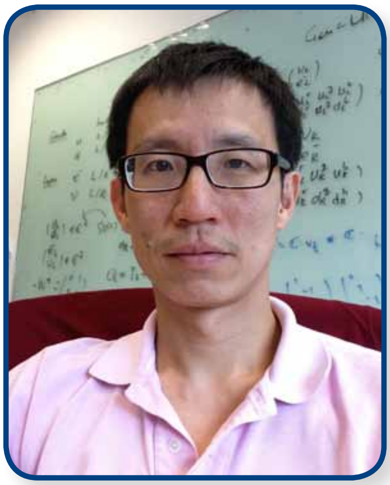

Professor Gan Wee Teck

Academic Profile

Prof Gan graduated with honours from Cambridge University in 1994 and obtained his PhD from Harvard University in 1998. He was a Veblen Research Instructor at Princeton University and the Institute for Advanced Study till 2001, after which he joined Princeton University as an Assistant Professor. This was followed by a faculty position at the University of California, San Diego where he was subsequently promoted to Associate Professor and then to full professorship in 2009. In 2011, he joined the Department of Mathematics at NUS.

Research Interests

- Number Theory and Representation Theory
- Automorphic forms, L-functions and the Langlands program

Contact Details

Department of Mathematics
National University of Singapore
Block S17, 10 Lower Kent Ridge Road
Singapore 119076

Tel: (+65) 6516-2739
Email: matgwt@nus.edu.sg
Webpage: http://www.math.nus.edu.sg/~matgwt

ELLIPTIC CURVES, MODULAR FORMS AND THE LANGLANDS PROGRAM

Professor Gan Wee Teck
Department of Mathematics

Innocuous Equations

Number theory is traditionally concerned with finding integer solutions to equations. For example, one may like to find integers A, B and C so that

$$A^2 + B^2 = C^2.$$

We all realize that solving this equation in integers is looking for right-angle triangles with integer sides, thanks to Pythagoras' theorem. One such triple of solutions is (3,4,5), but there are in fact infinitely many such Pythagorean triples and one knows (since antiquity) how to write all of them down.

However, Number Theory has the tendency of throwing up similar innocuous looking problems which turn out to be very difficult to solve. Here are two of them:

(i) (Fermat's Last Theorem)
Show that there are no nonzero integers satisfying $A^n + B^n = C^n$

(ii) (Congruent Number Problem)
Find all positive integers N which are the area of a right angle triangle with rational sides, i.e. such that the following system of simultaneous equations have solutions with A, B, C rational numbers:

$$A^2 + B^2 = C^2 \quad \text{and} \quad 2N = AB.$$

An integer N for which this system of equations have rational solutions is called a congruent number. For example, 6 is a congruent number since it is the area of right angle triangle with sides (3,4,5). The question is thus to determine if a given N is a congruent number.

Both these problems are easily understood by school children, but are notoriously hard to solve. Indeed, (i) was proposed by Fermat some 350 years ago, and was only resolved in 1995 by Andrew Wiles [1] (of Princeton University then). On the other hand, (ii) is still an open problem today.

It is natural to ask what significance the two problems above possess. As they stand, they are indeed mere idle curiosities, no more important than any other equations one might care to write down. However, in trying to resolve (i), generations of mathematicians were led to uncover many fundamental questions and subjects areas and to develop many sophisticated machineries, leading to the creation of the field of algebraic number theory. More pertinently, the eventual solution of (i) and the proposed approach to (ii) turns out to be related to an important class of objects known as Elliptic Curves.

Elliptic Curves

An elliptic curve is basically a curve in the plane described by a cubic equation of the form

$$Y^2 = aX^3 + bX + c,$$

with a, b, c rational numbers

Why are such cubic equations interesting? Well, it turns out that if one considers quadratic equations (like the Pythagorean equation), one knows that they have infinitely many rational solutions. On the other hand, if one considers equations of degree higher than 4 (such as the Fermat equation with large n), then an amazing theorem of Faltings [2] (winning him the Fields medal in 1986) says that they will only have finitely many rational solutions. Thus, cubic equations (i.e. elliptic curves) are very interesting because they happen to sit on the boundary between heaven and hell: which world do they belong to? The answer is: some elliptic curves will have finitely many rational points and some will have infinitely many. In fact, there is a very influential conjecture, the Birch-Swinnerton-Dyer conjecture (BSD) [3], which gives a criterion to decide whether a given elliptic curve E has finitely or infinitely many rational points. This criterion is expressed in terms of an analytic function, called the L-function L(s,E) of the elliptic curve, which is a function in a variable s. More precisely, BSD Conjecture: E has infinitely many rational solutions if and only if $L(1,E) = 0$.

The BSD conjecture is one of the seven Millennium Prize problems [4] singled out by the Clay Mathematics Institute: if you resolve it, you will receive US$1,000,000.

Here is how elliptic curves help in the problems (i) and (ii) above?

(i) (Fermat Last Theorem) One argues by contradiction. If a nonzero solution to Fermat's equation exists, we can use the nonzero integers (A,B,C) to write down an elliptic curve:

$$Y^2 = X\ (X - A^n)\ (X + B^n)$$

This elliptic curve will have some very special properties, so special that one begins to suspect that such a curve cannot exist. What Wiles did was to confirm this nonexistence.

(ii) (Congruent Number Problem) It is known that N is a congruent number if and only if the elliptic curve E_N defined by

$$Y^2 = X^3 - N^2X$$

has infinitely many rational solutions. By the BSD conjecture, this is conjecturally equivalent to $L(1, E_N) = 0$.

Thus, both problems (i) and (ii) are reduced to questions about elliptic curves. However, these questions about elliptic curves are still too hard to solve! It turns out that it would help a lot if one relates elliptic curves to another class of objects: Modular Forms. The connection between Elliptic Curves and Modular Forms is a very special case of a vast enterprise known as the Langlands Program.

The Langlands Program

The Langlands program owes its existence to the vision of Robert Langlands (Institute for Advanced Studies, Princeton) some 40 years ago (see [5]). It consists of a series of intricate conjectures which connects two seemingly unrelated and individually important areas of modern mathematics. One of these is number theory, which, as we noted above, is concerned with solving equations in integers; its modern study has evolved to that of a class of objects known as Galois representations (of which Elliptic Curves is an instance). The other is representation theory, of which a simple case is the theory of Fourier series; its modern study is concerned with a class of objects known as automorphic forms (of which Modular Forms is an instance). The deep conjectures of Langlands assert:

Galois representations and automorphic forms are, in very precise ways, essentially the same!

The "fact" that two classes of objects are the same is useful as it allows one to transfer a problem about one class of objects to the other, where it may be more readily solvable. In his resolution of Fermat's problem, what Wiles did was to build enough of this bridge between number theory and representation theory, so that he may transfer the question of nonexistence of a particular elliptic curve to the question of nonexistence of certain modular forms, and this latter question turns out to be trivial. For the congruent number problem, one needs to understand the L-function $L(s, E_N)$, and one expects that such L-functions are more easily understood if one has the bridge to pass to the world of modular forms.

To conclude, much of my own research has been focused on:

(a) Helping to build a part of the bridge or dictionary between number theory and representation theory; an example is my work with S. Takeda [6] on the local Langlands conjecture for GSp(4) and related groups.

(b) Using this dictionary as a tool to resolve interesting problems on either side of the Langlands program; an example is my work with B. H. Gross and D. Prasad [7] on some branching problems in representation theory.

The Langlands program has seen a lot of progress in the past decade, resulting in the proofs of many classic conjectures in number theory. Moreover, the underlying principle of the Langlands program is so universal that it has been applied in geometry and string theory. Some people have claimed that these ideas will lead to a grand unification of vastly different areas of mathematics. Only time will tell. ■

Reference

1. Wiles A., "Modular elliptic curves and Fermat's last theorem", *Ann. of Math.,* 141, no. 3, 443–551 (1995).

2. Faltings G., "Endlichkeitssätze für abelsche Varietäten über Zahlkörpern" [Finiteness theorems for abelian varieties over number fields], *Invent. Math 73,* no. 3, 349–366 (1983).

3. Birch B., Swinnerton-Dyer P., "Notes on Elliptic Curves (II)". *J. Reine Angew. Math. 165:* 79–108 (1965).

4. Clay Mathematics Institute, "Millenium Prize Problems", http://www.claymath.org/millennium/

5. Gelbart S., "An elementary introduction to the Langlands program", *Bull. Amer. Math. Soc. (N.S.)* 10, no. 2, 177–219 (1984).

6. Gan W. T. and Takeda, S., "The local Langlands conjecture for GSp(4)", *Ann. of Math.* (2) 173, no. 3, 1841-1882 (2011).

7. Gan W. T., Gross, B. H., Prasad D., "Symplectic local root numbers, central critical L-values and restriction problems in the representation theory of classical groups", *Asterisque* 346, 111-170 (2013).