On the number of binary quartic number fields

Ari Shnidman

Hebrew University of Jerusalem

November 3, 2023

Overview

Overview

Enumerating number fields

Conjecture (Malle)

As $X \to \infty$, the number of degree d number fields of discriminant less than X is $\sim c_d X$.

Known when $d \le 5$ (Davenport-Heilbronn for $d = 3$ and Bhargava for $d = 4, 5$).

Idea: parameterize rings of integers $\mathcal{O}_K$ as geometric objects.

- $d = 3$: $\operatorname{Spec} \mathcal{O}_K = \{f(x, y) = 0\} \subset \mathbb{P}^1_{\mathbb{Z}}$ (Delone-Faddeev)
- $d = 4$: $\operatorname{Spec} \mathcal{O}_K = \{q_1(x, y, z) = 0\} \cap \{q_2(x, y, z) = 0\} \subset \mathbb{P}^2_{\mathbb{Z}}$ (Bhargava).
- $d = 5$: $\operatorname{Spec} \mathcal{O}_K = \bigcap_{i=1}^5 \{q_i(x, y, z, w) = 0\} \subset \mathbb{P}^3_{\mathbb{Z}}$ (Bhargava).

Then count number of (isomorphism classes of such) objects with bounded discriminant using the geometry-of-numbers and the averaging method.

Analogy with curves

- $\operatorname{Spec} \mathcal{O}_K$ is a one-dimensional scheme.
- We can try to classify number fields as we do curves in algebraic geometry.
- The moduli space $\mathcal{M}_g$ is of general type for g large, so its rational points should be supported on a proper closed subvariety.
- Open question (for g large): are 100% of curves of genus g hyperelliptic?

This suggests that for number fields, we should:

1. Determine the different models for $\operatorname{Spec} \mathcal{O}_K$ (as closed subschemes of $\mathbb{P}^n_{\mathbb{Z}}$).
2. Determine their asymptotics.

Binary quartic rings

Definition

A number field K is *binary* if $\operatorname{Spec}\mathcal{O}_K \simeq \{f(x,y)=0\} \subset \mathbb{P}^1_{\mathbb{Z}}$ for some $f \in \mathbb{Z}[x,y]$.

In this case, if $f = \sum a_i x^{n-i} y^i$, then $\mathcal{O}_K$ has $\mathbb{Z}$-basis

$$1, a_0\theta, a_0\theta^2 + a_1\theta, \ldots, \sum_{i=0}^{n-2} a_i \theta^{n-1-i}$$

where θ is a root of $f(x,1)$.

Example

If $a_0 = \pm 1$, then $\mathcal{O}_K = \mathbb{Z}[\theta]$ is monogenic. Equivalently: $\operatorname{Spec}\mathcal{O}_K \hookrightarrow \mathbb{A}^1_{\mathbb{Z}}$.

Conjectures

Conjecture (Folklore)

For $d \geq 3$, 100% of degree d number fields are not monogenic, ordered by discriminant.

Conjecture (Bhargava-Shankar-Wang)

The number of monogenic degree d number fields of discriminant $< X$ is $\sim \alpha_d X^{\frac{1}{2}+\frac{1}{d}}$.

Conjecture (Bhargava-Shankar-Wang)

The number of binary degree d number fields of discriminant $< X$ is $\sim \beta_d X^{\frac{1}{2}+\frac{1}{d-1}}$.

Conjecture

For $d \geq 4$, 100% of degree d number fields are not binary, ordered by discriminant.

Main theorems

Theorem (Alpöge-Bhargava-S)

A positive proportion of quartic number fields of any fixed signature are not binary (despite having no local obstruction).

The proof will use the following:

Theorem (Alpöge-Bhargava-S)

A positive proportion of cubic number fields of any fixed signature are not monogenic (despite having no local obstruction).

Index form obstruction

Let K be a number field of degree d. The **index form**

$$\mathcal{O}_K/\mathbb{Z} \longrightarrow \bigwedge^d \mathcal{O}_K$$

defined by

$$r \mapsto 1 \wedge r \wedge \ldots \wedge r^{d-1}$$

is a homogeneous form $f_K(x_1, \ldots, x_{d-1})$ of degree $\binom{d}{2}$ in $d-1$ variables.

Lemma

K is monogenic if and only if $f_K(x_1, \ldots, x_{d-1})$ represents 1 or -1 over $\mathbb{Z}$.

Definition

We say K is *locally unobstructed to being monogenic* if either f_K represents 1 over $\mathbb{Z}_p$ for all primes p, or f_K represents -1 over $\mathbb{Z}_p$ for all primes p.

Overview

Main theorem for cubic fields

Theorem (Alpöge-Bhargava-S)

A positive proportion of cubic fields are not monogenic despite having no obstruction to being monogenic.

- So a positive proportion of cubic fields are not monogenic for truly global reasons.
- Akhtari-Bhargava proved the analogous theorem for cubic **rings**.
- I'll present a proof which is somewhat different from the arXiv/submitted version.

Outline of proof

A ring generator of $\mathcal{O}_K$ has minimal polynomial $f(t) = t^3 + at + b$ of discriminant $D = \mathrm{Disc}(K)$, hence gives an (almost) integral point P_K on the curve $-27y^2 = 4x^3 + D$. It gives an integral point on the isomorphic curve

$$E_D : y^2 = x^3 - 432D.$$

Consider the set $E_D(\mathbb{Z})_{max}$ of all such points and the map

$$\Psi_D : E_D(\mathbb{Z})_{max} \to E_D(\mathbb{Q})/2E_D(\mathbb{Q}).$$

The proof has three steps:

1. Show that the average size of $E_D(\mathbb{Q})/2E_D(\mathbb{Q})$ is at most 3.
2. Show that the fibers of Ψ_D are uniformly bounded.
3. Impose congruence conditions on D such that for half of such D, there are 2^{100} cubic fields of discriminant D.

Step 1: $\mathrm{avg}_D\, E_D(\mathbb{Q})/2E_D(\mathbb{Q}) \leq 3$

- Ph.D. theses of Ruth and Alpöge.
- More precisely, they prove $\mathrm{avg}_D\, \#\mathrm{Sel}_2(E_D) = 3$.
- The idea is to combine geometry-of-numbers (following Bhargava-Shankar) with the circle method.
- Crucial fact: this result is insensitive to congruence conditions on D.

Step 2: the fibers of ψ_D are uniformly bounded

Each point $P = (x_0, y_0) \in E_D(\mathbb{Z})$ in $E_D(Z)$ gives rise (by 2-descent) to a quartic polynomial

$$F_P(x) = x^4 - 6x_0x^2 + 8y_0x - 3x_0$$

Hence a quartic ring $Q_P = \mathbb{Z}[x]/(F_P)$ and a quartic algebra $W_P = \mathbb{Q}[x]/(F_P)$.

- $\Psi_D(P) = \Psi_D(P')$ if and only if $W_P \simeq W_{P'}$
- If so, then $Q_P \simeq Q_{P'}$ if and only if F_P and $F_{P'}$ are $\mathrm{GL}_2(\mathbb{Z})$-equivalent.
- At most 14 distinct points P' can exist such that $Q_{P'} \simeq Q_P$ (Akhtari).
- Problem: there are roughly $2^{\omega(D)}$ choices for the ring Q_P inside W_P.
- We show that if $P \in E_D(\mathbb{Z})_{max}$, then there is (essentially) just one possibility.

Step 3: Producing many cubic fields

Let $n = 2 \cdot 3 \cdot 5 \cdot 7 \cdot \dots \cdot 541$ be the 101-th primorial.

- We impose the following congruence conditions: take

$$D \in \left\{ -27dn^2 : d \text{ fundamental and } \left(\frac{d}{p}\right) = 1 \text{ for all } p \mid n \right\}$$

- Bhargava-Varma show that $\mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[3] = 0$ for at least half of such D.
- For positive such D, we give an explicit bijection

$$\{\text{cubic fields of discriminant } -27dn^2\} \longleftrightarrow \{\mathbb{Z}[\sqrt{d}]\text{-ideals of norm } n\}/\sim$$

  It follows that there are 2^{100} cubic fields of discriminant D.
- For negative such D, use class field theory!

Overview

Monogenic quartic fields

Theorem (Alpöge-Bhargava-S)

A positive proportion of quartic fields are not binary despite having no local obstruction to being monogenic.

- We will use the previous result and the cubic resolvent construction.
- If $\mathcal{O}_K$ corresponds to the pair $(q_1(X,Y,Z), q_2(X,Y,Z))$ with corresponding symmetric matrices (A_1, A_2), then the cubic resolvent ring R corresponds to the binary cubic form $f(x,y) = \det(A_1 x - A_2 y)$.

Binary quartics and monogenic cubics

Theorem (Wood)

$\mathcal{O}_K$ is binary if and only if R is monogenic.

Proof.

$\mathcal{O}_K$ is binary if and only if $\operatorname{Spec} \mathcal{O}_K$ embeds in a rational normal curve of degree 2, i.e. a smooth conic over $\mathbb{Z}$. This means we can take A_1 to have determinant ± 1. This is equivalent to saying that $f(x, y)$ represents 1 which is equivalent to saying that R is monogenic. □

Outline of proof

1. Use our family $\{K\}$ of non-monogenic cubic fields. For each K, consider the quartic field L_u in the Galois closure of $K(\sqrt{u})$, where u is a non-square unit.
2. Arrange for L_u to be locally unobstructed, using Fess's formula:

$$f_K(x^2, xy, y^2) = F_p(x, y)^3$$

3. Prove that the L_u that arise have all three possible signatures (using another result of Bhargava-Varma).

Thank you!