Regiomontanus PhD Seminar - Third Session

May 14th 2025

Elliptic curves and their use in cryptography

Pepijn Hulsbergen

The use of elliptic curves in cryptography is an examples of ”real-world” applications of mathematics. In this talk, we highlight the use of elliptic curves in ”public-key” cryptography. First, we gently introduce ourselves to elliptic curves and discuss an example. After that, we discuss the Elliptic Curve Diffie–Hellman Problem.

The Poincaré–Birkhoff theorem from a Hamiltonian systems perspective

Franz Schels

The Poincaré–Birkhoff theorem states that any area preserving twist map of the annulus has at least two fixed points. It was conjectured by Poincaré in 1912 and would establish the existence of infinitely many periodic orbits in the restricted three-body problem as a consequence. The theorem has a classical proof given by Birkhoff in 1913. After a short introduction to Hamiltonian systems, we outline a new proof of the theorem using more modern methods from Hamiltonian systems.