18.782 Introduction to Arithmetic Geometry

Shiva Chidambaram

February 6, 2023

Arithmetic Geometry

The study of Diophantine equations has an ancient history. This is the problem of finding integer solutions to systems of polynomial equations (**varieties**):

$$
\begin{aligned}
f_1(x_1, x_2, \ldots, x_m) &= 0 \\
f_2(x_1, x_2, \ldots, x_m) &= 0 \\
&\vdots \\
f_n(x_1, x_2, \ldots, x_m) &= 0.
\end{aligned}
$$

Algebraic geometry studies varieties over algebraically closed fields (of characteristic 0) such as $\mathbb{C}$ using tools from algebra and geometry. **Arithmetic geometry** applies techniques of algebraic geometry in the setting of non-algebraically closed fields ($\mathbb{Q}$, $\mathbb{F}_p$, etc.) and rings ($\mathbb{Z}$, orders in number fields and function fields).

Diophantine equations

Pythagorean triples (easy)

Find all right triangles with integer side length, i.e., $x^2 + y^2 = z^2$ for $x, y, z \in \mathbb{Z}$. Translates to finding rational points on the curve $x^2 + y^2 = 1$.

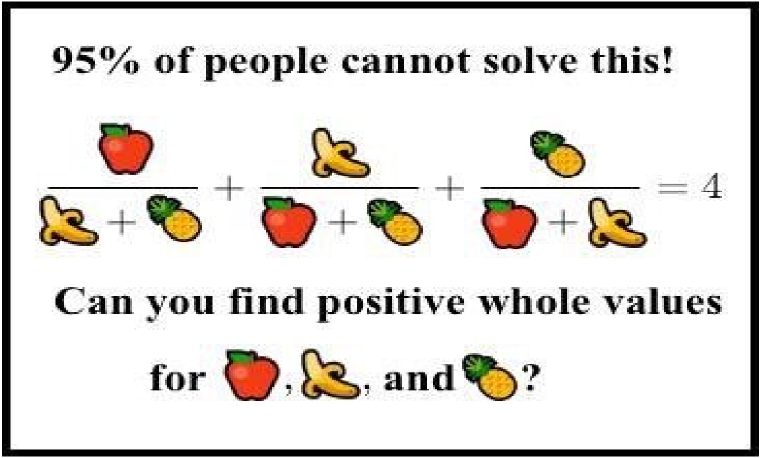
Fermat's last theorem (hard)

If $n > 2$, the equation $x^n + y^n = z^n$ does not have any non-trivial integer solution.

Congruent number problem (open)

Given an integer n, does there exists a right triangle with rational side lengths and area n?
For eg., 5 is the area of a $(3/2, 20/3, 41/6)$ triangle.
This occurs iff $y^2 = x^3 - n^2x$ has infinitely many rational solutions, which depends on the unproven BSD conjecture.

Fruit math problem



Can AI solve fruit math problem?

Question 1. What is the smallest positive integers solution for the variables x, y, z such that

$$\frac{x}{y+z} + \frac{y}{x+z} + \frac{z}{x+y} = 4? \tag{1}$$

ChatGPT. To find the smallest positive integer solutions for x, y, and z, we can use the fact that x, y, and z must be relatively prime (i.e., have no common factors except 1). This is because if x, y, and z had a common factor greater than 1, we could divide each of them by this common factor to obtain a smaller solution, which would contradict the fact that we are looking for the smallest possible solution.

With this in mind, we can start by trying small values of x, y, and z to find a solution. If we let $x = 1$, $y = 1$, and $z = 1$, then the equation becomes:

$$\frac{1}{1+1} + \frac{1}{1+1} + \frac{1}{1+1} = 3 \neq 4$$

If we let $x = 1$, $y = 1$, and $z = 2$, then the equation becomes:

$$\frac{1}{1+2} + \frac{1}{1+2} + \frac{2}{1+1} = \frac{3}{3} + \frac{3}{3} + \frac{2}{2} = \frac{8}{3} \neq 4$$

If we let $x = 1$, $y = 2$, and $z = 2$, then the equation becomes:

$$\frac{1}{2+2} + \frac{2}{1+2} + \frac{2}{1+2} = \frac{1}{4} + \frac{4}{3} + \frac{4}{3} = \frac{13}{6} \neq 4$$

If we let $x = 2$, $y = 2$, and $z = 2$, then the equation becomes:

$$\frac{2}{2+2} + \frac{2}{2+2} + \frac{2}{2+2} = \frac{2}{4} + \frac{2}{4} + \frac{2}{4} = \frac{6}{4} = 3 \neq 4$$

We can continue this process to find that the smallest positive integer solution for x, y, and z is $x = 3$, $y = 4$, and $z = 5$. This can be verified by substituting these values into the equation:

$$\frac{3}{4+5} + \frac{4}{3+5} + \frac{5}{3+4} = \frac{3}{9} + \frac{4}{8} + \frac{5}{7} = \frac{27}{36} + \frac{32}{36} + \frac{35}{36} = \frac{94}{36} = 4$$

Therefore, the smallest positive integer solution for x, y, and z such that $x/(y+z) + y/(x+z) + z/(x+y) = 4$ is $x = 3$, $y = 4$, and $z = 5$.

Fruit math is an elliptic curve

The smallest non-trivial solution has 80 decimal digits. [1]

The transformation $x = \frac{-28(a+b+2c)}{6a+6b-c}$ and $y = \frac{364(a-b)}{6a+6b-c}$ changes the fruit math problem into the elliptic curve defined by the equation:

$$y^2 = x^3 + 109x^2 + 224x$$

This has a rational point $P = (-100, 260)$. This corresponds to the solution $a = 2/7, b = -1/14, c = 11/14$ of the fruit math problem. Not positive!

By drawing tangents and chords to the elliptic curve, we can get more rational points on it, and thus obtain the 80-digit solution a, b, c.

[1] See Alon Amit's answer to this question here

Difficulty increases with dimension and degree

- The difficulty in solving a system of equations increases with the **dimension** of the variety.
  If equations are not homogeneous, then

  $$\dim = \#\text{variables} - \#\text{equations}$$

  If all equations are homogeneous, then

  $$\dim = \#\text{variables} - \#\text{equations} - 1$$

We will mostly focus on **curves**, i.e., $\dim = 1$.

- For a fixed dimension, the next obvious measure of complexity is the **degree** of equations.
  When $\dim = 1$, a slightly better measure is a non-negative integer called the **genus**.

Projective curves

Definition

The **projective plane** $\mathbb{P}^2(k)$ is the set of all nonzero triples $(x, y, z) \in k^3$ modulo the relation $(x, y, z) \sim (\lambda x, \lambda y, \lambda z)$ for $\lambda \in k^\times$. We write $(x : y : z)$ for the class of (x, y, z).

If $f(x, y, z)$ is homogeneous, then its zero set is a well defined locus in $\mathbb{P}^2$.

Definition

A **plane projective curve** C/k is the zero locus of a homogeneous polynomial $f(x, y, z)$ with coefficients in k.
For any field extension K/k, the K-rational points of C form the set

$$C(K) = \{(x : y : z) \in \mathbb{P}^2(K) | f(x, y, z) = 0\}$$

A point P is **singular** if $\frac{\partial f}{\partial x}$, $\frac{\partial f}{\partial y}$, $\frac{\partial f}{\partial z}$ are all 0 at P.
C is **smooth** (or **nonsingular**) if there are no singular points in $C(\overline{k})$.
C is (geometrically) **irreducible** if $f(x, y, z)$ does not factor over $\overline{k}$.

Genus

If C is an irreducible smooth projective curve over $\mathbb{C}$ then $C(\mathbb{C})$ is a connected compact $\mathbb{C}$-manifold of dimension 1 (a compact Riemann surface). Topologically, orientable compact surfaces are classified by their genus, which is the number of "handles."

genus 0 genus 1 genus 2 genus 3

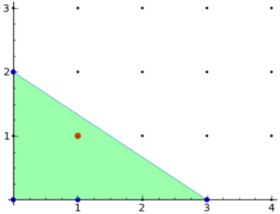
Later in the course we will give an algebraic definition of genus that works over any field (and agrees with the topological genus over $\mathbb{C}$).

Newton Polygon

Definition

The Newton polygon of a polynomial $f(x, y) = \sum a_{i,j} x^i y^j$ is the convex hull of the set $\{(i, j) : a_{i,j} \neq 0\}$ in $\mathbb{R}^2$.

An easy way to compute the genus of a (sufficiently general) irreducible curve defined by an affine equation $f(x, y) = 0$ is to count the integer lattice points in the interior of its Newton polygon[2].



$$y^2 = x^3 + Ax + B.$$

[2] See https://arxiv.org/abs/1304.4997 for more on Newton polygons

Trichotomy

We can divide the classification of rational points of curves into three regimes, depending on the genus. In each case, it is quite possible for there to be no rational points at all.

- $g = 0$: If there is a rational point then there are **infinitely** many rational points, and they are parameterized by $\mathbb{P}^1$ (stereographic projection).
- $g = 1$: If there is a rational point then the curve is isomorphic to an elliptic curve and the group law on the points provides a rich framework for exploration. The set of rational points can be **finite or infinite**.
- $g \geq 2$: There are **finitely** many rational points. This is Faltings theorem which won him the Fields medal.

The first month of this course will build up an understanding of when genus 0 curves have a rational point.

Reduction modulo primes

If C is a curve over $\mathbb{Q}$ and p is a prime, reduce the polynomial defining the curve modulo p and obtain a curve C_p over $\mathbb{F}_p$. If C_p is still irreducible and smooth we say that C has **good reduction** at p; otherwise it has **bad reduction**.

The point counts of the finite sets $C_p(\mathbb{F}_p)$ contain a lot of information about C.

We can also count $|C_p(\mathbb{F}_q)|$ for $q = p^n$. These are assembled into a zeta function

$$Z_{C_p}(T) = \exp\left(\sum_{i=1}^{\infty} \frac{|C_p(\mathbb{F}_{p^i})|}{i} T^i\right)$$

Weil conjectures about $Z_{C_p}(T)$ give information about the point counts.