SOME PROBLEMS IN DIOPHANTINE GEOMETRY
MINGLE TALK - 7TH OCTOBER

DANIEL LOUGHRAN

1. Introduction

A diophantine equation is a polynomial equation with integer coefficients where we wish to find solutions in the integers, or rational numbers. Some very simply examples are

(1) $x = y$,

(2) $2x + 2y = 1$.

Note that (1) has infinitely many solutions in the integers, but (2) has no solutions in the integers, since the left hand side is even but the right hand side is odd.

In my talk today, I hope to give you an idea of some problems in *diophantine geometry*. This way of thinking arose in the past hundred or so years (although some ideas can be traced back to the ancient Greeks), and it tries to solve Diophantine problems using methods and ideas from geometry. If I have enough time, I will also briefly highlight some aspects of my own research.

We shall see some examples of diophantine equations given by curves, and then show how these relate to the general theory. To highlight the geometric aspects we use the term *rational point* to refer to a solution in the rational numbers, and similarly with regard to integral solutions.

2. Examples

Consider the equation of the circle

$$C : x^2 + y^2 = 1,$$

which has only four integer solutions, but infinitely many rational solutions. To see this, note that $P = (1, 0)$ is one solution. If we choose a line through P with a rational gradient, this will interest the circle at one unique point, which is a point with rational coordinates. Thus we have found infinitely many solutions! And in fact, we have shown that the set of solutions is somehow naturally identified with $\mathbb{Q} \cup \{P\}$.

Now we shall look at equations of higher degree, consider the following curve

$$E : y^2 = x^3 - x + 1.$$

This is an example of an *elliptic curve*, which are well-known for their beauty. There are a few obvious rational points on this curve, for example $P_1 = (1, 1)$. However, if we try to do the previous trick of drawing a line through

this point, we get stuck, since in general it will intersect the curve in two more points not one, and there is no guarantee these will be rational solutions.

But there is hope yet! Taking a tangent to the point P_1, this intersects the curve at another point $P_2 = (-1, -1)$. Then we can reflect this in the $x-$axis to get the point $P_3 = (-1, 1)$. Now, drawing a line through P_1 and P_3 gives us another point $P_4 = (0, 1)$, and reflecting in the $x-$axis gives $P_5 = (0, -1)$. Now drawing a line through P_1 and P_5 gives $P_6 = (3, 5)$, etc... You can see that we can carry on this process to generate more points, however it is not clear whether or not this will eventually give us every solution, or even infinitely many solutions.

More generally, given any cubic curve, and two rational points P and Q on it, we can draw a line through them to get a third rational point $P * Q$. This is some kind of binary operation, and it would be nice if it had cool properties (such as giving a group law). Unfortunately it doesn't, however as a minor technical point if we reflect $P * Q$ in the $x-$axis, we get a new point $P + Q$. And it is this operation which gives us an abelian group law. Returning to the previous example, one can check in fact the point $P_1 = (1, 1)$ does in fact generate every solution to the equation, and so as abstract groups we have

$$E(\mathbb{Q}) \cong \mathbb{Z}.$$

3. General Theory

We have seen a few examples now of different kinds of diophantine equations, however, is there any method to this madness? It turns out, yes!

We shall consider diophantine equations of the form

$$f(x, y) = 0$$

where f is a polynomial with integer coefficients and degree d, which is non-singular over $\mathbb{C}$, that is - the solutions over $\mathbb{C}$ don't do anything silly like intersect them-self (this is to simplify our presentation, singularities are not that bad really).

Naively, for large degree, you would not expect not many solutions, since the $d-$th root of a rational number is not in general rational. This vague heuristic is in fact in some respects true as the following table shows.

Degree	Name	# rational solutions	Structure
$1, 2$	Rational Curves	0 or ∞	Parametrised by $\mathbb{Q}$
3	Elliptic Curves	$\leq \infty$	Finitely generated abelian group [Mor1922]
≥ 4	General Type	$< \infty$ [Fal1983]	?!

4. My Research

Every talk that you give in academia should give some reference to your own work, and this talk is no exception. Given that curves are so well understood, how does the theory stand for higher-dimensions i.e. when you have more variables? It turns out that there is not such a satisfactory picture.

For surfaces for example, even though there is a geometric classification, there are still many un-answered diophantine questions. By a surface I mean

the solution set to an equation of the form

$$f(x, y, z) = 0$$

where $f \in \mathbb{Z}[x, y, z]$. The case of degree 1 and 2 is well understood and similar to that of curves. The case of degree 3 is less well understood. For example consider the surface

$$x^3 + y^3 = z^3 + 1.$$

This has a whole family of solutions given by $x = z, y = 1$. This corresponds to a line in the surface. A general cubic surface contains 27 lines, and since these can be thought of as "trivial" solutions, it is natural to "remove" them and see what is left over. It turns out that in general there will still be infinitely many solutions left over, and I have been studying a way to somehow quantify the "density" of these solutions, on cubic surfaces and their generalizations, *del Pezzo surfaces*.

The conjecture is that after removing the lines, the density of solutions left over should be less than the density of solutions on the lines. This is known for a few specific (singular) surfaces, however a proof in general is currently out of reach. I am working on proving results for specific examples, to increase the wealth of information available.

References

[Mor1922] L.J. Mordell, On the rational solutions of the indeterminate equations of the third and fourth degrees, Proc Cam. Phil. Soc. 21, (1922) p. 179.

[Fal1983] Faltings, Gerd (1983). "Endlichkeitsstze fr abelsche Varietten ber Zahlkrpern". Inventiones Mathematicae 73 (3): 349366.