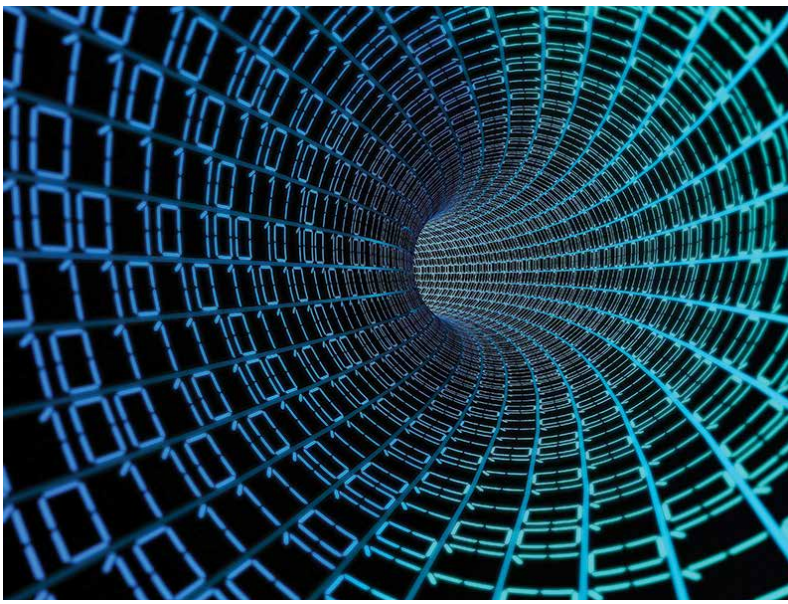
Mapping *P*-adic Spaces with Height Pairings

Professor Amnon Besser



Scientia

MAPPING *P*-ADIC SPACES WITH HEIGHT PAIRINGS

Professor Amnon Besser of Ben-Gurion University of the Negev and his colleagues are exploring *p*-adic numbers – one of the most difficult areas of number theory – in order to solve long-standing open problems bridging several fields of mathematics.

Solving Unsolvable Equations with a New Number System

If you are somewhat familiar with advanced mathematics, specifically number theory, it is likely you have heard of *p*-adic numbers. Often spoken of with reverence, and described as one of the most difficult areas in pure mathematics, *p*-adics are regarded as inaccessible to the public. However, they have many real-world applications, such as encryption algorithms, and have the potential to solve several problems in fundamental physics through theories such as *p*-adic quantum mechanics. The modular way in which *p*-adics retain information about the equivalence between different numbers is fundamental to the demonstration of Fermat's Last Theorem, as discovered by Andrew Wiles no less than 350 years since Fermat first stated it. In fact, the consequences of the *p*-adic number system stretch far beyond that. Although they started as a natural quirk derived from the need to solve Diophantine equations (polynomial equations in which only integer solutions are allowed), it is believed that they have deep implications touching upon the Birch and Swinnerton-Dyer conjecture and the Riemann Hypothesis – two open Millennium Prize Problems.

For Professor Amnon Besser of Ben-Gurion University of the Negev, *p*-adics have been a source of hope for finding a specific answer to a computational problem. Part of his problem involved an integration method developed by Robert Coleman, a method which is the *p*-adic equivalent of integration along a curve between two points. After his PhD, Professor Besser often used Coleman integration while delving into *p*-adic number theory. Later on, he heard that algorithms that compute a function called *p*-adic height could have important applications in cryptography. At that time, such an algorithm had already been produced, but Professor Besser felt he could create a better, more general one. Later on, he joined forces with Jennifer Balakrishnan, who was working on finding certain solutions specific to computing Coleman integrals. Their work produced a new method for computing a function called a *p*-adic height pairing, and facilitated the generalisation of Professor Besser's previous results.

Now, a large part of Professor Besser's research focuses on using numerical methods to find rational solutions of algebraic equations. Developing numerical methods can address situations where no exact solutions are known for a class of equations, by reducing the problem to number crunching. In general, these types of numerical solutions can help scientists and engineers when dealing with an ill-behaved function that models an aspect of applied research.

In order to have a better understanding of these problems, let's go back to the basics of *p*-adic number theory.

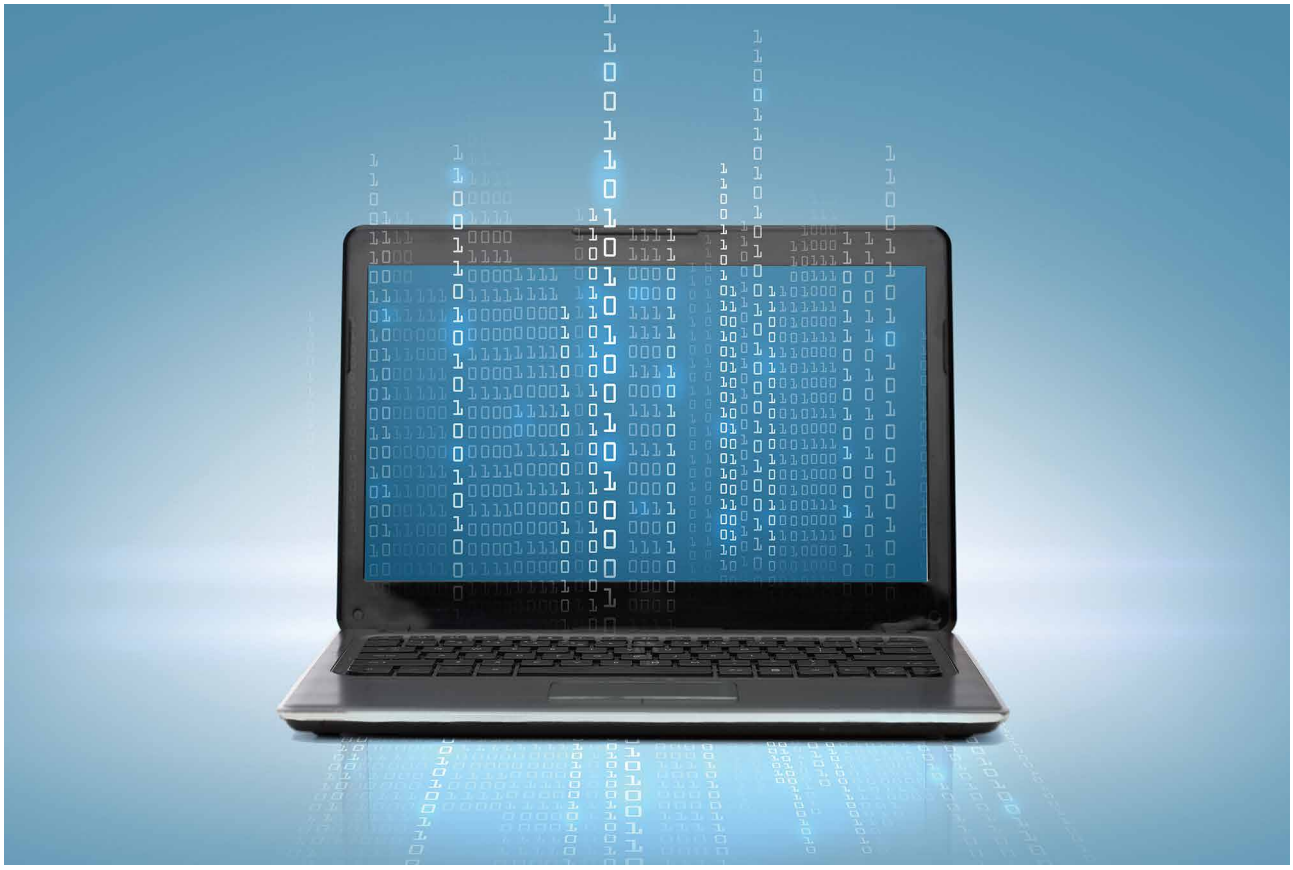
What Are *P*-adics?

P-adics were created from a desire to apply the techniques of power series methods to number theory, as a way to express certain numbers or mathematical problems in a tractable way. After all, number theory, or the queen of mathematics as Gauss called it, is famous for posing some of the most difficult conjectures in the entire field of mathematics. Thus, the idea to create tools that would transform intractable problems into approachable ones is a very natural strategy.

Just like complex and real numbers, *p*-adic numbers extend the rational number system Q and its associated arithmetic operations. If rational numbers can be expressed as a ratio between two integers p/q, real numbers are expressed as an endless decimal expansion. One such number is π and another is √2, and even 1 can be written as 1.000… or 0.999… for example, which is a sum of an infinite number of powers of 1/10. Unlike real numbers, *p*-adics are expressed as sums of powers of a prime number, usually denoted by p. Since the letter p is simply a placeholder for the base, replacing it with some number will yield base-dependent names like 2-adics or 17-adics and so on.

In a way, *p*-adic numbers are the opposite of real numbers. The difference derives from the ordering or closeness within the number system. If two real numbers that differ in the 10^{th} decimal digit are closer than two other numbers differing in the 2^{nd} decimal digits, for *p*-adics the concept of closeness is a much more interesting one. Albeit counterintuitive, this is thoroughly consistent within the *p*-adic number system. Thus, *p*-adics are close when their difference can be divided by a high power of p. The higher this power is, the closer the two numbers are said to be. In our example where p is a fixed prime and e a variable power, the difference between *p*-adics is divisible by pe and the numbers are close when e is very large. In other words, two decimal

‘I look for new methods for solving equations. I put the usual well-known numbers inside some bigger space from which one can cut out the pieces containing the solutions.’



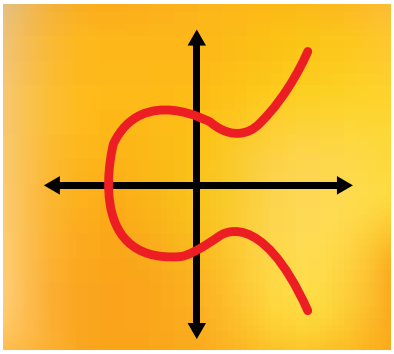
representations of a real number are close when the difference between them is a large negative power of 10, whereas two *p*-adic expansions are close when their difference is a large positive power of p. For *p*-adics, the concept of closeness opens the possibility to encode information about congruence of absolute value, which could be called their measure, in a new and interesting way.

In addition, *p*-adics can be considered opposites of real numbers in terms of their representations. Due to change of base, *p*-adic numbers are written from right to left, each digit added to the left increasing the precision of the number representation. Recall that expansions of real numbers are written the other way around, from left to right, with a finite number of digits before the decimal point and an infinite number of digits after it. *P*-adics, on the other hand, can have an infinite number of digits to the left. Moreover, the *p*-adic number system is based on the modular number system, like a clock that resets to zero when reaching 12-midnight, which means that the arithmetical operations behave differently from those of usual arithmetic. One reason why *p*-adics are a particularly neat number system is that the base must be a prime number, otherwise the set of all numbers obtained from arithmetic operations is not closed under these operations. In other words, you can divide *p*-adics with a non-prime base and get a number that was not part of the initial set.

Mapping the Path to Unique Solutions

Although *p*-adics in particular and number theory in general seem to be purely abstract mathematics, they are both born of the very simple goal of solving equations. As Professor Besser explains, ‘I look for new methods for solving equations. I put the usual well-known numbers inside some bigger space from which one can cut out the pieces containing the solutions.’

These equations are important for all types of applied problems in physics, engineering, finance, and other fields. In their simplest



Elliptic curve

form, the Diophantine equations that led to the development of *p*-adics can be written as $ax + by = c$, where x and y are variables and a, b and c are constants. In addition, *p*-adics methods can be used to study superelliptic equations, where $y^m = f(x)$, and hyperelliptic equations of the form $y^2 = f(x)$. The representations of these equations are often called curves in the formal language of mathematics due to their shape. Sometimes, these curves self-intersect to form a closed boundary.

The only solutions in integers to

$$y^2 = x^3(x-1)^2 + 1.$$

are $(2,\pm 3)$; $(1,\pm 1)$, $(0,\pm 1)$.

One of the peculiarities that follow from the rules of *p*-adics is that they cause unusual behaviour. In a geometric interpretation, *p*-adic numbers form a space much like the Euclidean flat space in which we live. However, their space has a completely foreign definition of the distance between two points, called a metric. In this space, the triangle inequality is stronger than in flat space. As Professor Besser points out, one consequence of this is that 'any two circles are either disjoint or one contains the other.' Because of this property, functions such as integrals, when defined over complex numbers, can be extended beyond their normal domain by creating analytical paths and moving from one point to the next. This technique, called analytic continuation, allows mathematicians to find rigorous answers to otherwise intractable problems, such as extending functions over singularities or summing certain series. However, these techniques conceal a trap in complex spaces. When following the analytic continuation of a function, the calculation may descend into a loop and retrieve multiple values for the same calculation. However, the strange behaviour of *p*-adic spaces does not support analytic continuation at all, resulting instead in a huge multivaluedness, too large for practical purposes.

Professor Besser found a way to overcome the problem of multi-valued results for the same function by continuing Coleman's work on integration. Recall that Coleman worked on defining the equivalent of integration under a curve for *p*-adics. Professor Besser interpreted Coleman's ideas in a way that led to a formal definition of paths. By making certain assumptions about the way in which the functions transform along the paths, 'these paths live on a discrete structure obtained by shrinking all the small circles in the *p*-adic world to points,' as Professor Besser explains. In this way, instead of working with a discrete space where functions would jump between circles, he went on to recover the continuum in the limit of the circles tending to zero. Moreover, the same operator that remembers how functions transform along the paths also maintains them as fixed and allows for unique answers to be found, thus eliminating the problem of multi-valued results. Although they are more difficult to define, Coleman integrals are better in some cases than complex integrals because they are single valued.

Meanwhile, Professor Besser's colleagues, including Minhyong Kim from Oxford, used a non-abelian generalisation of a method devised by Claude Chabauty in 1941 to find rational-valued points on curves with special properties. The Chabauty method allowed them to progress in theoretical directions, by showing that some Coleman integrals become equal to zero on rational solutions of certain equations. This important finding proved that these integrals have a finite number of solutions, because a Coleman integral can become 0 only a finite number of times.

During this time, Professor Besser focused on the practical question of actually finding the rational and integral solutions to equations using the Chabauty method. His approach involved using *p*-adic height pairings. The approach is based on the idea that rational solutions to equations can be added together in some sense. The advantage of the *p*-adic height pairing is that it transforms in a very simple way when solutions are added, and this leads to equations on the values of the height pairing at integral points. Based on Professor Besser's previous work, these equations can be expressed as a Coleman integral becoming zero. Although this seems like a simple enough exercise, there are in fact many categories of unsolvable equations. Solutions to these equations, as well as techniques used for their solution, could bring great advances in computer science and computational physics. 'One of the key points in the computation of Coleman integrals is the Kedlaya algorithm, which finds the number of solutions of certain equations modulo a prime p, a problem whose primary motivation is in the field of elliptic curve cryptography,' Professor Besser tells us. Recall that elliptic curves are representations of algebraic elliptic equations. Plotting the points of these equations results in curves which often self-intersect, forming a closed boundary. Elliptic curve cryptography uses such equations to generate much shorter secure public keys than those generated using other methods.

Professor Besser hopes to extend *p*-adic height pairings to more general cases and use them to solve badly behaved equations. The latter is an important step in understanding the relevant mathematics in a fundamental way, and in solving some of the most interesting open problems of the field.

Meet the researcher

Professor Amnon Besser
Department of Mathematics
Ben-Gurion University of the Negev
Beer-Sheva
Israel

Professor Amnon Besser currently holds a research position at the reputed Ben-Gurion University of the Negev in Israel, where he has been teaching since 1999. His research interests span number theory, *p*-adic integration and cohomology, Shimura varieties, automorphic forms, algebraic cycles and K-theory. Besser received his PhD in 1993 with a thesis in number theory on Universal families over Shimura curves. Throughout his career, he has held research positions in several famous institutions, such as Oxford University, Princeton, the Max Planck Institute for Mathematics, UCLA, and Arizona State University. He has authored over 30 papers that have been published in journals and presented at international conferences. From the standpoint of productivity and overall impact, his work has a calculated h-index of 8. Recently, he has been researching *p*-adic height pairings and integral points on hyperelliptic curves.

CONTACT

E: bessera@math.bgu.ac.il
W: https://www.math.bgu.ac.il/~bessera/

KEY COLLABORATORS

Jennifer Balakrishnan, Boston University
Steffen Müller, University of Oldenburg

FUNDING

Israel Science Foundation

REFERENCES

JS Balakrishnan, A Besser, JS Müller, Computing integral points on hyperelliptic curves using quadratic Chabauty, Mathematics of Computation, 2017, 86, 1403–1434.

JS Balakrishnan, A Besser, JS Müller, Quadratic Chabauty: *p*-adic Heights and Integral Points on Hyperelliptic Curves, Journal für die reine und angewandte Mathematik, 2016, 720, 51–79.

J Balakrishnan, A Besser, Coleman-Gross height pairings and the *p*-adic sigma function, Journal für die reine und angewandte Mathematik, 2015, 698, 89–104

JS Balakrishnan, A Besser, Computing Local *p*-adic Height Pairings on Hyperelliptic Curves, International Mathematics Research Notices, 2012, 11, 2405–2444.

Ben-Gurion University of the Negev