

Computational aspects of class group actions and applications to postquantum cryptography

Houben, M.R.

Citation

Houben, M. R. (2024, February 28). *Computational aspects of class group actions and applications to post-quantum cryptography*. Retrieved from https://hdl.handle.net/1887/3721997

Version:	Publisher's Version
License:	Licence agreement concerning inclusion of doctoral thesis in the Institutional Repository of the University of Leiden
Downloaded from:	https://hdl.handle.net/1887/3721997

Note: To cite this publication please use the final published version (if applicable).

Stellingen

behorende bij het proefschrift "Computational aspects of class group actions and applications to post-quantum cryptography"

(i) The Decisional Diffie-Hellman problem for class group actions on oriented elliptic curves can be broken, provided the class group has a non-trivial assigned character of sufficiently small modulus.

Chapter 4

(ii) Let \mathcal{O} be an imaginary quadratic order and let (E, ι) be an \mathcal{O} -oriented elliptic curve. Let f be a self-pairing on a cyclic subgroup of E that is compatible with all endomorphisms in $\iota(\mathcal{O})$. Let m be a positive integer. If the image of f contains a primitive m-th root of unity, then m divides the discriminant of \mathcal{O} .

Proposition 5.4.8

- (iii) There exists a modular curve C over \mathbf{Q} such that for every infinite sequence of imaginary quadratic integers τ_1, τ_2, \ldots in the complex upper half plane satisfying
 - (a) the norm $|\tau_i|^2$ of τ_i is divisible by 119 for all $i \in \mathbb{Z}_{>0}$; and
 - (b) the class number n_i of the imaginary quadratic order $\mathbf{Z}[\tau_i]$ is prime for all $i \in \mathbf{Z}_{>0}$; and
 - (c) the heights of the modular j-invariants satisfy

$$\lim_{i \to \infty} h(j(\tau_i)) / \log(\log(n_i)) = \infty,$$

it holds that

- (a) the modular curve C admits a real generalized class polynomial $H_{\tau_i}[C]$ associated to τ_i for all $i \in \mathbb{Z}_{>0}$; and
- (b) if each $H_{\tau_i}[C]$ is scaled to have coprime integral coefficients, we have

$$\lim_{i \to \infty} \frac{\log |H_{\tau_i}[j]|_{\infty}}{\log |H_{\tau_i}[C]|_{\infty}} = 72.$$

Here $H_{\tau_i}[j]$ denotes the minimal polynomial of $j(\tau_i)$ over **Q** (that is, the Hilbert class polynomial of $\mathbf{Z}[\tau_i]$) and $|P|_{\infty}$ denotes the maximum of the absolute values of the coefficients of a polynomial P.

Chapter 6

(iv) Radical isogeny formulae can be obtained by rational interpolation combined with the Chinese remainder theorem.

Section 7.4

Let $n \in \mathbf{Z}_{>0}$ be a positive integer and let p be a prime number. We say that a multivariate sequence of rational numbers $(a_{\mathbf{k}})_{\mathbf{k}\in\mathbf{Z}_{\geq 0}^{n}}$ satisfies the *Gauss* congruences at p if

 $a_{\mathbf{m}}$ is a *p*-adic integer and $a_{\mathbf{m}p^r} \equiv a_{\mathbf{m}p^{r-1}} \pmod{p^r}$

for all $\mathbf{m} \in \mathbf{Z}_{\geq 0}^n$ and all $r \in \mathbf{Z}_{>0}$. If $P(\mathbf{x}), Q(\mathbf{x}) \in \mathbf{Z}[\mathbf{x}] = \mathbf{Z}[x_1, \dots, x_n]$ are polynomials such that $Q(\mathbf{0}) \neq 0$, then the rational function $P(\mathbf{x})/Q(\mathbf{x})$ satisfies the *Gauss property* if the coefficient sequence of its power series expansion at **0** satisfies the Gauss congruences at all but finitely many prime numbers p.

(v) Let $P(\mathbf{x}), Q(\mathbf{x}) \in \mathbf{Z}[\mathbf{x}]$ be multivariate integer polynomials. Suppose that Q is linear (that is, of degree at most one) in each variable and that $Q(\mathbf{0}) \neq 0$. Then $P(\mathbf{x})/Q(\mathbf{x})$ satisfies the Gauss property if and only if the Newton polytope of P is contained in the Newton polytope of Q.

joint with Frits Beukers and Armin Straub

Let S be a set and let $f: S \to S$ be a function. If

$$f_n := \#\{x \in S \mid \underbrace{(f \circ \dots \circ f)}_{n \text{-fold composition}} (x) = x\}$$

is finite for all $n \in \mathbb{Z}_{>0}$ then we call f confined, and we define the Artin-Mazur zeta function of f as the formal power series $\zeta_f(z) := \exp\left(\sum_{n>1} f_n z^n/n\right)$.

(vi) The Artin–Mazur zeta function of a confined endomorphism of an algebraic group over the algebraic closure of a finite field is either rational (that is, an element of $\mathbf{C}(z)$) or transcendental over $\mathbf{C}(z)$.

joint with Jakub Byszewski and Gunther Cornelissen

(vii) Let k be an algebraically closed field of positive characteristic p > 0 and let $m \in \mathbf{Z}_{>1}$. Consider the map $f : \mathbf{P}^1(k) \to \mathbf{P}^1(k), x \mapsto x^m$. The Artin-Mazur zeta function of f is rational if and only if $p \mid m$. Otherwise, as a complex function, it admits a natural boundary along its circle of convergence.

joint with Jakub Byszewski and Gunther Cornelissen

- (viii) The Deuring correspondence is a bijection between subgroup schemes of a supersingular elliptic curve and ideals of its endomorphism ring.
- (ix) There should be more interplay between the field of post-quantum cryptography and the field of quantum computing.
- (x) Research in cryptography should not be dictated by the process of standardization.

Marc Houben Leiden, February 28, 2024