Oxford
Mathematics
Alphabet

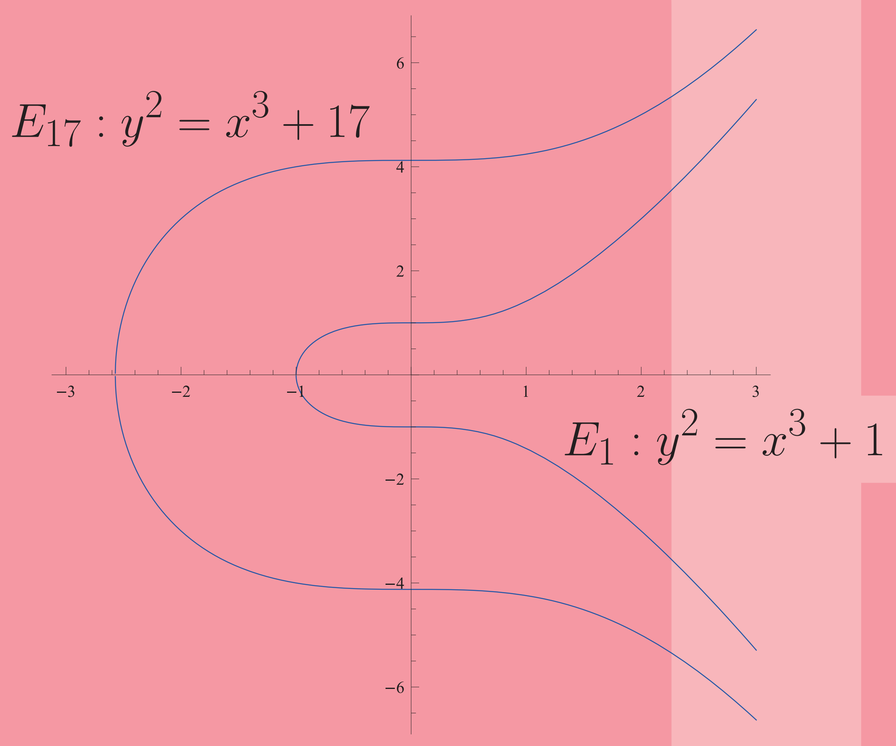
E *is for* elliptic curves

Appearing everywhere from state-of-the-art cryptosystems to the proof of Fermat's Last Theorem, elliptic curves play an important role in modern society and are the subject of much research in number theory today.

An elliptic curve E defined over the rational numbers (fractions) is a smooth plane curve of the form

$$y^2 = x^3 + Ax + B$$

together with a special point $\mathcal{O}$ "at infinity".

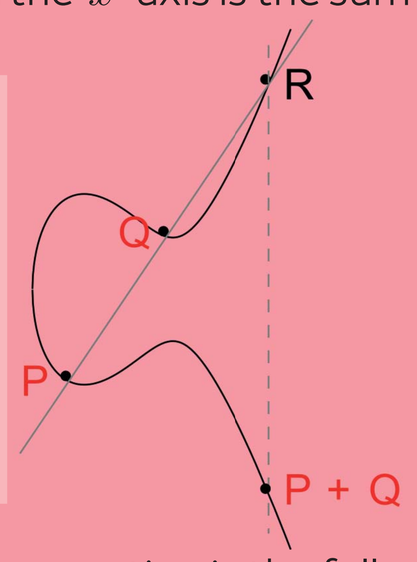


A fundamental problem in the study of elliptic curves is the following: given an elliptic curve E defined over the rationals, find its set $E(\mathbb{Q})$ of rational points. For example, the elliptic curve $E_1 : y^2 = x^3 + 1$ has precisely 6 rational points, given by the set $\{\mathcal{O}, (-1, 0), (0, \pm 1), (2, \pm 3)\}$. The elliptic curve $E_{17} : y^2 = x^3 + 17$ has, among its rational points, the following:

$$\mathcal{O}, (-1, \pm 4), (-2, \pm 3), (2, \pm 5), (4, \pm 9), \left(\frac{1}{4}, \pm\frac{33}{8}\right),$$
$$(8, \pm 23), \left(-\frac{8}{9}, \pm\frac{109}{27}\right), \left(\frac{19}{25}, \pm\frac{522}{125}\right), (43, \pm 282),$$
$$(52, \pm 375), \left(-\frac{64}{25}, \pm\frac{59}{125}\right), \left(\frac{94}{25}, \pm\frac{1047}{125}\right), \ldots$$

While E_1 has finitely many rational points, E_{17} has infinitely many rational points - something that cannot be seen by looking at their real-valued graphs.

It turns out that the set $E(\mathbb{Q})$ of rational points enjoys additional structure: it is an abelian group. This means that given rational points P and Q, there is a way to produce the sum $P + Q$, and this is another rational point. Indeed, there is a geometric way to carry out this addition. Draw the line through P and Q. This intersects the elliptic curve in a third rational point R, and the reflection of R in the x-axis is the sum $P + Q$, as seen here:



One difficult open question is the following: given an elliptic curve E over the rationals, how do we find the generators of $E(\mathbb{Q})$? In fact, giving an algorithm to calculate how many (independent infinite-order) generators there are - a quantity known as the algebraic rank of $E(\mathbb{Q})$ - would be a breakthrough. This is the subject of the Birch and Swinnerton-Dyer conjecture, one of the Clay Mathematics Institute's million-dollar Millennium Prize Problems.

Dr Jennifer Balakrishnan
Titchmarsh Research Fellow and Junior Research Fellow at Balliol College

UNIVERSITY OF OXFORD
Mathematical Institute

Oxford
Mathematics

For more about elliptic curves visit
www.maths.ox.ac.uk/r/alphabet