Counting solutions of systems of polynomial equations

Bas Edixhoven

Spring 1997

1 Systems of polynomial equations

Let us consider a system of equations of the following form:

$$\begin{aligned} f_1(x_1, x_2, \ldots, x_n) &= 0 \\ f_2(x_1, x_2, \ldots, x_n) &= 0 \\ &\vdots \\ f_m(x_1, x_2, \ldots, x_n) &= 0 \end{aligned}$$

where the f_i are polynomials with integer coefficients. Recall that a monomial in the variables x_j is just an expression of the form $x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$, with the exponents being positive integers (zero is considered to be positive). A polynomial with integer coefficients in the variables x_j is a linear combination of such monomials, with integer coefficients.

Example:

$$x^2 + ax + b = 0.$$

Here, counting the solutions is easy, because we have a formula for the solutions. If we want solutions in the real numbers, there are zero, one or two of them depending on the sign of the discriminant $a^2 - 4b$. If we want solutions in the complex numbers, and if we count them with multiplicities, then the number of solutions is always two.

Before we proceed to the case of more variables, I would like to say something about equations of higher degree in just one variable. The formula for the solutions of such an equation of degree two was already known to the Babylonians at

2000 BC. Similar formulas for the solutions of equations of degree 3 and 4 were discovered only in the 16th century. After that, a lot of time was spent in trying to find formulas for the equation of degree 5. Around 1830 it was shown by Galois that such formulas do in fact not exist (the formulas should involve only addition, subtraction, multiplication, division, powers and roots).

Another example:

$$x^2 + y^2 = 1.$$

So here we have two variables and one equation. The set of solutions with x and y real numbers is the circle of radius one, which is clearly an infinite set. Still, we would like to count the solutions in some useful sense. The key idea is to consider solutions in certain finite numer systems, called finite fields.

2 Finite fields

To see whether or not an $n$tuple $(x_1, \ldots, x_n)$ of real numbers is a solution of a system of polynomial equations, we only have to perform multiplications, additions and comparison with 0. In general, a set F that is equipped with two binary operations called sum (or addition) and product, and two distinct given elements called zero and one, satisfying the following properties,

1. for all x, y and z in F we have $(x + y) + z = x + (y + z)$,
2. for all x and y in F we have $y + x = x + y$,
3. for all x in F we have $x + 0 = x$,
4. for all x in F there exists a y in F such that $x + y = 0$,
5. for all x, y and z in F we have $(xy)z = x(yz)$,
6. for all x and y in F we have $yx = xy$,
7. for all x in F we have $x \cdot 1 = x$,
8. for all non-zero x in F there exists a y in F such that $xy = 1$,
9. for all x, y and z in F we have $x(y + z) = xy + xz$,

is called a field. The elements y in properties (4) and (8) are automatically unique, and denoted $-x$ and $1/x$ or x^{-1}, respectively. The sets of real and complex numbers, with their usual operations, are clearly fields. Another example of a field is given by the rational numbers. Yet other examples are given by rational functions and meromorphic functions. But there are also other examples, of a completely different type. For example, note that the only elements mentioned explicitly in the list of properties are 0 and 1. In fact, there are unique operations on the two element set $\{0, 1\}$ that make it into a field: one has to put $1 + 1 = 0$. This field, denoted $\mathbb{F}_2$, is quite useful in combinatorics. One gets other examples of finite fields as follows. For any integer $n \geq 2$, one can define a sum and product on the set $\{0, 1, \ldots, n-1\}$ by taking the remainder of the usual sum and product when divided by n. Another way to say this is that one writes integers in base n and considers only the last digit. A familiar example of this is the case $n = 12$, when one calculates with hours (5 hours after 8 o'clock it is 1 o'clock). For $n = 2$ we get our field $\mathbb{F}_2$. It is not hard to show that for an arbitrary n all properties for this set with these operations to be a field are satisfied, except possibly property (8). It turns out that that last property is satisfied if and only if n is a prime number (for example, for $n = 4$ the element 2 has no inverse). So for each prime number p we have constructed a finite field $\mathbb{F}_p$ of p elements. The classification of finite fields says the following: the number of elements of a finite field is a power of a prime number, for each power of a prime number there exists a finite field with that number of elements, and two such fields are "isomorphic". (Two fields are said to be isomorphic if one can pair their elements in a way that respects the sums and products.) The field with p^r elements will be denoted $\mathbb{F}_{p^r}$. Let us describe, for example, the field $\mathbb{F}_4$. Its four elements are 0, 1, z and $1 + z$. The addition is determined by: $1 + 1 = 0$ and $z + z = 0$. The multiplication is determined by: $z^2 = 1 + z$. The field $\mathbb{F}_9$ can be obtained by adjoining a square root of -1 to $\mathbb{F}_3$. Note the similarity with the construction of the complex numbers from the real numbers.

A positive integer n can be written as a sum $1 + 1 + \cdots + 1$, hence it defines, in any field, an element that we will still denote by n. Likewise, a negative integer can be written as a sum of -1's, hence also makes sense in any field. One has to be a little bit careful in doing this; for example, in $\mathbb{F}_{p^r}$ one has $p = 0$. We are now ready to count the solutions of a system S of polynomial equations with integer coefficients as in the beginning of this talk. For each prime number p and each integer $r \geq 1$ we define $N_S(p, r)$ to be the number of solutions of S in the field $\mathbb{F}_{p^r}$. The next step is to combine these numbers $N_S(p, r)$, for fixed S and varying p and r, into a suitable generating function.

3 The zeta function of a system of equations

Let us consider the famous Riemann zeta function:

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} = \prod_p \frac{1}{1 - \frac{1}{p^s}},$$

with the product taken over all prime numbers. This definition makes sense for real numbers $s > 1$, and, more generally, for complex numbers s with real part greater than 1. Riemann's zeta function extends to an analytic function on the complex plane with 1 removed (at 1, it has a pole of order one). This continuation satisfies a simple functional equation, relating $\zeta(s)$ and $\zeta(1-s)$. A very important question, posed by Riemann, is whether all zeroes of this continuation that have real part between 0 and 1 have real part exactly $1/2$. This question is very important in our understanding of the regularity of the distribution of prime numbers. Because the answer is not known at this moment, a lot of analytic number theory is done in two versions: one assuming that the answer is yes, and one assuming that it is no.

We are going to define, for each system of equations S as above, a function $\zeta_S(s)$, defined for complex numbers s with sufficiently big real part, such that Riemann's zeta function is the function associated to the system $x = 0$. So here is the definition:

$$\zeta_S(s) = \exp\left(\sum_{p,r} \frac{N_S(p,r)}{r} p^{-rs}\right).$$

It is easy to see that the sum in the definition converges when the real part of s is greater than one plus the number of variables in S. Using the fact that we have the following power series expansion:

$$-\log(1-x) = x + \frac{x^2}{2} + \frac{x^3}{3} + \cdots,$$

one sees that ζ_S is Riemann's zeta function if (and, in fact, only if) $N_S(p,r) = 1$ for all p and r. The function ζ_S contains very important properties of the system of equations S. It is expected that every ζ_S has a meromorphic continuation to the whole complex plane, with poles at prescribed places, and that certain identities, called functional equations, are satisfied among these continuations. At this moment there are a lot of conjectures concerning the values of these zeta functions at integers, but little is known about these values in general; in certain cases they are expected to give information on the solutions of S in the rational numbers.

The fact that a meromorphic continuation exists and that the functional equations are satisied in the one variable case was proved about 80 years ago. Spectacular progress was made a few years ago by Wiles, who proved the continuations to exist and the functional equations to hold for almost all systems of the form:

$$y^2 = x^3 + ax + b.$$

In this case, the problem was known as the Shimura-Taniyama-Weil conjecture. Of course, in the newspapers it was mentioned only that Wiles had proved Fermat's Last Theorem, since it was known to be implied by the Shimura-Taniyama-Weil conjecture, but the real result is the significant progress made in understanding zeta functions.

4 Geometry

The definition of the zeta function associated to a system of equations S implies immediately that we have the following factorization:

$$\zeta_S(s) = \prod_p \zeta_{S,p}(s),$$

where the product runs over all prime numbers, and the $\zeta_{S,p}$ are defined by:

$$\zeta_{S,p}(s) = \exp\left(\sum_{r\geq 1} \frac{N_S(p,r)}{r} p^{-rs}\right).$$

The functions $\zeta_{S,p}$ have a nice geometrical interpretation. So let us now fix a prime number p, and consider the function $\zeta_{S,p}$. The geometrical object in question will be the set $X_{S,p}$ of solutions of S in a field $\mathbb{F}_{p^\infty}$ that is somehow the union of all the $\mathbb{F}_{p^r}$. This set $X_{S,p}$ comes with a map to itself, such that the solutions of S in the field $\mathbb{F}_{p^r}$ is the set of fixed points of the rth iterate of that map. Let me describe these things in at least some detail.

The field $\mathbb{F}_{p^\infty}$, called an algebraic closure of $\mathbb{F}_p$, is obtained by adjoining to $\mathbb{F}_p$ all the roots of all polynomials in one variable with integer coefficients. In the field $\mathbb{F}_{p^\infty}$ we have $p = 0$. This simple identity has the following consequence:

> let x and y be elements of a field in which $p = 0$; then one has $(x+y)^p = x^p + y^p$.

To prove this result, one remarks that for $1 \leq i \leq p{-}1$ the binomial coefficient $\binom{p}{i} = p!/i!(p{-}i)!$ is divisible by p. For an integer a, considered as an element of a field in which $p = 0$, we find:

$$a^p = (1 + 1 + \cdots + 1)^p = (1^p + 1^p + \cdots + 1^p) = a,$$

which is known as Fermat's little theorem. (This identity gives us an efficient way to prove that a number is composite. For given a and n, with $0 \leq a \leq n$, to compute the remainder of a^n upon division by n takes at most about $3\log(n)$ multiplications of integers between 0 and n and the same number of elementary divisions by n of integers between 0 and n^2. This explains that there are lots of numbers that are known to be not prime, but of which no factorization is known.) Let now $r \geq 1$ be an integer, and let us consider the set of solutions in $\mathbb{F}_{p^\infty}$ of the equation $x^{p^r} = x$. It is clear that the set of solutions is closed under multiplication. The identity $(x + y)^p = x^p + y^p$ above shows that it is closed under addition, too. It is therefore not a big surprise that we have:

> $\mathbb{F}_{p^r}$ is the set of x in $\mathbb{F}_{p^\infty}$ satisfying $x^{p^r} = x$.

Let us now consider again the set $X_{S,p}$ of solutions of S in $\mathbb{F}_{p^\infty}$. Suppose that $(x_1, \ldots, x_n)$ is in $X_{S,p}$. Then we have, for $1 \leq i \leq m$:

$$f_i(x_1^p, x_2^p, \ldots, x_n^p) = (f_i(x_1, x_2, \ldots, x_n))^p = 0,$$

which shows that $(x_1^p, x_2^p, \ldots, x_n^p)$ is in $X_{S,p}$. It follows then that we have a map f from $X_{S,p}$ to itself, that sends $(x_1, x_2, \ldots, x_n)$ to $(x_1^p, x_2^p, \ldots, x_n^p)$, and that $N_S(p, r)$ is the number of fixed points f^r, the rth iteration of f.

Now there is a formalism, invented in the beginning of this century by Lefschetz, to count fixed points. It says that to a set such as $X_{S,p}$ one should (try to) associate a finite dimensional vector space, called a cohomology space, in such a way that a map like f induces a linear map from this vector space to itself, such that the trace of that map is the number of fixed points of f. (The linear map is given by a square matrix, the trace of it is the sum of its diagonal coefficients. There is in fact a technical condition: the fixed points should not be degenerate.)

In ordinary calculus in say three variables, such vector spaces represent obstructions against vector fields with zero curl to be gradients of functions, against vector fields with zero divergence to be curls of vector fields, and against functions being the divergence of a vector field.

A famous result obtained in this way, that was in fact the origin of the whole theory, is Brouwer's fixed point theorem:

> Every continuous map from the unit disk $\{(x, y) \mid x^2 + y^2 \leq 1\}$ in $\mathbb{R}^2$ to itself has at least one fixed point.

In the end of the 40's André Weil started to investigate systematically what the consequences would be for functions such as $\zeta_{S,p}$ if Lefschetz's formalism would work in the setting of algebraic geometry over finite fields. He showed that the $\zeta_{S,p}$ would in fact be rational functions in the variable p^{-s}, i.e., that there would be polynomials P and Q in one variable and with integer coefficients, depending on S and p, such that $\zeta_{S,p}(s) = P(p^{-s})/Q(p^{-s})$. Weil also conjectured properties of P and Q, such as their degrees and the absolute values of their roots, in geometrical terms, and he proved these conjectures in some cases. Before Grothendieck, in the end of the 50's, however, nobody knew how to construct the cohomology spaces for this. In the 60's, Grothendieck and his school carried out Grothendieck's ideas and proved most of Weil's conjectures. The last of Weil's conjectures was proved by Deligne in 1974. These results have since then had many applications. For example, one can count solutions over finite fields in order to get information such as the dimension of the cohomology spaces. One gets good estimates for trigonometric sums. There are relations with error correcting codes and other combinatorics. There has been an important feedback to complex algebraic geometry.

But the story is not finished. As I have already said, we know little about the product ζ_S of all the $\zeta_{S,p}$. Just a few months ago, Alain Connes (who was a Miller visiting professor some years ago, I think) seems to be making progress in the direction of a geometrical interpretation of zeta functions in the one variable case. The geometry is what he calls "non-commutative", and the cohomology spaces are infinite dimensional Hilbert spaces. Anyway, Connes has reduced the proof of the Riemann Hypothesis to proving a certain trace formula in a geometrical setting that is more general than the one where it is known at this moment.