Solutions to polynomials in two variables

Notes of the MASS Colloquium talk given by Professor Thomas Tucker
by Zachary Wampler and Xi (Amanda) Wang

Abstract

You may remember the quadratic formula for finding solutions to quadratic polynomials in one variable. It is natural to ask: are there formulas like this for polynomials of higher degree? The answer, roughly speaking, is yes. Going further, one might ask: what about polynomials in more than one variable? Here, the answer is far more complicated, and involves geometry in what may seem a surprising way. One famous example of this type of polynomial equation is the Fermat equation $x^n + y^n = z^n$.

1 Background

1.1 The quadratic formula

Professor Tucker began the talk with a brief discussion of the quadratic formula for polynomials of the form $ax^2 + bx + c$. The formula gives the roots of this polynomial as

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

What is remarkable about the formula is that it gives all solutions or roots of the polynomial in terms of the polynomial’s coefficients.

Similar formulas exist for polynomials of degree 3 or 4, i.e. $ax^3 + bx^2 + cx + d$ or $ax^4 + bx^3 + cx^2 + dx + e$, where each of the $a_i$ is an integer. Professor Tucker stressed that, while these formulas were more complicated, they still allow you to compute all solutions.

For polynomials of degree 5 or more, however, no such formula exists. The proof of this is due to the work of Abel and Galois, and it was proved in the early 19th century. But Professor Tucker was not interested in finding all solutions, just all rational solutions.

1.2 Rational solutions to polynomials

Next, we considered polynomials of the form

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$$

with $a_i \in \mathbb{Z}$. We would like to know if there are any rational numbers $\frac{b}{c}$ such that $f\left(\frac{b}{c}\right) = 0$. If there are, then we would like to know how to find them.
If we have a polynomial \( f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \) and we know that \( f\left(\frac{b}{c}\right) = 0 \), where \( b \) and \( c \) are relatively prime integers, then we have
\[
-a_0 = \frac{b}{c} \left( a_n \left(\frac{b}{c}\right)^n + \ldots + a_1 x_1 \right),
\]
so after clearing denominators \( b \) must divide \( a_0 c^n \). Since \( b \) and \( c \) are relatively prime, this means that \( b \) divides \( a_0 \).

Similarly, after multiplying through by \( (\frac{c}{b})^n \) we obtain
\[
a_n = \frac{c}{b} \left( a_0 \left(\frac{c}{b}\right)^{n-1} + \ldots + a_{n-1} \right),
\]
so \( c \) must divide \( a_n b^n \) and thus must divide \( a_n \).

Since \( a_n \) and \( a_0 \) are integers, there are only finitely many positive integers \( b \) and \( c \) such that \( b \) divides \( a_n \) and \( c \) divides \( a_0 \), so there are only finitely many rational numbers \( \frac{b}{c} \) to consider. So, to find any rational solutions to \( f(x) = 0 \), we need only check finitely many cases.

**Example 1.** Consider the following polynomial:
\[
f(x) = x^3 - 3x^2 + x - 3.
\]
We see that since the leading coefficient is 1 and the constant term is 3, the only possible rational solutions to \( f(x) = 0 \) are -1, 1, 3, -3. A quick check shows that \( f(3) = 0 \) and that there are no other rational solutions to \( f(x) = 0 \).

This is a working algorithm. That is, if the rational solutions exist, this method will produce them in finite time.

## 2 Polynomials in two variables

### 2.1 Pythagorean triples

We next turned our attention to a more complicated problem: finding rational or integer solutions to polynomials in two variables. A famous example of a polynomial of this type appears in Fermat’s last theorem, which says that for \( n \geq 3 \), there are no positive integers \( a, b, \) and \( c \) such that
\[
a^n + b^n = c^n,
\]
or equivalently, there are no rational numbers \( \frac{a}{b}, \frac{b}{c} \) such that
\[
\left(\frac{a}{c}\right)^n + \left(\frac{b}{c}\right)^n - 1 = 0.
\]

Pierre de Fermat claimed to have a proof of this theorem in 1637, but it was never published. The first known proof is due to Andrew Wiles in 1994.

Other examples include Pythagorean triples, integers \( a, b, c \) such that
\[
\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 - 1 = 0.
\]
Unlike the one variable case, the equation \( x^2 + y^2 - 1 = 0 \) has infinitely many rational solutions. On the other hand, Diophantus of Alexandria showed sometime in the third century AD that \( x = 1/4, y = 9/16 \) is a solution of the equation

\[
y^2 - x^8 - x^4 - x^2 = 0,
\]

and in 1997 Wetherell showed that it is the only nonzero solution, up to sign.

Clearly, the search for rational solutions is generally more difficult in the two-variable case. This raises several new questions. For example, is there a way to determine if a given two-variable polynomial has infinitely many solutions? If there are only finitely many solutions, is there an algorithm which will find them? Does the number of rational solutions depend on the degree of the polynomial?

### 2.2 Two-variable polynomials of degree 2 or 3

Professor Tucker then briefly discussed polynomials in two-variables of degree 2 and 3. Returning to the example of Pythagorean triples, we saw that the rational solutions could be parameterized by

\[
t \mapsto \left( \frac{t^{-1}}{t^2 + 1}, \frac{2t}{t^2 + 1} \right).
\]

Using this map, it is possible to count the approximate number of rational solutions whose numerator and denominator are both less than some fixed constant \( M \). For this particular equation, this number is approximately \( M \). Similar results can be obtained for other degree 2 polynomials.

For degree 3 polynomials in two-variables, things are still more complicated. Without going into great detail, professor Tucker explained that given 2 rational solutions to such a polynomial, one can construction a third by “adding” the first 2 together. Because of this, it is possible in many cases to construct infinitely many solutions. The construction comes with a caveat, however: the numerator and denominator of the point obtained by this addition method tend to be fairly large compared to the numerators and denominators of the pair used to construct it. This gives some intuition behind the result due to Louis Mordell (1922) which says that the number of rational points with numerator and denominator less than \( M \) on the curve defined by such a polynomial equation is approximately \( \log M \), significantly less than the case for degree 2.

### 2.3 Two-variable polynomials of degree 4 or more

For degrees 4 and higher, Mordell made the following conjecture, which was later proved by Faltings:

**Theorem:** If \( f(x, y) \) is a nonsingular polynomial of degree 4 or greater, then there are finitely many pairs of rational numbers \((b/c, d/e)\) such that \( f(b/c, d/e) = 0 \).

The observation which led to this conjecture and eventual theorem was that the rational solutions for polynomials with degree 2 or 3 are more sparsely distributed than in the case of degree 1.

A related conjecture is called the Mordell-Lang-Vojta conjecture. Professor Tucker did not give a precise statement, but explained that, “roughly speaking,” the conjecture says
that whenever a polynomial has infinitely many solutions there is an underlying addition law on some part of the geometric object that the polynomial equation defines.

2.4 The search for an algorithm

If we now restrict ourselves to working with the “good” polynomials of degree 4 in two variables, new problems emerge. The “bad” polynomials we would like to avoid correspond to curves with singularities, points at which the tangent space to the curve may not be defined. Disregarding such curves, professor Tucker can’t help but ask his favorite question: is there an algorithm for finding their rational points? Faltings theorem guarantees that there are only finitely many, but his proof does not give us any help in our search, Professor Tucker explained.

There is an approach which often works called the method of Chabauty and Coleman, but results are not guaranteed, so it is not effective. That is to say, it will not necessarily produce the solutions in finite time. There is also reason to doubt such an algorithm’s existence: Hilbert’s tenth problem, solved by Matiyasevich, Robinson, Davis and Putnam. The result is the following theorem.

**Theorem:** There is no process according to which it can be determined in a finite number of operations whether a polynomial equation $F(x_1, ..., x_n) = 0$ with integer coefficients has an integer solution.

This theorem does not directly imply that no rational solutions exist, nor does it imply the non-existence of an algorithm for the special case of two-variables.

2.5 One last question

The remainder of the talk was spent discussing a conjecture that has emerged from these problems, known as the “uniform boundedness question”. It asks:

*Is there a constant $C(n)$ such that any nonsingular polynomial equation $f(x, y) = 0$ of degree $n \geq 4$ has at most $C(n)$ solutions?*

Most mathematicians, according to professor Tucker, believe the answer to be “no”. But this conjecture is actually implied by the Mordell-Lang-Vojta conjecture, which most mathematicians do (or at least did) believe. The answer remains a mystery.