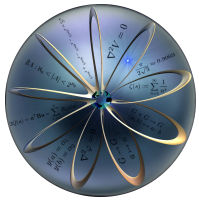

planetmath.org

Math for the people, by the people.

the arithmetic of elliptic curves

Canonical name	TheArithmeticOfEllipticCurves
Date of creation	2013-03-22 15:06:19
Last modified on	2013-03-22 15:06:19
Owner	alozano (2414)
Last modified by	alozano (2414)
Numerical id	15
Author	alozano (2414)
Entry type	Topic
Classification	msc 14H52
Classification	msc 11G05
Synonym	concepts in the theory of elliptic curves
Related topic	EllipticCurve
Related topic	CriterionOfNeronOggShafarevich
Related topic	HassesBoundForEllipticCurvesOverFiniteFields
Related topic	BirchAndSwinnertonDyerConjecture2
Related topic	RankOfAnEllipticCurve
Related topic	MazursTheoremOnTorsionOfEllipticCurves
Related topic	TorsionSubgroupOfAnEllipticCurveInjectsInTheReductionOfTheCurve

The Arithmetic of Elliptic Curves

An *elliptic curve* over a field K is a projective nonsingular curve E defined over K of genus 1 together with a point $O \in E$ defined over K. In the simple case $K = \mathbb{Q}$ every elliptic curve is isomorphic (over $\mathbb{Q}$) to a curve defined by an equation of the form:

$$y^2 = x^3 + Ax + B$$

where A, B are integers. The most remarkable feature of an elliptic curve is the fact that the group of points can be given the structure of a group.

The theory of elliptic curves is a very rich mix of algebraic geometry and number theory (arithmetic geometry). As in many other areas of number theory, the concepts are simple to state but the theory is extremely deep and beautiful. The intrinsic arithmetic of the points on an elliptic curve is absolutely compelling. The most prominent mathematicians of our time have contributed in the development of the theory. The ultimate goal of the theory is to completely understand the structure of the points on the elliptic curve over any field F and being able to find them.

1.1 Basic Definitions

1. For a basic exposition of the subject the reader should start with the entry `http://planetmath.org/EllipticCurve`elliptic curve (defines elliptic curve, the group law and gives some examples with graphs, also treats elliptic curves over the complex numbers).

2. Some basic objects attached to an elliptic curve: `http://planetmath.org/JInvariant`j-invariant, discriminant and invariant differential. The j-invariant `http://planetmath.org/J` elliptic curves up to isomorphism.

3. Isogeny, the dual isogeny and the Frobenius morphism.

4. Elliptic curves over finite fields: good reduction, bad reduction, multiplicative reduction, additive reduction, cusp, node.

5. One of the most important objects that one can associate to an elliptic curve is the `http://planetmath.org/LSeriesOfAnEllipticCurve`L-series (the entry defines the `http://planetmath.org/LSeriesOfAnEllipticCurve`L-series of an elliptic curve and also talks about analytic continuation).

6. The conductor of an elliptic curve is an integer quantity that measures the arithmetic complexity of the curve (the entry contains examples).

7. The Tate module of an elliptic curve (it is also defined in the entry inverse limit).

8. The canonical height on an elliptic curve (over $\mathbb{Q}$).

9. The height matrix and the elliptic regulator of an elliptic curve.

1.2 Elliptic Curves over Finite Fields

1. See `http://planetmath.org/BadReduction2`bad reduction.

2. The criterion of Néron-Ogg-Shafarevich.

3. Supersingular reduction.

4. Hasse's bound for elliptic curves over finite fields.

1.3 The Mordell-Weil Group $E(K)$

1. The structure of $E(K)$ is given by the Mordell-Weil theorem (see also `http://planetmath.org/RankOfAnEllipticCurve`this entry). The main two ingredients of the proof of the theorem are the concept of height function and the so-called descent theorem.

2. The free rank of the abelian group $E(K)$ is called the `http://planetmath.org/RankOfAnElli` of an elliptic curve (the entry contains examples).

3. Together with the Mordell-Weil group, one defines two other rather important groups: the Selmer groups and the Tate-Shafarevich group. The Tate-Shafarevich group (or "Sha") measures the failure of the Hasse principle on the elliptic curve.

4. Some examples: Mordell curves.

1.4 The Torsion Subgroup of $E(K)$

1. The Nagell-Lutz Theorem.
2. Mazur's theorem on torsion of elliptic curves (a classification of all possible torsion subgroups).
3. Examples of torsion subgroups of elliptic curves (includes examples of all possible subgroups).
4. A way to determine the torsion group: the torsion subgroup of an elliptic curve injects in the reduction of the curve.

1.5 Computing the Rank

1. Read about the `http://planetmath.org/RankOfAnEllipticCurve`rank.
2. A bound for the rank of an elliptic curve.

1.6 Complex Multiplication

1. Definition of the `http://planetmath.org/EndomorphismRing`endomorphism ring and complex multiplication.
2. Examples of elliptic curves with complex multiplication.
3. A connection between complex multiplication and class field theory: abelian extensions of quadratic imaginary number fields.
4. Definition of Grössencharacters, in general.

1.7 Famous Problems and Conjectures

1. Fermat's Last Theorem was finally solved using the theory of elliptic curves and modular forms.
2. The Birch and Swinnerton-Dyer conjecture (relating the L-series of an elliptic curve with the algebraic rank).
3. The Taniyama-Shimura-Weil Conjecture (now a theorem!).

1.8 Cryptography

1. Cryptography and Number Theory.
2. The elliptic curve discrete logarithm problem.
3. The Diffie-Hellman key exchange.

References

[1] James Milne, *Elliptic Curves*, online course notes. `http://www.jmilne.org/math/CourseNotes/math679.html`http://www.jmilne.org/math/Co

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

[3] Joseph H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer-Verlag, New York, 1994.

[4] Goro Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*. Princeton University Press, Princeton, New Jersey, 1971.

Note: If you want to contribute to this entry, please send an email to the author (alozano).