Math 8620 – Algebraic Geometry: Elliptic curves

Lloyd West

Introduction

This course is a first introduction to algebraic and arithmetic geometry, focusing on the geometry and arithmetic of curves, especially elliptic curves.

To give a flavor of the course, the next section introduces elliptic curves very briefly.

Elliptic Curves

An **elliptic curve** is defined by a certain kind of cubic equation in two variables; for example

$$E: y^2 = x^3 - 25x \tag{0.0.1}$$

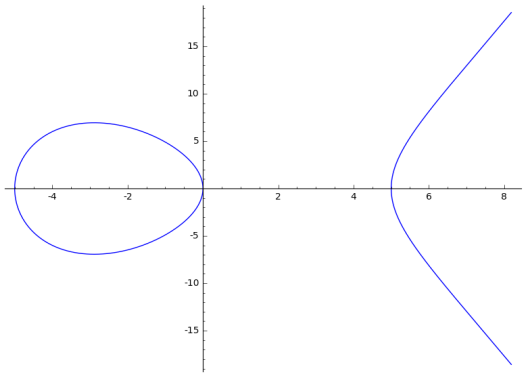
Let K be any field containing $\mathbb{Q}$. Then we can define the following set

$$E(K) = \{(\alpha, \beta) \in K \times K : \beta^2 = \alpha^3 - 25\alpha\} \cup \{\mathcal{O}\}$$

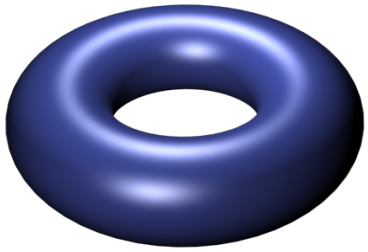
consisting of solutions to the equation E in the field K, together with a special element $\mathcal{O}$.

Remarkably, the solutions set $E(K)$ is endowed with a natural **abelian group structure** for which $\mathcal{O}$ is the identity element.

We can plot the set of real solutions, $E(\mathbb{R}) - \{\mathcal{O}\}$, as a plane curve:

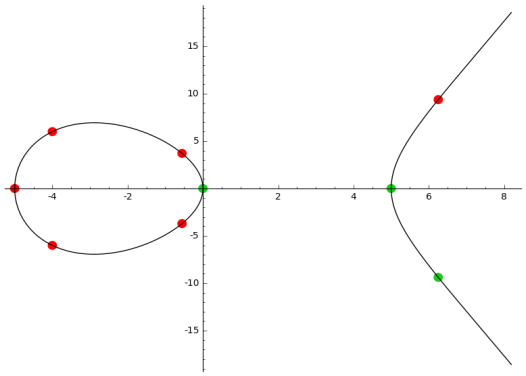


However, the geometric nature of the solution set is best seen over the complex numbers; the set $E(\mathbb{C})$ has the structure of a **complex torus**:



Over the complex numbers, the group structure may be described very simply using the nineteenth century theory of Weierstrass $\wp$-functions: this theory gives an isomorphism $E(\mathbb{C}) \cong \mathbb{C}/(\mathbb{Z} + \omega\mathbb{Z})$, for a certain $\omega \in \mathbb{C} - \mathbb{R}$.

The *arithmetic* theory of elliptic curves is much more subtle. Here is a plot of some of the **rational points** – i.e. points in $E(\mathbb{Q})$ – for the curve given by equation (1):



It is know that the group $E(\mathbb{Q})$ of rational points of an elliptic curve is **finitely generated** (this is the celebrated 1922 theorem of Mordel). In the above picture the three generators have been colored green.

As a finitely generated abelian group, $E(\mathbb{Q})$ decomposes as

$$E(\mathbb{Q}) = E_{\text{tors}}(\mathbb{Q}) \oplus \mathbb{Z}^r$$

The number of non-torsion generators r is called the **rank** of $E(\mathbb{Q})$. In the example, the torsion subgroup $E_{\text{tors}}(\mathbb{Q})$ is generated by the two green points on the x-axis. The remaining green point is a generator of the non-torsion part; the rank in this example is 1.

There is an effective algorithm to determine the torsion part $E_{\text{tors}}(\mathbb{Q})$ for any given elliptic curve E. Moreover, by a deep result of Mazur, we know that $|E_{\text{tors}}(\mathbb{Q})| \leqslant 16$

In contrast, the rank of a general elliptic curve remains a very mysterious quantity. There is an algorithm to compute the rank of a given curve, based on the method of **descent**, dating back to Fermat (1600s), but it is still not known to terminate unconditionally. For a 'typical' elliptic curve, r tends to be small, mostly 0 or 1. Recent work of Bhargava and Shankar (2011) has shown that the 'average' rank of elliptic curves over $\mathbb{Q}$ is at most 7/6. On the other hand, curves are known that have $r = 24$. It is not known whether r can be arbitrarily large.

We can often obtain information about the rank and many other aspects of E by studying the **reduction mod** p; that is, by studying the set of solutions $E(\mathbb{F}_{p^n})$ over finite fields. For example, the famous conjecture of Birch and Swinnerton-Dyer links the rank to the sizes of $E(\mathbb{F}_p)$ as p varies (this information is encoded in the **L-function** of the curve).

The groups $E(\mathbb{F}_{p^n})$ are the source of exceptionally secure and efficient cryptographic codes. Accordingly **elliptic curve cryptography** underlies a great deal of modern commerce.

Elliptic curves are ubiquitous in number theory. Many ancient and appealing problems such as **congruent number problem** lead directly to a deep study of elliptic curves. Define an integer to be a **congruent number** if it is the area of a right triangle with three rational number sides. For example, 6 is congruent number, since it is the area of the 3,4,5 triangle. It turns out that determining whether a prime p is a congruent number is equivalent to determining the whether the rank of the elliptic curve

$$E_p : y^2 = x^3 - p^2 x$$

is positive. The problem of finding an algorithm to solve this question has been around for at least 1000 years. It remains unsolved.

Course Aims

In the first third of the course, students will learn the necessary concepts and theorems from algebraic geometry needed to define the group law on an elliptic curve, both in terms of the cord-and-tangent construction and in terms of Jacobians of genus one curves. Key topics include: affine and projective varieties; dimension; (non)-singular points and tangent space; properties of morphisms; intersection multiplicity; divisors; genus; Riemann-Hurwitz; Riemann-Roch; Jacobians. In this section we shall not aim for complete generality, aiming instead at a working knowledge of algebraic geometry of curves.

In the remainder of the semester, students will learn complete proofs of the basic results about the arithmetic of elliptic curves – such as the Mordell-Weil theorem. In the process, students will become familiar with the following widely-applicable ideas from arithmetic geometry:

- abelian varieties and isogenies
- models over local and global fields
- moduli (j-line)
- reduction mod $\mathfrak{p}$
- zeta-functions
- statement of Weil Conjectures for curves
- heights
- descent (in the sense of Fermat)
- local-to-global principle
- torsors and Galois actions
- Galois cohomology (up to $\mathfrak{n} = 2$ only)
- Selmer and Tate-Shafarevich groups

Depending on time, additional topics may be covered, such as applications to cryptography, higher genus curves and L-functions.

In exercises, students will become proficient in applying these concepts to prove theoretical results and to make concrete computations with elliptic curves (for example, computing rational points by descent), both 'by hand' and with computer packages such as sage.

This course will complement the Galois-Grothendieck seminar Fall 2016 topic of Abelian Varieties; accordingly, students are encouraged to attend at least the first few weeks of that seminar. This course should also be excellent preparation for students wishing to attend the arithmetic geometry conference and mini-course by Dick Gross at UVA in spring 2017.

Prerequisites

Galois Theory is the only essential prerequisite. Exposure to algebraic number theory and commutative algebra will be very helpful, but are not required.

Reading

The course text will be Silverman's *Arithmetic of Elliptic Curves* [Sil09].

For an easy to read introduction, I recommend Silverman and Tate's *Rational Points on Elliptic Curves* [ST92] or Cassels, *Lectures on elliptic curves* [Cas91].

The following survey articles are highly recommended:

- Mazur, *Arithemetic on curves* [Maz86]
- Ho, *How many rational points does a random curve have?* [Ho14]
- Rubin and Silverberg, *A brief guide to algebraic number theory* [RS02]

We shall refer to the following texts for background in Algebraic Geometry or Number Theory:

- Shafarevich, *Basic algebraic geometry. 1* [Sha13]
- Swinnerton-Dyer, *A brief guide to algebraic number theory* [SD01]
- Cassels and Fröhlich, *Algebraic number theory* [CF67]

There are many good books on elliptic curves. The following is an incomplete suggestion for additional reading:

- Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves* [Sil94]
- Koblitz, *Introduction to elliptic curves and modular forms* [Kob84]
- Washington, *Elliptic curves: Number theory and cryptography* [Was08]
- Knapp, *Elliptic curves* [Kna92]
- Husemöller, *Elliptic curves* [Hus04]
- Lang, *Elliptic Functions* [Lan87]
- Szpiro, *Séminaire sur les Pinceaux de Courbes Elliptiques* [Szp90]

References

[Cas91] J. W. S. Cassels, *Lectures on elliptic curves*, London Mathematical Society Student Texts, vol. 24, Cambridge University Press, Cambridge, 1991. MR 1144763

[CF67] J. W. S. Cassels and A. Fröhlich, *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, Thompson, Washington, D.C., 1967. MR 0222054

[Ful89] William Fulton, *Algebraic curves*, Advanced Book Classics, Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989, An introduction to algebraic geometry, Notes written with the collaboration of Richard Weiss, Reprint of 1969 original. MR 1042981

[Ho14] Wei Ho, *How many rational points does a random curve have?*, Bull. Amer. Math. Soc. (N.S.) **51** (2014), no. 1, 27–52. MR 3119821

[Hus04] Dale Husemöller, *Elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 111, Springer-Verlag, New York, 2004, With appendices by Otto Forster, Ruth Lawrence and Stefan Theisen. MR 2024529

[Kna92] Anthony W. Knapp, *Elliptic curves*, Mathematical Notes, vol. 40, Princeton University Press, Princeton, NJ, 1992. MR 1193029

[Kob84] Neal Koblitz, *Introduction to elliptic curves and modular forms*, Graduate Texts in Mathematics, vol. 97, Springer-Verlag, New York, 1984. MR 766911

[Lan87] Serge Lang, *Elliptic functions*, second ed., Graduate Texts in Mathematics, vol. 112, Springer-Verlag, New York, 1987, With an appendix by J. Tate. MR 890960

[Maz86] Barry Mazur, *Arithmetic on curves*, Bull. Amer. Math. Soc. (N.S.) **14** (1986), no. 2, 207–259. MR 828821

[RS02] Karl Rubin and Alice Silverberg, *Ranks of elliptic curves*, Bull. Amer. Math. Soc. (N.S.) **39** (2002), no. 4, 455–474 (electronic). MR 1920278

[SD01] H. P. F. Swinnerton-Dyer, *A brief guide to algebraic number theory*, London Mathematical Society Student Texts, vol. 50, Cambridge University Press, Cambridge, 2001. MR 1826558

[Sha13] Igor R. Shafarevich, *Basic algebraic geometry. 1*, third ed., Springer, Heidelberg, 2013, Varieties in projective space. MR 3100243

[Sil94] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994. MR 1312368

[Sil09] ———, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR 2514094

[ST92] Joseph H. Silverman and John Tate, *Rational points on elliptic curves*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992. MR 1171452

[Szp90] L. Szpiro, *Séminaire sur les pinceaux de courbes elliptiques (paris, 1988)*, Astérisque (1990), no. 183, 7–18. MR 1065151

[Was08] Lawrence C. Washington, *Elliptic curves*, second ed., Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2008, Number theory and cryptography. MR 2404461