Geometric quadratic chabauty and other topics in number theory

Lido, G.M.

Samenvatting

Geometric quadratic Chabauty and other topics in number theory

Dit proefschrift bestaat uit drie delen.

Het eerste gedeelte betreft een methode van Chabauty die het mogelijk maakt om in bepaalde gevallen de rationale punten van een algebraische kromme C van geslacht $g > 1$ te vinden. Chabauty's methode bestaat eruit om voor een priemgetal p de doorsnede van de Mordell-Weil groep van de Jacobiaan met de p-adische punten van de kromme C te bestuderen. Als de rang r van de Mordell-Weil groep kleiner is dan het geslacht, dan leidt de methode tot een eindige deelverzameling van $C(\mathbb{Q}_p)$ die $C(\mathbb{Q})$ bevat. In onze benadering vervangen we J door een product T van $\mathbb{G}_{\mathrm{m}}$-torsoren over J. Om precies te zijn, T is een product van pullbacks van de Poincaré-torsor en we maken gebruik van de biextensiestructuur om de gehele punten van T te parametriseren. Wanneer $r-g+1$ kleiner is dan de rang van de Néron-Severi-groep van J, dan stelt onze methode ons in staat om een eindige verzameling van $\mathbb{Q}_p$-punten van C te bepalen die $C(\mathbb{Q})$ bevat.

Het tweede gedeelte van dit proefschrift gaat over automorfismen van Cartan modulaire krommen. De meeste literatuur over Cartan modulaire krommen betreft krommen van priem niveau p. De niet-cuspidale rationale punten van deze krommen corresponderen met elliptische krommen waarvoor de Galoisrepresentatie op de p-torsiepunten niet surjectief is. Ons resultaat betreft ook Cartan-krommen die niet noodzakelijk priemniveau hebben. We bewijzen dat als het niveau voldoende hoog is, deze krommen alleen maar de voor de hand liggende, naar het bovenhalfvlak liftbare automorfismen toelaten. Voor Cartan-krommen van priemniveau p is dit al het geval voor $p > 11$. Het belangrijkste nieuwe ingrediënt in ons bewijs is een diepgaande studie, voor een grote klasse van modulaire krommen, van de actie van de Hecke-operatoren op de elliptische punten en de spitsen. We generaliseren een klassieke methode om de graad van het definitielichaam van een automorfisme u te begrenzen. Tenslotte bewijzen we dat u in essentie met de

Hecke-operatoren commuteert. Hieruit volgt dat u zowel de spitsen als de elliptische punten behoudt. Standaard topologische eigenschappen van afdekkingen impliceren dan dat u naar het bovenhalfvlak $\mathbb{H}$ lift.

Het laatste gedeelte van dit proefschrift betreft de discrete logaritme in eindige lichamen van kleine karakteristiek. Het probleem is om, gegeven een eindig lichaam K van karakteristiek p en kardinaliteit $> p^p$ en gegeven een voortbrenger g van K^* en een element $h \in K^*$, een exponent z te bepalen zodat $h = g^z$. We geven een probabilistische algoritme om dit probleem op te lossen in quasi-polynomiale tijd: $\log(\#K)^{O(\log\log\#K)}$. Een heuristisch polynomiaal algoritme was al eerder gegeven door Joux, Barbulescu, Gaudry en Thomé. Hun voornaamste idee bestond eruit een element in K aan te geven waarop het Frobeniusautomorfisme op een "eenvoudige" manier werkt. Ons idee is om niet één maar twee elementen in K te geven. Deze twee elementen zijn de coördinaten van een punt op een elliptische kromme. Dankzij de groepsstructuur is de actie van Frobenius "eenvoudig". Omdat er zoveel keus is voor de elliptische kromme, is het makkelijk in te zien dat elk eindig lichaam van kleine karakteristiek ingebed kan worden in een iets groter lichaam dat twee zulke elementen bevat. Op deze manier kunnen we de heuristieke benadering vervangen door een bewijs dat ons algoritme quasi-polyniomiaal is.