Endomorphisms and decompositions of Jacobians

Jeroen Sijsling, Universität Ulm

Let C be a curve over a number field, with Jacobian J, and let End (J) be the endomorphism ring of J. The ring End (J) is typically isomorphic to ZZ, but the cases where it is larger are interesting for many reasons, most of all because the corresponding curves can then often be matched with relatively simple modular forms.

We give a provably correct algorithm to verify the existence of additional endomorphisms on a Jacobian. As described in the talk by Lombardo, it is also possible to obtain upper bounds on the rank of End (J). Together, these methods make it possible to completely and explicitly determine the endomorphism ring End (J) starting from an equation for C, with acceptable running time when the genus of C is small.

The algorithms generalize without problem to morphisms between different Jacobians, and thus enable one to decompose a Jacobian of a curve up to isogeny. Time permitting, we will also describe this process and its inverse, namely that of gluing curves along their n-torsion, in particular the case of obtaining a genus-3 curve by gluing a genus-1 curve and a genus-2 curve along their 2-torsion.

The first part is joint work with Edgar Costa, Nicolas Mascot, and John Voight, and the second part is work in progress with Jeroen Hanselman.