INTRODUCTION TO DIOPHANTINE EQUATIONS

In the early 20th century, Thue made an important breakthrough in the study of diophantine equations. His proof is one of the first examples of the polynomial method. His proof influenced a lot of later work in number theory, including diophantine equations, transcendental number theory, and later exponential sums. In this lecture, we will introduce some basic questions and conjectures and explain what Thue proved.

1. Naive guesses about diophantine equations

The most famous diophantine equation is the Fermat equation $x^d + y^d - z^d = 0$. For $d = 2$ there are many integer solutions, and for $d \geq 3$ there are no positive integer solutions. The proof of the second part is extremely deep and hard. But is there any simple reason to expect that this situation is likely? In this section, we explore some naive guesses about diophantine equations.

Suppose that P is a homogeneous polynomial of degree d in n variables, with integer coefficients. Let us consider the equation $P(x) = A$, for some integer A. Let's try to guess how many solutions this equation is likely to have. Let's try to guess the number of solutions of size $|x| \sim 2^s$.

$$\text{Guess the size of the set} \{x \in \mathbb{Z}^n | P(x) = A, |x| \sim 2^s\}.$$

Notice that if $|x| \sim 2^s$, then $|P(x)| \lesssim 2^{sd}$. It's hard to say much else about $P(x)$ based on the information so far, so we make a primitive probabilistic model.

For each x with $|x| \sim 2^s$, let $\tilde{P}(x)$ be a random integer of norm $\leq 2^{sd}$. The expected size of the set $\{x \in \mathbb{Z}^n | \tilde{P}(x) = A, |x| \sim 2^s\}$ is $\sim 2^{ns}/2^{ds} = 2^{(n-d)s}$. If the polynomial P "behaved randomly", then the set of solutions of size $|x| \sim 2^s$ would be $\sim 2^{(n-d)s}$. This suggests the following naive conjectures.

Naive conjecture 1. *If $degP < n$, then the equation $P(x) = A$ has infinitely many integer solutions, and the number of solutions of size $\sim 2^s$ is $\sim 2^{(n-d)s}$.*

Naive conjecture 2. *If $degP > n$, then the equation $P(x) = A$ has only finitely many integer solutions.*

(The case $degP = n$ is more delicate. Our heuristic gives that the number of solutions of size $\sim 2^s$ is ~ 1, which would suggest infinitely many solutions. But having no solutions would not be such a large departure from the estimate in the heuristic...)

These conjectures are both false, but they are still useful.

We give some counterexamples.

Consider the equation $2x + 2y = 1$. Our model predicts it should have many solutions, but it has none because the left-hand side is always even. Therefore, naive conjecture 1 is false. (To fix this particular counterexample, we should also assume that the equation has lots of solutions modulo p for some small primes p.)

Consider the equation $(x^2 + y^2 - z^2)^{10} = 0$. This equation has degree 20 in 3 variables, but every Pythagorean triple is a solution. There are also examples in two variables. The equation $(x - y)^{10} = 1$ has infinitely many solutions. The equation $x^2 - 2y^2 = 1$ has infinitely many solutions (approximately one for each scale $|x| \sim 2^s$, as predicted by the heuristic). Therefore, the equation $(x^2 - 2y^2)^{10} = 1$ has infinitely many solutions. (We can rule out these particular counterexamples by insisting that P is irreducible.)

Although the conjectures are false, they give some useful intuition. If the degree $d > n$ and there are infinitely many solutions, then that seems to be a big coincidence, and one may hope that there is some structure that explains what is happening.

Two of the big achievements in diophantine equations from the early 1900's confirm this intuition. The circle method of Hardy-Littlewood proves that equations have lots of solutions if the number of variables is much larger than the degree and if nothing bad happens modulo p for small primes p. Thue proved that Naive Conjecture 2 is actually true in two variables, as long as the polynomial is irreducible.

Theorem 1.1. *(Thue) Suppose $P \in \mathbb{Z}[x, y]$ is a homogeneous polynomial with degree ≥ 3 which is irreducible (over $\mathbb{Z}$). If A is any integer, then the equation $P(x) = A$ has only finitely many integer solutions.*

2. Diophantine approximation

Thue actually proved an even stronger theorem about rational approximations of algebraic numbers. To see the connection, let us consider the equation $x^3 - 2y^3 = 7$. If $(x, y) \in \mathbb{Z}^2$ solves this equation, then we see that

$$(\frac{x}{y})^3 - 2 = 7y^{-3}.$$

Therefore, x/y is a good approximation of the cube root of 2, especially if y is large. A short calculation shows that

$$|2^{1/3} - \frac{x}{y}| \lesssim |y|^{-3}.$$

These are really very good rational approximations. For context, consider the following.

Proposition 2.1. *For any $\epsilon > 0$, for almost every real number β, there are only finitely many integer solutions to the inequality*

$$|\beta - \frac{x}{y}| \leq |y|^{-2-\epsilon}. \qquad (*)$$

(The proof is a standard exercise in measure theory. Consider all the β in an interval so that $(*)$ has a solution with $y > Y$. This set is a union of intervals of total length $\lesssim Y^{-\epsilon}$.)

Although it's easy to prove this result for almost every $\beta \in \mathbb{R}$, it's hard to check it for any particular β, say $\beta = 2^{1/3}$. Liouville gave the first estimates about diophantine approximation of algebraic numbers.

Proposition 2.2. *(Liouville, 1840's?) If β is an irrational algebraic number and $\frac{x}{y}$ is a rational number, then*

$$|\beta - \frac{x}{y}| \geq c(\beta)|y|^{-deg(\beta)}.$$

Recall that an algebraic number is a solution to a polynomial with integer coefficients. The degree $deg\beta$ is the minimal degree of such a polynomial.

We will use a couple basic facts about algebraic numbers. There is actually a unique minimal polynomial Q with $Q(\beta) = 0$. (Minimal here means that the degree and the size of the coefficients are minimal.) The polynomial Q will be irreducible over $\mathbb{Z}$, and so it will have no rational roots. This polynomial also has $Q'(\beta) \neq 0$.

Proof. Notice that $Q(x/y)$ is a non-zero rational number. The denominator can be taken to be $y^{deg(\beta)}$. Therefore, $|Q(x/y)| \geq |y|^{-deg(\beta)}$. If x/y is very close to β, then

$$|Q(x/y)| = |Q(\beta) + Q'(\beta)(\beta - x/y)| + \text{ lower order terms } \sim |Q'(\beta)||\beta - x/y|.$$

□

For example, $|2^{1/3} - \frac{x}{y}| \geq c|y|^{-3}$. This inequality is not strong enough to say anything about the number of solutions of $x^3 - 2y^3 = 7$. If we look back inside the proof of the Liouville inequality, it boils down to saying that $x^3 - 2y^3 = 0$ has no integer solutions and so $|x^3 - 2y^3| \geq 1$. But this does nothing to constrain the solutions of $x^3 - 2y^3 = 7$. However, an inequality even slightly stronger than Liouville's does constrain the solutions to diophantine equations.

Theorem 2.3. *(Thue) If β is an irrational algebraic number, and $\gamma > \frac{deg(\beta)+2}{2}$, then there are only finitely many integer solutions to the inequality*

$$|\beta - \frac{x}{y}| \leq |y|^{-\gamma}.$$

The diophantine approximation theorem implies the diophantine equations theorem for the following reason. ...

3. Outline of Thue's proof

In this section we outline Thue's proof, and we explain how it is analogous to other arguments we have seen. We recall the main steps in the polynomial method by outlining the proof of the finite field Nikodym theorem.

Outline of the proof of finite field Nikodym: Suppose that N is a small Nikodym set in $\mathbb{F}^n$.

(1) Find a non-zero polynomial P with controlled degree that vanishes on N. (Use parameter counting.)
(2) Because N is a Nikodym set, the polynomial P must also vanish at many other points. (Vanishing lemma.)
(3) The polynomial P vanishes at too many points, so it must be zero. Contradiction.

Here is the outline of Thue's proof. Suppose that the algebraic number β has two very good rational approximations r_1 and r_2.

(1) Find a non-zero polynomial $P \in \mathbb{Z}[x, y]$ with controlled degree and coefficients that vanishes to high order at (β, β). (Use parameter counting.)
(2) Because r_1 and r_2 are good approximations of β, the polynomial must also vanish to high order at (r_1, r_2).
(3) The polynomial P vanishes too much at (r_1, r_2), and so it must be zero. Contradiction.

The first step took Thue the longest to figure out. In the special case that β is the d^{th} root of a rational number, he constructed the polynomial P by hand with some difficulty. In this way, we was able to prove his finiteness theorem only for equations of the form $Ax^d + By^d = C$. After trying hard to construct the polynomial P for other values of β, Thue realized that he could find it by parameter counting.

Another important point about Thue's proof is that it uses two good rational approximations r_1 and r_2. It might seem simpler to start with one rational approximation r and try to get a contradiction. But it seems very difficult to do this. We will come back to this point more later.

3.1. **Final comment.** Suppose that α and β are two algebraic numbers. Then $\alpha+\beta$ is an algebraic number. Why? This is a bit in the same spirit as the polynomial method...

18.S997 The Polynomial Method
Fall 2012