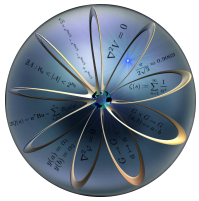

planetmath.org

Math for the people, by the people.

Hasse's bound for elliptic curves over finite fields

Canonical name	HassesBoundForEllipticCurvesOverFiniteFields
Date of creation	2013-03-22 13:55:41
Last modified on	2013-03-22 13:55:41
Owner	alozano (2414)
Last modified by	alozano (2414)
Numerical id	5
Author	alozano (2414)
Entry type	Theorem
Classification	msc 14H52
Synonym	Hasse's bound
Related topic	LSeriesOfAnEllipticCurve
Related topic	EllipticCurve
Related topic	BadReduction
Related topic	ArithmeticOfEllipticCurves

Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$ with $q = p^r$ elements ($p \in \mathbb{Z}$ is a prime). The following theorem gives a bound of the size of $E(\mathbb{F}_q)$, N_q, i.e. the number points of E defined over $\mathbb{F}_q$. This was first conjectured by Emil Artin (in his thesis!) and proved by Helmut Hasse in the 1930's.

Theorem 1 (Hasse)**.**

$$\mid N_q - q - 1 \mid \leq 2\sqrt{q}$$

Remark: Let $a_p = p + 1 - N_p$ as in the definition of the L-series of an ellitpic curve. Then Hasse's bound reads:

$$\mid a_p \mid \leq 2\sqrt{p}$$

This fact is key for the convergence of the L-series of E.