Introduction

The study of number fields is one of the central topics in number theory. Let $n$ be a natural number. A number field $K$ of degree $n$ is a field of characteristic 0 which is an $n$-dimensional vector space over $\mathbb{Q}$.

- Degree 2 number fields, or quadratic fields, are obtained by adding the square root to the field $\mathbb{Q}$.

$$K = \mathbb{Q}(\sqrt{D}) = \mathbb{Q} \cdot 1 \oplus \mathbb{Q} \cdot \sqrt{D}$$

- Number fields of degree 3, or cubic fields, are obtained by adding the solution of a cubic equation to the field $\mathbb{Q}$. E.g:

$$\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q} \cdot 1 \oplus \mathbb{Q} \cdot \sqrt[3]{2} \oplus \mathbb{Q} \cdot \sqrt[3]{4}$$
Any \( f = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in \mathbb{Q}[x] \) defines a number field \( K \)

\[
K := \mathbb{Q}[x]/(f(x)) : \mathbb{Q} \cdot 1 \oplus \mathbb{Q} \cdot \alpha \oplus \ldots \oplus \mathbb{Q} \cdot \alpha^{n-1}
\]

An \( \alpha \in K \) is an algebraic integer if there is a polynomial

\[
g = x^n + b_{n-1}x^{n-1} + \ldots + b_0 \quad \text{with integer coefficients such that} \quad g(\alpha) = \alpha^n + b_{n-1}\alpha^{n-1} + \ldots + b_0 = 0.
\]

The set \( \mathcal{O}_K \) of all algebraic integers in \( K \) is a subring of \( K \).
• $K = \mathbb{Q}(\sqrt{2})$ i $\alpha = \sqrt{2}$. As $\sqrt{2}$ is a root of $x^2 - 2 \in \mathbb{Z}[x]$, we see that $\sqrt{2} \in \mathcal{O}_K$.

• If we take $\alpha = \sqrt{2}/2$, the minimal polynomial $g$ of $\alpha$ is equal to $x^2 - 1/2$, and $\sqrt{2}/2 \notin \mathcal{O}_K$. In fact $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}] = \mathbb{Z} \cdot 1 \oplus \mathbb{Z} \cdot \sqrt{2}$.

• Another example: $K = \mathbb{Q}(\sqrt{5})$. Notice that $\alpha = \frac{1+\sqrt{5}}{2}$ is a root of $f = x^2 - x - 1$, and so $\alpha \in \mathcal{O}_K$. In fact $\mathcal{O}_K = \mathbb{Z}[\alpha] \supset \mathbb{Z}[\sqrt{5}]$. 
For any number field, $\mathcal{O}_K$ is a ring of rank $n$: it is free and of rank $n$ as a $\mathbb{Z}$-module. In other words, there are: $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$ such that

$$\mathcal{O}_K = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n.$$ 

$\mathcal{O}_K$ is the maximal ring of rank $n$ in $K$: every other ring of rank $n$ in $K$ is contained in $\mathcal{O}_K$.

Every $\alpha \in \mathcal{O}_K$ defines the ring:

$$\mathbb{Z}[\alpha] = \{P(\alpha) : P \in \mathbb{Z}[x]\} \subset \mathcal{O}_K.$$ 

$\mathbb{Z}[\alpha]$ is a ring of rank $n$, with a $\mathbb{Z}$-basis $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$.

Not every ring of rank $n$ is of the form $\mathbb{Z}[\alpha]$! Example: consider the cubic field $K = \mathbb{Q}(\beta)$, where $\beta$ is a root of $x^3 - x^2 - 2x - 8$. One can show that the ring of integers of $\mathcal{O}_K$ is not equal to $\mathbb{Z}[\alpha]$ for any $\alpha$ in $\mathcal{O}_K$.  

Lazar Radičević  
Ring parametrizations and counting numbl  
November 7, 2023  5 / 27
Discriminant of a number field is a numerical invariant that measures its complexity.

Discriminant of a rank $n$ ring $R$: we view $R$ as a free $\mathbb{Z}$-module of rank $n$. Every $\alpha \in R$ defines a linear map $R \to R$ by multiplication: $\beta \mapsto \alpha \cdot \beta$. Define the trace $\text{Tr}(\alpha) \in \mathbb{Z}$ as the trace of this linear map.

We then define a symmetric bilinear form on $R \times R$ by $\langle \alpha, \beta \rangle = \text{Tr}(\alpha \beta)$.

The discriminant of $R$ is defined as the discriminant of this quadratic form.

Concretely, for a $\mathbb{Z}$-basis $\alpha_1, \ldots, \alpha_n$ of $R$, $\text{Disc}(R)$ is the determinant of the $n \times n$ matrix $(\text{Tr}(\alpha_i \alpha_j))_{ij}$.

Discriminant of $K$ is defined as the discriminant of the ring of integers $\mathcal{O}_K$. 
If $R = \mathbb{Z}[x]/(f(x))$, where $f \in \mathbb{Z}[x]$ is monic, $\text{Disc}(R) = \text{Disc}(f)$.

$\text{Disc}(\mathbb{Z}[\sqrt{D}]) = 4D$

For $f = x^3 + px + q$, we have $\mathbb{Z}[x]/(f(x)) = -4p^3 - 27q^2$.

Discriminant can also be interpreted as the covolume of the lattice of $R$ in the Minkowski embedding.

Example: the ring $\mathbb{Z}[\sqrt{-1}]$ is the lattice of points $a + bi$ in $\mathbb{C}$ with $a, b \in \mathbb{Z}$. 

\[
\text{Disc}(\mathbb{Z}[\sqrt{D}]) = 4D
\]

\[
\text{Disc}(\mathbb{Z}[\sqrt{-1}]) = 4 \cdot (-1) = -4
\]
Asymptotic distribution of number fields

The starting point:

**Theorem (Hermite)**

*For every* $X > 0$, *there are only finitely many number fields* $K$ *with* $\text{Disc}(K) < X$.

Let $D(X, n)$ be the set of degree $n$ number fields with $|\text{Disc}(K)| < X$, and let $N(X, n) := |D(X, n)|$. Can we say something about behaviour of $N(X, n)$ as $X \to \infty$?

**Conjecture**

*The limit*

$$\lim_{X \to \infty} \frac{N(X, n)}{X}$$

*exists and is equal to a positive real constant* $c(n)$. 

This conjecture has been proven for $2 \leq n \leq 5$.

For $n = 2$ the proof is simple - all quadratic fields can be listed as $\mathbb{Q}(\sqrt{D})$, where $D$ is a squarefree integer. Discriminant of $\mathbb{Q}(\sqrt{D})$ is equal to $D$ if $D \equiv 1 \pmod{4}$, or to $4D$, if $D \equiv 2, 3 \pmod{4}$.

An elementary analytic number theory argument shows that the limit $c(n)$ exists and is equal to $6/\pi^2$.

Proof by counting the proportion of squarefree integers.
For $n = 3$, the conjecture has been proven by Davenport and Heilbronn in 1971. The cases $n = 4$ and $n = 5$ have been proven by Bhargava in 2005 and 2010.

The proof has two parts.

First part: Delone-Faddeev correspondence is a parametrization of all rings of rank 3 by binary integer cubic forms $f(x, y) \in \mathbb{Z}[x, y]$.

Then, using methods from the geometry of numbers, we count the binary cubic forms $f(x, y)$ of bounded discriminant.
From now on $n = 3$.

The simplest representation of a cubic field is as $\mathbb{Q}[x]/(f(x))$, where $f = x^3 + ax^2 + bx + c \in \mathbb{Q}[x]$. By rescaling the coordinate $x$, we may assume $a, b, c \in \mathbb{Z}$.

But it is not easy to work out what the discriminant of the field is from this representation: - discriminant of $f$ is the discriminant of the ring $\mathbb{Z}[x]/(f(x))$, which often won’t be equal to the full ring of integers $\mathcal{O}_K$.

It is not simple to decide when two polynomials define the same field - we don’t want to overcount.
A binary cubic is a polynomial of the form

\[ f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3 \]

Let \( V_\mathbb{Z} \) be the set of all binary cubic forms with integer coefficients. Consider the following action of the group \( GL_2(\mathbb{Z}) \) on \( V_\mathbb{Z} \):

\[
\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot f(x, y) = (ad - bc)^{-1} f(ax + cy, bx + dy)
\]

In other words, \( g \cdot f(x, y) = \det(g)^{-1} f((x, y) \cdot g) \).
Let $R$ be a cubic ring, with a $\mathbb{Z}$-basis $1, \omega, \theta$. Write

$$\omega \theta = A \cdot 1 + B \cdot \omega + C \cdot \theta$$

for $A, B, C \in \mathbb{Z}$.

We normalize this basis so that $\omega \theta \in \mathbb{Z}$, by replacing $\omega' = \omega - C \cdot 1$ and $\theta' = \theta - B \cdot 1$. 

Lazar Radičević

Ring parametrizations and counting numl

November 7, 2023
The structure of the ring $R$ is determined by the multiplication table for the basis $1, \omega, \theta$. For every normal basis, there are constants $a, b, c, d, k, l, m \in \mathbb{Z}$ for which

$$\omega \theta = k$$
$$\omega^2 = m - b\omega + a\theta$$
$$\theta^2 = l - d\omega + c\theta$$

If we know $a, b, c, d, k, l, m$, we can determine each product

$$(A_1 + B_1\omega + C_1\theta)(A_2 + B_2\omega + C_2\theta).$$
Multiplication is associative: $\omega \cdot \omega \theta = \omega^2 \cdot \theta$ and $\omega \theta \cdot \theta = \omega \cdot \theta^2$. So

$$\omega \cdot k = (m - b\omega + a\theta) \cdot \theta = m\theta - bk + a(l - d\omega + c\theta)$$

$$= al - bk - ad \cdot \omega + (m + ac) \cdot \theta$$

$$k \cdot \theta = \omega \cdot (l - d\omega + c\theta) = l\omega - d(m - b\omega + a\theta) + ck$$

$$= ck - dm + (l + db) \cdot \omega - ad \cdot \theta$$

Equating the coefficients, we find

$$k = -ad$$

$$m = -ac$$

$$l = -bd$$

So $a, b, c$ and $d$ determine uniquely $k, l$ and $m$. 
Key observation: Every quadruple $a, b, c, d \in \mathbb{Z}$, with $k, l, m$ given as above, determines a cubic ring $R$ with commutative and associative multiplication!

The Delone-Fadeev correspondence: to the cubic form $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ we associate the cubic ring $R_f$ determined by the quadruple $a, b, c, d$.

For a given ring $R$, $a, b, c$ and $d$ are uniquely determined by the choice of the normal basis $\omega, \theta$. 
How do we move from one normal basis of $R$ to another?

$\omega, \theta$ defines the basis of the free $\mathbb{Z}$-module $R / \mathbb{Z} \cdot 1$ through the canonical mapping $R \to R / \mathbb{Z} \cdot 1$. Each basis $\bar{\omega}, \bar{\theta}$ of the module $R / \mathbb{Z} \cdot 1$ lifts uniquely to a normal basis $\omega, \theta$.

Two normal bases $\omega, \theta$ and $\omega', \theta'$ are related by $g \in \text{GL}_2(\mathbb{Z})$ with $g \cdot \bar{\omega}' = \bar{\omega}$ and $g \cdot \bar{\theta}' = \bar{\theta}$

$$\bar{\omega} = A \cdot \bar{\omega}' + B \cdot \bar{\theta}'$$
$$\bar{\theta} = C \cdot \bar{\omega}' + D \cdot \bar{\theta}'$$

for $g = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \text{GL}_2(\mathbb{Z})$.

The basis $\omega, \theta$ is obtained by normalizing the basis $g \cdot \omega', g \cdot \omega'$.

If $f$ and $f'$ are binary cubic forms for these two bases, then $f' = g \cdot f$. Conversely, if $f_1$ and $f_2$ are two binary cubic forms with $f_1 = g \cdot f_2$, the rings $R_{f_1}$ and $R_{f_2}$ are isomorphic in a natural way.
Theorem (Delone-Faddeev)

The mapping \( f \mapsto R_f \) defines a bijection between the set of \( \text{GL}_2(\mathbb{Z}) \) equivalence classes of binary cubic forms with integer coefficients and the set of cubic rings, considered up to isomorphism.

- If \( f = x^3 - 2y^3 \), then the ring \( R_f \cong \mathbb{Z}[\sqrt[3]{2}] \) and the basis 1, \( \omega \), \( \theta \) corresponds to the basis 1, \( \sqrt[3]{2} \), \( \sqrt[3]{4} \).
- If the form \( f \) is irreducible, \( R_f \) is a domain.
- For irreducible forms \( f = x^3 + cxy^2 + dy^3 \), \( R_f \cong \mathbb{Z}[\alpha] \), where \( \alpha \) is the root of the polynomial \( f(x, 1) = x^3 + cx + d \). The basis 1, \( \omega \), \( \theta \) corresponds to the basis 1, \( \alpha \), \( \alpha^2 \).
- We also get various "exotic" rings if \( f \) is not irreducible - for example, if \( f = 0 \), \( R_f = \mathbb{Z}[x, y]/(x^2, xy, y^2) \). If \( f = x^3 \), \( R_f = \mathbb{Z}[x]/(x^3) \).
The discriminant of the cubic form $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ is defined as

$$\text{Disc}(f) = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd$$

We have $\text{Disc}(f) = \text{Disc}(R_f)$, and $\text{Disc}(g \cdot f) = \text{Disc}(f)$ for every $g \in \text{GL}_2(\mathbb{Z})$, i.e. $\text{Disc}(f)$ is $\text{GL}_2(\mathbb{Z})$-invariant.
Davenport-Heilbronn theorem

**Theorem (Davenport-Heilbronn)**

Let $N_3(A, B)$ be the number of cubic fields $K$, up to isomorphism, with $A < \text{Disc}(K) < B$. Then

$$N_3(0, X) = \frac{1}{12\zeta(3)} X + o(X),$$

$$N_3(-X, 0) = \frac{1}{4\zeta(3)} X + o(X)$$
We can also count cubic rings.

**Theorem**

Let $M_3(A, B)$ be the number of cubic rings $R$, up to isomorphism, with $A < \text{Disc}(R) < B$. Then

\[
M_3(0, X) = \frac{\pi^2}{24} X + o(X),
\]
\[
M_3(-X, 0) = \frac{\pi^2}{72} X + o(X)
\]

By the Delone-Faddeev correspondence $M_3(A, B)$ is the number of $GL_2(\mathbb{Z})$-equivalence classes of binary cubic forms $f$ with $A < \text{Disc}(f) < B$. 
We count cubic forms using geometry of numbers.

Let $V_\mathbb{R} = \{ ax^3 + bx^2y + cxy^2 + dy^3 : a, b, c, d \in \mathbb{R} \} \cong \mathbb{R}^4$.

We construct a fundamental domain $\mathcal{F}$ for the action of $GL_2(\mathbb{Z})$ on $V_\mathbb{R}$ - a set $\mathcal{F}$ containing a representative of each $GL_2(\mathbb{Z})$-class in $V_\mathbb{R}$.

The number of $GL_2(\mathbb{Z})$-classes $[f]$ with $A < \text{Disc}(f) < B$ is the number of cubic forms $f$ in $\mathcal{F}$ with integer coefficients and $A < \text{Disc}(f) < B$.

We want to estimate the number of points $\mathcal{F}$ with integer coordinates and the discriminant in this range.
To count integer points we use the following result of Davenport.

**Theorem**

Let $\mathcal{R}$ be a bounded, semi-algebraic multiset in $\mathbb{R}^n$ having maximum multiplicity $m$, and which is defined by at most $k$ polynomial inequalities each having degree at most $l$. Then the number of integer lattice points (counted with multiplicity) contained in the region $\mathcal{R}$ is is

$$\text{Vol}(\mathcal{R}) + O(\max\{\text{Vol}(\bar{\mathcal{R}}), 1\})$$

where $\text{Vol}(\bar{\mathcal{R}})$ denotes the greatest $d$-dimensional volume of any projection of $\mathcal{R}$ onto a coordinate subspace obtained by equating $nd$ coordinates to zero, where $d$ takes all values from 1 to $n - 1$. The implied constant in the second summand depends only on $n, m, k$ and $l$. 
Proof sketch

- First step: Write down a fundamental domain $\mathcal{F}$.
- Key point: there are only two orbits for the action of $\text{GL}_2(\mathbb{R})$ the space $\mathcal{V}_\mathbb{R}$ of real binary cubics.
- The two orbits are $\text{GL}_2(\mathbb{R}) \cdot f_1$ and $\text{GL}_2(\mathbb{R}) \cdot f_2$ where $f_1$ has 3 real roots and $f_2$ has one real root.
- So a fundamental domain can be expressed in terms of the fundamental domain for $\text{GL}_2(\mathbb{R})/\text{GL}_2(\mathbb{Z})$, and this essentially the well-known fundamental domain for $\text{SL}_2(\mathbb{Z})$ acting on the upper half plane.
Define $\mathcal{R}_X(\mathcal{F}) = \{ f \in \mathcal{F} : \text{Disc}(f) < X \}$. We want to count integer points in $\mathcal{R}_X(\mathcal{F})$.

We show the equality $\text{Vol}(\mathcal{R}_X(\mathcal{F})) = C \cdot X$, for a suitable constant $C > 0$.

We don’t need all integer points in $\mathcal{R}_X(\mathcal{F})$ - just the ones that correspond to irreducible forms, since those correspond to non-degenerate rings.

Now we apply Davenport’s result to count integer points. Applying the theorem directly to the region $\mathcal{R}_X(\mathcal{F})$ is not good enough. We remove a thin cusp from $\mathcal{R}_X(\mathcal{F})$, which has a small volume but many integer points. These points correspond to degenerate rings, so that we can ignore them.
To count cubic fields, we only want to count maximal orders. These can be characterised by a mod $p^2$ condition for every prime $p$.

Analogous to the quadratic situation: we don’t want to count rings of the form $\mathbb{Z}[\sqrt{p^2D}] = \mathbb{Z}[p\sqrt{D}]$.

Bhargava, Shankar and Tsimerman improve on this by using not only one fundamental domain, but they instead average over a continuous family of them.

This makes applying Davenport’s theorem simpler, and it also allows them to prove a secondary error term:

$$N_3(0, X) = \frac{1}{12\zeta(3)}X + \frac{4\zeta(1/3)}{5\Gamma(2/3)^3\zeta(5/3)}X^{5/6} + O(X^{5/6-1/48+\epsilon})$$
Thanks for listening!