

Description of Research
(non-technical)
Michael P. Knapp

I have attempted to write this description on a level that can be understood by an undergraduate student who has had two semesters of calculus. I hope that I have succeeded. If you believe that something is written poorly, please feel free to email me and offer any suggestions for improvement. If you are looking for a more advanced account of my research, please read the grant proposal that I submitted to the National Science Foundation in October 2001 (the references cited in the proposal are here).

I think that this is very readable as an html document, but that the formatting is a bit nicer as a pdf file. If you'd rather read that, then just click here.

My research is in the field of number theory, and is closely related to the problem of determining whether an equation or system of equations has a solution in which all of the variables are integers. This has been considered an interesting problem in math for a long time, at least since the time of the ancient Greeks, who considered a problem insoluble unless there was a solution in integers. For example, the Greeks would have said that the equation $2x - 1 = 0$ has no solutions because there is no integer that you can substitute for x which makes the equation true. Unfortunately, it can be proven that there is no procedure that you can always follow no matter what equation (or system of equations) you are given which can tell whether the equation has an integral solution. In fact, this is even true if we only care about polynomial equations. So it might seem right away that there is no way to make any good progress on this problem.

However, it turns out that it is possible to get results if instead of talking about any polynomial, we only talk about **homogeneous** polynomials. These are polynomials in several variables with the property that if you look at every term individually, then adding up the degrees of the variables in the term always gives you the same number. This number is called the **degree of the polynomial**. For example, one homogeneous polynomial of degree 5 would be

$$x^5 + 6xyz^3 - 2y^2w^3 + st^4.$$

This is a polynomial in 6 variables, and if you look for example at the term $6xyz^3$, the sum of the degrees is $1 + 1 + 3 = 5$ (remember that $x = x^1$). Similarly, if you look at the term $2y^2w^3$, the sum of the degrees is $2 + 3$, which is also 5. Homogeneous polynomials are also called **forms**.

I'm interested in finding values of the variables which are integers and make the form equal to zero. If you think about it for a minute, you'll see that this is easy. For example, in the polynomial above, we can just set all of the variables equal to zero. Even better, if you think about the definition, you'll see that this trick works for any homogeneous polynomial.

This is because every term has to contain at least one variable. The solution in which all of the variables are set to zero is called the **trivial zero** of a form (or system). I am interested in determining whether there are **nontrivial zeros**, in other words, zeros with at least one variable not equal to zero.

Now, there are certainly forms with no nontrivial zeros. For example, the form

$$x_1^2 + x_2^2 + x_3^3 + \cdots + x_n^2$$

has no nontrivial zeros no matter how many variables there are. This happens because the square of any nonzero integer is positive. If even one variable is nonzero, there would be a positive term in the sum, and we could never get a negative term to cancel it out. Another example is the form

$$x^3 - 2y^3.$$

Cubes of integers can be both positive and negative (for example $(-2)^3 = -8$), so that's not the problem here. Suppose however that there was a way to make this form equal to zero with x and y not equal to zero. Then you could do algebra on the equation

$$x^3 - 2y^3 = 0$$

to get

$$\frac{x}{y} = 2^{1/3}.$$

But $2^{1/3}$ is the cube root of 2, which is irrational. So this is impossible when x and y are integers (because if x and y are integers, then x/y is a rational number). The problem in this case turns out to be that there aren't enough variables in the form. If there are too few variables, then having a nontrivial zero in integers might cause impossible things to happen.

The amazing thing is that these are the only types of problems that can arise. It turns out that if the degree of a form is odd (because odd powers can be both positive and negative) and there are enough variables, then the form always has a nontrivial zero. In fact, a similar statement is true for systems of forms too. If the degree of each form is odd (the forms can have different degrees) and there are enough total variables, then the system has a nontrivial zero. In other words, you can assign integers to all the variables with at least one variable nonzero such that all of the forms are equal to zero.

Now, the interesting question to ask is "how many variables are enough?" This is the question I try to answer. However, instead of using regular integers like $-3, 0, 5$ and so on, I try to find zeros of the forms in what are called **p -adic integers**. Before I tell you what that means, let me just say first that it is possible to show that if there is a nontrivial zero in ordinary integers, then there is also a nontrivial zero in p -adic integers. Also, in order to use one of the standard methods to attack this problem in regular integers, it is often necessary to first have an answer that works for p -adic integers. So it's often important to know about

p -adic zeros before we can find out about zeros in ordinary integers.

So what is a p -adic integer? Well, they are pretty complicated to define, so I won't try to give you the definition here. Fortunately however, I can tell you what it means to say that a polynomial has a zero in p -adic integers without defining these integers themselves. First, let me say that the " p " in " p -adic" represents a prime number, and there is a set of p -adic integers for every prime p . So there is a set of 2-adic integers, a different set of 3-adic integers, other sets of 5-adic integers, 7-adic integers, 11-adic integers and so on. So when we have an equation to solve, we want to pick the value of p first and then solve the equation in p -adic integers for that specific value of p .

Now, suppose that $f(x)$ is a polynomial and p is a prime number (I'll do a couple of specific examples in a minute). Then to say that $f(x)$ has a zero in the p -adic integers means that you can find values of x that make $f(x)$ divisible by every power of p . For example, suppose that $f(x) = x^2 + 2$ and we want to know whether $f(x)$ has a zero in the 3-adic integers. First, we need to see if we can find a value of x which makes $f(x)$ divisible by 3. In fact, we can do this since if $x = 1$ then we get $f(1) = 1^2 + 2 = 3$, which is certainly divisible by 3. Now, we need to see if we can make $f(x)$ divisible by $3^2 = 9$. This time, setting $x = 1$ doesn't work. But letting $x = 4$ works since $f(4) = 18 = (9)(2)$. (Note that it is perfectly OK to use different values of x at each step. Also note that we do not have to make $f(x)$ equal to 9. We only have to make it divisible by 9.) Now we test whether we can make $f(x)$ divisible by $3^3 = 27$, and we find that $x = 5$ works this time. In fact, it is possible to show that if we test 3^4 or 3^5 or any power of 3, then we will always be able to make $f(x)$ divisible by that number. So the equation $x^2 + 2 = 0$ has a solution in the 3-adic integers.

Now let's look at a different example. We'll still let $f(x) = x^2 + 2$, but now we'll see if there is a zero of this in the 5-adic integers. First, we need to see if we can make $f(x)$ divisible by 5. But if we try $x = 1, 2, 3, 4, \dots$, we'll quickly realize that no value of x works. (Of course, for a mathematician, just trying a bunch of values isn't enough. We have to prove that there really are no values of x that work no matter how high you go.) Since we can't even make $f(x)$ divisible by 5, we know right away that the equation $x^2 + 2 = 0$ has no solutions in the 5-adic integers.

These two examples already show some interesting things about p -adic integers. The first example shows that the p -adic integers are not the same as the ordinary integers, since the equation $x^2 + 2 = 0$ has no solutions in the ordinary integers but does have solutions in the 3-adic integers. The second example shows that the p -adic integers are different for different values of p , since the equation $x^2 + 2 = 0$ has solutions in the 3-adic integers but has no solutions in the 5-adic integers.

It turns out that there are many differences between the p -adic integers and the regular integers. For example, the p -adic integers are not ordered in the way that regular integers

are. In other words, given two p -adic integers, there is no way in which you can say that one of them is “greater” than the other. This concept of order just doesn’t make sense in the p -adic world. A consequence of this is that in the p -adic world, there is no concept of “positive” and “negative” numbers. After all, you normally think of positive numbers as those that are greater than zero. If you can’t define what “greater than” means, then how can you define positive?

Another way in which p -adic integers are different is in when forms have nontrivial zeros. It turns out that a form of any degree has a nontrivial p -adic zero as long as there are enough variables, and the same is true for systems of forms. So in the p -adic world, the degrees don’t have to be odd anymore. The exact questions that I work on are about how many variables are needed to ensure that (systems of) forms have nontrivial p -adic zeros.

In particular, most of my work has dealt with **diagonal** forms. That is, forms with no cross-terms. So a typical diagonal form might look like

$$x^5 + 3y^5 + 12z^5 - 5w^5 + \dots .$$

There is a conjecture called **Artin’s conjecture** about how many variables are needed to ensure that any diagonal form has a p -adic zero. The conjecture says that if R is the number of forms, and their degrees are d_1, d_2, \dots, d_R (some degrees can be the same, others can be different), then there will always be a nontrivial p -adic zero, no matter what p is, as long as there are at least

$$d_1^2 + d_2^2 + \dots + d_R^2 + 1$$

variables. In other words, there will be a nontrivial 2-adic zero, a nontrivial 3-adic zero (which will almost certainly be different), a nontrivial 5-adic zero, and so on. This conjecture is definitely true when $R = 1$, i.e. when there is only one form, but nobody has ever been able to prove it for any other number of forms.

One of the results that I have proven is that if there are many forms (say the number of forms is R) and all of the degrees of the forms are the same (say they’re all equal to d), then there’s a nontrivial p -adic zero, no matter what p is, as long as there are at least $4R^2d^2$ variables. (Artin’s conjecture says that $Rd^2 + 1$ variables should be enough, but I don’t know how to prove that yet.) If d is even and large then this is the best-known bound. If d is odd, or if d is even and small, then other people have found better bounds than mine. That is, they have found smaller numbers of variables that are guaranteed to work. I won’t say exactly what “large” means here, but if you know the value of R , then you can figure out what “large” means for that value of R . A particular value of d might be large for some values of R but small for other values of R .

Another theorem that I have proven is that if there are two (and only two) diagonal forms, the degrees are both odd, and one of the degrees is at least 31, then Artin’s conjecture is true. As you might guess from this result, it is easier to deal with odd degrees than

even degrees. One project that I am currently working on is to prove this theorem without the restriction that one of the degrees is at least 31.

I have proven several other theorems related to solving systems of forms in p -adic integers, but they are a bit more complicated to explain and my goal here is to attempt to keep this description reasonably straightforward. So I won't mention these other theorems here. If you are interested, please check out the Papers and Preprints section of my website. There you can find abstracts for each of the research papers I have written, and can even look at the papers themselves.

I hope that you have enjoyed reading this explanation of my research, and that you have found it reasonably clear. As I said at the beginning, if some parts are confusing, please feel free to email me about them. If you are interested in learning more about this subject, I would be happy to talk to you about it. Or, you could try reading a more advanced account of this field. My research statement focuses on the specific problems that I work on. Another good source, which covers much more, is the article "Diophantine problems in many variables: the role of additive number theory" by Trevor Wooley, which appears in the book *Topics in Number Theory* (Kluwer Academic Publishers, 1999).