

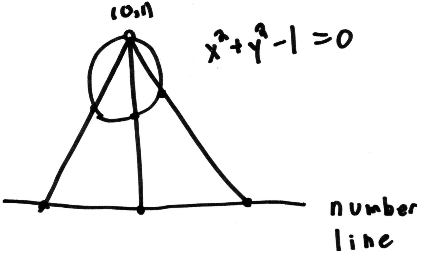
$$x^2 + y^2 - 1 = 0.$$

Two-variable polynomials of degree 2

Two-variable polynomials of degree 2 may have infinitely many solutions. You may recall that there are infinitely many Pythagorean triples $A^2 + B^2 = C^2$. Dividing through as we saw before gives infinitely many solutions to

$$x^2 + y^2 - 1 = 0.$$

Another way of seeing that there are infinitely many solutions to $x^2 - y^2 - 1 = 0$ is with the following picture, which gives a one-to-one correspondence between the curve $x^2 + y^2 - 1 = 0$ in the Cartesian plane (minus a single point) and the usual number line.



More on two-variable polynomials of degree 2

The one-to-one correspondence on the last page can be written as

$$t \mapsto \left(\frac{t^2 - 1}{t^2 + 1}, \frac{2t}{t^2 + 1} \right)$$

which sends the usual number line to the locus of $x^2 + y^2 - 1 = 0$ in the Cartesian plane.

More on two-variable polynomials of degree 2

The one-to-one correspondence on the last page can be written as

$$t \mapsto \left(\frac{t^2 - 1}{t^2 + 1}, \frac{2t}{t^2 + 1} \right)$$

which sends the usual number line to the locus of $x^2 + y^2 - 1 = 0$ in the Cartesian plane.

Using this correspondence, we count the number of rational points on $x^2 + y^2 - 1 = 0$ with numerator and denominator less than some fixed constant M. We see that

$$\# \left\{ \left(\frac{b}{c}, \frac{d}{e} \right) \quad \middle| \quad \left(\frac{b}{c} \right)^2 + \left(\frac{d}{e} \right)^2 = 1 \text{ and } |b|, |c|, |d|, |e| \leq M \right\} \sim M.$$

More on two-variable polynomials of degree 2

The one-to-one correspondence on the last page can be written as

$$t \mapsto \left(\frac{t^2 - 1}{t^2 + 1}, \frac{2t}{t^2 + 1} \right)$$

which sends the usual number line to the locus of $x^2 + y^2 - 1 = 0$ in the Cartesian plane.

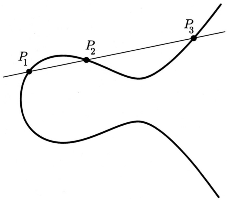
Using this correspondence, we count the number of rational points on $x^2 + y^2 - 1 = 0$ with numerator and denominator less than some fixed constant M. We see that

$$\# \left\{ \left(\frac{b}{c}, \frac{d}{e} \right) \quad | \quad \left(\frac{b}{c} \right)^2 + \left(\frac{d}{e} \right)^2 = 1 \text{ and } |b|, |c|, |d|, |e| \leq M \right\} \sim M.$$

In other words, there are quite a lot of rational points on the curve $x^2 + y^2 - 1 = 0$.

Two-variable polynomials of degree 3

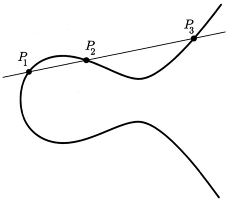
In the case of a two-variable polynomial $f(x, y)$ of degree 3, any straight line intersects our curve $f(x, y) = 0$ in three points. Thus, given two rational points we can "add them together" to get a third as in this picture below (where we have "$P_1 + P_2 = P_3$").



"Adding" Two Points on a Cubic Curve

Two-variable polynomials of degree 3

In the case of a two-variable polynomial $f(x, y)$ of degree 3, any straight line intersects our curve $f(x, y) = 0$ in three points. Thus, given two rational points we can "add them together" to get a third as in this picture below (where we have "$P_1 + P_2 = P_3$").

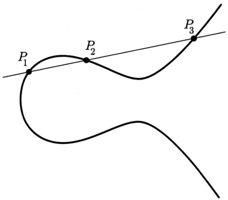


"Adding" Two Points on a Cubic Curve

This often allows us to generate infinitely many rational points on the curve.

Two-variable polynomials of degree 3

In the case of a two-variable polynomial $f(x, y)$ of degree 3, any straight line intersects our curve $f(x, y) = 0$ in three points. Thus, given two rational points we can "add them together" to get a third as in this picture below (where we have "$P_1 + P_2 = P_3$").



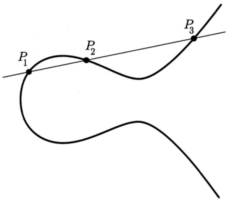
"Adding" Two Points on a Cubic Curve

This often allows us to generate infinitely many rational points on the curve. The points are more sparsely spaced though

$$\#\left\{\left(\frac{b}{c}, \frac{d}{e}\right) \quad \middle| \quad f(b/c, d/e) = 0 \text{ and } |b|, |c|, |d|, |e| \leq M\right\} \sim \log M.$$

Two-variable polynomials of degree 3

In the case of a two-variable polynomial $f(x, y)$ of degree 3, any straight line intersects our curve $f(x, y) = 0$ in three points. Thus, given two rational points we can "add them together" to get a third as in this picture below (where we have "$P_1 + P_2 = P_3$").



"Adding" Two Points on a Cubic Curve

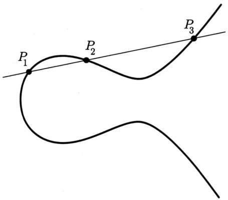
This often allows us to generate infinitely many rational points on the curve. The points are more sparsely spaced though

$$\#\left\{\left(\frac{b}{c}, \frac{d}{e}\right) \quad | \quad f(b/c, d/e) = 0 \text{ and } |b|, |c|, |d|, |e| \leq M\right\} \sim \log M.$$

This is due to Mordell (1922).

Two-variable polynomials of degree 3

In the case of a two-variable polynomial $f(x, y)$ of degree 3, any straight line intersects our curve $f(x, y) = 0$ in three points. Thus, given two rational points we can "add them together" to get a third as in this picture below (where we have "$P_1 + P_2 = P_3$").



"Adding" Two Points on a Cubic Curve

This often allows us to generate infinitely many rational points on the curve.The points are more sparsely spaced though

$$\#\left\{\left(\frac{b}{c}, \frac{d}{e}\right) \quad | \quad f(b/c, d/e) = 0 \text{ and } |b|, |c|, |d|, |e| \leq M\right\} \sim \log M.$$

This is due to Mordell (1922). Note that in general $f(x, y) = 0$ gives a curve and we refer to rational solutions as rational points

Two-variable polynomials of degree 4 or more

How about for polynomials of degree 4 or more?

Conjecture

(Mordell conjecture, 1922) If $f(x, y)$ *is a "good" polynomial of degree 4 or greater, then there are finitely many pairs of rational numbers* $(b/c, d/e)$ *such that* $f(b/c, d/e) = 0$.

Two-variable polynomials of degree 4 or more

How about for polynomials of degree 4 or more?

Conjecture

(Mordell conjecture, 1922) If $f(x,y)$ is a "good" polynomial of degree 4 or greater, then there are finitely many pairs of rational numbers $(b/c, d/e)$ such that $f(b/c, d/e) = 0$.

The first real progress on this came in the 1960s when Mumford showed that the $\log M$ that appeared in degree 3 was at most $\log \log M$ in the case of degree 4 or more, and when Manin proved it for "function fields" (which are analogs of the rational numbers).

Two-variable polynomials of degree 4 or more

How about for polynomials of degree 4 or more?

Conjecture

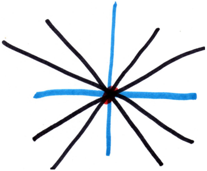
(Mordell conjecture, 1922) If $f(x, y)$ is a "good" polynomial of degree 4 or greater, then there are finitely many pairs of rational numbers $(b/c, d/e)$ such that $f(b/c, d/e) = 0$.

The first real progress on this came in the 1960s when Mumford showed that the $\log M$ that appeared in degree 3 was at most $\log \log M$ in the case of degree 4 or more, and when Manin proved it for "function fields" (which are analogs of the rational numbers).

The theorem was finally was proved by Faltings in 1983 and reproved by Faltings and Vojta in a more exact form in 1991.

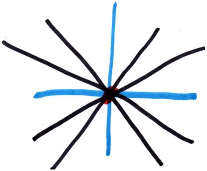
"Bad polynomial" #1

Here's some polynomials where we clearly do have infinitely many rational solutions despite being of degree 4. Here's a picture of the curve corresponding to the equation $x^4 - 5x^2y^2 + 4y^4 = 0$, which is just the union of four lines, so clearly has infinitely many rational points on it.



“Bad polynomial” #1

Here’s some polynomials where we clearly do have infinitely many rational solutions despite being of degree 4. Here’s a picture of the curve corresponding to the equation $x^4 - 5x^2y^2 + 4y^4 = 0$, which is just the union of four lines, so clearly has infinitely many rational points on it.

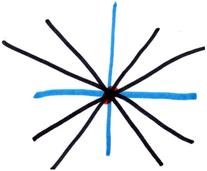


Note that the four lines come from the fact that

$$x^4 - 5x^2y^2 + 4y^4 = (x - y)(x + y)(x - 2y)(x + 2y).$$

"Bad polynomial" #1

Here's some polynomials where we clearly do have infinitely many rational solutions despite being of degree 4. Here's a picture of the curve corresponding to the equation $x^4 - 5x^2y^2 + 4y^4 = 0$, which is just the union of four lines, so clearly has infinitely many rational points on it.



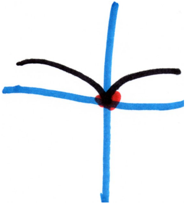
Note that the four lines come from the fact that

$$x^4 - 5x^2y^2 + 4y^4 = (x - y)(x + y)(x - 2y)(x + 2y).$$

Notice that all four points meet at the origin so there is no clear "direction" for the curve there.

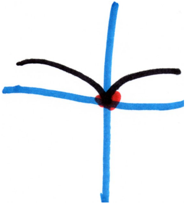
“Bad polynomials” #2

Here’s another polynomial equation of degree greater than or equal to 4 that has infinitely many rational points on it: $x^2 - y^5 = 0$.



“Bad polynomials” #2

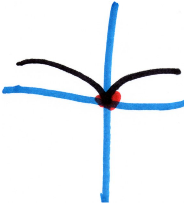
Here's another polynomial equation of degree greater than or equal to 4 that has infinitely many rational points on it: $x^2 - y^5 = 0$.



Note that this curve can be parametrized by $t \mapsto (t^5, t^2)$.

“Bad polynomials” #2

Here’s another polynomial equation of degree greater than or equal to 4 that has infinitely many rational points on it: $x^2 - y^5 = 0$.



Note that this curve can be parametrized by $t \mapsto (t^5, t^2)$.

Notice that here again the curve has no clear “direction” at the origin.

Tangent vectors

The technical term for the direction a curve is moving in at a point (x_0, y_0) is the tangent vector (up to scaling). It can be defined as

$$\left(-\frac{\partial f}{\partial y}(x_0, y_0), \frac{\partial f}{\partial x}(x_0, y_0)\right).$$

Tangent vectors

The technical term for the direction a curve is moving in at a point (x_0, y_0) is the tangent vector (up to scaling). It can be defined as

$$\left(-\frac{\partial f}{\partial y}(x_0, y_0), \frac{\partial f}{\partial x}(x_0, y_0)\right).$$

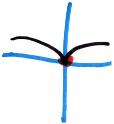
When both partials are zero, there is no well-defined tangent vector. One easily sees that this is the case, for example, for $x^2 - y^5$ at the origin $(0, 0)$.

Tangent vectors

The technical term for the direction a curve is moving in at a point (x_0, y_0) is the tangent vector (up to scaling). It can be defined as

$$\left(-\frac{\partial f}{\partial y}(x_0, y_0), \frac{\partial f}{\partial x}(x_0, y_0)\right).$$

When both partials are zero, there is no well-defined tangent vector. One easily sees that this is the case, for example, for $x^2 - y^5$ at the origin $(0, 0)$.



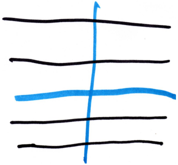
A geometric condition

Being nonsingular is a geometric condition, so one has to check not just over the real numbers $\mathbb{R}$ but over all of the complex numbers $\mathbb{C}$.

A geometric condition

Being nonsingular is a geometric condition, so one has to check not just over the real numbers $\mathbb{R}$ but over all of the complex numbers $\mathbb{C}$.

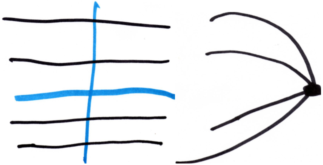
One also has to check the so-called "points at infinity". This can be seen from considering the case of four parallel lines. Clearly, the lines contain infinitely many rational points, but there is no singularity in the Cartesian plane.



A geometric condition

Being nonsingular is a geometric condition, so one has to check not just over the real numbers $\mathbb{R}$ but over all of the complex numbers $\mathbb{C}$.

One also has to check the so-called "points at infinity". This can be seen from considering the case of four parallel lines. Clearly, the lines contain infinitely many rational points, but there is no singularity in the Cartesian plane.



But the lines all meet "at infinity" in the projective plane, which is the natural place to compactify curves in the Cartesian plane.

A proper statement of the Mordell Conjecture

So here is a formal statement of the Mordell conjecture.

A proper statement of the Mordell Conjecture

So here is a formal statement of the Mordell conjecture.

Theorem

(Mordell conjecture/Faltings theorem) If $f(x, y)$ *is a nonsingular polynomial of degree 4 or greater, then there are finitely many pairs of rational numbers* $(b/c, d/e)$ *such that* $f(b/c, d/e) = 0$.

A proper statement of the Mordell Conjecture

So here is a formal statement of the Mordell conjecture.

Theorem

(Mordell conjecture/Faltings theorem) If $f(x, y)$ is a nonsingular polynomial of degree 4 or greater, then there are finitely many pairs of rational numbers $(b/c, d/e)$ such that $f(b/c, d/e) = 0$.

We should also make a note about the pictures we have been drawing. It may look like there are lots of points on these curves and hence lots of rational solutions. However, the pictures are over the *real numbers*, not the rational numbers. Thus, the points we see do not necessarily correspond to *rational* solutions.

A proper statement of the Mordell Conjecture

So here is a formal statement of the Mordell conjecture.

Theorem

(Mordell conjecture/Faltings theorem) If $f(x, y)$ is a nonsingular polynomial of degree 4 or greater, then there are finitely many pairs of rational numbers $(b/c, d/e)$ such that $f(b/c, d/e) = 0$.

We should also make a note about the pictures we have been drawing. It may look like there are lots of points on these curves and hence lots of rational solutions. However, the pictures are over the *real numbers*, not the rational numbers. Thus, the points we see do not necessarily correspond to *rational* solutions.

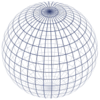
It turns out that what really matters is what the curves look like over the *complex numbers*.

Curves over the complex numbers

When you take the set of all complex numbers a and b such that $f(a, b) = 0$, you get a two-dimensional object.
Here's what a curve of degree 2 looks like over the complex numbers.

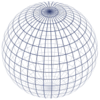
Curves over the complex numbers

When you take the set of all complex numbers a and b such that $f(a, b) = 0$, you get a two-dimensional object.
Here's what a curve of degree 2 looks like over the complex numbers.

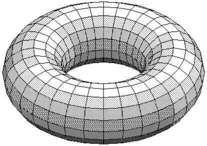


Curves over the complex numbers

When you take the set of all complex numbers a and b such that $f(a, b) = 0$, you get a two-dimensional object.
Here's what a curve of degree 2 looks like over the complex numbers.



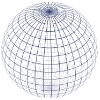
Here's what a curve of degree 3 looks like. It has one hole.



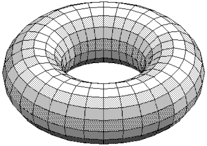
Curves over the complex numbers

When you take the set of all complex numbers a and b such that $f(a, b) = 0$, you get a two-dimensional object.

Here's what a curve of degree 2 looks like over the complex numbers.



Here's what a curve of degree 3 looks like. It has one hole.

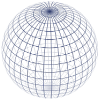


A nonsingular curve of degree 4 has three holes. It looks like this:

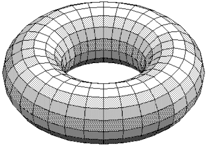
Curves over the complex numbers

When you take the set of all complex numbers a and b such that $f(a,b) = 0$, you get a two-dimensional object.

Here's what a curve of degree 2 looks like over the complex numbers.



Here's what a curve of degree 3 looks like. It has one hole.



A nonsingular curve of degree 4 has three holes. It looks like this:

Addition laws on curves

We noted before that curves coming from polynomials of of degree 3 have an addition law on them.

Addition laws on curves

We noted before that curves coming from polynomials of of degree 3 have an addition law on them.

We also noted that curves corresponding to polynomials of degree 2 have a one-one correspondence with the usual number line, which gives them the addition law from the usual number line!

Addition laws on curves

We noted before that curves coming from polynomials of of degree 3 have an addition law on them.

We also noted that curves corresponding to polynomials of degree 2 have a one-one correspondence with the usual number line, which gives them the addition law from the usual number line!

It turns out that a curve with more than one hole in it cannot have an addition law on it.

Addition laws on curves

We noted before that curves coming from polynomials of of degree 3 have an addition law on them.

We also noted that curves corresponding to polynomials of degree 2 have a one-one correspondence with the usual number line, which gives them the addition law from the usual number line!

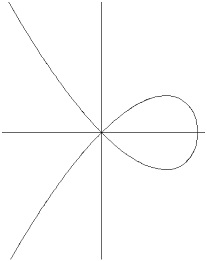
It turns out that a curve with more than one hole in it cannot have an addition law on it.

When you have a singularity, it looks like a hole but it is not really one. This is why singular curves are different from nonsingular ones.

A nodal cubic

Look for example at the "nodal cubic" defined by

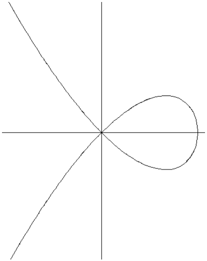
$$y^2 - x^2(1 - x) = 0$$



A nodal cubic

Look for example at the "nodal cubic" defined by

$$y^2 - x^2(1 - x) = 0$$

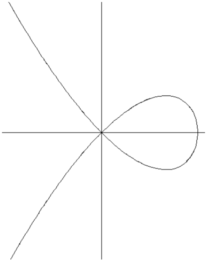


One sees what looks like a hole. However, it can be disentangled (the technical term is *desingularized*) so that the hole disappears.

A nodal cubic

Look for example at the "nodal cubic" defined by

$$y^2 - x^2(1 - x) = 0$$



One sees what looks like a hole. However, it can be disentangled (the technical term is *desingularized*) so that the hole disappears.

In this case, what one ends up with is a degree three polynomial that has "as many" rational solutions as a degree two polynomial equation. That is one gets M – rather than rather than $\log M$ – solutions with numerator and denominator bounded by M.

Mordell-Lang-Vojta philosophy of solutions

The *Mordell-Lang-Vojta conjecture* (proved in some cases by Faltings, Vojta, and McQuillan) says the following roughly.

Mordell-Lang-Vojta philosophy of solutions

The *Mordell-Lang-Vojta conjecture* (proved in some cases by Faltings, Vojta, and McQuillan) says the following roughly.

Conjecture

Whenever a polynomial equation (in any number of variables) has infinitely many solutions there is an underlying addition law on some part of the geometric object that the polynomial equation defines.

Mordell-Lang-Vojta philosophy of solutions

The *Mordell-Lang-Vojta conjecture* (proved in some cases by Faltings, Vojta, and McQuillan) says the following roughly.

Conjecture

Whenever a polynomial equation (in any number of variables) has infinitely many solutions there is an underlying addition law on some part of the geometric object that the polynomial equation defines.

In the case of two-variable polynomials, the geometric object will be the entire curve. In three or more variables, it becomes more complicated.

Finding all the solutions

Knowing that a nonsingular polynomial of degree 4 in two variables has only finitely many solutions is hardly the end of the story. Faltings' proof says very little about finding all the solutions.

Finding all the solutions

Knowing that a nonsingular polynomial of degree 4 in two variables has only finitely many solutions is hardly the end of the story. Faltings' proof says very little about finding all the solutions.

Question

Is there an algorithm for finding all the rational solutions to a nonsingular polynomial of degree 4?

Finding all the solutions

Knowing that a nonsingular polynomial of degree 4 in two variables has only finitely many solutions is hardly the end of the story. Faltings' proof says very little about finding all the solutions.

Question

Is there an algorithm for finding all the rational solutions to a nonsingular polynomial of degree 4?

Answer: No one knows. There is an approach, called the method of Coleman-Chabauty which often seems to work but there is no guarantee that it will work in a particular situation. On the negative side there is something called Hilbert's Tenth Problem, solved by Matiyasevich, Robinson, Davis, and Putnam. I'll state it roughly in Hilbert's language.

Hilbert's tenth problem

Theorem

There is no process according to which it can be determined in a finite number of operations whether a polynomial equation $F(x_1, \ldots, x_n) = 0$ with integer coefficients has an integer solution (that is, some $b_1, \ldots, b_n$ such that $F(b_1, \ldots, b_n) = 0$.

In other words, there is no general algorithm for determining whether or not a multivariable polynomial equation has an integer solution.

Hilbert's tenth problem

Theorem

There is no process according to which it can be determined in a finite number of operations whether a polynomial equation $F(x_1, \ldots, x_n) = 0$ with integer coefficients has an integer solution (that is, some $b_1, \ldots, b_n$ such that $F(b_1, \ldots, b_n) = 0$.

In other words, there is no general algorithm for determining whether or not a multivariable polynomial equation has an integer solution. A few points:

- It is not known whether or not such an algorithm exists for determining whether there is a *rational* solution.

Hilbert's tenth problem

Theorem

There is no process according to which it can be determined in a finite number of operations whether a polynomial equation $F(x_1, \ldots, x_n) = 0$ *with integer coefficients has an integer solution (that is, some* $b_1, \ldots, b_n$ *such that* $F(b_1, \ldots, b_n) = 0$.

In other words, there is no general algorithm for determining whether or not a multivariable polynomial equation has an integer solution. A few points:

- It is not known whether or not such an algorithm exists for determining whether there is a *rational* solution.
- It is not known whether or not such an algorithm exists when we look at polynomials with only two variables.

How many solutions?

For a one variable equation $F(x) = 0$, we know that if we have solutions $\alpha_1, \ldots, \alpha_n$, then

$$F(x) = (x - \alpha_1) \cdots (x - \alpha_n).$$

So a one-variable polynomial equation has at most n rational solutions.

How many solutions?

For a one variable equation $F(x) = 0$, we know that if we have solutions $\alpha_1, \ldots, \alpha_n$, then

$$F(x) = (x - \alpha_1) \cdots (x - \alpha_n).$$

So a one-variable polynomial equation has at most n rational solutions.
Two-variable polynomial equations can have more than n solutions: they can have at least n^2. Take for example polynomial equations like

$$(x - 1)(x - 2) \cdots (x - n) - (y - 1)(y - 2) \cdots (y - n) = 0.$$

This has n^2 rational solutions. But nevertheless one can ask the following.

How many solutions?

For a one variable equation $F(x) = 0$, we know that if we have solutions $\alpha_1, \ldots, \alpha_n$, then

$$F(x) = (x - \alpha_1) \cdots (x - \alpha_n).$$

So a one-variable polynomial equation has at most n rational solutions.
Two-variable polynomial equations can have more than n solutions: they can have at least n^2. Take for example polynomial equations like

$$(x-1)(x-2)\cdots(x-n) - (y-1)(y-2)\cdots(y-n) = 0.$$

This has n^2 rational solutions. But nevertheless one can ask the following.

How many solutions?

Question

Is there a constant $C(n)$ such that any nonsingular polynomial equation $f(x, y) = 0$ of degree $n \geq 4$ has at most $C(n)$ solutions?

How many solutions?

Question

Is there a constant $C(n)$ such that any nonsingular polynomial equation $f(x, y) = 0$ of degree $n \geq 4$ has at most $C(n)$ solutions?

This is is called the "uniform boundedness question".

How many solutions?

Question

Is there a constant $C(n)$ such that any nonsingular polynomial equation $f(x, y) = 0$ of degree $n \geq 4$ has at most $C(n)$ solutions?

This is is called the "uniform boundedness question".

This is a conjecture that many (most?) do not believe, but...

How many solutions?

Question

Is there a constant $C(n)$ such that any nonsingular polynomial equation $f(x,y) = 0$ of degree $n \geq 4$ has at most $C(n)$ solutions?

This is is called the "uniform boundedness question".

This is a conjecture that many (most?) do not believe, but...

It turns out that would be implied by the Mordell-Lang-Vojta conjecture mentioned earlier, and many (most?) do (did?) believe that.

How many solutions?

Question

Is there a constant $C(n)$ such that any nonsingular polynomial equation $f(x, y) = 0$ of degree $n \geq 4$ has at most $C(n)$ solutions?

This is is called the "uniform boundedness question".

This is a conjecture that many (most?) do not believe, but...

It turns out that would be implied by the Mordell-Lang-Vojta conjecture mentioned earlier, and many (most?) do (did?) believe that.

So it is a true mystery.

A "proof" of something simpler

The proof of the Mordell conjecture is quite difficult, but we would like to give some kind of a proof of something related. So let us look at a simpler question, involving *integer* solutions to a special type of polynomial equation.

A “proof” of something simpler

The proof of the Mordell conjecture is quite difficult, but we would like to give some kind of a proof of something related. So let us look at a simpler question, involving *integer* solutions to a special type of polynomial equation.

- Let $f(x, y)$ be a *homogeneous polynomial*, that is one where every term has the same degree, e.g. $f(x, y) = 2x^3 + 5xy^2 + y^3$.

A "proof" of something simpler

The proof of the Mordell conjecture is quite difficult, but we would like to give some kind of a proof of something related. So let us look at a simpler question, involving *integer* solutions to a special type of polynomial equation.

- Let $f(x,y)$ be a *homogeneous polynomial*, that is one where every term has the same degree, e.g. $f(x,y) = 2x^3 + 5xy^2 + y^3$.
- Suppose that $f(x,y)$ factors over the $\mathbb{C}$ as

$$f(x,y) = (x - \alpha_1 y) \cdots (x - \alpha_n y)$$

for some $\alpha_i \in \mathbb{C}$ with *no two* α_i *equal to each other*.

A "proof" of something simpler

The proof of the Mordell conjecture is quite difficult, but we would like to give some kind of a proof of something related. So let us look at a simpler question, involving *integer* solutions to a special type of polynomial equation.

- Let $f(x, y)$ be a *homogeneous polynomial*, that is one where every term has the same degree, e.g. $f(x, y) = 2x^3 + 5xy^2 + y^3$.
- Suppose that $f(x, y)$ factors over the $\mathbb{C}$ as

  $$f(x, y) = (x - \alpha_1 y) \cdots (x - \alpha_n y)$$

  for some $\alpha_i \in \mathbb{C}$ with *no two* α_i *equal to each other*.
- Suppose the degree n of f is at least 3 and that all the coefficients of f are integers.

A “proof” of something simpler continued

Letting $f(x, y)$ be on the previous page, an equation

$$f(x, y) = m \quad \text{for } m \text{ an integer}$$

is called a *Thue equation*.

A "proof" of something simpler continued

Letting $f(x, y)$ be on the previous page, an equation

$$f(x, y) = m \quad \text{for } m \text{ an integer}$$

is called a *Thue equation*. Thue proved there were finitely *integer* solutions (b, c) to such an equation in 1909. This is the first serious theorem in the area.

A "proof" of something simpler continued

Letting $f(x, y)$ be on the previous page, an equation

$$f(x, y) = m \quad \text{for } m \text{ an integer}$$

is called a *Thue equation*. Thue proved there were finitely *integer* solutions (b, c) to such an equation in 1909. This is the first serious theorem in the area.

To sketch Thue's proof is simple. We write

$$m = f(b, c) = (b - \alpha_1 c) \cdots (b - \alpha_n c)$$

and divide by c^n and take absolute values to get

$$\left| \left(\frac{b}{c} - \alpha_1 \right) \cdots \left(\frac{b}{c} - \alpha_n \right) \right| = \frac{|m|}{|c|^n}$$

A "proof" of something simpler continued

Letting $f(x, y)$ be on the previous page, an equation

$$f(x, y) = m \quad \text{for } m \text{ an integer}$$

is called a *Thue equation*. Thue proved there were finitely *integer* solutions (b, c) to such an equation in 1909. This is the first serious theorem in the area.

To sketch Thue's proof is simple. We write

$$m = f(b, c) = (b - \alpha_1 c) \cdots (b - \alpha_n c)$$

and divide by c^n and take absolute values to get

$$\left| \left(\frac{b}{c} - \alpha_1 \right) \cdots \left(\frac{b}{c} - \alpha_n \right) \right| = \frac{|m|}{|c|^n}$$

Since the α_i are not equal, they cannot be too close together so we have

$$\left| \frac{b}{c} - \alpha_i \right| \leq \frac{M}{|c|^n}$$

for some constant M (not depending on b and c).

Diophantine approximation

So we are reduced to showing that we cannot have

$$\left|\frac{b}{c} - \alpha_i\right| \leq \frac{M}{|c|^n}$$

infinitely often for any complex α_i that is algebraic of degree $n >= 3$ (that is, a solution to a polynomial equation of degree $n >= 3$ over the integers). This is what Thue showed to prove his theorem. This technique is called *diophantine approximation*.

Diophantine approximation

So we are reduced to showing that we cannot have

$$\left| \frac{b}{c} - \alpha_i \right| \leq \frac{M}{|c|^n}$$

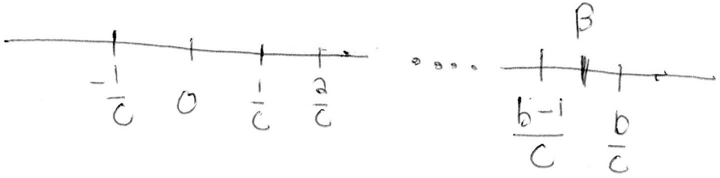
infinitely often for any complex α_i that is algebraic of degree $n >= 3$ (that is, a solution to a polynomial equation of degree $n >= 3$ over the integers). This is what Thue showed to prove his theorem. This technique is called *diophantine approximation*. We will prove something weaker, but first a picture with an idea. If β is a real number, then we can always get infinitely many b/c within $1/c$ of it. See the following picture.

Diophantine approximation

So we are reduced to showing that we cannot have

$$\left|\frac{b}{c} - \alpha_i\right| \leq \frac{M}{|c|^n}$$

infinitely often for any complex α_i that is algebraic of degree $n >= 3$ (that is, a solution to a polynomial equation of degree $n >= 3$ over the integers). This is what Thue showed to prove his theorem. This technique is called *diophantine approximation*. We will prove something weaker, but first a picture with an idea. If β is a real number, then we can always get infinitely many b/c within $1/c$ of it. See the following picture.



Liouville's theorem

Thus, it makes sense to think that there is some bound on the number r such that we can get a rational number $\frac{b}{c}$ within $\frac{1}{|c|^r}$ of β. The following is due to Liouville (1844).

Liouville's theorem

Thus, it makes sense to think that there is some bound on the number r such that we can get a rational number $\frac{b}{c}$ within $\frac{1}{|c|^r}$ of β. The following is due to Liouville (1844).

Theorem

Let β be an irrational complex number such that there exists a polynomial f of degree n over the integers such that $f(\beta) = 0$. There is a constant $M > 0$ such that

$$\left|\frac{b}{c} - \beta\right| \geq \frac{M}{|c|^n} \quad \textit{for all rational } b/c$$

Liouville's theorem

Thus, it makes sense to think that there is some bound on the number r such that we can get a rational number $\frac{b}{c}$ within $\frac{1}{|c|^r}$ of β. The following is due to Liouville (1844).

Theorem

Let β be an irrational complex number such that there exists a polynomial f of degree n over the integers such that $f(\beta) = 0$. There is a constant $M > 0$ such that

$$\left|\frac{b}{c} - \beta\right| \geq \frac{M}{|c|^n} \quad \textit{for all rational } b/c$$

Note that the constant M here is not the same as the one for Thue's theorem, so this does *not* imply the finiteness of solutions to Thue's equation.

Proof of Liouville's theorem

Since $f(\beta) = 0$, we may write

$$f(x) = (x - \beta)g(x) \tag{1}$$

for some polynomial g such that $g(\beta) \neq 0$ (note that after dividing through we may assume that $(x - \beta)$ only divides f once).

Proof of Liouville's theorem

Since $f(\beta) = 0$, we may write

$$f(x) = (x - \beta)g(x) \tag{1}$$

for some polynomial g such that $g(\beta) \neq 0$ (note that after dividing through we may assume that $(x - \beta)$ only divides f once). Then $|g|$ is bounded from above near β by some constant D, so

$$|g(b/c)| < D \tag{2}$$

Proof of Liouville's theorem

Since $f(\beta) = 0$, we may write

$$f(x) = (x - \beta)g(x) \tag{1}$$

for some polynomial g such that $g(\beta) \neq 0$ (note that after dividing through we may assume that $(x - \beta)$ only divides f once). Then $|g|$ is bounded from above near β by some constant D, so

$$|g(b/c)| < D \tag{2}$$

Now since f has integer coefficients, we have

$$|f(b/c)| = \left| a_n \frac{b^n}{c^n} + \cdots + a_0 \right| \geq \frac{1}{|c|^n}$$

Proof of Liouville's theorem

Since $f(\beta) = 0$, we may write

$$f(x) = (x - \beta)g(x) \tag{1}$$

for some polynomial g such that $g(\beta) \neq 0$ (note that after dividing through we may assume that $(x - \beta)$ only divides f once). Then $|g|$ is bounded from above near β by some constant D, so

$$|g(b/c)| < D \tag{2}$$

Now since f has integer coefficients, we have

$$|f(b/c)| = \left| a_n \frac{b^n}{c^n} + \cdots + a_0 \right| \geq \frac{1}{|c|^n}$$

Plugging b/c into (1), and letting $M = 1/D$ in (2) gives

$$\left| \beta - \frac{b}{c} \right| \geq \frac{M}{|c|^n}.$$

Conclusion

The proof of the Mordell conjecture by Faltings-Vojta is simply a much more complicated version of the proof of Liouville's theorem.