

Introduction to Arithmetic Geometry

18.782

David Roe

September 2, 2020

Arithmetic geometry

Algebraic geometry studies systems of polynomial equations (**varieties**):

$$f_1(x_1, \dots, x_n) = 0$$

$$\vdots$$

$$f_m(x_1, \dots, x_n) = 0$$

using a mixture of tools from algebra (ideals, discriminants, field extensions) and geometry (intersections, connectedness, tangent spaces and singularities). Classically, it focuses on algebraically closed fields of characteristic 0, such as \mathbb{C} .

Seeking solutions with all $x_i \in \mathbb{Z}$ originated in the ancient world; such **Diophantine equations** range from easy to literally impossible (Hilbert's 10th problem).

Arithmetic geometry applies the techniques of algebraic geometry in the setting of non-algebraically closed fields (\mathbb{Q} , \mathbb{F}_p , number fields) and rings (\mathbb{Z} , orders in number fields and function fields). Diophantine equations still form a core of the subject, but spinoffs hold great interest of their own (crypto, coding theory).

Diophantine examples

Pythagorean triples (easy)

Find all right triangles with integer side lengths. Translates to finding rational points on $x^2 + y^2 = 1$.

Fermat's last theorem (very hard)

No nontrivial rational points on $x^n + y^n = 1$ for $n > 2$. Solved in 1995 after 350 years of attempts.

Congruent numbers (unsolved)

Find all right triangles with rational side lengths and integral area. Translates to determining whether $y^2 = x^3 - n^2x$ has infinitely solution, which depends on the unproven BSD conjecture.

Fruit math

The following wonderful meme circulated a few years ago:

95% of people cannot solve this!

$$\frac{\text{🍎}}{\text{🍌} + \text{🍌}} + \frac{\text{🍌}}{\text{🍌} + \text{🍌}} + \frac{\text{🍌}}{\text{🍌} + \text{🍌}} = 4$$

Can you find positive whole values
for 🍌, 🍌, and 🍌?

This translates to finding rational solutions on the elliptic curve

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

Positivity occurs when x lies in one of two intervals. There are infinitely many solutions; in the smallest the three fruit each have 80 decimal digits. [1]

Changing the 4 to other integers can yield far larger solutions (trillions of digits for 896). The fact that such enormous solutions result from such a simple equation is connected to **Hilbert's 10th problem**: there is no algorithm that takes as input a Diophantine equation and outputs whether or not it has a solution.

Difficulty

The most important factor controlling the difficulty in solving a Diophantine equation is its **dimension**, which is roughly the difference between the number of variables and the number of equations (minus 1 if all equations are homogeneous, as we'll see when we discuss **projective space**). We will mostly focus on **curves**, which is the case of dimension 1.

For a fixed dimension, the next obvious measure of complexity is the **degree**. It turns out that a slightly better measure is the **genus**, a non-negative integer.

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

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

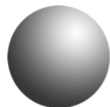
A point $P \in C(K)$ is **singular** if $\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}, \frac{\partial f}{\partial z}$ all vanish at P .

C is **smooth** (or **nonsingular**) if there are no singular points in $C(\bar{k})$.

C is (geometrically) **irreducible** if $f(x, y, z)$ does not factor over \bar{k} .

Genus

If C is an irreducible smooth projective curve over \mathbb{C} then $C(\mathbb{C})$ is a connective 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



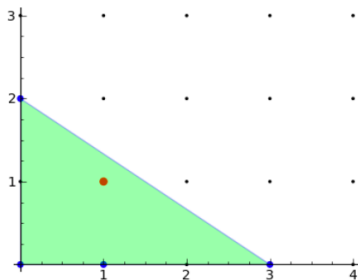
genus 3

We will see how to define this invariant algebraically later in the course, but for a sufficiently general plane curve it can be computed using the Newton polygon.

Newton polygon

Newton polygons will arise in two different contexts this term. For a plane curve defined by $f(x, y) = \sum a_{ij}x^i y^j$, the **Newton polygon** is the convex hull of $\{(i, j) : a_{ij} \neq 0\}$ in \mathbb{R}^2 .

The genus of a sufficiently general irreducible smooth plane curve can be computed as the number of interior integer lattice points in its Newton polygon:



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

Behavior by genus

We can divide the classification of the 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.

- In genus 0, if there is a rational point then the set of rational points is parameterized by \mathbb{P}^1 (stereographic projection). The first month of this course will build up an understanding of when genus 0 curves have a rational point.
- In genus 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.
- In larger genus, there are finitely many rational points (this theorem of Faltings won him the Fields medal). Again, there are often no points at all [2].

Reduction modulo primes



If C is a curve over \mathbb{Q} and p is a prime, you can reduce the polynomial defining C modulo p and obtain a curve C_p over \mathbb{Q} . If C_p is still irreducible and smooth we say that C has **good reduction** at p ; otherwise it has **bad reduction**. You can learn a lot about C by counting $C_p(\mathbb{F}_p)$, which is a finite set.

You can also count $|C_p(\mathbb{F}_q)|$ for q a power of p . These are assembled into a zeta function

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

The Weil conjectures give us information about the point counts via this function.

References

-  Alon Amit. *How do you find positive integer solutions to $\frac{x}{y+z} + \frac{y}{z+x} + \frac{z}{z+y} = 4$.*
<https://www.quora.com/How-do-you-find-the-positive-integer-solutions-to-frac-z-+-frac-y-z+x-+-frac-z-x+y-4>, March 2020.
-  Manjul Bargava. *Most hyperelliptic curves over \mathbb{Q} have no rational points.*
arXiv:1308.0395.