Arithmetic of quadratic integers.

1. Review of Elementary Number Theory

- Main object of study: $\mathbb{Z}$.

What do we know about $\mathbb{Z}$?

- We have the operations addition, subtraction, and multiplication. (no division, e.g. $\frac{1}{2} \notin \mathbb{Z}$.)
- It is built additively from 1.
- It is built multiplicatively from the set of primes $2, 3, 5, 7, 11, \cdots$.
- The prime factorization of an integer is unique!

  Theorem 1.1 (The Fundamental Theorem of Arithmetic - FTOA)**.** *Every $n \in \mathbb{Z}$ with $n \neq \pm 1$ can be written uniquely in the form*

  $$n = \pm p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$$

  where $p_1 < p_2 < \cdots < p_n$ are prime numbers and $e_1, \cdots, e_n$ are positive integers.

- The uniqueness part of the theorem can come in handy!
  Simple Example: find all the integer solutions of $x^2 - y^2 = 15$.

  $$(x - y)(x + y) = 3 \times 5.$$

  By Unique Factorization: $(x - y, x + y) = \pm(3, 5), (5, 3), (1, 15), (15, 1)$.
  Integer Solutions: $(|x|, |y|) = (8, 7), (4, 1)$.

Harder problems: how could we show that the following equations have no integer solutions?

- $x^3 = y^2 + 2 = (y - \sqrt{-2})(y + \sqrt{-2})$.
- $x^3 = y^2 + 51$.

To factor these equations, we need "quadratic integers"

2. The quadratic integers

Let α be a complex number.

$$\mathbb{Z}[\alpha] := \{p(\alpha) : p \in \mathbb{Z}[x]\}.$$

Throughout the talk, let D be a discriminant.

Definition 2.1. *The ring of discriminant D quadratic integers is defined to be $\mathcal{O}_D := \mathbb{Z}[\frac{D+\sqrt{D}}{2}]$.*

One can show

$$\mathcal{O}_D = \mathbb{Z} + \left(\frac{D + \sqrt{D}}{2}\right)\mathbb{Z},$$

i.e. $1, \frac{D+\sqrt{D}}{2}$ are the additive building blocks of $\mathcal{O}_D$.

Definition 2.2.

$$\mathbb{Q}(\sqrt{D}) := \{x + y\sqrt{D} : x, y \in \mathbb{Q}\}$$

The norm map is the function $N : \mathbb{Q}(\sqrt{D}) \to \mathbb{Z}$ defined by

$$N(x + y\sqrt{D}) = (x + y\sqrt{D})(x - y\sqrt{D}) = x^2 - Dy^2.$$

Definition 2.3. *We say that $\alpha \in \mathcal{O}_D$ is **irreducible** if there are no $\gamma, \beta \in \mathcal{O}_D$ such that $\alpha = \beta\gamma$ and $|N(\beta)| < |N(\alpha)|$ and $|N(\gamma)| < |N(\alpha)|$.*

Examples: 2,3, $1 \pm \sqrt{-5}$ are irreducible in $\mathcal{O}_{-20}$.

FTOA does not hold hold in $\mathcal{O}_D$, e.g. $2 \times 3 = (1 - \sqrt{-5})(1 + \sqrt{-5})$.

3. The class group

Goal: Find a way to describe or measure the degree to which unique factorization fails.
For simplicity, assume that D is a fundamental discriminant. This means:

- D is square-free and $D \equiv 1 \pmod 4$, or
- D is a multiple of 4 and $D/4 \equiv 2, 3 \pmod 4$.

A fractional ideal is a set $\alpha\mathcal{O}_D + \beta\mathcal{O}_D =: (\alpha, \beta)$, where $\alpha, \beta \in \mathbb{Q}(\sqrt{D})$. A fractional ideal is principal if it is of the form $\alpha\mathcal{O}_D$, where $\alpha \in \mathbb{Q}(\sqrt{D})$.
Ideals can be preferable to numbers because ideals in $\mathcal{O}_D$ factor uniquely into prime ideals.

- The prime ideals of $\mathcal{O}_D$ have a nice description relating them to the primes of $\mathbb{Z}$.

Theorem 3.1. *The primes are given by:*

- *(p) where $p \in \mathbb{Z}$ is an integer prime for which D is not a square modulo p. We say such a prime p is inert.*
- *Nontrivial ideals P_1, P_2 where $P_1P_2 = (p)$, where $p \in \mathbb{Z}$ is an integer prime, for example if p factors in $\mathcal{O}_D$. If $p|D$ then p ramifies, if $p \nmid D$ then p splits.*

Example: $D = -20$

$$2 \times 3 = (1 - \sqrt{-5})(1 + \sqrt{-5}).$$

implies the ideal factorization

$$(2) \cdot (3) = (6) = (1 - \sqrt{-5}) \cdot (1 + \sqrt{-5})$$

Factoring into prime ideals,

$$\begin{aligned}
&(2) \cdot (3) \\
&= (2, (1 + \sqrt{-5}))^2 \cdot (3, (1 + \sqrt{-5})) \cdot (3, (1 - \sqrt{-5})) \\
&= (2, (1 + \sqrt{-5}))(3, (1 + \sqrt{-5})) \cdot (2, (1 + \sqrt{-5}))(3, (1 - \sqrt{-5})) \\
&= (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})
\end{aligned}$$

The ideals in the middle are nonprincipal, 2 ramifies, 3 splits. Since nonprincipal ideals obstruct unique factorization, we want to measure the prevalence on nonprincipal ideals.

Definition 3.2. *The class group of* $\mathbb{Q}(\sqrt{D})$ *is*

$$Cl(D) := (\textit{frac. ideals of } \mathcal{O}_D)/(\textit{ principal frac. ideals of } \mathcal{O}_D)$$

The class number of $\mathbb{Q}(\sqrt{D})$ *is*

$$h(D) := |Cl(D)| < \infty.$$

We have that $h(D) = 1 \iff \mathcal{O}_D$ has unique factorization into primes.
Theme for the rest of the talk: the behavior of $h(D)$ as D varies.

4. The size of the class number

Gauss (1798): formulated conjectures about the size of $h(D)$.
$D > 0$: Gauss' Conjectured Infinitely many $D > 0$ have $h(D) = 1$.b

- Cohen-Lenstra heuristics predict $h(D) = 1$ for ≈ 75 % of $D > 0$ with D or $D/4$ prime, but it is not known that $h(D) = 1$ for infinitely many D.

For the rest of the talk, assume $D < 0$.
Gauss' conjecture for $D < 0$: For any h, there are only finitely many $D < 0$ such that $h(D) = h$.

- **Heilbronn:** $h(D) \to \infty$ as $D \to -\infty$
- **Baker, Heegner, Stark:** $h(D) = 1$ for exactly 9 negative D.
- **Siegel:** For any $\epsilon > 0$, $|D|^{\frac{1}{2}-\epsilon} \ll h(D) \ll |D|^{\frac{1}{2}+\epsilon}$.
- **Gross-Zagier, Goldfeld, Oesterlé:** $C_\epsilon(\log(D))^{1-\epsilon} \leq h(D)$.

Open question: finding better effective lower bounds of $h(D)$ when $D < 0$.

5. Divisibility properties of $h(D)$

Let ℓ be prime, and $D < 0$.
Question: how often is $h(D)$ a multiple of ℓ?

- **Gauss (1800):** $2 \nmid h(D)$ when $|D|$ is prime.
- **Hartung:** For any p, $p \nmid h(D)$ for infinitely many D.
- **Davenport-Heilbronn** If $\epsilon > 0$, for sufficiently large X $\frac{\#\{-X<D<0:3\nmid h(D)\}}{\#\{-X<D<0\}} \geq \frac{1}{2} - \epsilon$.
- **Conjecture (Cohen-Lenstra):**

$$\lim_{X\to\infty} \frac{\#\{-X < D < 0 : p \nmid h(D)\}}{\#\{-X < D < 0\}} = \prod_{n=1}^{\infty} \left(1 - \frac{1}{p^n}\right)$$

- **Kohnen-Ono (1999):** For any $\epsilon > 0$, for sufficiently large X

$$\#\{-X < D < 0 : p \nmid h(D)\} \geq \left(\frac{2(p-2)}{\sqrt{3}(p-1)} - \epsilon\right) \frac{\sqrt{X}}{\log X}.$$

6. Class number divisibility and local conditions

We've been discussing the behavior of $h(D)$ as D varies over all discriminants. What if we restrict the set of discriminants? For example, we might want certain primes to be inert or split in our ring. For such problems, the mere existence of a single quadratic field satisfying the prescribed properties is often elusive.

Question: Given a finite set of local conditions (e.g. specified primes that must split, ramify, or remain inert), can we find $D < 0$ such that $\mathbb{Q}(\sqrt{D})$ satisfies these local conditions and $\ell \nmid h(D)$?

Theorem 6.1. *Bruinier (1999) Let $\ell \geq 3$ be prime. Let $\Sigma = S_0 \cup S_+ \cup S_-$ be finite disjoint sets of odd primes, such that for all $p \in \Sigma$, $p \not\equiv \pm 1, 0 \pmod{\ell}$.*

There exists $D < 0$ with $\ell \nmid h(D)$ such that:

1. *For all $p \in S_-$, p is inert in $\mathbb{Q}(\sqrt{D})$.*
2. *For all $p \in S_0$, p ramifies in $\mathbb{Q}(\sqrt{D})$.*
3. *For all $p \in S_+$, p splits in $\mathbb{Q}(\sqrt{D})$.*

- Proof uses the modular form θ^3.

Theorem 6.2 (Wiles (2015))**.** *Let $\ell \geq 3$ be prime. Let $\Sigma = S_0 \cup S_+ \cup S_-$ be finite disjoint sets of odd primes, $\ell \notin \Sigma$, such that:*

- *S_0 contains no $p \equiv 1 \pmod{\ell}$*
- *S_+ contains no $p \equiv -1 \pmod{\ell}$*
- *S_- contains no p which is $1 \pmod{\ell}$ and $-1 \pmod{4}$.*

There exists $D < 0$ with $\ell \nmid h(D)$ such that:

1. *For all $p \in S_-$, p is inert in $\mathbb{Q}(\sqrt{D})$.*
2. *For all $p \in S_0$, p ramifies in $\mathbb{Q}(\sqrt{D})$.*
3. *For all $p \in S_+$, p splits in $\mathbb{Q}(\sqrt{D})$.*

- Proof uses Shimura curves and Galois representations.

Theorem 6.3. *Theorem (B, Raum, Richter, 2024+) Let $\ell \geq 2$ be a prime and S_+ a finite set of odd primes. Then there exists an imaginary quadratic field $\mathbb{Q}(\sqrt{D})$ satisfying*

1. *$\ell \nmid h(D)$,*
2. *$\mathbb{Q}(\sqrt{D})$ is split at each prime of S_+.*

- No control over which primes are inert or ramify, but the primes that split can be arbitrary.
- Proof uses mock modular forms.