PROJECT: MODULAR ARITHMETIC OF QUATERNION NORMS

BEGELEIDER: JONATHAN LOVE

Given two positive rational numbers a and b, we can define a *definite quaternion algebra over* $\mathbb{Q}$

$$B(-a,-b) := \{w + xi + yj + zk \mid w,x,y,z \in \mathbb{Q}\}$$

with a multiplication structure determined by the identities

$$i^2 = -a,\ j^2 = -b,\ ij = k,\ ji = -k.$$

Any element $z := w + xi + yj + zk \in B(-a,-b)$ has a *trace*, $\mathrm{Tr}(z) := 2w \in \mathbb{Q}$, and a *norm*, $\mathrm{N}(z) := w^2 + ax^2 + by^2 + abz^2 \in \mathbb{Q}$. We say a set $A \subseteq B(-a,-b)$ is an *integral ideal* if it is a subgroup under addition, the trace and norm of every element in A is an integer, and A contains a basis for $B(-a,-b)$ as a vector space over $\mathbb{Q}$.

Problem 1. *Let A be an integral ideal in a definite quaternion algebra over $\mathbb{Q}$, and let $c, d \in \mathbb{Z}$ with $d \neq 0$. What is the proportion of elements of A with norm congruent to $c \bmod d$? More precisely, what is*

$$\lim_{X\to\infty} \frac{\#\{z \in R : N(z) \leq X,\ N(z) \equiv c \bmod d\}}{\#\{z \in R : N(z) \leq X\}}?$$

For example, if A is a *maximal order* in $B(-a,-b)$ (that is, an integral ideal that is also a subring, and not contained in any other integral ideal), then the proportion of elements in A with odd norm ($1 \bmod 2$) appears to always be either $\frac{3}{4}$ or $\frac{3}{8}$, depending on the values of a and b. Why aren't elements of odd and even norm equally plentiful, and where do these proportions $\frac{3}{4}$ and $\frac{3}{8}$ come from?

This problem has applications in cryptography: one of the steps in a recent algorithm [1] requires finding an element of a quaternion ideal that satisfies certain congruence conditions modulo powers of 2 and 3. The authors of this preprint give a conjectural answer to a special case of Problem 1 [1, Conjecture 6], and give an analysis of their algorithm that's conditional on this conjecture.

The goal of this project is to resolve Problem 1 for as wide of a class of quaternion ideals as possible. The student will learn about the basics of quaternion algebras and ideals, both over $\mathbb{Q}$ and over p-adic number fields. Depending on the interest of the student, there will be opportunities to conduct computational experiments to form conjectures, and/or to explore connections and applications to supersingular isogeny graphs and isogeny-based cryptography.

To get a better feel for what this problem is asking, you can run the following Magma code (for example using https://magma.maths.usyd.edu.au/calc/). Play around with the parameters and see what proportions you get. For starters, what happens if you change the -5 to some other negative integer?

```
B := QuaternionAlgebra< Rationals() | -1, -5 >;
c := 1; d := 2; maxnorm := 100;
A := MaximalOrder(B);
total := Enumerate(A, 0, maxnorm);
congruence := [ z : z in total | Norm(z) mod d eq c ];
print 1.0 * #congruence / #total;
```

References

[1] Wouter Castryck, Mingjie Chen, Riccardo Invernizzi, Gioella Lorenzon, and Frederik Vercauteren. *Breaking and Repairing SQIsign2D-East*. Cryptology ePrint Archive, Paper 2024/1453. 2024. URL: https://eprint.iacr.org/2024/1453.