From Local to Global in Number Theory

Samit Dasgupta

Duke University

June 21, 2019

Local and Global

local: 1: characterized by or relating to position in space: having a definite spatial form or location

2(a): of, relating to, or characteristic of a particular place: not general or widespread

(b): of, relating to, or applicable to part of a whole

Local and Global

local: 1: characterized by or relating to position in space: having a definite spatial form or location

2(a): of, relating to, or characteristic of a particular place: not general or widespread

(b): of, relating to, or applicable to part of a whole

Local and Global

global: 1(a): of, relating to, or involving the entire world.

(b): of or relating to a spherical celestial body (such as the moon)

2: of, relating to, or applying to a whole (such as a mathematical function or a computer program)

Example: Ants on a circle

Click here for animation of zooming in on a circle

Ants on a circle

This is a **failure** of drawing *global* inferences from *local* data.

Every ant thinks the circle is “flat.” Even if you talk to all the ants at the same time, you can’t figure out the global information that the circle loops back to itself.

The ants can’t tell the difference between a straight line and a circle.

Ants on a circle

This is a **failure** of drawing *global* inferences from *local* data.

Every ant thinks the circle is “flat.” Even if you talk to all the ants at the same time, you can’t figure out the global information that the circle loops back to itself.

The ants can’t tell the difference between a straight line and a circle.

Ants on a circle

This is a **failure** of drawing *global* inferences from *local* data.

Every ant thinks the circle is “flat.” Even if you talk to all the ants at the same time, you can’t figure out the global information that the circle loops back to itself.

The ants can’t tell the difference between a straight line and a circle.

Number Theory

Broadly speaking, number theory is motivated by two types of questions:

1. What is the distribution of primes? (e.g. are there infinitely many? how many are there less than 1,000,000? Are there infinitely many twin primes?)

2. What are the integer solutions to polynomial equations? (e.g. $x^2 + y^2 = z^2$, $x^n + y^n = z^n$).

Number Theory

Broadly speaking, number theory is motivated by two types of questions:

1. What is the distribution of primes? (e.g. are there infinitely many? how many are there less than 1,000,000? Are there infinitely many twin primes?)

2. What are the integer solutions to polynomial equations? (e.g. $x^2 + y^2 = z^2$, $x^n + y^n = z^n$).

Number Theory

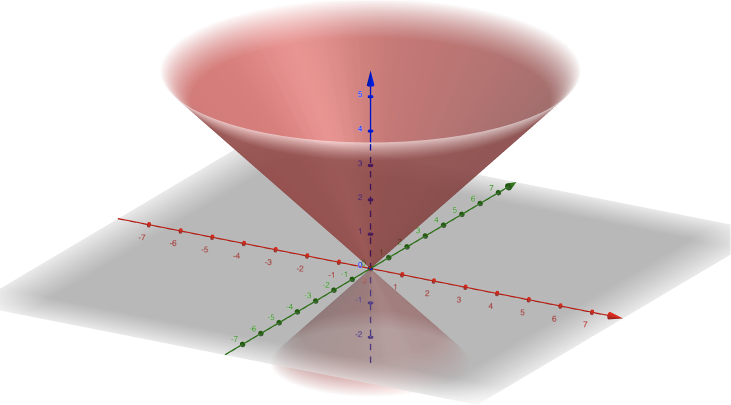
Broadly speaking, number theory is motivated by two types of questions:

1. What is the distribution of primes? (e.g. are there infinitely many? how many are there less than 1,000,000? Are there infinitely many twin primes?)

2. What are the integer solutions to polynomial equations? (e.g. $x^2 + y^2 = z^2$, $x^n + y^n = z^n$).

Real solutions

Real solutions are “easier.” Pythagorean eqn: $x^2 + y^2 = z^2$



Integer solutions

But number theorists are interested in the integer (or rational) solutions to equations.

Integers $= \mathbf{Z}$, Rationals $= \mathbf{Q}$

$3^2 + 4^2 = 5^2$

$5^2 + 12^2 = 13^2$

$9^2 + 40^2 = 41^2$

$\vdots$

First Question — Are there *any* integer solutions?

Consider the equation $x^2 + y^2 + 4 = 0$.

First Question — Are there *any* integer solutions?

Consider the equation $x^2 + y^2 + 4 = 0$.

There are no real solutions, since the left side is always positive, so there are no integer solutions.

First Question — Are there *any* integer solutions?

Consider the equation $x^2 + x = 2y + 1$.

First Question — Are there *any* integer solutions?

Consider the equation $x^2 + x = 2y + 1$.

There are no integer solutions since the left side is always even, and the right side is always odd.

Parity is x mod 2

Asking whether a number is odd or even is asking:
"When we divide the number by 2, is the remainder 0, or 1?"

More generally, given a positive integer n, we can define $x \pmod{n}$ to be the remainder when we divide x by n.

Parity is x mod 2

Asking whether a number is odd or even is asking:
"When we divide the number by 2, is the remainder 0, or 1?"

More generally, given a positive integer n, we can define $x \pmod{n}$ to be the remainder when we divide x by n.

Modular arithmetic

We define $\mathbf{Z}/n = \{0, 1, 2, \ldots, n-1\}$, the set of possible remainders when you divide by n.

We can consider solutions to equations in $\mathbf{Z}/n$.

The equation $y^2 = x^3 + 2$ has the solution $(x, y) = (3, 2)$ in $\mathbf{Z}/5$, since $2^2 \equiv 29 \equiv 4 \pmod{5}$.

Modular arithmetic

We define $\mathbf{Z}/n = \{0, 1, 2, \ldots, n-1\}$, the set of possible remainders when you divide by n.

We can consider solutions to equations in $\mathbf{Z}/n$.

The equation $y^2 = x^3 + 2$ has the solution $(x, y) = (3, 2)$ in $\mathbf{Z}/5$, since $2^2 \equiv 29 \equiv 4 \pmod 5$.

Modular arithmetic

We define $\mathbf{Z}/n = \{0, 1, 2, \ldots, n-1\}$, the set of possible remainders when you divide by n.

We can consider solutions to equations in $\mathbf{Z}/n$.

The equation $y^2 = x^3 + 2$ has the solution $(x, y) = (3, 2)$ in $\mathbf{Z}/5$, since $2^2 \equiv 29 \equiv 4 \pmod{5}$.

Another example

$x^3 - x = y^2 + 1$

The left side is always 0 mod 3.

The right side is always 1 or 2 mod 3.

Since there are no solutions in $\mathbf{Z}/3$, there are no solutions in $\mathbf{Z}$.

Another example

$z^4 - z^2 - 1 = x^2 + y^2$

Left side is always 3 mod 4.

Right side is always $0, 1$, or 2 mod 4.

Since there are no solutions in $\mathbf{Z}/4$, there are no solutions in $\mathbf{Z}$.

Local and Global in Number theory

Global means looking for solutions to an equation in $\mathbf{Z}$ or $\mathbf{Q}$.

Local means looking for solutions in $\mathbf{R}$ or mod p^m for every prime p and integer $m \geq 1$.

Local to Global principle: If a polynomial equation has solutions in $\mathbf{R}$ and mod p^m for all primes p and $m \geq 1$, does it necessarily have solutions in $\mathbf{Z}$?

Hasse's principle

A **quadratic** polynomial has solutions in $\mathbf{Z}$ if and only if it has solutions in $\mathbf{R}$ and mod p^m for every prime p and $m \geq 1$.

Selmer's famous example

However, Hasse's principle does not hold once we pass the realm of quadratic polynomials.

The equation $3x^3 + 4y^3 + 5z^3 = 0$ has nontrivial solutions in $\mathbf{R}$ and mod p^m for all primes p, $m \geq 1$, but no nontrivial solutions in $\mathbf{Z}$.

Selmer's famous example

However, Hasse's principle does not hold once we pass the realm of quadratic polynomials.

The equation $3x^3 + 4y^3 + 5z^3 = 0$ has nontrivial solutions in $\mathbf{R}$ and mod p^m for all primes p, $m \geq 1$, but no nontrivial solutions in $\mathbf{Z}$.

When does a cubic equation have a rational solution?

There is an algorithm, called *descent*, which can determine if a given cubic equation has a solution.

It is an open conjecture as to whether this algorithm always terminates!

Proving that this algorithm terminates is a huge open problem in number theory.

When does a cubic equation have a rational solution?

There is an algorithm, called *descent*, which can determine if a given cubic equation has a solution.

It is an open conjecture as to whether this algorithm always terminates!

Proving that this algorithm terminates is a huge open problem in number theory.

When does a cubic equation have a rational solution?

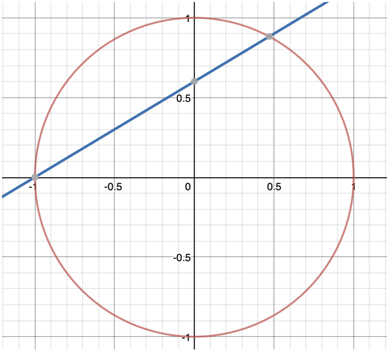
There is an algorithm, called *descent*, which can determine if a given cubic equation has a solution.

It is an open conjecture as to whether this algorithm always terminates!

Proving that this algorithm terminates is a huge open problem in number theory.

Finding all solutions, if we know they exist

Quadratics: Pythagorean example, $x^2 + y^2 = 1$.



Start with the point $(-1, 0)$.

Line with rational slope t through this point: $y = t(x + 1)$.

It must intersect circle at another rational point. $(x, y) = (\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2})$.

Integer solutions

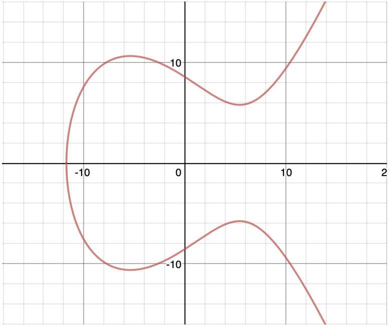
If we write $t = m/n$, and scale through the denominator, we get a paramaterization of all primitive integer solutions to $x^2 + y^2 = z^2$:

$$(x, y, z) = (n^2 - m^2, 2mn, n^2 + m^2).$$

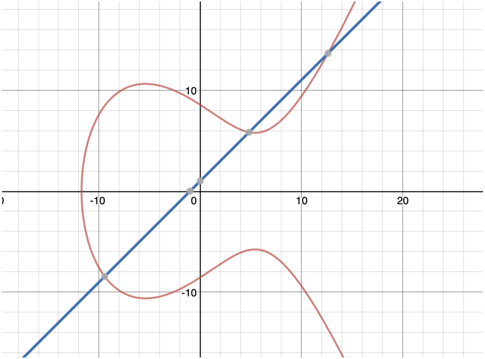
Elliptic Curves

A (nonsingular) cubic equation in two variables with at least one rational solution is called an *elliptic curve*.

After a change of variables, these can always be written $y^2 = x^3 + bx + c$.

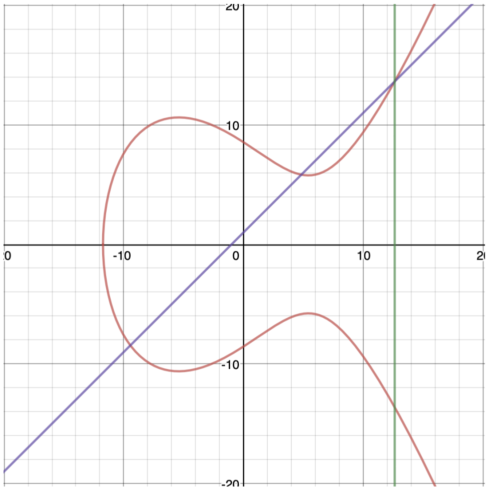


Composition Law



If we start from a rational point, and draw a line with rational slope, the other two points of intersection need not be rational.

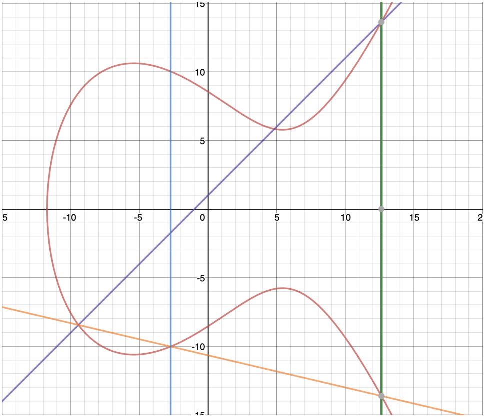
But if we start with *two* rational points, then the third point has to be rational.



A simpler way to get a new rational point is to flip across the x-axis.

We can keep doing this procedure repeatedly—drawing lines between two points we have, taking the third point of intersection, and flipping.

Mordell's Theorem



All the rational points on the curve can be obtain from this process starting with only finitely many.

The minimum number of points you need, excluding the "torsion points", is called the rank r.

Studying the rank

Intuitively, the bigger r is, the more rational points there are on the curve.

For a given curve, can we figure out r?

In the 1960s, Birch and Swinnerton-Dyer explored whether there is a local-to-global principle at work here.

Studying the rank

Intuitively, the bigger r is, the more rational points there are on the curve.

For a given curve, can we figure out r?

In the 1960s, Birch and Swinnerton-Dyer explored whether there is a local-to-global principle at work here.

Studying the rank

Intuitively, the bigger r is, the more rational points there are on the curve.

For a given curve, can we figure out r?

In the 1960s, Birch and Swinnerton-Dyer explored whether there is a local-to-global principle at work here.

Birch–Swinnerton-Dyer conjecture

For each prime p, let N_p be the number of solutions to the equation of the curve mod p.

For example, for $y^2 = x^3 + 1$ and $p = 5$, we have the points $(0, 1), (0, 4), (2, 2), (2, 3), (4, 0), \infty$, so $N_p = 6$.

Birch and Swinnerton–Dyer found that

$$\prod_{p \leq x} \frac{N_p}{p}$$

grew faster as a function of x, the larger r was.

Birch–Swinnerton-Dyer conjecture

For each prime p, let N_p be the number of solutions to the equation of the curve mod p.

For example, for $y^2 = x^3 + 1$ and $p = 5$, we have the points $(0,1), (0,4), (2,2), (2,3), (4,0), \infty$, so $N_p = 6$.

Birch and Swinnerton–Dyer found that

$$\prod_{p \leq x} \frac{N_p}{p}$$

grew faster as a function of x, the larger r was.

Birch–Swinnerton-Dyer conjecture

For each prime p, let N_p be the number of solutions to the equation of the curve mod p.

For example, for $y^2 = x^3 + 1$ and $p = 5$, we have the points $(0,1), (0,4), (2,2), (2,3), (4,0), \infty$, so $N_p = 6$.

Birch and Swinnerton–Dyer found that

$$\prod_{p \leq x} \frac{N_p}{p}$$

grew faster as a function of x, the larger r was.

Birch–Swinnerton-Dyer conjecture

More precisely, they conjectured

$$\prod_{p \leq x} \frac{N_p}{p} \sim C(\log x)^r$$

for some non-zero constant C, where r is the rank of the curve.

This is one of the most important unsolved problems in all of mathematics.

Birch–Swinnerton-Dyer conjecture

More precisely, they conjectured

$$\prod_{p \leq x} \frac{N_p}{p} \sim C(\log x)^r$$

for some non-zero constant C, where r is the rank of the curve.

This is one of the most important unsolved problems in all of mathematics.

The Unit equation

Consider the equation:

$$xy - 1 = 0.$$

Then $N_p =$ number of solutions mod p is equal to $p - 1$.

$$\prod_{p \leq x} \frac{N_p}{p} = \prod_{p \leq x} \frac{p-1}{p} = \prod_{p \leq x} \left(1 - \frac{1}{p}\right).$$

The Unit equation

Consider the equation:

$$xy - 1 = 0.$$

Then $N_p =$ number of solutions mod p is equal to $p-1$.

$$\prod_{p \leq x} \frac{N_p}{p} = \prod_{p \leq x} \frac{p-1}{p} = \prod_{p \leq x} \left(1 - \frac{1}{p}\right).$$

Geometric Series

Let's consider the inverse of this:

$$\prod_{p \le x} \frac{1}{1 - 1/p}.$$

Using

$$\frac{1}{1-r} = 1 + r + r^2 + r^3 + \cdots ,$$

we get

$$\prod_{p \le x} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \cdots \right).$$

Geometric Series

Let's consider the inverse of this:

$$\prod_{p \le x} \frac{1}{1 - 1/p}.$$

Using

$$\frac{1}{1-r} = 1 + r + r^2 + r^3 + \cdots ,$$

we get

$$\prod_{p \le x} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \cdots \right).$$

Geometric Series

Let's consider the inverse of this:

$$\prod_{p \leq x} \frac{1}{1 - 1/p}.$$

Using

$$\frac{1}{1-r} = 1 + r + r^2 + r^3 + \cdots ,$$

we get

$$\prod_{p \leq x} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \cdots \right).$$

Unique Factorization

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

$$1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\frac{1}{6}+\frac{1}{8}+\frac{1}{9}+\cdots=$$

the sum of $1/n$ for all n whose prime factors are $2, 3, 5$.

In the limit

If we send $x \to \infty$, then we get

$$\prod_{p \text{ prime}} \frac{1}{1 - 1/p} = \sum_{n=1}^{\infty} \frac{1}{n} = \infty.$$

From this it follows there are infinitely many primes.

(This was Euler's proof.)

In the limit

If we send $x \to \infty$, then we get

$$\prod_{p \text{ prime}} \frac{1}{1 - 1/p} = \sum_{n=1}^{\infty} \frac{1}{n} = \infty.$$

From this it follows there are infinitely many primes.

(This was Euler's proof.)

Riemann Zeta Function

Riemann realized that you should study, more generally,

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

where s is a complex number.

That sum only converges for s with real part > 1, but Riemann showed how to define it for all s.

Riemann Zeta Function

Riemann realized that you should study, more generally,

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

where s is a complex number.

That sum only converges for s with real part > 1, but Riemann showed how to define it for all s.

Some special values

$$\zeta(2) = 1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \cdots = \frac{\pi^2}{6}.$$

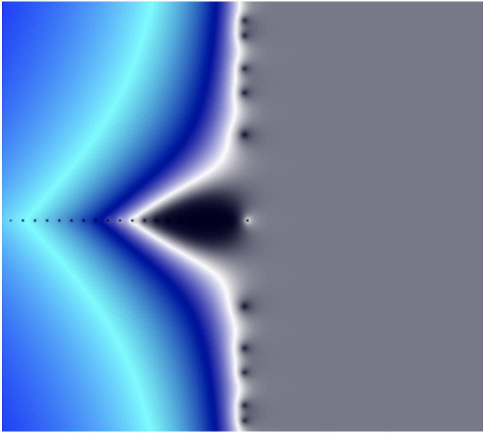
$$\zeta(4) = 1 + \frac{1}{2^4} + \frac{1}{3^4} + \frac{1}{4^4} + \cdots = \frac{\pi^4}{90}.$$

$$\zeta(2k) = 1 + \frac{1}{2^{2k}} + \frac{1}{3^{2k}} + \frac{1}{4^{2k}} + \cdots = C_k \cdot \pi^{2k},$$

where C_k is a rational number related to Bernoulli Numbers.

The Riemann Hypothesis

Conjecture. Other than $\zeta(-2k) = 0$ for $k > 0$ an integer, we can only have $\zeta(s) = 0$ if the real part of s is $1/2$.



The Birch–Swinnerton-Dyer conjecture, revisited

Theorem (Hasse)

For any elliptic curve E and any prime p, the integer $a_p = p + 1 - N_p$ satisfies $|a_p| < 2\sqrt{p}$.

B-SD product

$$\prod_p \frac{N_p}{p} = \prod_p \frac{1 - a_p + p}{p}.$$

Introduce s variable:

$$L(E, s) = \prod_p \frac{1}{1 - a_p p^{-s} + p^{1-2s}}.$$

Intuitively,

$$L(E, 1) = \left(\prod_p \frac{N_p}{p} \right)^{-1}.$$

The Birch–Swinnerton-Dyer conjecture, revisited

Theorem (Hasse)

For any elliptic curve E and any prime p, the integer $a_p = p + 1 - N_p$ satisfies $|a_p| < 2\sqrt{p}$.

B-SD product

$$\prod_p \frac{N_p}{p} = \prod_p \frac{1 - a_p + p}{p}.$$

Introduce s variable:

$$L(E, s) = \prod_p \frac{1}{1 - a_p p^{-s} + p^{1-2s}}.$$

Intuitively,

$$L(E, 1) = \left(\prod_p \frac{N_p}{p} \right)^{-1}.$$

The Birch–Swinnerton-Dyer conjecture, revisited

Theorem (Hasse)

For any elliptic curve E and any prime p, the integer $a_p = p + 1 - N_p$ satisfies $|a_p| < 2\sqrt{p}$.

B-SD product

$$\prod_p \frac{N_p}{p} = \prod_p \frac{1 - a_p + p}{p}.$$

Introduce s variable:

$$L(E,s) = \prod_p \frac{1}{1 - a_p p^{-s} + p^{1-2s}}.$$

Intuitively,

$$L(E,1) = \left(\prod_p \frac{N_p}{p}\right)^{-1}.$$

The Birch–Swinnerton-Dyer conjecture, revisited

Theorem (Hasse)

For any elliptic curve E and any prime p, the integer $a_p = p + 1 - N_p$ satisfies $|a_p| < 2\sqrt{p}$.

B-SD product

$$\prod_p \frac{N_p}{p} = \prod_p \frac{1 - a_p + p}{p}.$$

Introduce s variable:

$$L(E, s) = \prod_p \frac{1}{1 - a_p p^{-s} + p^{1-2s}}.$$

Intuitively,

$$L(E, 1) = \left(\prod_p \frac{N_p}{p} \right)^{-1}.$$

The Birch–Swinnerton-Dyer conjecture, revisited

Conjecture

E has infinitely many rational solutions (i.e. $r > 1$) if and only if $L(E, 1) = 0$.

More generally,

$$ord_{s=1} L(E, s) = r.$$