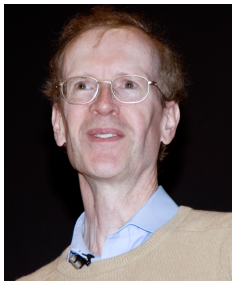


Sir Andrew John Wiles,
Abel Prize Laureate 2016

THE MODULARITY THEOREM

The modularity theorem asserts that every elliptic curve defined over the rational numbers is modular. In this note we give some background for the theorem, introducing the two involved concepts, elliptic curves and modular forms.

Denote by $\mathbb{H}$ the upper half of the complex plane, i.e. all complex numbers of positive imaginary part. A **modular form** of weight $2k$ for some positive integer k is a holomorphic function f on $\mathbb{H}$, such that for all integer 2×2-matrices $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ we have

$$f(\alpha z) = (cz + d)^{2k} f(z)$$

and such that f is holomorphic at the point of infinity, i.e. as $z \to i\infty$.

The action of the 2×2-matrix α on $z \in \mathbb{H}$ is given by the Möbius transformation

$$z \mapsto \frac{az + b}{cz + d}$$

Substituting $\alpha = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ we see that

$$f(z + 1) = f(z)$$

i.e the function is translation invariant. Since

$$e^{2\pi i(z+1)} = e^{2\pi iz + 2\pi i} = e^{2\pi iz}$$

we can write f as a function of $q = e^{2\pi iz}$. The condition that f is holomorphic at $z = i\infty$ is equivalent to the function being holomorphic at $q = 0$, so we can write

$$f(z) = \sum_{n \geq 0} a_n \, q^n, \quad q = e^{2\pi iz}$$

A famous modular form is the so-called **discriminant** function,

$$\Delta(z) = q \prod_{r=1}^{\infty} (1 - q^r)^{24}, \quad q = e^{2\pi iz}$$

Using this modular form we can produce another example

$$f(z) = \sqrt[12]{\Delta(z)\Delta(11z)}$$

The Fourier expansion of $f(z)$ as a function in q is given by

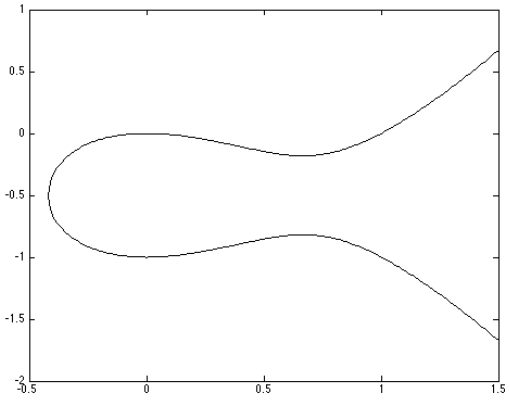
$$q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 \\ - 2q^9 - 2q^{10} + q^{11} - 2q^{12} + \dots$$

We will come back to this series, but first we introduce the other concept involved, elliptic curves.

Elliptic curves is a class of plane curves defined by polynomials of degree three. The equation

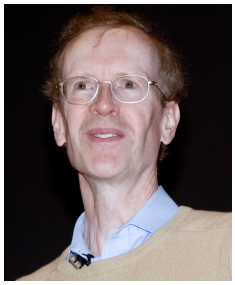
$$y^2 + y = x^3 - x^2$$

is an example of an **elliptic curve**.



The graph of the elliptic curve

$$E = \{(x, y) \in \mathbb{R}^2 \mid y^2 + y = x^3 - x^2\}$$



Sir Andrew John Wiles, Abel Prize Laureate 2016

We are interested in the number of integer solutions of the above equation modulo a prime number p, i.e. we look for solutions of the equation among the set of remainders $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$ when dividing by p. As an example let $p = 11$. Then $(x, y) = (10, 4)$ is a solution. The reason for that is that both sides of the equation give the same remainder when divided by 11;

$$4^2 + 4 = 20 \equiv 9 \pmod{11}$$

and

$$10^3 - 10^2 = 900 \equiv 9 \pmod{11}$$

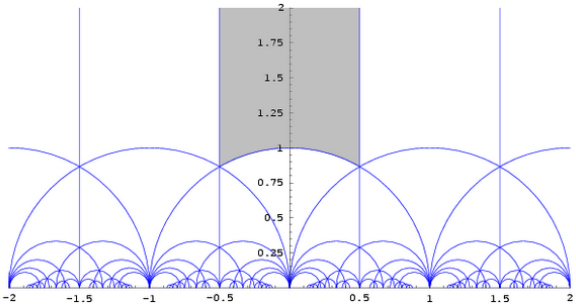
Let $\#E_p$ be the number of solutions of the above equation in the set of remainders $\mathbb{Z}_p$. For each prime number p let

$$a_p = p - \#E_p$$

For $p = 2$ there are 4 solutions of the given equation, $(0, 0)$, $(0, 1)$, $(1, 0)$ and $(1, 1)$, i.e. all possible remainders are solutions, and $a_2 = -2$. For $p = 3$ we have also four solutions; $(0, 0)$, $(0, 2)$, $(1, 0)$, $(1, 2)$, and $a_3 = -1$. For the next primes we have $a_5 = 1$ and $a_7 = -2$.

The surprising fact is that for each prime number p, the number a_p for this elliptic curve equals the Fourier coefficient of the modular form $f(z) = \sqrt[12]{\Delta(z)\Delta(11z)}$ given above. This type of phenomenon was first observed by Tanyama-Shimura, resulting in the TSW conjecture. TSW became a theroem and changed name to "The modularity Theorem" when Wiles gave a proof of it. Wiles proved that every semi-stable elliptic curve is modular. This is a nice way to say that the similarity of the two sequences of numbers, the Fourier coefficients of the modular form and the number of solutions modulo primes of the elliptic curve, is no coincidence.

The last piece of the FLT puzzle was introduced be Gerhard Frey. He claimed that if there exists a non-trivial solution of FLT, then there exist a non-modular elliptic curve. This conjecture was extended further by Jean-Pierre Serre and later proved by Ken Ribet.



The figure illustrate the action on the upper half-plan of the modular group $SL_2(\mathbb{Z})$. The grey area is often called the fundamental area.

p	$\#E_p$	a_p
2	4	-2
3	4	-1
5	4	1
7	9	-2
11	10	1
13	9	4
17	19	-2
19	19	0

The sequence of numbers in the last column should be compared to the prime number coefficients of the Fourier expansion of the modular form $\sqrt[12]{\Delta(z)\Delta(11z)}$ given on the previous page.