Massive new mathematical database keeps web and banking security ahead of the curve

by Manjil Saikia - Tuesday, May 10, 2016

http://gonitsora.com/massive-new-mathematical-database-keeps-web-banking-security-ahead-curve/

On Tuesday 10th of May mathematicians from 12 countries will formally launch a massive mathematical database of mathematical objects including elliptic curves, and a special class of zeroes, that has already been deployed to protect our bank accounts and solve mathematical problems in physics and in prime number theory.

Professor John Cremona at the University of Warwick is the lead UK researcher on a project that has catalogued over a billion mathematical items in six terabytes of data including: “elliptic curves”, “Modular forms” “L-functions” and “non-trivial” zeros, in a research initiative known as the *L-Functions and Modular Forms Database Project* which can be found at: http://www.lmfdb.org/

These mathematical items are all a significant part of the information that underpins what are known as L-functions. These help shape our understanding of prime numbers and key parts of mathematical physics, and they also power much of the way we protect our online bank accounts, use and understand cryptography, and underpin web security.

Elliptic curves arise naturally in many parts of mathematics, and can be described by a simple cubic equation. They form the basis of cryptographic protocols used by most of the major internet companies, including Google, Facebook, and Amazon. Modular forms are more mysterious objects: complex functions with an almost unbelievable degree of symmetry.

One of the great triumphs in mathematics of the late 20th century was achieved by Sir Andrew Wiles in his proof of Fermat’s Last Theorem, a famous proposition by Pierre de Fermat that went unproved for more than 300 years despite the efforts of generations of mathematicians. The essence of Wiles's prize winning proof established a long conjectured relationship between elliptic curves and modular forms.

Elliptic curves and modular forms are connected via their L-functions. The remarkable relationship between elliptic curves and modular forms established by Wiles is mapped by the LMFDB, where one can travel from one world to another with the click of a mouse and view the L-functions that connect the two worlds.

Professor John Cremona said:

> “The objects in our database aren’t just of interest to mathematicians. Some of them are part of a great many people’s daily lives. Elliptic curves for instance are often the standard mechanism used to validate the security in secure web transactions such as internet banking or even the transactions we undertake with our credit and debit cards”
>
> “My first contribution to this area was to create some physical printed tables of these

mathematical objects which joined a small group of paper based resources, such as the 1976 Antwerp IV tables of elliptic curves, that mathematicians have been hoarding, treasuring and using for decades.“

“However, even since the arrival of the world wide web, tables and databases have been scattered among a variety of personal web pages including my own. To use them, you had to know who to ask, download data, and deal with a wide variety of formats. A few had more sophisticated interfaces, but there was no consistency. It is an odd but really exciting experience, to see direct interest in my own personal online table transforming into increasing citation and use of the new database.”

This database was built to provide tools that could help tackle the “Riemann hypothesis” one of the Millennium Prize Problems nominated by the Clay Mathematics Institute. I also hope that it will be a useful tool for researchers of the Clay Millennium problems, the Birch--Swinnerton-Dyer conjecture on the set of rational solutions to equations defining an elliptic curve. I was privileged to be one of Professor Bryan Birch’s doctoral students and I would be delighted if this work was used to held prove the Birch and Swinnerton-Dyer conjecture”

Bristol University’s Professor Brian Conrey, said:

“We are mapping the mathematics of the 21st century. The LMFDB is both an educational resource and a research tool which will become indispensable for future exploration.”

“The LMFDB team includes mathematicians from more than a dozen research areas, all of whom are building connections between their seemingly separate specialties. Most of us are aware of these relationships in an abstract way, but it takes real work to actually figure out all the details. These details are made available on the LMFDB website, for everyone to explore and perhaps discover something new.”

Commenting on the project Dr Kristin Lauter, head of the Cryptography Group at Microsoft Research, said:

“LMFDB provides a valuable resource for both pure and applied research mathematicians. For example, minimal polynomials of algebraic special values of a variety of modular forms are useful in generating curves for use in cryptography. In addition to cataloging data which can be useful in applications, the database will also be a rich source of new research problems and directions.”

- The project is supported by a grant of £2,246,114 from EPSRC, and additional support from the US National Science Foundation. The full research team on the UK grant funded part of L-Functions and Modular Forms Database Project include: the Principal Investigator Professor John Cremona from the University of Warwick and support from colleagues at the University of Washington, Seattle, the Abdus Salam ICTP, the American Institute of Mathematics and the

University of Waterloo

- The Riemann hypothesis is a conjecture that the Riemann zeta function the Riemann zeta function has its zeros only at the negative even integers and the complex numbers with real part 1/2. It is a 157-year-old problems which many consider to be the most important outstanding problem in mathematics, and is one of the $1M Millennium Prize Problems nominated by the Clay Mathematics Institute.
- The most basic L-function is known as the Riemann zeta function, named after the German mathematician Bernhard Riemann who described its properties in 1859. Riemann found the first 4 zeros of his zeta function by a pen and paper calculation, and in 1953 Alan Turing used one of the earliest electronic computers to locate more than 1100 of them. Much recent research has focused on the pattern of the zeros: are they randomly spaced along their line, or is there some underlying music? The data provided by the LMFDB is invaluable for researchers studying these questions
- The three events to launch the LMFDB on May 10 include: A workshop at the American Institute of Mathematics, in San Jose, California; a public talk and reception at Dartmouth College, in Hanover, New Hampshire, including a webcast; and a workshop at the University of Bristol, UK, sponsored by the Heilbronn Institute.

Featured Image Courtesy: Shutterstock
