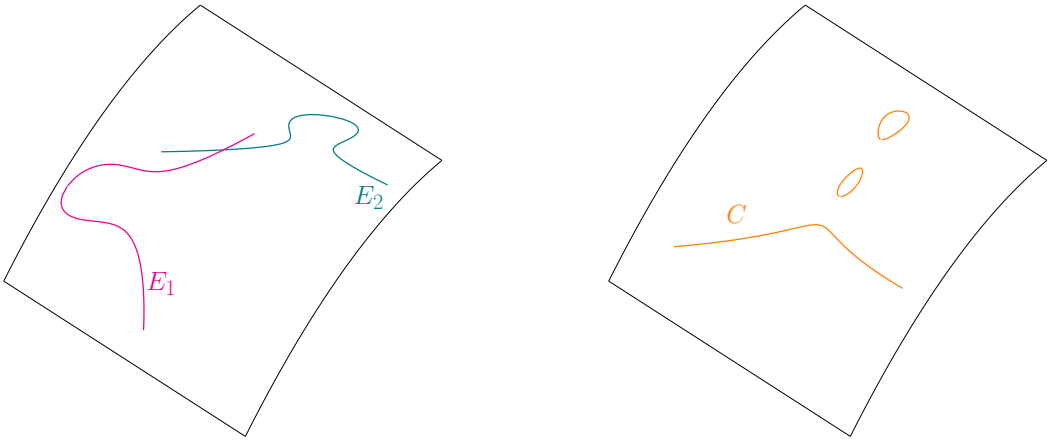
Triples of elliptic curves with level structure



Throughout the past centuries, elliptic curves have been a topic of interest in various fields of mathematics. More recently, they have gained a lot of attention in the world of cryptography due to some interesting properties they possess. Applications such as iMessage and Bitcoin make extensive use of ECDSA, a primitive that is based on the discrete logarithm problem on elliptic curves.

However, in 1994 Peter Shor formulated an algorithm to solve this problem on a quantum computer. Even though quantum computers are nowhere near practical, the research of elliptic curves has shifted from working on a single elliptic curve to working with certain maps - called isogenies - between distinct elliptic curves. One of the most efficient isogeny-based protocols was SIKE, which was in the running for post-quantum standardization up until the summer of 2022, when it got taken down by an attack in higher dimension. This attack provides a new and powerful toolbox for isogeny-based cryptography, both from a constructive angle as well as a cryptanalytic approach.

The two-dimensional generalization of an elliptic curve is called an abelian surface A, which breaks down into two possible categories as seen above: either a product of two elliptic curves $E_1 \times E_2$ or (the Jacobian of) a hyperelliptic curve C. For certain cryptographic protocols, it is imperative to know how many distinct maximal isotropic subgroups isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^2$ such objects have. Generically, this number is easy to determine, but nontrivial automorphisms of A can significantly lower it.

The aim of this project is to take a look at dimension three, where abelian threefolds can be one of four categories. Very concretely, the goal is to count the number of maximal isotropic subgroups isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^3$ for any possible elliptic product $E_1 \times E_2 \times E_3$. The student should preferably have some background (or at the very least strong interest) in group theory and algebraic geometry.

Practicalities

Promoter:	Frederik Vercauteren		
Daily supervisor:	Thomas Decru	thomas.decru@esat.kuleuven.be	office B01.10
Nature of the work:	40% literature, 30% theoretical, 30% software		
Number of students:	1		

 © 2026-2027 COSIC