

Towards a database of isogeny graphs

Enric Florit - efz1005@gmail.com
Universitat de Barcelona

Gerard Finol - gerardfinol@gmail.com
Universitat Rovira i Virgili

The isogeny graphs $\Gamma_1(\ell; p)$

- An **elliptic curve** E over a finite field \mathbb{F}_q has equation $E: y^2 = x^3 + Ax + B$. The j -invariant

$$j(E) = 1728 \frac{4A^3}{4A^3 + 27B^2}$$

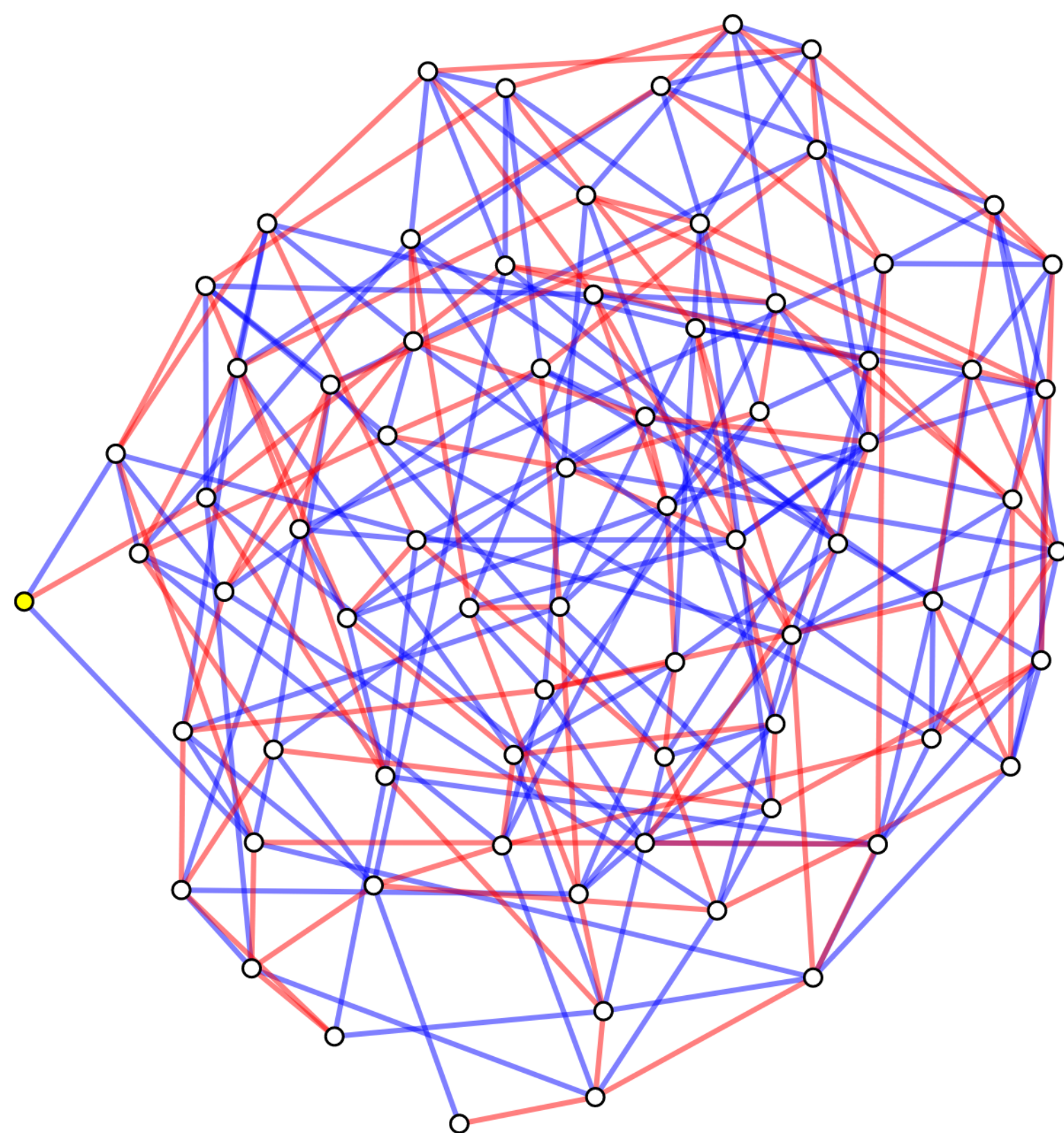
gives the isomorphism class of the curve. The curve is **supersingular** if its **endomorphism ring** is an order in a **quaternion algebra**.

- An **isogeny** of degree ℓ is a finite morphism of elliptic curves

$$\varphi: E \rightarrow E'$$

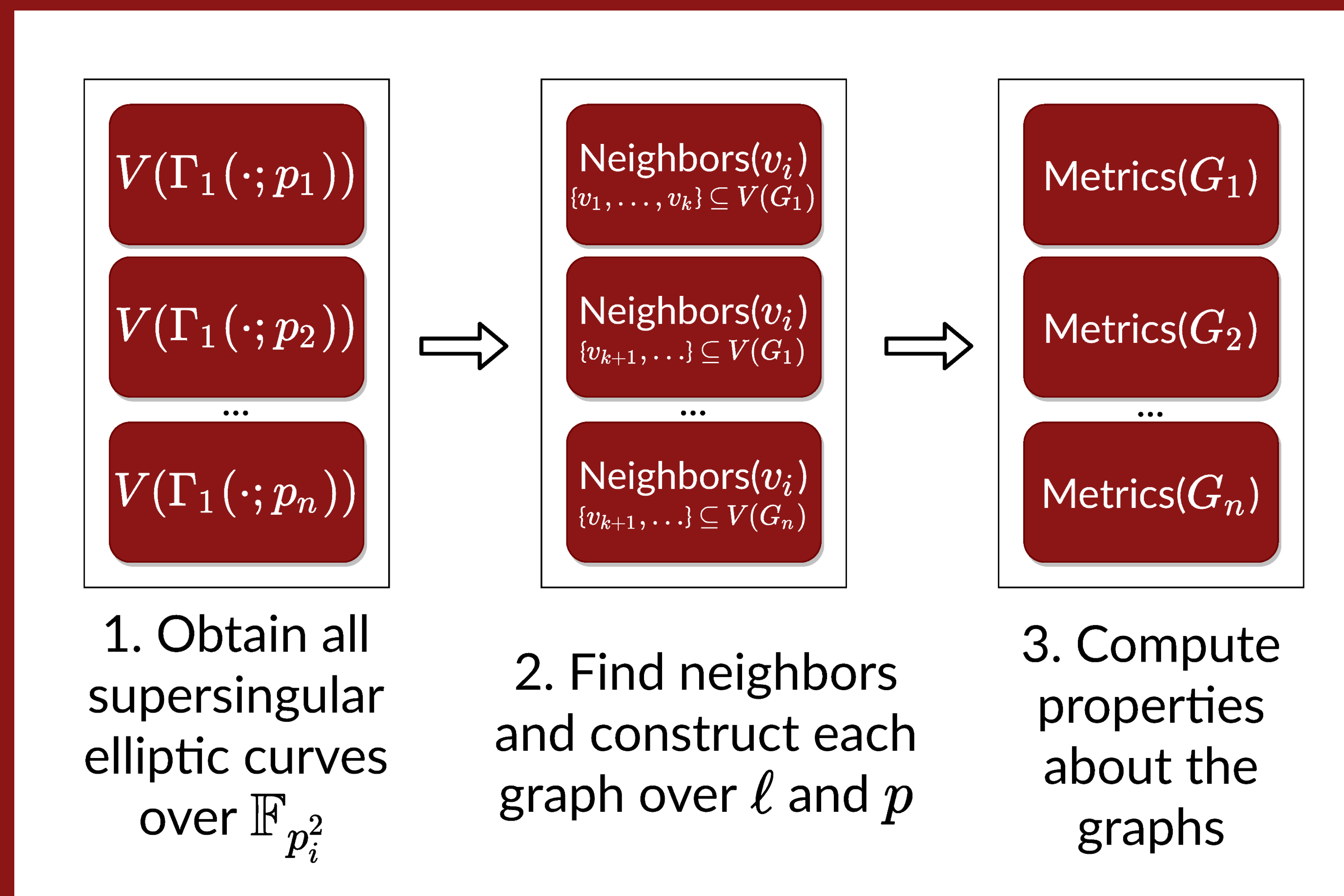
such that $|\ker \varphi| = \ell$.

- The **supersingular isogeny graph** $\Gamma_1(\ell; p)$ is the graph of supersingular j -invariants over \mathbb{F}_p and degree- ℓ isogenies between them. It is an $(\ell + 1)$ -regular **Ramanujan graph**.



$\Gamma_1(2; 863)$ and $\Gamma_1(3; 863)$ superimposed.

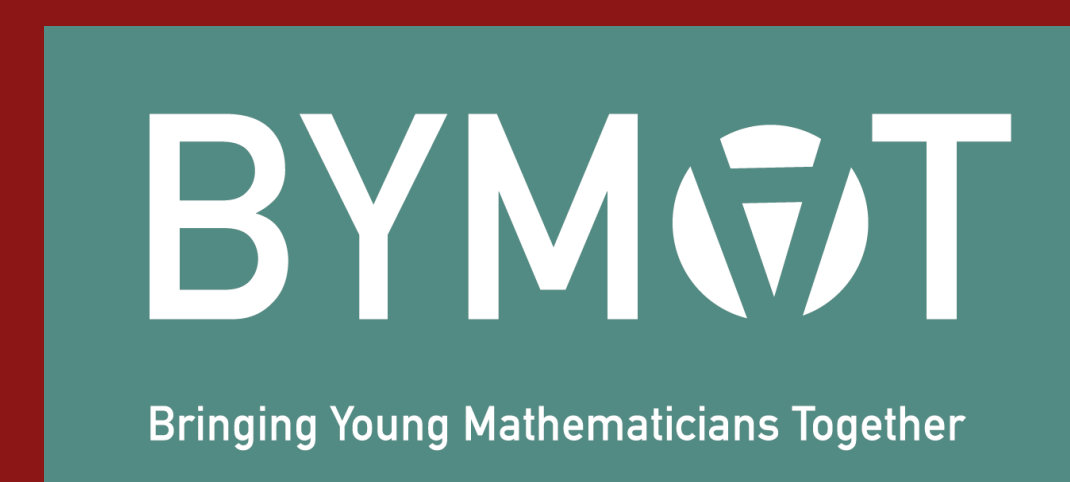
We are building an open library of supersingular isogeny graphs of elliptic curves using serverless computing



Each step is computed in parallel



Visit the website:
isogenies.enricflorit.com

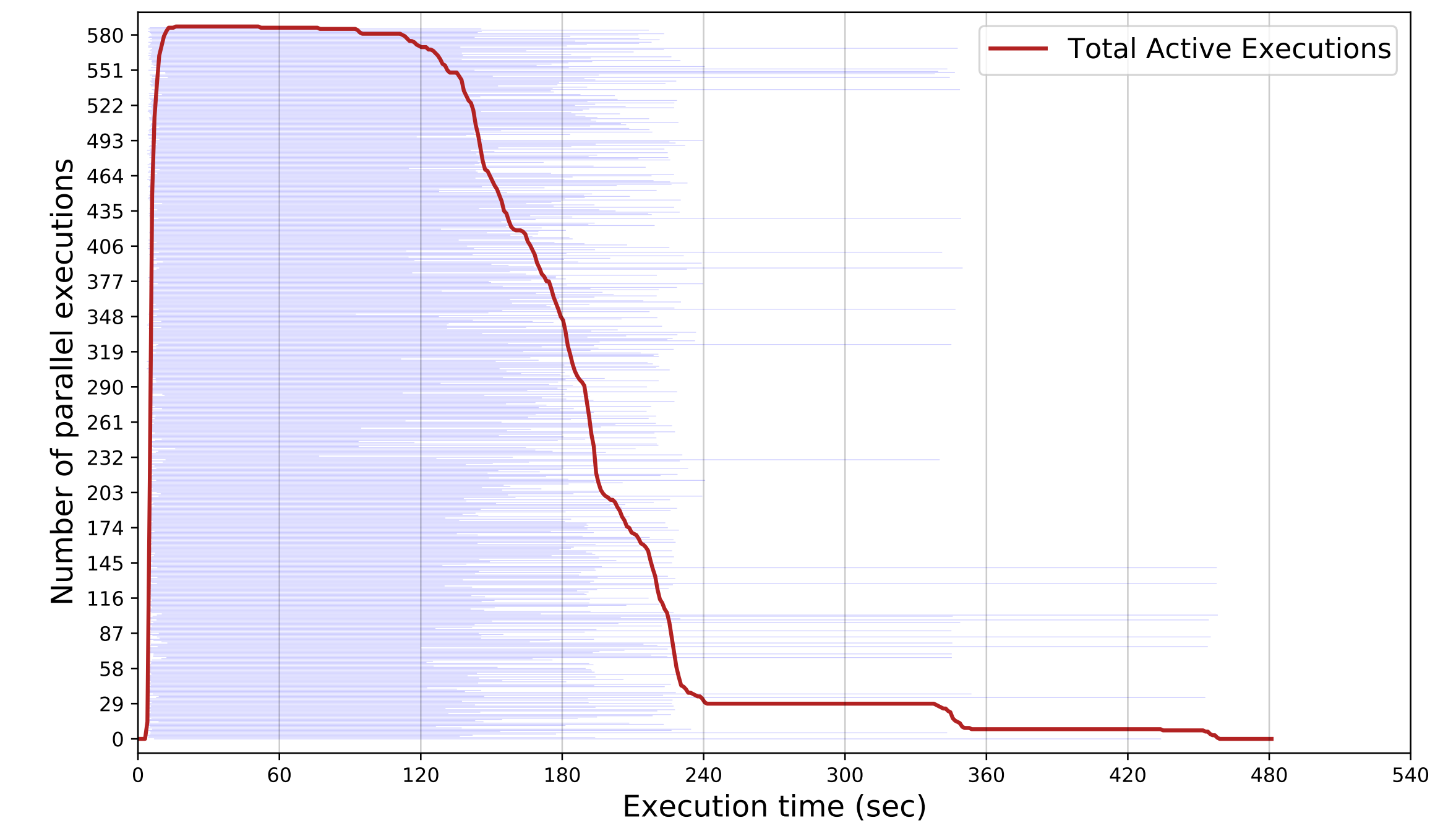


Computing isogenies

For each prime ℓ , the ℓ th modular polynomial $\Phi_\ell(X, Y) \in \mathbb{Z}[X, Y]$ satisfies $\Phi_\ell(j(E), j(E')) = 0 \iff$ there is a degree- ℓ isogeny from E to E' . The roots of $\Phi_\ell(j, Y)$ are the **neighbors** of j .

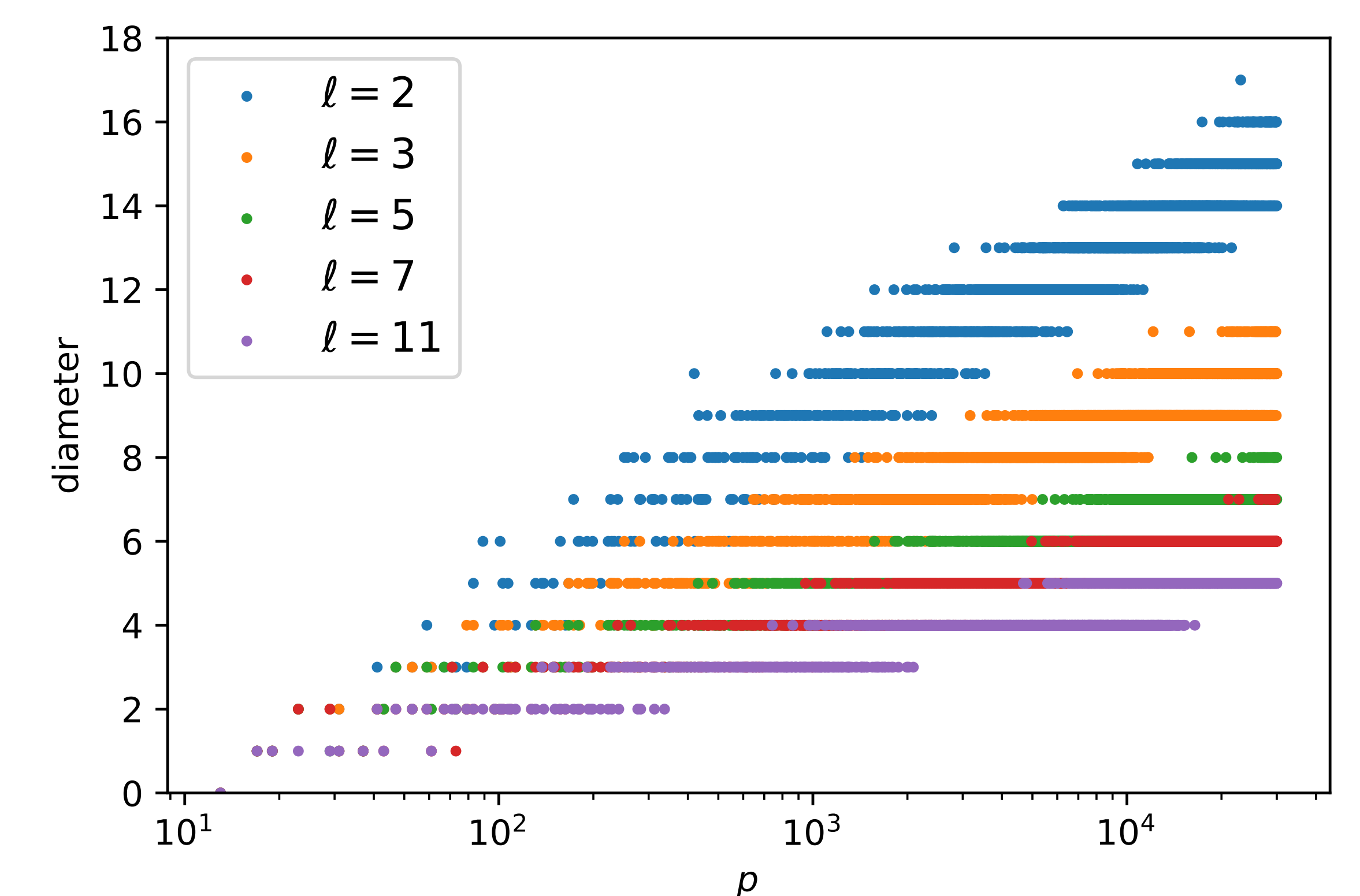
Serverless computing with Lithops

Using lithops we can run hundreds of parallel distributed threads to compute graphs.



Histogram of the computation of $\Gamma_1(11; 4010173)$, overall time of 458 seconds.

Graph diameters



The diameter of $\Gamma_1(\ell; p)$ grows as $\log p$, as predicted by the Ramanujan property.

Main references

- [1] S. Arpin et al., "Adventures in Supersingularland", *arXiv preprint arXiv:1909.07779* 2019.
- [2] J. Sampe et al., "Towards Multicloud Access Transparency in Serverless Computing", *IEEE Software* 2020, DOI 10.1109/MS.2020.3029994.