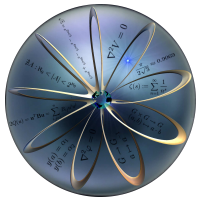

planetmath.org

Math for the people, by the people.

Mazur's theorem on torsion of elliptic curves

Canonical name	MazursTheoremOnTorsionOfEllipticCurves
Date of creation	2013-03-22 13:51:59
Last modified on	2013-03-22 13:51:59
Owner	alozano (2414)
Last modified by	alozano (2414)
Numerical id	5
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	Mazur's theorem

Theorem 1 (Mazur)**.** *Let $E/\mathbb{Q}$ be an elliptic curve. Then the torsion subgroup $E_{\text{torsion}}(\mathbb{Q})$ is exactly one of the following groups:*

$$\mathbb{Z}/N\mathbb{Z} \quad 1 \leq N \leq 10 \quad \textit{or} \quad N = 12$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z} \quad 1 \leq N \leq 4$$

Note: see Nagell-Lutz theorem for an efficient algorithm to compute the torsion subgroup of an elliptic curve defined over $\mathbb{Q}$.

References

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

[2] Barry Mazur, *Modular curves and the Eisenstein ideal*, IHES Publ. Math. 47 (1977), 33-186.

[3] Barry Mazur, *Rational isogenies of prime degree*, Invent. Math. 44 (1978), 129-162.