Fabien Mehdi Pazuki

My Research

Diophantine problems

Diophantine problems are at the crossroads of two deep and ancient fields in mathematics: number theory and geometry. A Diophantine problem is by definition given by the following classical setting: take a polynomial $P \in \mathbb{Z}[X_1, \dots, X_n]$ in several variables (one could even consider a system given by several polynomials). Is there any n-tuple $(a_1, \dots, a_n) \in \mathbb{Z}^n$ such that $P(a_1, \dots, a_n) = 0$? If yes, are there finitely many or infinitely many? Can one count these solutions? Is there a way to list all the solutions? So the goal is to find *integral* solutions to polynomial equations, that's a question from *number theory*, and often the proof involves a lot of *geometry* coming from the nature of the *complex* solutions $(z_1, \dots, z_n)$.

One often generalizes the setting: the coefficients of the polynomials are taken in a number field K (a number field is a finite extension of $\mathbb{Q}$, think of $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{2})$ for instance, which are both number fields of degree 2), and we search for solutions in the same number field.

Elliptic curves

My first direction of research concerns a particular class of Diophantine problems. Let K be a number field. Choose an equation of the following form, where X, Y, Z are variables and A, B are numbers in K.

$$Y^2Z = X^3 + AXZ^2 + BZ^3.$$

Whenever this equation is smooth (no common solutions with all the partial derivatives), it defines what is called an *elliptic curve*, which turns out to be a projective variety of dimension 1 equipped with an algebraic group structure. An important theorem concerning these equations is the Mordell-Weil Theorem. Let E be an elliptic curve defined over K, consider the set $E(K)$ of points on the curve E with coordinates in K. Then the Mordell-Weil Theorem tells us that the set $E(K)$ is a commutative group which is finitely generated. Hence it can be written

$$E(K) \simeq \mathbb{Z}^{r_K} \times E(K)_{torsion},$$

where $r_K \geq 0$ is an integer called the rank of the elliptic curve over K and $E(K)_{torsion}$ is a finite subgroup consisting of all torsion elements, *i.e.* all elements of finite order for the group law. The questions that naturally arise now are the following: how can we compute the rank exactly? Is it possible to compute the torsion subgroup? Is it possible to find explicit generators, hence describe all the points on the curves?

Height theory

To prove powerful statements about Diophantine equations, one of the key tools is called *height functions.* The use of height functions is already important to obtain the Mordell-Weil Theorem. The height of a point with coordinates in a number field measures its *arithmetic complexity.* Let us take an easy example, pick an elliptic curve given by the equation $Y^2Z = X^3 + Z^3$, then let $P = [X : Y : Z]$ be a point on E with coordinates in $\mathbb{Z}$, one can even choose the coordinates to be coprime integers, by homogeneity. With this normalization, one defines the function $h([X : Y : Z]) = \log \max\{|X|, |Y|, |Z|\}$. Fix a real number M. It is easy to understand that there are only finitely many triples $(X, Y, Z) \in \mathbb{Z}^3$ lying on the curve and such that $h([X : Y : Z]) \leq M$. This finiteness property (in the more general setting) is called the Northcott property and is crucial in many proofs of Diophantine geometry. A

height function always verifies the Northcott property, by definition: a set of points with coordinates in a fixed number field and with bounded height is a finite set.

Height functions have thus played a major role in proving finiteness statements. Another very famous consequence are the proofs of the Mordell Conjecture, asserting that any algebraic curve of genus $g \geq 2$ (defined over a number field) has only finitely many rational points over any fixed number field. The first proof was given by Faltings, who obtained the Fields medal for this result. Let us remark here that an elliptic curve is of genus $g = 1$.

A more general setting

A often in mathematics, one way to study a problem is to first generalize it. Another topic in my research interests is the theory of abelian varieties. What is an abelian variety? A natural generalization of elliptic curves, but in higher dimensions. It is an object given by a system of polynomial equations in several variables, which is projective and equipped with a group structure. Elliptic curves are abelian varieties of dimension 1. As in this case, one can prove the Mordell-Weil Theorem in higher dimension and study the same questions: what is the rank, what are the torsion points, what are the generators. As in the case of elliptic curves, there is a nice height theory over abelian varieties, but slightly more intricate.

How about... changing the base field?

The arithmetic of curves and more general varieties depends a lot on the base field, *i.e.* the field over which the variety is defined. Another setting where height theory works well is the case of *global function fields*. Let $\mathcal{C}$ be an algebraic curve defined over a finite field $\mathbb{F}_q$, where q is a prime power. Let $K = \mathbb{F}_q(\mathcal{C})$ be the field of rational functions defined on the curve with coefficients in $\mathbb{F}_q$. Let X be another curve, projective and defined over K. Is it possible to find points on X with coordinates in the field K? If yes, are there only finitely many? Can one list them? Take the following example: the curve $\mathcal{C} = \mathbb{P}^1$ and $q = 4$. Then $K = \mathbb{F}_4(t)$, where t is just representing the function $t \to t$. Let X be a hyperelliptic curve (of genus 2) given by

$$Y^2Z^3 = X^5 + (t^2 - t^5)Z^5.$$

Then the point $P = [t : t : 1]$ is a rational point on the curve. A general theorem shows that the number of points on a curve of genus bigger than 2 with coordinates in such a function field is finite as long as the curve is not *isotrivial* (which essentially amounts to say that it is not isomorphic to a constant curve).

How about... iterating a morphism on a projective variety?

Take a projective variety V defined over a number field K. Let $\phi : V \to V$ be a morphism. Suppose there is a point P on V with coordinates in K, and define the forward orbit

$$\mathcal{O}_\phi(P) = \{P, \phi(P), \phi(\phi(P)), \ldots\}.$$

A classical question is then: how many integral points can be found on such forward orbits? It turns out that whenever the morphism ϕ is *polarized* (there exist an integer $d \geq 2$ and a line bundle $\mathcal{L}$ on V such that $\phi^*\mathcal{L} = \mathcal{L}^{\otimes d}$), such questions are in fact also linked with height theory!