Isogenies of elliptic curves over finite fields

Sebastian Alexander Spindler

Technical University of Munich

Abstract

In the ongoing search for quantum-safe cryptography, isogenies between elliptic curves have received heightened attention as a possible foundation for modern cryptographic protocols. The first natural question hence is when two elliptic curves over a finite field are isogenous, i.e. when one can find an isogeny between two such elliptic curves, and this question finds a strikingly simple and efficiently computable answer in Tate's isogeny theorem. For efficiency, however, one would like to work with "small" isogenies only - luckily, this is possible in the special class of supersingular elliptic curves via the so-called supersingular isogeny graph.

Notation

We fix a finite field k of characteristic p and order q, so that $p \in \mathbb{N}$ is a prime and q is a power of p; for simplicity we assume $p \geq 5$. Furthermore we let $\ell \in \mathbb{N}$ denote a prime and write $\overline{k}$ for a fixed algebraic closure of k.

Preliminary I: Elliptic curves

An *elliptic curve* E over k is a projective variety given by a homogeneous equation

$$Y^2Z = X^3 + aXZ^2 + bZ^3$$

where $a, b \in k$ satisfy $4a^3 + 27b^2 \neq 0$. Via the *dehomogenization* $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$ we identify E with the set

$$\{(x,y) \in \overline{k}^2 \colon y^2 = x^3 + ax + b\} \cup \{\mathbf{O}\},$$

where the *point at infinity* $\mathbf{O}$ corresponds to the unique projective solution

$$[0 : 1 : 0]$$

of the curve equation with $Z = 0$. Similarly we can also identify the *k-rational points $E(k)$ of E* with the set

$$\{(x,y) \in k^2 \colon y^2 = x^3 + ax + b\} \cup \{\mathbf{O}\}.$$

Note that the elliptic curve E carries an Abelian group law given by the simple rule that the three intersection points of any line with the curve add up to the point at infinity, which acts as the neutral element of the group.

Preliminary II: Isogenies

A *k-isogeny* $\phi\colon E \to E'$ between two elliptic curves over k is a map given by rational functions with coefficients in k that is not constant and maps the neutral element of E to the neutral element of E'. Such a map is automatically a surjective group homomorphism with a finite kernel, and we can associate to it the *dual isogeny*

$$\widehat{\phi}\colon E' \to E,$$

allowing us to consider the equivalence relation of elliptic curves over k being *k-isogenous*. Moreover, we can define the *degree of ϕ* as the field extension degree

$$\deg \phi \coloneqq [\overline{k}(E) : \phi^* \overline{k}(E')]$$

of the induced function field extension, and this degree can roughly be understood as the size of the isogeny.

Example: Multiplication-by-m isogeny

For any elliptic curve E over k and $m \in \mathbb{Z} \setminus \{0\}$ we can always consider the *multiplication-by-m isogeny*

$$[m] \colon E \to E,\ P \mapsto m \cdot P$$

given by taking the m-fold sum of the input point. The subgroup of *m-torsion points* $E[m]$ of E is defined as the kernel of $[m]$, i.e.

$$E[m] \coloneqq \ker[m].$$

Tate's isogeny theorem

Two elliptic curves E, E' over k are k-isogenous if and only if they have the same number of k-rational points, i.e. $\#E(k) = \#E'(k)$. This result follows from a stronger theorem that is also due to Tate and generalizes to *Abelian varieties*, which can be understood as higher-dimensional analogues of elliptic curves. Interestingly, even when proving the statement only for elliptic curves, one crucial reduction step requires consideration of the product variety $E \times E'$ and hence naturally leads to the setting of Abelian varieties. To prove Tate's theorem in either case, many tools from algebraic number theory, representation theory, topology, category theory and algebraic geometry are required - below we highlight just one of them.

Inverse limits

Roughly speaking, inverse limits provide a way to understand infinite algebraic structures via a backwards step-by-step progression of corresponding finite structures along a *directed* index set. In the proof of Tate's theorem, the following three inverse limits play crucial roles:

1. The *absolute Galois group* $\mathrm{Gal}(\overline{k}|k)$ is the inverse limit of the Galois groups of finite extensions $F|k$ with $F \subseteq \overline{k}$, ordered by inclusion, via the canonical restriction maps.
2. The ring of *ℓ-adic integers* $\mathbb{Z}_\ell$ is the inverse limit of the finite rings $\{\mathbb{Z}/\ell^n\mathbb{Z}\}_{n\in\mathbb{N}}$ with respect to the canonical reduction maps $\mathbb{Z}/\ell^m\mathbb{Z} \to \mathbb{Z}/\ell^n\mathbb{Z}$ for $m \geq n$.
3. The *(integral) ℓ-adic Tate module* $T_\ell(E)$ of an elliptic curve E over k is the inverse limit of the torsion groups $\{E[\ell^n]\}_{n\in\mathbb{N}}$ under the multiplication maps $[\ell^{m-n}]\colon E[\ell^m] \to E[\ell^n]$ for $m \geq n$.

Supersingular elliptic curves

An elliptic curve E over k is called *supersingular* if $\#E(k) \equiv 1 \bmod p$, and it is called *ordinary* otherwise. In view of Tate's isogeny theorem and the well-known Hasse bound

$$|\#E(k) - q - 1| \leq 2\sqrt{q},$$

a straightforward case distinction shows that any two supersingular elliptic curves over k are isogenous over a finite extension of k. However, an even stronger result holds.

The supersingular isogeny graph

We assume $\ell \neq p$. The *supersingular isogeny graph* $\mathcal{G}_{\mathrm{s}}(\overline{\mathbb{F}}_p, \ell)$ has as vertices the isomorphism classes of supersingular elliptic curves that are defined over some finite field of characteristic p, and edges corresponding (up to an equivalence relation) to degree ℓ isogenies between representatives of the isomorphism classes. With some deep results from the theory of quadratic forms and lattices or from the theory of modular forms, one can prove that the supersingular isogeny graph $\mathcal{G}_{\mathrm{s}}(\overline{\mathbb{F}}_p, \ell)$ is connected, i.e. we can find between any two supersingular elliptic curves over a finite field an isogeny (possibly defined over an extension field) of ℓ-power degree. Moreover, any such isogeny can be expressed as a composition of degree ℓ isogenies.

Selected references

[1] J. Tate, "Endomorphisms of Abelian Varieties over Finite Fields". In: *Inventiones mathematicae* 2.2 (Apr. 1966), pp. 134-144.

[2] D. Kohel, "Endomorphism rings of elliptic curves over finite fields". PhD thesis. 1996. Available here (last visited on May 10, 2023).

[3] J. H. Silverman, *The Arithmetic of Elliptic Curves*. 2nd ed. Graduate Texts in Mathematics 106. Springer New York, 2009.

[4] S. D. Galbraith, *Mathematics of Public Key Cryptography*. Cambridge University Press, 2012.