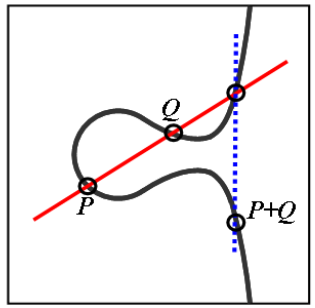
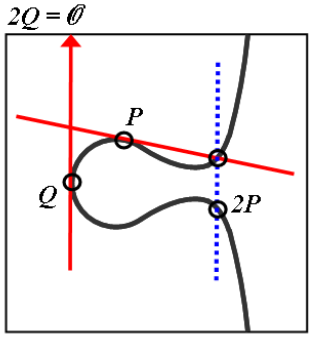
THEOREM OF THE DAY

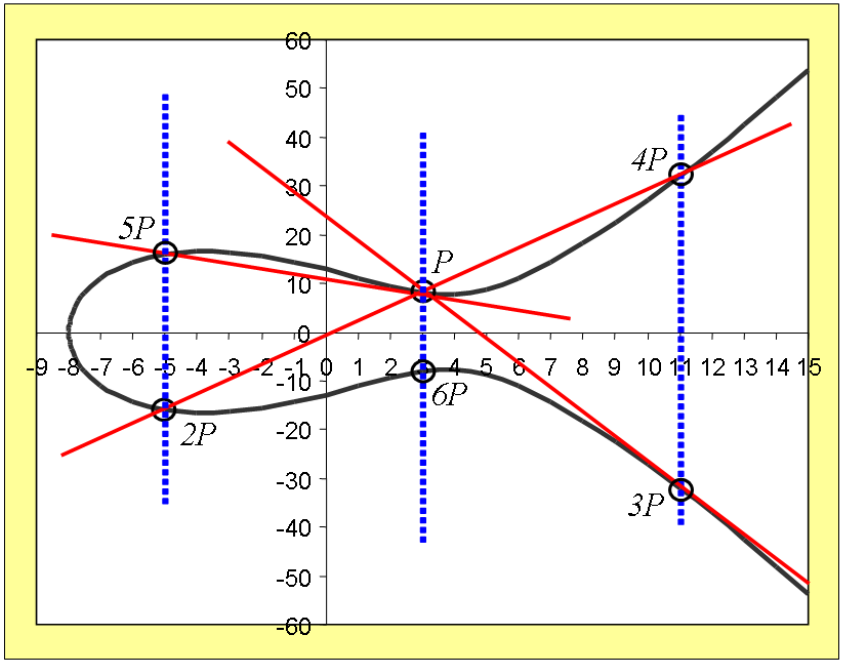
The Lutz-Nagell Theorem *For the elliptic curve $y^2 = x^3 + ax^2 + bx + c$, with a, b, and c integers and having (non-zero) discriminant function $D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$, let $P = (X, Y)$ be a rational point of finite order greater than 1. Then X and Y are integers and either Y divides D or $Y = 0$ and P has order 2.*

Addition of points P and Q on elliptic curve E: $P + Q$ is the mirror image of the unique third point at which the line through P and Q again intersects E. If the line is a tangent at, say, P, then this third point is at P itself. If the line is vertical ($Q = -P$) then the third point is taken to be 'the point at infinity', denoted $\mathscr{O}$; thus $P + -P = \mathscr{O}$.

Doubling of a point on E: take the tangent to E at that point; if the tangent is vertical (as at Q, here) then, as above, it meets E again at point $\mathscr{O}$: $2P = \mathscr{O}$, and P is said to have 'order 2'. Otherwise, $2P$ is defined to be the mirror image of where the tangent (which counts as a double intersection) meets E for the third time.







The points of an elliptic curve E, together with the point $\mathscr{O}$ (the identity), form an abelian group under addition, carried out as shown above left. The graph, above right, shows the elliptic curve $E : y^2 = x^3 - 43x + 166$. Consider the two points $P = (3, 8)$ and $2P = (-5, -16)$. We get $3P = (3, 8) + (-5, -16) = (11, -32)$. Continuing, $3P + P$ is just the mirror image of $3P$ because the line from $3P$ to P is a tangent at $3P$. By the same token, doubling $3P$ makes $6P$ the mirror image of P, and now $7P = P + 6P = \mathscr{O}$. The point $P = (3, 8)$ thus has *finite order* 7, because $7P = \mathscr{O}$. Note that the discriminant of E, which has value $D = -425984$, is divisible by 8, as guaranteed by Lutz-Nagell. The curve meets the x-axis at $(-7.9865..., 0)$ which has order 2 but is non-rational (thus failing narrowly to illustrate the final case of the Lutz-Nagell theorem!)

The structure of the group defined by an elliptic curve is largely determined by the points of finite order. The importance of this group is amply demonstrated by Andrew Wiles' resolution of Fermat's Last Theorem by proving that all rational elliptic curves define modular forms. The Lutz-Nagell theorem, discovered in the 1930s by Elisabeth Lutz, in France, and Trygve Nagell, in Norway, is thus an indispensable tool in algebraic number theory.

Web link: www.theoremoftheday.org/Docs/RezaAkhtar.pdf, Reza Akhtar's notes (the origin of my the example curve E).

Further reading: *Rational Points on Elliptic Curves* by Joseph H. Silverman and John Tate, Springer-Verlag, New York, 1994.