Isogeny graphs of elliptic curves over finite fields

Alexandre Benoist

February 3, 2025

1 Description of the project

Let K be a field. Roughly, an elliptic curve E over K is the set of solutions $(x, y) \in K^2$ of a cubic equation of the form

$$y^2 = x^3 + ax + b$$

where $(a, b) \in K^2$. It is equipped with a group law, which concretely means that it is possible to add points on the curve. Thus, it is a geometric object (curve), endowed with an algebraic structure. They are fundamental in number theory, where they have many applications, the most famous one being the proof of Fermat's last theorem by Wiles. Beyond pure mathematics, elliptic curves defined over finite fields are regularly used in cryptography.

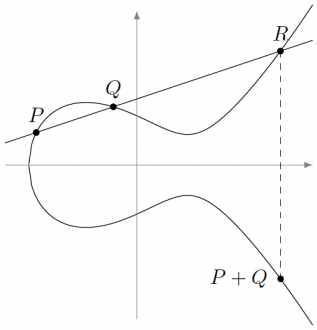

Figure 1: Group law on an elliptic curve

Seen as groups, the morphisms between elliptic curves are called isogenies. The degree of an isogeny is the size of its kernel. Isogenies of degree ℓ between elliptic curves defined over a finite field $\mathbb{F}_q$ are usually represented on an isogeny graph, whose vertices are elliptic curves, and whose edges are the isogenies of degree ℓ between them. If K is a finite field, there is only a finite set of elliptic curves defined over K, so the isogeny graph is finite. Such graphs have a particular structure: they look like volcanoes most of the time (but not always).

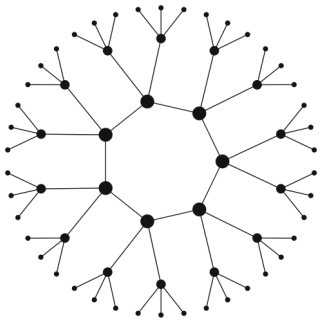

Figure 2: A 3-isogeny graph over $\mathbb{F}_{6007}$

2 Aim of the project

In the first weeks of the projects, students will discover the basic theory of elliptic curves over finite fields and with the following concepts: isogenies, trace of Frobenius, j-invariant, modular polynomials.

Then, the goal of the project is to build some isogeny graphs, firstly for small values of q and ℓ. A particular focus will be given on graphs that are not volcanoes, to see how they look like. The main tool will be the computer algebra software *SageMath* because of its many features for elliptic curves and isogenies. This will lead to a gallery of isogeny graphs.

Depending on the time, another direction could be to use the gallery previously created in order to investigate the dependence of typical quantities of isogeny graphs (e.g. the size of the crater, depth of the volcano ...) in function of the parameters ℓ and q. This could be achieved by generating relevant graphs.

3 Prerequisites

No particular background needed. Programming experience with Python could be useful, but not strictly necessary.

4 References

[1] D. Kohel. "Endomorphism rings of elliptic curves over finite fields". PhD thesis. University of California at Berkeley, 1996.

[2] J. H. Silverman. The Arithmetic of Elliptic Curves. 2nd ed. Springer, 2009.

[3] The LMFDB Collaboration. "The L-functions and modular forms database" (Release 1.2.1), https://www.lmfdb.org, 2024.

[4] SageMath, "The Sage Mathematics Software System" (Version 10.2), The Sage Developers, https://www.sagemath.org, 2024.