Introduction

In 1637, Pierre de Fermat, a famous French amateur mathematician, lawyer by profession, wrote an innocuous note in his copy of Arithmeticæ by Diophantus of Alexandria:

It can never happen that the sum of two numbers raised to n-th powers is a sum of another n-th power.

Unfortunately his margin was too short to contain a proof...

Pierre de Fermat

Taniyama–Shimura Conjecture

For over 350 years the general proof of Fermat’s Last Theorem was considered to be inaccessible. In 1984 Gerhard Frey observed that every Fermat’s solution can be linked to an elliptic curve – an algebraic object with well-defined arithmetic operation of addition of points. This remark was then used by Jean-Pierre Serre, a Fields medalist, and Ken Ribet to reduce the proof of Fermat’s Last Theorem to the statement about modularity of elliptic curves, the Taniyama–Shimura conjecture.

This task was accomplished partially by Sir Andrew Wiles, a British mathematician and his former student Richard Taylor in 1995, [4, 5].

For this achievement Wiles received a Silver Plaque from the International Mathematical Union in 1998, was made a Knight Commander of the Order of the British Empire by the Queen in 2000 and received the Abel Prize in 2016.

Prof. Andrew Wiles

Generalized Fermat Conjecture

When the proof of Last Fermat’s Theorem was complete, people started to wonder if it is possible to solve other equations of the form

\[ x^p + y^q = z^r \]

in coprime integers, for given positive exponents \( p, q, r \). For small exponents we can actually find solutions but the conjecture says that for \( p, q, r > 2 \) we should not expect any solutions at all. A few examples of non-trivial solutions:

\[ 13^3 + 7^3 = 2^8, \quad 71^7 - (-17)^7 = 2^2, \quad 21063928^3 - (-76271)^3 = 286, \]
\[ 2213459^3 + 1414^7 = 645, \quad 15312283^3 + 9282^3 = 113^7, \]
\[ 30042907^3 + (-96222)^3 = 43^7, \quad 1549034^3 + (-15613)^3 = 33^7 \]

(Few examples of non-trivial solutions)

Beal Prize

In 1997, Daniel Andrew Beal, an American banker and mathematics enthusiast, established a prize for any person who can prove or disprove Generalized Fermat Conjecture.

Currently the prize amount is US $1,000,000. The funds are held in trust by the American Mathematical Society.

References


Our work

To this enormous endeavour, I’ve been introduced through a collaboration with Michael Stoll (Bayreuth University, Bavaria, Germany) and Nuno Freitas (University of British Columbia, Vancouver, Canada). We have solved the most difficult yet handled case of the Generalized Fermat Conjecture, using a spectrum of genuinely new techniques. [3]. We managed to show [2] that the equation

\[ x^2 + y^3 = z^{11} \]

has no primitive and non-trivial solutions except for \( (\pm 37)^2 + (-2)^3 = 1^{11} \).

We also initiate the study of equations of the form \( x^2 + y^2 = z^p \) for primes \( p \) larger than 11.

Our method uses elliptic curves of Frey type. However, this time we actually do have solutions which poses real problems! We study the moduli space of such solutions and analyse how those solutions vary in \( p \)-adic families.

We even had to use algorithms relying on the Generalized Riemann Hypothesis in order to finish the calculations in less than a few days (otherwise it would be a few years...).

Computer calculations

In our work complicated algebraic manipulations necessary for the proof are only accomplished by using highly sophisticated algorithms designed for computer algebra systems.

The community gained from us several implementations of number theoretical techniques that will be used by future researchers.

Number theory beyond mathematics

Elliptic curves - objects that we study in our joint work - are a good example of proliferation of number theory into the modern world.

One can find them in cryptography and in state-of-the-art algorithms for secure communication (NSA current standards). They are used also in encryption protocols on chip credit cards.

Higher dimensional analogues of elliptic curves, Calabi-Yau manifolds, are popular among theoretical physicists, who use them to describe models of the universe.

(B)lucky prime 13 and beyond

In future work we would like to solve other instances of the equation \( x^2 + y^2 = z^p \) for large primes. Current techniques allow us to deal with exponents 17 and 19 and with a bit of luck with 13 too. To gain insight into higher exponents we need to develop genuinely new computational methods because even using the most powerful computers won’t help!