The typical elasticity of a quadratic order

Steve Fan

Joint with Paul Pollack (University of Georgia)

October 22, 2024

Elements: the dawn of arithmetic

Let $\mathbb{N} = \{1, 2, 3, ...\}$ be the set of positive integers. There are two basic binary operations on $\mathbb{N}$: addition "$+$" and multiplication "$\times$", the latter of which leads naturally to the notions of divisibility and factorization.

Let $\mathbb{P} \subseteq \mathbb{N}$ be the subset consisting of all $n > 1$ for which there are no positive integers $a, b > 1$ such that $n = ab$. The elements of $\mathbb{P}$ are called *primes* or *irreducibles*. It was known to Euclid that every $n > 1$ can be written as a product of finitely many primes.

Elements: the dawn of arithmetic

Let $\mathbb{N} = \{1, 2, 3, ...\}$ be the set of positive integers. There are two basic binary operations on $\mathbb{N}$: addition "$+$" and multiplication "$\times$", the latter of which leads naturally to the notions of divisibility and factorization.

Let $\mathbb{P} \subseteq \mathbb{N}$ be the subset consisting of all $n > 1$ for which there are no positive integers $a, b > 1$ such that $n = ab$. The elements of $\mathbb{P}$ are called *primes* or *irreducibles*. It was known to Euclid that every $n > 1$ can be written as a product of finitely many primes.

In his treatise *Elements*, Euclid demonstrated two important properties of primes:

1. $\#\mathbb{P} = \infty$.
2. If $a, b \in \mathbb{N}$ and $p \in \mathbb{P}$ are such that $p \mid ab$, then $p \mid a$ or $p \mid b$.

Property 2 is commonly used as the definition of prime elements of a commutative ring, while the one given above often serves as the definition of irreducible elements.

The missing element

Euclid proved the existence of prime factorization. Although he was probably aware that the prime factorization of a positive integer >1 is unique apart from rearrangement of its prime factors, he did not try to state it explicitly, let alone write down a proof of it. Nor did many mathematicians that came after him, who confidently took the idea of unique factorization for granted. Gauss seems to be the first to provide a precise statement of unique factorization of $\mathbb{N}$ as well as a rigorous proof.

Theorem 1.1 (The fundamental theorem of arithmetic)

Every positive integer $n > 1$ admits a prime factorization which is unique up to the order of its prime factors.

Gauss' proof of the fundamental theorem given in his book "Disquisitiones Arithmeticae" is based on Property 2 discovered by Euclid. Arguably, Euclid could have proved this theorem if he had tried.

Unique factorization in $\mathbb{Z}$

The fundamental theorem can be reformulated as the following for the ring of rational integers $\mathbb{Z} := \pm\mathbb{N} \cup \{0\}$.

Theorem 1.2 (Unique prime factorization in $\mathbb{Z}$)

Every $n \in \mathbb{Z} \setminus \{0, \pm 1\}$ admits a prime factorization $n = p_1 \cdots p_k$ with $p_1, ..., p_k \in \pm\mathbb{P}$ for some $k \in \mathbb{N}$, and this factorization is unique up to the order of the prime factors $p_1, ..., p_k$ and up to unit factors ± 1.

The uniqueness part says that if $n = p_1 \cdots p_k = q_1 \cdots q_\ell$ are two prime factorizations of n, then we must have (1) $k = \ell$ and (2) there exists a rearrangement $q_{j_1}, ..., q_{j_k}$ of $q_1, ..., q_k$ such that $q_{j_i} = \pm p_i$ for all $1 \leq i \leq k$.

The notion of prime factorization extends naturally to that of factorization into irreducible elements in a general integral domain.

Irreducible factorization in a domain

Let D be a domain. A nonzero nonunit element of D is *irreducible* if it cannot be written as a product of two nonunit elements.

Irreducible factorization in a domain

Let D be a domain. A nonzero nonunit element of D is *irreducible* if it cannot be written as a product of two nonunit elements.

A domain D is a *unique factorization domain (UFD)* if every nonzero nonunit element of D can be written as a product of finitely many irreducibles uniquely up to the order of the factors and up to units.

Example 1 (Examples of UFD)

1. Principle ideal domains (PIDs): $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}[e^{2\pi i/3}]$, $\mathbb{Z}_p$, $K[x]$ and $K[[x]]$ with K a field, etc.
2. The polynomial ring $D[x_1, ..., x_k]$, where D is a UFD.

Irreducible factorization in a domain

Let D be a domain. A nonzero nonunit element of D is *irreducible* if it cannot be written as a product of two nonunit elements.

A domain D is a *unique factorization domain (UFD)* if every nonzero nonunit element of D can be written as a product of finitely many irreducibles uniquely up to the order of the factors and up to units.

Example 1 (Examples of UFD)

1. Principle ideal domains (PIDs): $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}[e^{2\pi i/3}]$, $\mathbb{Z}_p$, $K[x]$ and $K[[x]]$ with K a field, etc.
2. The polynomial ring $D[x_1, ..., x_k]$, where D is a UFD.

In a UFD, an element is prime iff it is irreducible. So any factorization into irreducibles in a UFD is a genuine prime factorization.

Lamé's dream

In 1847, Lamé, who had solved Fermat's equation $x^7 + y^7 = z^7$, presented to the Paris Academy an outline of what he believed was a complete proof of Fermat's Last Theorem. His proof rests on the assumption that the ring of integers $\mathbb{Z}[e^{2\pi i/p}]$ of any cyclotomic field $\mathbb{Q}(e^{2\pi i/p})$ is a UFD.

Lamé's dream

In 1847, Lamé, who had solved Fermat's equation $x^7 + y^7 = z^7$, presented to the Paris Academy an outline of what he believed was a complete proof of Fermat's Last Theorem. His proof rests on the assumption that the ring of integers $\mathbb{Z}[e^{2\pi i/p}]$ of any cyclotomic field $\mathbb{Q}(e^{2\pi i/p})$ is a UFD.

Liouville: "I'm skeptical. The UFD assumption is unjustified."

Lamé's dream

In 1847, Lamé, who had solved Fermat's equation $x^7 + y^7 = z^7$, presented to the Paris Academy an outline of what he believed was a complete proof of Fermat's Last Theorem. His proof rests on the assumption that the ring of integers $\mathbb{Z}[e^{2\pi i/p}]$ of any cyclotomic field $\mathbb{Q}(e^{2\pi i/p})$ is a UFD.

Liouville: "I'm skeptical. The UFD assumption is unjustified."

Cauchy: "Looks promising. I'm also very close to having a solution based on a similar idea."

Lamé's dream

In 1847, Lamé, who had solved Fermat's equation $x^7 + y^7 = z^7$, presented to the Paris Academy an outline of what he believed was a complete proof of Fermat's Last Theorem. His proof rests on the assumption that the ring of integers $\mathbb{Z}[e^{2\pi i/p}]$ of any cyclotomic field $\mathbb{Q}(e^{2\pi i/p})$ is a UFD.

Liouville: "I'm skeptical. The UFD assumption is unjustified."

Cauchy: "Looks promising. I'm also very close to having a solution based on a similar idea."

Wantzel: "I have a proof that $\mathbb{Z}[e^{2\pi i/p}]$ is a UFD. You see, though I only considered $p = 2, 3$, the proof generalizes easily."

Lamé's dream

In 1847, Lamé, who had solved Fermat's equation $x^7 + y^7 = z^7$, presented to the Paris Academy an outline of what he believed was a complete proof of Fermat's Last Theorem. His proof rests on the assumption that the ring of integers $\mathbb{Z}[e^{2\pi i/p}]$ of any cyclotomic field $\mathbb{Q}(e^{2\pi i/p})$ is a UFD.

Liouville: "I'm skeptical. The UFD assumption is unjustified."

Cauchy: "Looks promising. I'm also very close to having a solution based on a similar idea."

Wantzel: "I have a proof that $\mathbb{Z}[e^{2\pi i/p}]$ is a UFD. You see, though I only considered $p = 2, 3$, the proof generalizes easily."

Cauchy: "Hold on, your argument doesn't work when $p \geq 5$."

Lamé's dream

In 1847, Lamé, who had solved Fermat's equation $x^7 + y^7 = z^7$, presented to the Paris Academy an outline of what he believed was a complete proof of Fermat's Last Theorem. His proof rests on the assumption that the ring of integers $\mathbb{Z}[e^{2\pi i/p}]$ of any cyclotomic field $\mathbb{Q}(e^{2\pi i/p})$ is a UFD.

Liouville: "I'm skeptical. The UFD assumption is unjustified."

Cauchy: "Looks promising. I'm also very close to having a solution based on a similar idea."

Wantzel: "I have a proof that $\mathbb{Z}[e^{2\pi i/p}]$ is a UFD. You see, though I only considered $p = 2, 3$, the proof generalizes easily."

Cauchy: "Hold on, your argument doesn't work when $p \geq 5$."

Liouville: "Okay guys. I just read an article written by Mr. Kummer which confirmed the failure of unique factorization in $\mathbb{Z}[e^{2\pi i/23}]$."

Dedekind's ideal theory

We now know that $\mathbb{Z}[e^{2\pi i/p}]$ is a UFD iff $p \leq 19$, thanks to Montgomery (1971) and Uchida (1971). A simpler example of a non-UFD is $\mathbb{Z}[\sqrt{-5}]$, the ring of integers of $\mathbb{Q}(\sqrt{-5})$. In this domain, we have

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

where $2, 3, 1 + \sqrt{-5}$, and $1 - \sqrt{-5}$ are all irreducible but not prime!

Dedekind's ideal theory

We now know that $\mathbb{Z}[e^{2\pi i/p}]$ is a UFD iff $p \leq 19$, thanks to Montgomery (1971) and Uchida (1971). A simpler example of a non-UFD is $\mathbb{Z}[\sqrt{-5}]$, the ring of integers of $\mathbb{Q}(\sqrt{-5})$. In this domain, we have

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

where $2, 3, 1+\sqrt{-5}$, and $1-\sqrt{-5}$ are all irreducible but not prime!

Nonetheless, Dedekind showed that the nonzero proper ideals of a number ring do possess unique factorizations into prime ideals.

More precisely, every nonzero proper ideal I of the ring of integers

$$\mathcal{O}_K := \{\alpha \in K \colon f(\alpha) = 0 \text{ for some monic } f \in \mathbb{Z}[x]\}$$

of a number field K admits a factorization $I = P_1 \cdots P_k$ unique up to the order of the prime ideal factors $P_1, \ldots, P_k \subseteq \mathcal{O}_K$.

For instance, we have in $\mathbb{Z}[\sqrt{-5}]$ that

$$(6) = \left(2, 1+\sqrt{-5}\right)^2 \left(3, 1+\sqrt{-5}\right) \left(3, 1-\sqrt{-5}\right).$$

Measuring unique factorization: class group

For a number field K, let I_K be the collection of nonzero fractional ideals of $\mathcal{O}_K$ and P_K the collection of nonzero principal fractional ideals of $\mathcal{O}_K$. They become abelian groups under multiplication.

The ideal class group $\mathrm{Cl}(K)$ of K is defined by $\mathrm{Cl}(K) := I_K/P_K$.

We define the class number $h(K)$ of K by $h(K) := \#\mathrm{Cl}(K)$.

Measuring unique factorization: class group

For a number field K, let I_K be the collection of nonzero fractional ideals of $\mathcal{O}_K$ and P_K the collection of nonzero principal fractional ideals of $\mathcal{O}_K$. They become abelian groups under multiplication.

The ideal class group Cl(K) of K is defined by Cl$(K) := I_K/P_K$.

We define the class number $h(K)$ of K by $h(K) := \#$Cl(K).

It can be shown that $h(K) < \infty$ and that

$$h(K) = 1 \Longleftrightarrow \mathcal{O}_K \text{ is a PID} \Longleftrightarrow \mathcal{O}_K \text{ is a UFD.}$$

So Cl(K) measures how far $\mathcal{O}_K$ is from being a UFD.

Since $h(\mathbb{Q}(\sqrt{-5})) = 2$ and $h(\mathbb{Q}(e^{2\pi i/23})) = 3$, $\mathbb{Z}[e^{2\pi i/23}]$ is farther from being a UFD than $\mathbb{Z}[\sqrt{-5}]$.

Searching for UF$\mathcal{O}$s

Let $K_d = \mathbb{Q}(\sqrt{d})$ be a quadratic number field, where $d \in \mathbb{Z}$ is square-free.

For imaginary quadratic fields ($d < 0$), it was conjectured by Gauss (1801) and proved by Heegner (1952), Baker (1966), Stark (1967), et al., that

$$h(K_d) = 1 \Longleftrightarrow d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}.$$

Little is known about real quadratic fields ($d > 0$). It is an open conjecture that $h(K_d) = 1$ for infinitely many $d > 0$. In fact, it is not even known if there are infinitely many number fields with class number 1.

In general, pinpointing UFDs is hard!

Introducing elasticity

We have seen that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD. For the factorization

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

uniqueness fails only halfway, since both factorizations contain exactly 2 irreducible factors. In general, what if we concentrate on length?

Introducing elasticity

We have seen that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD. For the factorization

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

uniqueness fails only halfway, since both factorizations contain exactly 2 irreducible factors. In general, what if we concentrate on length?

A domain D is *atomic* if every nonzero nonunit element in D can be factored into irreducibles (such as $\mathcal{O}_K$). Given nonzero nonunit $\alpha \in D$, the *length spectrum* $\mathcal{L}(\alpha)$ of α is the set of the lengths of all possible irreducible factorizations of α. We define the *elasticity* $\rho(\alpha)$ of α by

$$\rho(\alpha) := \frac{\sup \mathcal{L}(\alpha)}{\inf \mathcal{L}(\alpha)}.$$

The elasticity $\rho(D)$ of D is then defined to be the supremum of $\rho(\alpha)$ over all nonzero nonunits $\alpha \in D$.

Stretching a domain

Elasticity quantifies the failure of unique factorization in the length aspect while being blind to the irreducible factors themselves.

An atomic domain D is a *half-factorial domain (HFD)* if for every nonzero nonunit $\alpha \in D$, all the factorizations of α share the same length, namely, the same number of irreducible factors. Such domains are the stiffest, since they have the smallest elasticity, i.e., 1.

Stretching a domain

Elasticity quantifies the failure of unique factorization in the length aspect while being blind to the irreducible factors themselves.

An atomic domain D is a *half-factorial domain (HFD)* if for every nonzero nonunit $\alpha \in D$, all the factorizations of α share the same length, namely, the same number of irreducible factors. Such domains are the stiffest, since they have the smallest elasticity, i.e., 1.

Theorem 2.1 (Carlitz, 1960)

The ring of integers of a number field K is a HFD iff $h(K) \in \{1, 2\}$.

Since $h(\mathbb{Q}(\sqrt{-5})) = 2$, $\mathbb{Z}[\sqrt{-5}]$ is a HFD.

On the other hand, Kummer's example $\mathbb{Z}[e^{2\pi i/23}]$ is not a HFD because $h(\mathbb{Q}(e^{2\pi i/23})) = 3$.

The Davenport constant

For any finite abelian group G, the *Davenport constant* $D(G)$ is the smallest $D \in \mathbb{N}$ such that any sequence $\{g_i\}_{i=1}^{D} \subseteq G$ has a nonempty subsequence whose product equals the identity.

The Davenport constant

For any finite abelian group G, the *Davenport constant* $D(G)$ is the smallest $D \in \mathbb{N}$ such that any sequence $\{g_i\}_{i=1}^{D} \subseteq G$ has a nonempty subsequence whose product equals the identity.

Proposition 2.2

Let G be an abelian group of order n. Then the following holds.

1. $D(G) \leq n$ *with equality precisely when* G *is cyclic.*
2. *If* G *has invariant factor decomposition*

$$G \cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}, \qquad d_1 \mid d_2 \mid \cdots \mid d_r,$$

then

$$D(G) \geq D^*(G) := 1 + \sum_{i=1}^{r}(d_i - 1).$$

Consequently, $D(G) \geq \frac{\log 2n}{\log 2}$.

Elasticity meets Davenport

Theorem 2.3 (Steffan (1986), Valenza (1990), Narkiewicz (1995))

For any number field K, we have

$$\rho(\mathcal{O}_K) = \max\left\{1, \frac{1}{2}D(\mathsf{Cl}(K))\right\}.$$

For instance, if $\mathcal{O}_K$ is not a UFD, then

$$\mathcal{O}_K \text{ is a HFD} \overset{\text{Thm } 2.3}{\iff} D(\mathsf{Cl}(K)) = 2 \overset{\text{Prop } 2.2}{\iff} h(K) = 2.$$

Theorem 2.3 also shows that $\mathcal{O}_K$ becomes more and more elastic as the class group $\mathsf{Cl}(K)$ inflates.

Elasticity meets Davenport

Theorem 2.3 (Steffan (1986), Valenza (1990), Narkiewicz (1995))

For any number field K, we have

$$\rho(\mathcal{O}_K) = \max\left\{1, \frac{1}{2}D(\mathsf{Cl}(K))\right\}.$$

For instance, if $\mathcal{O}_K$ is not a UFD, then

$$\mathcal{O}_K \text{ is a HFD} \overset{\text{Thm } 2.3}{\iff} D(\mathsf{Cl}(K)) = 2 \overset{\text{Prop } 2.2}{\iff} h(K) = 2.$$

Theorem 2.3 also shows that $\mathcal{O}_K$ becomes more and more elastic as the class group $\mathsf{Cl}(K)$ inflates.

Unfortunately, we do not have a general formula for $D(G)$ of an arbitrary finite abelian group G. Olson (1969) showed that $D(G) = D^*(G)$ if G is a p-group or $G = \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}$ with $d_1 \mid d_2$.

A quick proof of $\rho(\mathcal{O}_K) \leq \frac{1}{2}D(\mathsf{Cl}(K))$

Proof of $\rho(\mathcal{O}_K) \leq \frac{1}{2}D(\mathsf{Cl}(K))$.

Suppose that $\mathcal{O}_K$ is not a UFD, so that $D := D(\mathsf{Cl}(K)) \geq 2$. For every nonzero nonunit $\alpha \in \mathcal{O}_K$, let $\Omega_K(\alpha)$ denote the number of prime ideal factors of $\alpha\mathcal{O}_K$. Fix an arbitrary nonzero nonunit $\alpha \in \mathcal{O}_K$, and suppose $\alpha = \pi_1 \cdots \pi_m = \rho_1 \cdots \rho_n$ are two irreducible factorizations of α, where $m \geq n$. It suffices to prove $m/n \leq D/2$ when $m > n$.

Observation. We may assume, without loss of generality, that none of the π_i is prime. If some π_i is prime, then π_i is a unit multiple of ρ_j for some j. Canceling the factor π_i from both factorizations of α yields two irreducible factorizations of α/π_i of lengths $m-1$ and $n-1$, respectively, with ratio $(m-1)/(n-1) > m/n$. Repeating this procedure until none of the π_i left is prime, we obtain two irreducible factorizations of some $\beta \mid \alpha$ with length ratio $> m/n$.

A quick proof of $\rho(\mathcal{O}_K) \leq \frac{1}{2}D(\mathsf{Cl}(K))$

Proof of $\rho(\mathcal{O}_K) \leq \frac{1}{2}D(\mathsf{Cl}(K))$.

We claim that $\Omega_K(\rho_j) \leq D$ for every $1 \leq j \leq n$. To see this, assume to the contrary that $\rho_j\mathcal{O}_K = P_1 \cdots P_s$ with $s > D$. After rearranging the prime ideal factors, we may assume $[P_1] \cdots [P_D] = [\mathcal{O}_K]$, by the definition of $D = D(\mathsf{Cl}(K))$. Let $\beta \in \mathcal{O}_K$ be a generator of $P_1 \cdots P_D$. Then $\rho_j\mathcal{O}_K = (\beta\mathcal{O}_K)\, P_{D+1} \cdots P_s$, which implies $\beta \mid \rho_j$. But ρ_j is irreducible. So ρ_j is a unit multiple of β. Hence, $\mathcal{O}_K = P_{D+1} \cdots P_s$, which is impossible.

A quick proof of $\rho(\mathcal{O}_K) \leq \frac{1}{2}D(\mathsf{Cl}(K))$

Proof of $\rho(\mathcal{O}_K) \leq \frac{1}{2}D(\mathsf{Cl}(K))$.

We claim that $\Omega_K(\rho_j) \leq D$ for every $1 \leq j \leq n$. To see this, assume to the contrary that $\rho_j\mathcal{O}_K = P_1 \cdots P_s$ with $s > D$. After rearranging the prime ideal factors, we may assume $[P_1] \cdots [P_D] = [\mathcal{O}_K]$, by the definition of $D = D(\mathsf{Cl}(K))$. Let $\beta \in \mathcal{O}_K$ be a generator of $P_1 \cdots P_D$. Then $\rho_j\mathcal{O}_K = (\beta\mathcal{O}_K)\, P_{D+1} \cdots P_s$, which implies $\beta \mid \rho_j$. But ρ_j is irreducible. So ρ_j is a unit multiple of β. Hence, $\mathcal{O}_K = P_{D+1} \cdots P_s$, which is impossible.

By $\alpha\mathcal{O}_K = \rho_1\mathcal{O}_K \cdots \rho_n\mathcal{O}_K$, we have

$$\Omega_K(\alpha) = \sum_{j=1}^{n} \Omega_K(\rho_j) \leq Dn.$$

On the other hand, since none of the π_i is prime, we have $\Omega_K(\pi_i) \geq 2$ for each $1 \leq i \leq m$. Thus $\Omega_K(\alpha) \geq 2m$. Combining this with the upper bound for $\Omega_K(\alpha)$ above completes the proof. □

Orders of the day

Let K be a number field. An *order in* K is a subring of $\mathcal{O}_K$ containing a $\mathbb{Q}$-basis for K.

If K is quadratic, then an order in K is simply a subring of $\mathcal{O}_K$ properly containing $\mathbb{Z}$. Orders in K are in one-to-one correspondence with $\mathbb{N}$: For each $f \in \mathbb{N}$, there is a unique order $\mathcal{O}_f$ with index $[\mathcal{O}_K : \mathcal{O}_f] = f$, i.e.,

$$\mathcal{O}_f = \mathbb{Z} \oplus f\mathcal{O}_K = \{\alpha \in \mathcal{O}_K : \alpha \equiv a \pmod{f\mathcal{O}_K} \text{ for some } a \in \mathbb{Z}\}.$$

Conversely, every order $\mathcal{O}$ in K is of the form $\mathcal{O}_f$ for some $f \in \mathbb{N}$, with the maximal order $\mathcal{O}_K = \mathcal{O}_1$. The integer f is called the *conductor* of $\mathcal{O}_f$.

Example 2

Let $K = \mathbb{Q}(\sqrt{5})$ with $\mathcal{O}_K = \mathbb{Z}[\omega]$, where $\omega = (\sqrt{5}+1)/2$. Then

$$\mathcal{O}_2 = \mathbb{Z} \oplus 2\mathcal{O}_K = \mathbb{Z}[\sqrt{5}].$$

HFDs among orders

Since non-maximal orders are not integrally closed, they cannot be UFDs. But they can still be HFDs!

Theorem 3.1 (Coykendall, 2001)

$\mathbb{Z}[\sqrt{-3}]$ is the only half-factorial non-maximal order in an imaginary quadratic field.

Conjecture (Coykendall, 2001)

1. *There are infinitely many pairs (K, f), where K is a real quadratic field and $f \in \mathbb{N}$, for which $\mathcal{O}_f$ is a HFD in K.*
2. *There are infinitely many $f \in \mathbb{N}$ for which $\mathcal{O}_f$ is a HFD in $\mathbb{Q}(\sqrt{2})$.*

HFDs among orders

Since non-maximal orders are not integrally closed, they cannot be UFDs. But they can still be HFDs!

Theorem 3.1 (Coykendall, 2001)

$\mathbb{Z}[\sqrt{-3}]$ is the only half-factorial non-maximal order in an imaginary quadratic field.

Conjecture (Coykendall, 2001)

1. *There are infinitely many pairs (K, f), where K is a real quadratic field and $f \in \mathbb{N}$, for which $\mathcal{O}_f$ is a HFD in K.*
2. *There are infinitely many $f \in \mathbb{N}$ for which $\mathcal{O}_f$ is a HFD in $\mathbb{Q}(\sqrt{2})$.*

Theorem 3.2 (Pollack, 2023&2024)

1 is true, and 2 is true assuming GRH. Moreover, on GRH, every $(n+1)/2$ with $n \in \mathbb{N} \cup \{\infty\}$ occurs as the elasticity of infinitely many orders in $\mathbb{Q}(\sqrt{2})$.

How elastic?

Given a quadratic number field K with discriminant Δ, what is the typical size of $\rho(\mathcal{O}_f)$ of an order $\mathcal{O}_f$ in K?

In general, the elasticity of an order may be infinite. A theorem due to Halter-Koch (1995) asserts that an order $\mathcal{O}$ in a number field K has finite elasticity precisely when every nonzero prime ideal of $\mathcal{O}$ lies below a unique prime ideal of $\mathcal{O}_K$. Thus, if K is quadratic, then an order $\mathcal{O}_f$ in K has finite elasticity precisely when f is *split-free*, meaning that f is free of prime factors that split completely in K.

How elastic?

Given a quadratic number field K with discriminant Δ, what is the typical size of $\rho(\mathcal{O}_f)$ of an order $\mathcal{O}_f$ in K?

In general, the elasticity of an order may be infinite. A theorem due to Halter-Koch (1995) asserts that an order $\mathcal{O}$ in a number field K has finite elasticity precisely when every nonzero prime ideal of $\mathcal{O}$ lies below a unique prime ideal of $\mathcal{O}_K$. Thus, if K is quadratic, then an order $\mathcal{O}_f$ in K has finite elasticity precisely when f is *split-free*, meaning that f is free of prime factors that split completely in K.

Moreover, the number of split-free integers in $[1, x]$ is $\sim cx/\sqrt{\log x}$ for some constant $c > 0$. So, given any quadratic field K, almost all orders in K have elasticity ∞. This suggests that the proper object of study is not $\rho(\mathcal{O}_f)$ for all conductors $f \in \mathbb{N}$, but its restriction to split-free f.

Main results

Theorem 3.3 (F. and Pollack, 2024)

If K is a fixed imaginary quadratic field, then for almost all split-free f,

$$\rho(\mathcal{O}_f) = f/(\log f)^{\frac{1}{2}\log_3 f + \frac{1}{2}C_K + O((\log_4 f)^3/\log_3 f)},$$

where C_K is constant. Here and below, "for almost all split-free f" means for all but $o(x/\sqrt{\log x})$ split-free numbers $f \le x$, as $x \to \infty$.

The typical elasticity of a real quadratic order turns out to be quite smaller.

Theorem 3.4 (F. and Pollack, 2024)

If K is a fixed real quadratic field, then conditionally on GRH, for almost all split-free f,

$$\rho(\mathcal{O}_f) = (\log f)^{\frac{1}{2} + O(1/\log_4 f)}.$$

Class group revisited

For each $f \in \mathbb{N}$, let $I_K(f)$ denote the group of fractional ideals of K generated by integral ideals comaximal with $f\mathcal{O}_K$, with $I_K(1) = I_K$.

Let $P_K(f)$ denote the subgroup of $I_K(f)$ generated by principal ideals $\alpha\mathcal{O}_K$, where $\alpha \equiv a \pmod{f\mathcal{O}_K}$ for some $a \in \mathbb{Z}$ with $\gcd(a, f) = 1$, with $P_K(1) = P_K$.

The *class group* $\mathrm{Cl}(\mathcal{O}_f)$ of the order $\mathcal{O}_f$ is defined to be the quotient $I_K(f)/P_K(f)$, with $\mathrm{Cl}(\mathcal{O}_1) = \mathrm{Cl}(K)$.

Class group revisited

For each $f \in \mathbb{N}$, let $I_K(f)$ denote the group of fractional ideals of K generated by integral ideals comaximal with $f\mathcal{O}_K$, with $I_K(1) = I_K$.

Let $P_K(f)$ denote the subgroup of $I_K(f)$ generated by principal ideals $\alpha\mathcal{O}_K$, where $\alpha \equiv a \pmod{f\mathcal{O}_K}$ for some $a \in \mathbb{Z}$ with $\gcd(a, f) = 1$, with $P_K(1) = P_K$.

The *class group* $\mathsf{Cl}(\mathcal{O}_f)$ of the order $\mathcal{O}_f$ is defined to be the quotient $I_K(f)/P_K(f)$, with $\mathsf{Cl}(\mathcal{O}_1) = \mathsf{Cl}(K)$.

We have seen that

$$\rho(\mathcal{O}_K) = \max\left\{1, \frac{1}{2}D(\mathsf{Cl}(K))\right\}.$$

In a similar vein, we relate $\rho(\mathcal{O}_f)$ to $D(\mathsf{Cl}(\mathcal{O}_f))$.

The recipe

1. Relate $\rho(\mathcal{O}_f)$ to $D(\mathsf{Cl}(\mathcal{O}_f))$:

$$\frac{1}{2}D(\mathsf{Cl}(\mathcal{O}_f)) \leq \rho(\mathcal{O}_f) \leq \max\left\{\frac{1}{2}D(\mathsf{Cl}(\mathcal{O}_f)) + \frac{3}{2}\Omega(f), 1\right\}.$$

It can be shown that the quantity $\Omega(f)$ is typically of a smaller order than $D(\mathsf{Cl}(\mathcal{O}_f))$. Hence, $\rho(\mathcal{O}_f) \approx \frac{1}{2}D(\mathsf{Cl}(\mathcal{O}_f))$ most of the time.

The recipe

1. Relate $\rho(\mathcal{O}_f)$ to $D(\mathsf{Cl}(\mathcal{O}_f))$:

$$\frac{1}{2}D(\mathsf{Cl}(\mathcal{O}_f)) \leq \rho(\mathcal{O}_f) \leq \max\left\{\frac{1}{2}D(\mathsf{Cl}(\mathcal{O}_f)) + \frac{3}{2}\Omega(f), 1\right\}.$$

It can be shown that the quantity $\Omega(f)$ is typically of a smaller order than $D(\mathsf{Cl}(\mathcal{O}_f))$. Hence, $\rho(\mathcal{O}_f) \approx \frac{1}{2}D(\mathsf{Cl}(\mathcal{O}_f))$ most of the time.

2. Use the *principle subgroup* $\mathsf{PrinCl}(\mathcal{O}_f)$ as a proxy for $\mathsf{Cl}(\mathcal{O}_f)$:

$$D(\mathsf{PrinCl}(\mathcal{O}_f)) \leq D(\mathsf{Cl}(\mathcal{O}_f)) \leq h(K)D(\mathsf{PrinCl}(\mathcal{O}_f)),$$

where $\mathsf{PrinCl}(\mathcal{O}_f)$ is defined as the quotient

$$(\mathcal{O}_K/f\mathcal{O}_K)^\times/\langle\text{images of integers coprime to } f\text{, units of } \mathcal{O}_K\rangle,$$

which we identify with $(I_K(f) \cap P_K)/P_K(f) \leq \mathsf{Cl}(\mathcal{O}_f)$ of index $h(K)$.

The recipe

3. Pass from $\mathrm{PrinCl}(\mathcal{O}_f)$ to the *pre-class group* $\mathrm{PreCl}(\mathcal{O}_f)$:

$$\mathrm{PreCl}(\mathcal{O}_f) := (\mathcal{O}_K/f\mathcal{O}_K)^\times/\langle \text{images of integers prime to } f\rangle.$$

Thus, $\mathrm{PrinCl}(\mathcal{O}_f) = \mathrm{PreCl}(\mathcal{O}_f)/\left(\text{image of } \mathcal{O}_K^\times\right)$. It is not hard to show that $\#\mathrm{PreCl}(\mathcal{O}_f) = \psi(f)$, where

$$\psi(f) := f\prod_{p\mid f}\left(1-\frac{\chi(p)}{p}\right),$$

and $\chi := (\Delta/\cdot)$ is the Kronecker symbol. The group $\mathrm{PreCl}(\mathcal{O}_f)$ is a close cousin of the more familiar $(\mathbb{Z}/n\mathbb{Z})^\times$ whose order is $\varphi(n)$.

The recipe

4. If K is imaginary, then

$$\frac{D(\mathsf{PreCl}(\mathcal{O}_f))}{D\left(\text{image of } \mathcal{O}_K^\times\right)} \leq D(\mathsf{PrinCl}(\mathcal{O}_f)) \leq D(\mathsf{PreCl}(\mathcal{O}_f)),$$

where $D\left(\text{image of } \mathcal{O}_K^\times\right) \leq \#\mathcal{O}_K^\times \leq 6$. Hence, $D(\mathsf{PrinCl}(\mathcal{O}_f))$ is within a factor of 6 of $D(\mathsf{PreCl}(\mathcal{O}_f))$.

On the other hand, it is known that for any finite abelian group G,

$$1 \leq \frac{D(G)}{\mathsf{Exp}(G)} \leq 1 + \log \frac{\#G}{\mathsf{Exp}(G)},$$

where $\mathsf{Exp}(G)$ is the exponent of G. Applying this to $G = \mathsf{PreCl}(\mathcal{O}_f)$, we have

$$1 \leq \frac{D(\mathsf{PreCl}(\mathcal{O}_f))}{\mathsf{Exp}(\mathsf{PreCl}(\mathcal{O}_f))} \leq 1 + \log \frac{\psi(f)}{\mathsf{Exp}(\mathsf{PreCl}(\mathcal{O}_f))}.$$

The recipe

5. If K is real, then $\mathsf{PrinCl}(\mathcal{O}_f)) \cong \mathsf{PreCl}(\mathcal{O}_f)/\langle\text{image of } \varepsilon\rangle$, where $\varepsilon > 1$ is the normalized fundamental unit of $\mathcal{O}_K$. Let

$$\ell(f) := \frac{\#\mathsf{PreCl}(\mathcal{O}_f)}{\#\mathsf{PrinCl}(\mathcal{O}_f)},$$

which can be described concretely as the least positive integer ℓ for which $\varepsilon^\ell \in \mathcal{O}_f$. Clearly, $\#\mathsf{PrinCl}(\mathcal{O}_f) = \psi(f)/\ell(f)$. We exploit

$$1 \le \frac{D(\mathsf{PrinCl}(\mathcal{O}_f))}{\mathsf{Exp}(\mathsf{PrinCl}(\mathcal{O}_f))} \le 1 + \log \frac{\#\mathsf{PrinCl}(\mathcal{O}_f)}{\mathsf{Exp}(\mathsf{PrinCl}(\mathcal{O}_f))}.$$

The recipe

5. If K is real, then $\mathsf{PrinCl}(\mathcal{O}_f) \cong \mathsf{PreCl}(\mathcal{O}_f)/\langle\text{image of } \varepsilon\rangle$, where $\varepsilon > 1$ is the normalized fundamental unit of $\mathcal{O}_K$. Let

$$\ell(f) := \frac{\#\mathsf{PreCl}(\mathcal{O}_f)}{\#\mathsf{PrinCl}(\mathcal{O}_f)},$$

which can be described concretely as the least positive integer ℓ for which $\varepsilon^\ell \in \mathcal{O}_f$. Clearly, $\#\mathsf{PrinCl}(\mathcal{O}_f) = \psi(f)/\ell(f)$. We exploit

$$1 \leq \frac{D(\mathsf{PrinCl}(\mathcal{O}_f))}{\mathsf{Exp}(\mathsf{PrinCl}(\mathcal{O}_f))} \leq 1 + \log \frac{\#\mathsf{PrinCl}(\mathcal{O}_f)}{\mathsf{Exp}(\mathsf{PrinCl}(\mathcal{O}_f))}.$$

Hence, we have reduced the proof of our theorems to the estimation of

- $\mathsf{Exp}(\mathsf{PreCl}(\mathcal{O}_f))$ when K is imaginary;
- $\mathsf{Exp}(\mathsf{PrinCl}(\mathcal{O}_f))$ and $\ell(f)$ when K is real.

The exponent of $\mathsf{PreCl}(\mathcal{O}_f)$

Chinese Remainder Theorem $\Rightarrow \mathsf{PreCl}(\mathcal{O}_f) \cong \prod_{p^k \| f} \mathsf{PreCl}(\mathcal{O}_{p^k})$, whence

$$\mathsf{Exp}(\mathsf{PreCl}(\mathcal{O}_f)) = \mathsf{lcm}\left\{\mathsf{Exp}(\mathsf{PreCl}(\mathcal{O}_{p^k})) \colon p^k \parallel f\right\},$$

which is an analogue to the familiar definition of the Carmichael function

$$\lambda(n) := \mathsf{Exp}\left((\mathbb{Z}/n\mathbb{Z})^{\times}\right) = \mathsf{lcm}\left\{\mathsf{Exp}\left((\mathbb{Z}/p^k\mathbb{Z})^{\times}\right) \colon p^k \parallel n\right\}.$$

The lemma below, due essentially to Halter-Koch, determines almost all of the exponents $\mathsf{PreCl}(\mathcal{O}_{p^k})$.

Lemma 3.5

If $p > 3$ is inert or ramified in K, then $\mathsf{PreCl}(\mathcal{O}_{p^k})$ is cyclic.

The exponent of $\mathsf{PreCl}(\mathcal{O}_f)$

Chinese Remainder Theorem $\Rightarrow \mathsf{PreCl}(\mathcal{O}_f) \cong \prod_{p^k \| f} \mathsf{PreCl}(\mathcal{O}_{p^k})$, whence

$$\mathsf{Exp}(\mathsf{PreCl}(\mathcal{O}_f)) = \mathsf{lcm}\left\{\mathsf{Exp}(\mathsf{PreCl}(\mathcal{O}_{p^k}))\colon p^k \parallel f\right\},$$

which is an analogue to the familiar definition of the Carmichael function

$$\lambda(n) := \mathsf{Exp}\left((\mathbb{Z}/n\mathbb{Z})^\times\right) = \mathsf{lcm}\left\{\mathsf{Exp}\big((\mathbb{Z}/p^k\mathbb{Z})^\times\big)\colon p^k \parallel n\right\}.$$

The lemma below, due essentially to Halter-Koch, determines almost all of the exponents $\mathsf{PreCl}(\mathcal{O}_{p^k})$.

Lemma 3.5

If $p > 3$ is inert or ramified in K, then $\mathsf{PreCl}(\mathcal{O}_{p^k})$ is cyclic.

An immediate corollary of Lemma 3.5 is that for all split-free $f \in \mathbb{N}$,

$$L'(f) \mid \mathsf{Exp}(\mathsf{PreCl}(\mathcal{O}_f)) \mid L(f).$$

The exponent of PreCl$(\mathcal{O}_f)$

Recall that Exp(PreCl$(\mathcal{O}_f)$) is sandwiched by $L(f)$ and $L'(f)$, where

$$L(f) := \mathrm{lcm}\{\psi(p^k) : p^k \parallel f\},$$
$$L'(f) := \mathrm{lcm}\{\psi(p^k) : p^k \parallel f,\, p > 3\}.$$

In particular, $L(f)$ may be viewed as an analogue to $\lambda(n)$.

The exponent of $\mathsf{PreCl}(\mathcal{O}_f)$

Recall that $\mathsf{Exp}(\mathsf{PreCl}(\mathcal{O}_f))$ is sandwiched by $L(f)$ and $L'(f)$, where

$$L(f) := \mathsf{lcm}\{\psi(p^k) : p^k \parallel f\},$$
$$L'(f) := \mathsf{lcm}\{\psi(p^k) : p^k \parallel f, p > 3\}.$$

In particular, $L(f)$ may be viewed as an analogue to $\lambda(n)$.

Proposition 3.6 (F. and Pollack, 2024)

For almost all split-free f,

$$L(f) = f/(\log f)^{\frac{1}{2}\log_3 f + \frac{1}{2}C_K + O((\log_4 f)^3/\log_3 f)}.$$

The same estimate holds with $L'(f)$ replacing $L(f)$.

Our proof adapts the argument of Erdős, Pomerance, and Schmutz (1991) on the typical size of $\lambda(n)$.

Back to the real world

Let K be real quadratic. We still need to estimate $\mathrm{Exp}(\mathrm{PrinCl}(\mathcal{O}_f))$ and $\ell(f)$.

Back to the real world

Let K be real quadratic. We still need to estimate $\mathrm{Exp}(\mathrm{PrinCl}(\mathcal{O}_f))$ and $\ell(f)$.

Proposition 3.7 (F. and Pollack, 2024)

Let K be a real quadratic field. Under GRH, we have, for almost all split-free f,

1. $\mathrm{Rad}\left(\mathrm{Exp}(\mathrm{PrinCl}(\mathcal{O}_f))\right) = (\log f)^{\frac{1}{2}+O(1/\log_4 f)}$,
2. $\mathrm{Exp}(\mathrm{PrinCl}(\mathcal{O}_f)) = \mathrm{Rad}\left(\mathrm{Exp}(\mathrm{PrinCl}(\mathcal{O}_f))\right)(\log f)^{O(1/\log_4 f)}$,
3. $L(f)/\ell(f) = (\log f)^{O(1/\log_4 f)}$.

The treatment of $\ell(f)$ requires a GRH-conditional version of the Chebotarev density theorem due to Serre (1981).

The proof Proposition 3.7 borrows ideas from Pollack (2021) on the normal order of $\omega(\varphi(n)/\lambda(n))$, and from the proof of a result on the largest prime factor of $\lambda(n)/\ell_a(n)$ due to Li and Pomerance (2003), from which a GRH-conditional central limit theorem for $\omega(\ell_a(n))$, first established by Murty and Saidak (2001), can be recovered, where $\ell_a(n)$ denotes the order of $a \pmod n$.

One more thing:

One more thing: the normal order of an additive function

An important tool for studying the normal order of an additive function is the Turán–Kubilius inequality. Let $f\colon \mathbb{N} \to \mathbb{C}$ be an additive function. Define

$$A_f(x) := \sum_{p^k \leq x} \frac{f(p^k)}{p^k} \left(1 - \frac{1}{p}\right),$$

which we may think of as an approximation to the mean value of f over $[1, x]$. The Turán–Kubilius inequality asserts that

$$\frac{1}{x} \sum_{n \leq x} |f(n) - A_f(x)|^2 \ll B_f(x),$$

where

$$B_f(x) := \sum_{p^k \leq x} \frac{|f(p^k)|^2}{p^k}.$$

Thus, if $B_f(x) = o(|A_f(x)|^2)$, then $f(n) \approx A_f(x)$ for almost all $n \in \mathbb{N} \cap [1, x]$.

Attaching weight

Let $\alpha\colon \mathbb{N} \to \mathbb{R}_{\geq 0}$ be a multiplicative function with $S_\alpha(x) := \sum_{n \leq x} \alpha(n)$. Suppose that there exist $c_\alpha, \delta > 0$, $\sigma \geq 0$ and $\kappa \in \mathbb{R}$, such that

1. uniformly for all $x \geq 1$ and all squarefree $a \in \mathbb{N} \cap [1, x^\delta]$ with at most two prime factors,

$$\sum_{\substack{n \leq x \\ (n,a)=1}} \alpha(n) = c_\alpha x^\sigma (\log 3x)^{\kappa-1} \left(F_\alpha(a)^{-1} + O\left(\frac{1}{\log\log 3x} \right) \right), \quad (1)$$

where

$$F_\alpha(a) := \prod_{p \mid a} \sum_{k \geq 0} \frac{\alpha(p^k)}{p^{k\sigma}} < \infty;$$

2. for all $x \geq 2$,

$$\sum_{p^k \leq x} \frac{\alpha(p^k)}{p^{k\sigma}} \log p^k \ll \log x. \quad (2)$$

A heavy gem: weighted Turán–Kubilius

Theorem 3.8 (F. and Pollack, 2024)

Let $\alpha\colon \mathbb{N} \to \mathbb{R}_{\geq 0}$ be a multiplicative function satisfying the conditions ① *and* ② *on the previous slide. Then for any additive function $f\colon \mathbb{N} \to \mathbb{C}$, we have*

$$S_\alpha(x)^{-1} \sum_{n \leq x} \alpha(n) \left| f(n) - A_{\alpha,f}(x) \right|^2 \ll B_{\alpha,f}(x) \tag{3}$$

for all $x \geq 1$, where

$$A_{\alpha,f}(x) := \sum_{p^k \leq x} \alpha(p^k) F_\alpha(p)^{-1} \frac{f(p^k)}{p^{k\sigma}},$$

$$B_{\alpha,f}(x) := \sum_{p^k \leq x} \alpha(p^k) \frac{|f(p^k)|^2}{p^{k\sigma}} \left(1 - \frac{\log p^k}{\log 3x}\right)^{\min(\kappa-1,0)}.$$

The implied constant in (3) *depends at most on δ, κ and the implied constants in* (1) *and* (2).

Weighted Turán–Kubilius in action

Fixing a quadratic field K with discriminant Δ, we take $\alpha = 1_{\text{split-free}}$, with partial sums $S_\alpha(x) = c_\alpha x(\log 3x)^{-1/2}(1 + O(1/\log 3x))$, where

$$c_\alpha = \sqrt{\frac{1}{\pi L(1,\chi)} \cdot \frac{|\Delta|}{\varphi(|\Delta|)}} \prod_{p \text{ inert}} \left(1 - \frac{1}{p^2}\right)^{-1/2}, \quad \text{with } \chi := (\Delta/\cdot).$$

A crucial step in determining the typical size of $L(f)$ is to estimate the following cutoff of $\log \psi(f)$:

$$h(f) := \sum_{\substack{p \le y \log y \\ p^k \| \psi(f)}} \log p^k, \quad \text{where } y = \log\log x.$$

An application of our weighted Turán–Kubilius inequality to $h(f)$ yields

$$\left| h(f) - \frac{1}{2} y \log y - \frac{1}{2} y \log_2 y - \frac{c'}{2} y \right| < \frac{y}{\log y}$$

for all but $o(x/\sqrt{\log x})$ split-free $f \le x$, where c' is a constant depending on Δ.

"A peculiar beauty reigns in the realm of mathematics, a beauty which resembles not so much the beauty of art as the beauty of nature and which affects the reflective mind, which has acquired an appreciation of it, very much like the latter."

— Ernst Eduard Kummer