



Universiteit
Leiden
The Netherlands

Random walks on Arakelov class groups

Boer, K. de

Citation

Boer, K. de. (2022, September 22). *Random walks on Arakelov class groups*. Retrieved from <https://hdl.handle.net/1887/3463719>

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/1887/3463719>

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

Samenvatting

Het hoofdonderwerp van deze dissertatie is de *Arakelov straalklassegroep* van een getallenlichaam, een algebraïsch object dat zowel de ideaalklassestructuur als de eenhedenstructuur van een getallenlichaam omvat. Het hoofdresultaat van deze thesis betreft het feit dat zekere specifieke *toevalsbewegingen* op de Arakelov straalklassegroep resulteren in een eindpunt dat uniform random verdeeld is over deze groep, onder aanname van een uitgebreide variant van de Riemann hypothese (hoofdstuk 4). Bijna alle andere resultaten in dit werk vloeien voort uit dit feit.

Als een direct gevolg, kunnen we met behulp van deze toevalsbewegingen op de Arakelov klassegroep aantonen dat het vinden van een kortste vector in een gegeven (mogelijk ingewikkeld) ideaalrooster computationeel niet veel moeilijker is dan het vinden van een kortste vector in een random ideaalrooster van een vast gekozen getallenlichaam (hoofdstuk 5).

Een ander resultaat maakt gebruik van deze toevalsbewegingen om rigoureus en op een efficiënte wijze elementen uit idealen van een getallenlichaam te samplen op zodanige manier dat het quotiënt van het betreffende element en ideaal uit een bepaalde vooraf gekozen ideaalverzameling komt. De successkans van dit samplen is dan evenredig met de analytisch-getaltheoretische *dichtheid* van de ideaalverzameling op een zeker punt. Een interessante toepassing van dit resultaat verkrijgt men wanneer men voor de betreffende ideaalverzameling de verzameling van priemidealen neemt en voor het getallenlichaam een cyclotomisch lichaam. In dat geval luidt de stelling dat men op efficiënte wijze elementen in idealen van cyclotomische lichamen kan vinden zodanig dat het quotiënt van het betreffende element en ideaal

‘bijna’ een priemideaal is. Dat wil zeggen dat dit quotiënt bestaat uit het product van een groot priemideaal en eventueel meerdere kleinere priemidealen (hoofdstuk 6).

Het doel van bovenstaand sampling algoritme is om heuristische argumenten voor bepaalde algoritmen in de getaltheorie, zoals ideaalklasse- en eenheden-groepalgoritmes, te vervangen door rigoureuze bewijzen. In deze dissertatie is het op deze manier gelukt om formeel te bewijzen dat een algoritme voor het machtrestsymbool, een polynomiale looptijd heeft. Van de looptijd van dit algoritme was voorheen alleen *heuristisch* aangetoond dat deze polynomiaal begrensd was (hoofdstuk 7).

Een deel van deze thesis dat wat meer op zichzelf staat, betreft een kwantumalgoritme voor een continue variant van het *hidden subgroup problem* en een volledige analyse van dit algoritme (hoofdstuk 3). Dit algoritme kan toegepast worden om Arakelov straalklassiegroepen expliciet te berekenen; dit moet echter nog wel nauwkeurig onderzocht en bewezen worden.