# Nagell-Lutz theorem

| | |
|---|---|
| Canonical name | NagellLutzTheorem |
| Date of creation | 2013-03-22 13:52:02 |
| Last modified on | 2013-03-22 13:52:02 |
| Owner | alozano (2414) |
| Last modified by | alozano (2414) |
| Numerical id | 4 |
| Author | alozano (2414) |
| Entry type | Theorem |
| Classification | msc 14H52 |
| Related topic | EllipticCurve |
| Related topic | MordellWeilTheorem |
| Related topic | RankOfAnEllipticCurve |
| Related topic | TorsionSubgroupOfAnEllipticCurveInjectsInTheReductionOfTheCurve |
| Related topic | ArithmeticOfEllipticCurves |
| Defines | Nagell-Lutz theorem |

The following theorem, proved independently by E. Lutz and T. Nagell, gives a very efficient method to compute the torsion subgroup of an elliptic curve defined over $\mathbb{Q}$.

**Theorem 1** (Nagell-Lutz Theorem)**.** *Let $E/\mathbb{Q}$ be an elliptic curve with Weierstrass equation:*

$$y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Z}$$

*Then for all non-zero torsion points $P$ we have:*

1. *The coordinates of $P$ are in $\mathbb{Z}$, i.e.*

$$x(P), y(P) \in \mathbb{Z}$$

2. *If $P$ is of order greater than $2$, then*

$$y(P)^2 \quad \textit{divides} \quad 4A^3 + 27B^2$$

3. *If $P$ is of order $2$ then*

$$y(P) = 0 \quad \textit{and} \quad x(P)^3 + Ax(P) + B = 0$$

# References


[1] E. Lutz, *Sur l'equation $y^2 = x^3 - Ax - B$ dans les corps p-adic*, J. Reine Angew. Math. 177 (1937), 431-466.

[2] T. Nagell, *Solution de quelque problemes dans la theorie arithmetique des cubiques planes du premier genre*, Wid. Akad. Skrifter Oslo I, 1935, Nr. 1.

[3] James Milne, *Elliptic Curves*, `http://www.jmilne.org/math/CourseNotes/math679.htmlonli` course notes.

[4] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*. Springer-Verlag, New York, 1986.