

## BSc-project: Opsommen van krommen over eindige lichamen

Begeleider: Marco Streng

Uit [1]: “We present an algorithm that, for every fixed genus  $g$ , will enumerate all hyperelliptic curves of genus  $g$  over a finite field  $k$  of odd characteristic in quasilinear time; that is, the time required for the algorithm is  $\tilde{O}(q^{2g-1})$ , where  $q = \#k$ .”

Dit gaat over isomorfieklassen van krommen gegeven door vergelijkingen van de vorm  $y^2 = f(x)$  met  $\deg(f) = 2g + 2$ .

Daar zijn vast wel wat generalisaties van te bedenken, zoals iets met superelliptische krommen van de vorm  $y^3 = f(x)$ .

### Voorkennis

Algebra 1–3 (Galoistheorie, groepswerkingen, polynomen, eindige lichamen). Bij voorkeur ook het BM-vak Algebraic Curves.

### Referenties

- [1] Everett W. Howe. Enumerating hyperelliptic curves over finite fields in quasilinear time. Accepted for publication in Research in Number Theory, Sixteenth Algorithmic Number Theory Symposium (ANTS XVI), <https://antsmath.org/ANTSXVI/papers/Howe.pdf>, 2024.