Sign changes and the construction of supersingular elliptic curves

Dr. B. Kane, Department of Mathematics

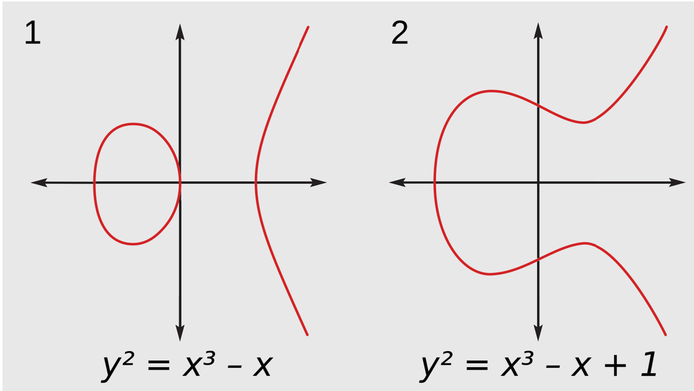
Elliptic curves have recently appeared in cryptography after playing a vital role in the solution of Fermat's Last Theorem; that for $n > 2$ there is no non-trivial integral solution to $x^n + y^n = z^n$. **Elliptic curves** are solutions to

$$y^2 = f(x) \ ,$$

where $f(x)$ is a degree 3 polynomial (such as $f(x) = x^3 - x$).

There is a natural question about how to construct an elliptic curve with a given endomorphism ring; roughly speaking, nice functions from the elliptic curve to itself. An algorithm was devised to do so by Chevyrev and Galbraith.

Unfortunately, although Chevyrev and Galbraith could prove that the algorithm would give the correct answer if it stopped, they were unable to prove that it halted. Instead, they were able to show that it would halt unless an unusual situation occurred. They conjectured that this indeed never occurred. The project in question showed that their conjecture was true, and in turn, that their algorithm indeed halts.



Examples of elliptic curves.
Source: GYassineMrabetTalk, CC BY-SA 3.0

One of the main steps of the project was to move the question from one area to another. The conjecture essentially states that there are no two theta functions that "look the same locally" but the coefficients of one dominates the other one. A **theta function** has the shape

$$\vartheta(\tau) = \sum_{\vec{x}} e^{2\pi i Q(x)\tau} \ .$$

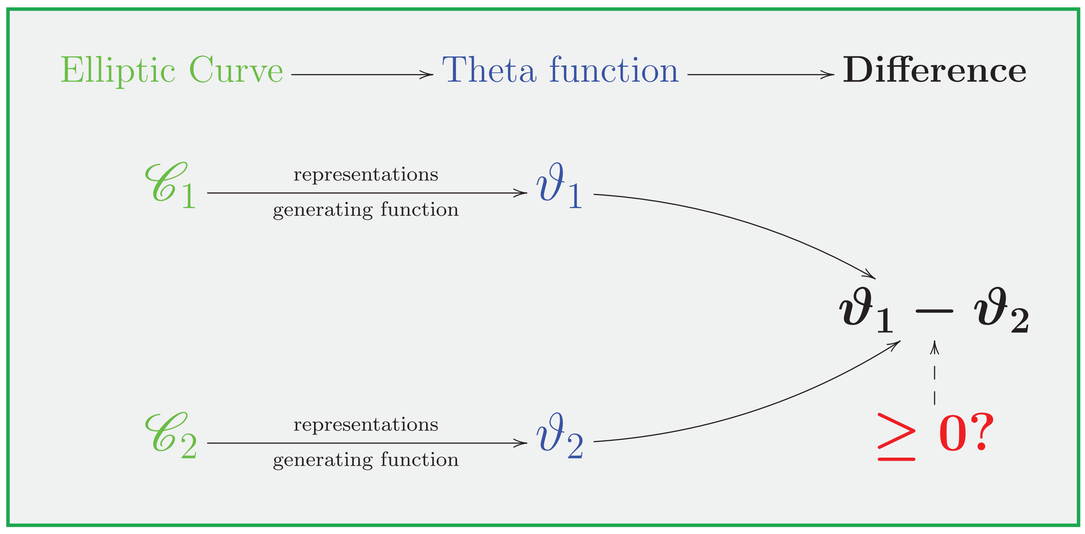
Here Q is a **quadratic form** (like a sum of squares $Q(x, y) = x^2 + y^2$). Writing $\vartheta(\tau) = \sum_{n \geqslant 0} a(n) e^{2\pi i n \tau}$, their conjecture basically says that for $Q = Q_1$ and $Q = Q_2$, one cannot have the $a(n)$ always bigger for Q_1. These theta functions are special, though; they satisfy a lot of symmetry and their difference is known as a cuspidal modular form (cusp form). Fourier coefficients of cusp forms alternate, leading to the conjecture's resolution.

There are natural questions remaining. Firstly, one can consider sign changes in a related question when quadratic forms are replaced with quadratic polynomials. Secondly, the speed of the algorithm depends on the first sign change, so one can investigate how quickly the first sign change occurs. There are some good known results for integral weight modular forms in this direction, but we require half-integral weight for this application.

Weight	Level/ form	Bound
integer k	p/ any	$k^{6+\varepsilon} p^{4+\varepsilon}$
integer k	N/ eigenform	$(k^2 N)^{2+\varepsilon}$
half-integer $k - \frac{1}{2}$	N/ any	$(k+N)^{5+\varepsilon} N$
Conjecture: $\frac{3}{2}$	p/ any	$p^{1+\varepsilon}$

Known bounds for first sign changes

The investigation of sign changes has a long history going back at least to Siegel, but its applicability to combinatorial and arithmetic questions seems to be a new direction. It would be interesting to see if there are other questions where control of the sign changes leads to better understanding of combinatorial identities or inequalities.



Further Reading:

- K. Fung and B. Kane, *On sign changes of cusp forms and the halting of an algorithm to construct a supersingular elliptic curve with a given endomorphism ring*, preprint.
- D. Jetchev and B. Kane, *Equidistribution of Heegner points and ternary quadratic forms*, Math. Ann. **350** (2011), 501-532.