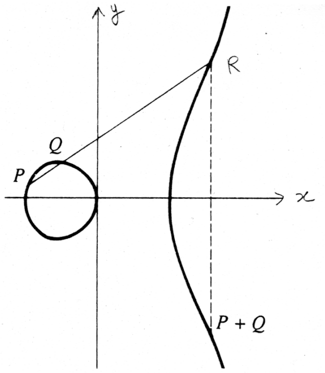
Rational torsion points on elliptic curves

Amod Agashe
agashe@math.fsu.edu

An *elliptic curve* is the set of solutions to an equation of the form $y^2 = x^3 + ax + b$, where a and b are rational numbers such that $4a^3 + 27b^2 \neq 0$. For example, if we take $a = -1$ and $b = 0$, then we get the equation $y^2 = x^3 - x$, whose graph consists of the two thick curved pieces in the figure below:



Elliptic curves have been studied for decades, and have recently found applications in cryptography.

Our interest is in the set of points on an elliptic curve whose coordinates are rational numbers; such points are called *rational points* on the elliptic curve. For example, $(1, 0)$ is a rational point on the curve $y^2 = x^3 - x$ sketched in the figure above.

One of the nice properties of elliptic curves is that given two points P and Q on the curve, we can find a third point, called the "sum" of P and Q, and denoted $P + Q$, as follows. We first join P and Q by a straight line (if $P = Q$, we take the tangent at $P = Q$). This straight line will intersect the curve at another point; call it R. Then we draw a vertical line through R, which will interesect the curve at yet another point; we define $P + Q$ to be this latter point. This process is illustrated in the figure above. If P and Q are rational points, then so is $P + Q$.

There is a special point on the curve called the *zero element* which lies infinitely high up on the y-axis. Any vertical line (i.e., a line parallel to the y-axis) is considered to pass through this point. The set of all rational points along with the zero element is closed under the addition operation described above, and is said to form a *group*.

Our goal is to study the rational points which when added to themselves finitely many times give the zero element (i.e., the procedure for adding such a point to itself produces a vertical line after finitely many attempts). Such points are called *torsion points*. In our research conducted under the FYAP grant, we took an initial first step in describing where such points "come from" and how many such points there are. There is much more work to be done in order to get a completely satisfactory answer, and we have a program for a significant part of the problem. Our work has applications to the Birch and Swinnerton-Dyer conjecture, part of which is one of the seven Clay millenial prize problems that carry a million dollar reward each for their resolution.