Elliptic Curves over $\mathbb{Q}$

**Theorem 1 (Mordell, 1922):** If $E/\mathbb{Q}$ is an elliptic curve, then $E(\mathbb{Q})$ is finitely generated, i.e. there exist finitely many points $P_1, \ldots, P_s \in E(\mathbb{Q})$ such that every $P \in E(\mathbb{Q})$ has the form $P = \sum n_i P_i$ (for some $n_i \in \mathbb{Z}$). Thus, the torsion subgroup

$$E(\mathbb{Q})_{tor} := \bigcup_{N \geq 1} E(\mathbb{Q})[N]$$

is finite and there is an integer $r \geq 0$ such that

$$E(\mathbb{Q}) \simeq E(\mathbb{Q})_{tor} \times \mathbb{Z}^r.$$

**Remark 1)** There is no general (proved) algorithm for determining $E(\mathbb{Q})$ or even for calculating the rank $r$. However, there is a conjectural algorithm (which depends on the validity of the Birch/Swinnerton-Dyer Conjecture).

**Remark 2)** The torsion subgroup $E(\mathbb{Q})_{tor}$ is relatively easy to determine by using the Theorem of Nagell-Lutz (see below). Moreover, from a deep Theorem of Mazur (1978) it follows that

$$|E(\mathbb{Q})_{tor}| \leq 16.$$

**Theorem 2 (Nagell-Lutz):** Let $E/\mathbb{Q}$ be an elliptic curve defined by $y^2 = f(x)$ with $f(x) \in \mathbb{Z}[x]$ a monic cubic. Then:

$$P = (x, y) \in E(\mathbb{Q})_{tor} \Rightarrow x, y \in \mathbb{Z} \text{ and either } y = 0 \text{ or } y | \Delta_E.$$

**Remark:** It is clear that there are only finitely many pairs $(x, y)$ which satisfy the condition on the right hand side.
Example 1) \( E : y^2 = x^3 + 1 \) and \( P = (2, 3) \).

We have \( P \in E(\mathbb{Q})[6] \leq E(\mathbb{Q})_{tor} \) (because \( 4P = (0, -1) = -2P \)). Here \( \Delta_E = -432 = -2^43^3 \), and so \( 3|\Delta_E \).

2) \( E : y^2 = x^3 - 36x \) and \( P = (-3, 9) \).

Here \( 2P = \left(\frac{25}{4}, -\frac{35}{8}\right) \). Thus (by Nagell-Lutz) \( 2P \notin E(\mathbb{Q})_{tor} \), and hence also \( P \notin E(\mathbb{Q})_{tor} \).

Thus: the converse of the Nagell-Lutz Theorem does not hold. Indeed, \( P = (-3, 9) \) has integer coordinates and \( 9|64(36)^3 = \Delta_E \), but \( P \notin E(\mathbb{Q})_{tor} \).

Remark: The curves \( E_n : y^2 = x^3 - n^2x \) are closely connected with the problem of classifying areas of right rational triangles ( = right angled triangles with rational sides), for we have:

Fact: If \( n > 0 \) is a squarefree integer, then there exists a right rational triangle of area \( n \Leftrightarrow E_n \) has a point of infinite order.

Example. The triangle with sides \((3, 4, 5)\) has area \( \frac{1}{2}3(4) = 6 \), so by the above Fact the curve \( E_6 \) has a point of infinite order. Indeed, \( P = (-3, 9) \) is such a point; cf. Example 2 above.

Note: More information about areas of rational right triangles can be found in the textbook

N. Koblitz, Introduction to Elliptic Curves and Modular Forms

Indeed, Koblitz uses the above question of areas of rational right triangles as a motivation for studying elliptic curves and modular forms.