Subadditivität von Minimale-Norm-Ziffernmengen und imaginär-quadratische Basen mit Spur ± 2

Mögliches Thema für eine Bachelorarbeit

Hintergrund

Zum Berechnen von Vielfachen, wie es beispielsweise bei kryptographischen Anwendungen vorkommt, wird oft ein double-and-add (bzw. square-and-multiply, falls multiplikativ geschrieben) Algorithmus verwendet. Dieser verwendet die Binärdarstellung einer Zahl. Um effizientere Algorithmen zu erhalten, können andere (größere) Ziffernmengen und andere Basen verwendet werden, z.B. die Basis 2, aber Ziffern $D = \{-1, 0, 1\}$ oder aber auch nicht-ganzzahlige Basen, wie die Nullstelle eines Polynoms (kommend von elliptischen Kurven).

Kurzbeschreibung

Sei nun eine imaginär-quadratische Basis (präziser: eine Nullstelle von $X^2 - pX + q$ mit $p = \pm 2$ und ganzzahligem $q \geq 2$) gegeben. Wir arbeiten in einem (von der Basis abhängigen) Gitter in der Ebene. Eine Minimale-Norm-Ziffernmenge (siehe Abbildung 1) besteht aus Punkten dieses Gitters, welche durch ein Rechteck mit Mittelpunkt 0 bestimmt werden.

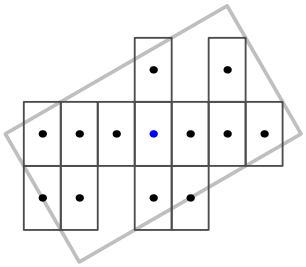

Abbildung 1: Eine Minimale-Norm-Ziffernmenge.

Wir interessieren uns für eine spezielle Eigenschaft der Ziffernmenge, nämlich der Subadditivität. Für Minimale-Norm-Ziffernmengen gibt es eine Heuristik um diese Eigenschaft zu untersuchen: Es sind Punkte in dem Gitter, welche gewisse Kriterien erfüllen, zu finden. Ziel der Bachelorarbeit ist es,

- diese Heuristik zu implementieren,
- damit festzustellen, welche Ziffernmengen subadditiv sind und welche nicht, und
- eine Vermutung für das allgemeine Verhalten zu bekommen bzw. unendliche Familien von subadditiven und nicht-subadditiven Ziffernmengen zu erhalten.

Geometrie 🔋, *Coding* 🪫, *Zahlentheorie* ▭

Kontakt

Daniel Krenn
Institut für Mathematik
Raum I.2.06
daniel.krenn@aau.at

Weitere Themen aus dem Bereich der diskreten Mathematik auf Anfrage.