Stretching

the Truth about Non-Unique Factorization

Paul Pollack
University of Georgia

Unique factorization?

Let D be an integral domain. A nonzero, nonunit element $\pi \in D$ is **irreducible** if π cannot be written as a product of two nonunits.

A domain D is a **unique factorization domain (UFD)** if every nonzero nonunit is a product of irreducibles and this expression is unique up to order and up to unit factors.

Unique factorization?

Let D be an integral domain. A nonzero, nonunit element $\pi \in D$ is **irreducible** if π cannot be written as a product of two nonunits.

A domain D is a **unique factorization domain (UFD)** if every nonzero nonunit is a product of irreducibles and this expression is unique up to order and up to unit factors.

More precisely, we require that if $\pi_1 \cdots \pi_k = \rho_1 \ldots \rho_\ell$, with all the π_i and ρ_j irreducible, then

(a) $k = \ell$,

(b) after rearranging, π_i is a D-unit multiple of ρ_i for all $i = 1, 2, \ldots, k$.

Unique factorization's greatest hits

In a first algebra course, one meets several instances where unique factorization holds. Some of the most prominent are ...

$\mathbb{Z}$: the ring of rational integers,

$F[x]$: polynomials over a field F,

$\mathbb{Z}[i]$: the **Gaussian integers** $a + bi$ with $a, b \in \mathbb{Z}$.

It's interesting to trace the history of the proofs. Arguably Euclid could have proved $\mathbb{Z}$ possessed unique factorization, except that he never quite tried to do so. The first complete proof for $\mathbb{Z}$ seems due to Gauss in his *Disquisitiones*.

The proofs for $F[x]$ and $\mathbb{Z}[i]$ are also due to Gauss. Gauss looked at the arithmetic of $F[x]$ in an unpublished Section VIII of the *Disquisitiones* and he investigated the number theory of $\mathbb{Z}[i]$ while looking at 4th power reciprocity.

. . . and misses

These examples can lull one into a false sense of security!

The following near-canonical example of non-unique factorization is helpful to keep students on their toes: In the ring $\mathbb{Z}[\sqrt{-5}]$,

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

This is a *genuine* example of non-unique factorization: all of $2, 3$, $1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ are irreducible in $\mathbb{Z}[\sqrt{-5}]$. Furthermore, the only units in $\mathbb{Z}[\sqrt{-5}]$ are ± 1, so there is no chance that the irreducibles on the left are unit multiples of those on the right.

. . . and misses

These examples can lull one into a false sense of security!

The following near-canonical example of non-unique factorization is helpful to keep students on their toes: In the ring $\mathbb{Z}[\sqrt{-5}]$,

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

This is a *genuine* example of non-unique factorization: all of $2, 3$, $1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ are irreducible in $\mathbb{Z}[\sqrt{-5}]$. Furthermore, the only units in $\mathbb{Z}[\sqrt{-5}]$ are ± 1, so there is no chance that the irreducibles on the left are unit multiples of those on the right.

Thus, $\mathbb{Z}[\sqrt{-5}]$ is not a UFD! But as we will see later in this talk, it's close.

. . . and misses

These examples can lull one into a false sense of security!

The following near-canonical example of non-unique factorization is helpful to keep students on their toes: In the ring $\mathbb{Z}[\sqrt{-5}]$,

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

This is a *genuine* example of non-unique factorization: all of $2, 3$, $1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ are irreducible in $\mathbb{Z}[\sqrt{-5}]$. Furthermore, the only units in $\mathbb{Z}[\sqrt{-5}]$ are ± 1, so there is no chance that the irreducibles on the left are unit multiples of those on the right.

Thus, $\mathbb{Z}[\sqrt{-5}]$ is not a UFD! But as we will see later in this talk, it's close.

What could that possibly mean?

Where will we look?

We will be primarily interested in rings coming from number fields.

A **number field** is a finite extension $K/\mathbb{Q}$. For each number field K, we let $\mathcal{O}_K$ (the **ring of integers of** K) denote the integral closure of $\mathbb{Z}$ in K. Concretely,

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

Examples

- $\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$
- $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})} = \mathbb{Z}[\sqrt{-5}]$
- $\mathcal{O}_{\mathbb{Q}(\sqrt[3]{2})} = \mathbb{Z}[\sqrt[3]{2}]$
- $\mathcal{O}_{\mathbb{Q}(\sqrt{5})} = \mathbb{Z}[(1+\sqrt{5})/2]$.

Paradise lost and paradise regained

The example of $\mathbb{Z}[\sqrt{-5}]$ shows that $\mathcal{O}_K$ is not always a UFD. But this is not the end of the story!

Dedekind proved that while elementwise factorization in $\mathcal{O}_K$ need not be unique, one always has unique factorization of ideals. That is, every nonzero ideal of $\mathcal{O}_K$ factors uniquely as a product of nonzero prime ideals. (Old-fashioned books, and old-fashioned people, call this the "Fundamental theorem of ideal theory".)

How much goes wrong?

How we might quantify the failure of elementwise unique factorization?

First of all, let's get units out of the picture.

Let $\mathrm{IntPrin}(K)$ denote the collection of nonzero principal ideals of $\mathcal{O}_K$. We can view $\mathrm{IntPrin}(K)$ as a monoid under ideal multiplication. This has the same multiplicative structure as $\mathcal{O}_K \setminus \{0\}$, but without the influence of the pesky units.

Let $\mathrm{IntId}(K)$ denote the collection of nonzero ideals of $\mathcal{O}_K$. Dedekind says: $\mathrm{IntId}(K)$ is a monoid that possesses unique factorization!

So one way to quantify non-unique factorization would be to answer: How far away is $\mathrm{IntPrin}(K)$ from $\mathrm{IntId}(K)$?

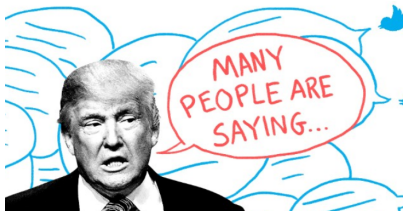
How much goes wrong? ctd.

Let $\mathrm{Id}(K)$ be the group of nonzero fractional ideals of K, and let $\mathrm{Prin}(K)$ denote the group of nonzero principal fractional ideals. (These are the groups generated by $\mathrm{IntId}(K)$ and $\mathrm{IntPrin}(K)$.) The **class group** of $\mathcal{O}_K$ is defined as the quotient

$$\mathrm{Cl}(\mathcal{O}_K) = \mathrm{Id}(K)/\mathrm{Prin}(K).$$

One can show: $\mathcal{O}_K$ is a UFD precisely when $\mathrm{Cl}(\mathcal{O}_K)$ is trivial.

$\mathrm{Cl}(\mathcal{O}_K)$ need not be trivial, but a basic fact from algebraic number theory is that $\mathrm{Cl}(\mathcal{O}_K)$ is always finite.



Very common to hear: "the class group measures the failure of unique factorization."

The class group knows everything about the failure of unique factorization. The hard part is getting it to speak!

To elaborate, let's revisit $\mathbb{Z}[\sqrt{-5}]$. We saw already that uniqueness of factorization fails here, since $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

The class group knows everything about the failure of unique factorization. The hard part is getting it to speak!

To elaborate, let's revisit $\mathbb{Z}[\sqrt{-5}]$. We saw already that uniqueness of factorization fails here, since $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$. It's less well-known that **uniqueness fails only halfway!** Recall uniqueness means: If $\pi_1 \cdots \pi_k = \rho_1 \ldots \rho_\ell$, with all π_i and ρ_j irreducible, then

(a) $k = \ell$,

(b) after rearranging, π_i is a unit multiple of ρ_i for all $i = 1, 2, \ldots, k$.

Condition (a) turns out to be just fine!

A classy explanation

We say a domain D is a **half-factorial domain** (**HFD**) if every nonzero nonunit element of D factors as a product of irreducibles, and any two factorizations of the same element share the same number of irreducible factors.

Theorem (Carlitz, 1960)

Let K be a number field. If $\#\mathrm{Cl}(\mathcal{O}_K) = 1$ or 2, then $\mathcal{O}_K$ is an HFD, and vice-versa.

Since $\mathbb{Q}(\sqrt{-5})$ has class number 2, its ring of integers $\mathbb{Z}[\sqrt{-5}]$ is an HFD, as claimed.

On the other hand, $\mathbb{Q}(\sqrt{-23})$ has class number 3. Here $3 \cdot 3 \cdot 3 = (2 + \sqrt{-23})(2 - \sqrt{-23})$, showing half-uniqueness fails.

Stretching, the truth

Let D be a domain where every nonzero nonunit factors into irreducibles. (This is true for all the $\mathcal{O}_K$.) For each nonzero nonunit $\alpha \in D$, we define the **length spectrum** of α by

$$\mathcal{L}(\alpha) = \{\text{all lengths } k \text{ of irreducible factorizations } \alpha = \pi_1 \cdots \pi_k\}.$$

We define the **elasticity** of α by

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

Finally, we define the elasticity $\rho(D)$ of D by

$$\rho(D) = \sup_{\alpha} \rho(\alpha).$$

So $\rho(D) = 1$ if and only if D is an HFD.

Fun. Theorem of Stretchiness

Let K be a number field.

Theorem (Valenza, Narkiewicz, Steffan)

Assume $\mathcal{O}_K$ is not a UFD. Then

$$\rho(\mathcal{O}_K) = \frac{1}{2} \cdot \textit{Davenport constant of } \mathrm{Cl}(\mathcal{O}_K).$$

OK, but what is the Davenport constant? For a finite abelian group G, the Davenport constant $D(G)$ is the smallest positive integer D such that any length D sequence

$$g_1, g_2, \ldots, g_D$$

of elements of G has some nonempty subsequence whose product is the identity.

Orientation

Exercises

If G is a finite abelian group of size n, then

(a) $D(G) \leq n$, with equality when G is cyclic,

(b) $D(G) - 1 \geq \frac{\log n}{\log 2}$, with equality when n is an elementary abelian 2-group.

Remarkably, even though $D(G)$ is known exactly for all p-groups, we do not have a formula for $D(G)$ in general.

Sketch of the lower bound

We sketch a proof that $\rho(\mathcal{O}_K) \geq \frac{1}{2}D$.

We need the following theorem of Landau: Every class in $\mathrm{Cl}(\mathcal{O}_K)$ is represented by infinitely many nonzero prime ideals of $\mathcal{O}_K$.

Let $D = D(\mathrm{Cl}(\mathcal{O}_K))$. By the definition of D, and the fact above, we can choose prime ideals $P_1, \dots, P_{D-1}$ so that $P_1, \dots, P_{D-1}$ has no nonempty subsequence multiplying to the identity in $\mathrm{Cl}(\mathcal{O}_K)$.

We can then choose P_D in the inverse class of $P_1 \cdots P_{D-1}$. Then $P_1 \cdots P_D$ is principal, say $P_1 \cdots P_D = \pi\mathcal{O}_K$.

Then π is irreducible: If $\pi = \alpha\beta$, with α, β nonunits, then the prime ideal factorization of $\alpha\mathcal{O}_K$ or $\beta\mathcal{O}_K$ would give a nonempty subsequence of $P_1, \dots, P_{D-1}$ multiplying to the identity.

Back to Fun. Stretchiness

If we choose $Q_1, \ldots, Q_D$ prime ideals in the classes inverse to $P_1, \ldots, P_D$, respectively, then by the same argument,

$$Q_1 \cdots Q_D = \rho \mathcal{O}_K,$$

where ρ is irreducible in $\mathcal{O}_K$.

Now consider $\rho\pi$. On the one hand, this is a product of two irreducibles: ρ and π.

Back to Fun. Stretchiness, ctd.

On the other hand,

$$\rho\pi\mathcal{O}_K = (P_1Q_1)\cdots(P_DQ_D).$$

Each $P_iQ_i = \gamma_i\mathcal{O}_K$ for some γ_i. So up to unit factors,

$$\rho\pi = \gamma_1\cdots\gamma_D.$$

If we decompose the γ_i into irreducibles, the right-hand side will involve at least D irreducibles, while the left will involve 2 irreducibles. Hence,

$$\rho(\mathcal{O}_K) \geq \frac{D}{2}.$$

Surveying our successes

It is natural to ask how badly unique factorization fails (or fails to fail) as one looks across families of number rings. Very little is known here.

This is not for lack of trying!

Let's zero in on the most well-studied case: Quadratic fields. The questions here go back to Gauss (binary quadratic forms).

Surveying our successes, ctd.

For imaginary quadratic fields, meaning $K = \mathbb{Q}(\sqrt{d})$ with $d < 0$, we know that unique factorization holds only finitely often. The largest in absolute value is $d = -163$ (Baker–Heegner–Stark). Moreover, from work of Heilbronn, the size of the class group (class number) tends to infinity as $d \to -\infty$. So factorization gets "worse and worse".

For $d > 0$, the situation is expected to be rather different. We expect that the class group is trivial infinitely often. In fact, heuristics of Cohen–Lenstra predict that the class number of $\mathbb{Q}(\sqrt{p})$ should be 1 for about 75.4% of all primes p.

Surveying our successes, ctd.

There's been remarkable progress towards the Cohen–Lenstra heuristics in recent years. But existing methods do not establish even that

$$\#\mathrm{Cl}(\mathbb{Q}(\sqrt{d})) < 10^{10^{10}}$$

for infinitely many squarefree d !

So it seems that if we want to find infinitely many UFDs, we're out of luck!

A new hope?

Question (Coykendall): What about HFDs? Can we find infinitely many half-factorial domains by wandering in the land of quadratic fields?

It's tempting to answer no. For $\mathcal{O}_K$ to be half-factorial, one needs (Carlitz) that $\#\mathrm{Cl}(\mathcal{O}_K) \leq 2$. This inequality holds for only finitely many imaginary quadratic fields K. And *for all we can prove*, it happens for only finitely many real quadratic K too.

But . . . $\mathcal{O}_K$ is not the only game in town. We can look at subrings of $\mathcal{O}_K$!

Orders in the court

Let K be a quadratic field. An **order** in K is a subring of $\mathcal{O}_K$ properly containing $\mathbb{Z}$. The ring $\mathcal{O}_K$ itself is referred to as the **maximal order**.

The orders in K are in one-to-one correspondence with positive integers f. Each order has the form

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

we call f the **conductor** of the order.

Nonmaximal orders cannot be UFDs (they are not integrally closed) but can be HFDs!

Half-truths

Conjecture (Coykendall, 2001)

(a) *There are infinitely many HFDs as you vary over all quadratic fields and all orders contained in those fields.*

(b) *There are infinitely many HFDs as you vary among the orders in the quadratic field* $\mathbb{Q}(\sqrt{2})$.

Half-truths

Conjecture (Coykendall, 2001)

(a) *There are infinitely many HFDs as you vary over all quadratic fields and all orders contained in those fields.*

(b) *There are infinitely many HFDs as you vary among the orders in the quadratic field* $\mathbb{Q}(\sqrt{2})$.

Theorem (P., 2023)

(a) *is true, and* (b) *is true assuming GRH.*

I knew you were trouble. . .

Determining the elasticity of a nonmaximal order is somewhat delicate. In a perfect world, one might hope that $\rho(\mathcal{O})$ was a simple function of the class group of $\mathcal{O}$, the way it is for maximal orders $\mathcal{O}$.

Troubling example

$\mathbb{Z}[5i]$ has class number 2.

I knew you were trouble. . .

Determining the elasticity of a nonmaximal order is somewhat delicate. In a perfect world, one might hope that $\rho(\mathcal{O})$ was a simple function of the class group of $\mathcal{O}$, the way it is for maximal orders $\mathcal{O}$.

Troubling example

$\mathbb{Z}[5i]$ has class number 2. But $\rho(\mathbb{Z}[5i]) = \infty$!

Exercises

(a) $5(2+i)^k$ is irreducible in $\mathbb{Z}[5i]$ for every k, as is $5(2-i)^k$.

(b) $5(2+i)^k \cdot 5(2-i)^k = \underbrace{5 \cdot 5 \cdot 5 \cdots 5}_{k+2 \text{ times}}$.

Hence, $\rho(\mathbb{Z}[5i]) \geq \frac{k+2}{2}$.

Halter-Koch: order of conductor f has finite elasticity $\iff$ f is not divisible by any prime split in K.

Half-factorial orders

Half-factorial orders in quadratic fields were characterized arithmetically by Halter-Koch and (independently) Coykendall.

Theorem (Coykendall, 2001)

If K is imaginary quadratic, and $\mathcal{O}$ is a half-factorial order in K not the maximal order, then $K = \mathbb{Q}(\sqrt{-3})$ and $\mathcal{O} = \mathbb{Z}[\sqrt{-3}]$.

The characterization in the real quadratic case is not as simple. For simplicity, we state only partial results.

Real-quadratic half-factorial orders

Theorem (Halter-Koch, Coykendall)

Let K be a real quadratic field. The following conditions are necessary for $\mathcal{O}_f$ to be half-factorial:

- *$\mathcal{O}_K$ is half-factorial (hence, $\#\mathrm{Cl}(\mathcal{O}_K) = 1$ or 2),*
- *$f = p$ or $2p$, where p is prime (and p odd when $f = 2p$),*
- *p is inert in K.*

Furthermore, if $\mathcal{O}_K$ is half-factorial and p is inert in K, then

$$\mathcal{O}_p \text{ is an HFD} \iff \mathrm{Cl}(\mathcal{O}_p) = \mathrm{Cl}(\mathcal{O}_K).$$

(Recall: There is a canonical surjection $\mathrm{Cl}(\mathcal{O}_p) \twoheadrightarrow \mathrm{Cl}(\mathcal{O}_K)$.)

Real-quadratic HFDs, ctd.

Suppose K is a real quadratic field. Let p be a prime inert in K. The condition that $\mathrm{Cl}(\mathcal{O}_p) = \mathrm{Cl}(\mathcal{O}_K)$ can be reformulated in terms of units.

Let ϵ be the fundamental unit of $\mathcal{O}_K$. Then

$$\mathrm{Cl}(\mathcal{O}_p) = \mathrm{Cl}(\mathcal{O}_K) \iff u = p+1 \text{ is the smallest positive integer for which } \epsilon^u \in \mathcal{O}_p.$$

This follows, e.g., from the class number formula for $\mathcal{O}$.

It's at least easy to see that $\epsilon^{p+1} \in \mathcal{O}_p$. Remember, $\mathcal{O}_p$ consists of the elements of $\mathcal{O}_K$ congruent to a rational integer mod $p\mathcal{O}_K$. Working modulo p in $\mathcal{O}_K$,

$$\epsilon^{p+1} \equiv \epsilon \cdot \epsilon^p \equiv N\epsilon \pmod{p}.$$

Real-quadratic HFDs, ctd.

When is $u = p + 1$ the smallest positive integer for which $\epsilon^u \in \mathcal{O}_p$?

We can view $\mathbb{Z}/p\mathbb{Z}$ as a subfield of $\mathcal{O}_K/p\mathcal{O}_K$ (as usual). We want $u = p + 1$ to be the smallest positive integer for which ϵ^u is the identity in the quotient

$$G_p := (\mathcal{O}_K/p\mathcal{O}_K)^\times/(\mathbb{Z}/p\mathbb{Z})^\times.$$

The group G_p has size $\frac{p^2-1}{p-1} = p + 1$.

Hence: We are asking for ϵ mod p to generate G_p.

Real-quadratic HFDs, ctd.

Upshot. Let K be a fixed real quadratic field of class number 1 or 2. Then $\mathcal{O}_p$ is an HFD for infinitely many primes p if and only if there are infinitely many primes p, inert in K, for which (the image of) ϵ generates

$$G_p = (\mathcal{O}_K/p\mathcal{O}_K)^\times/(\mathbb{Z}/p\mathbb{Z})^\times.$$

Do we expect this?

Alan: Must assume $N\epsilon = -1$. (Otherwise the order of ϵ divides $\frac{p+1}{2}$ for all odd inert p.)

OK, **then** do we expect this?

Looking back, with a view forward

What we are asking for is reminscent of a nearly century-old conjecture of Emil Artin.

Conjecture

Let g be an integer, not -1 and not a square. Then there are infinitely many primes p for which (the image of) g generates the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$.

Looking back, with a view forward

What we are asking for is reminscent of a nearly century-old conjecture of Emil Artin.

Conjecture

Let g be an integer, not -1 and not a square. Then there are infinitely many primes p for which (the image of) g generates the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$.

Artin's conjecture is still open. However, in 1967 Hooley proved that Artin's conjecture follows from the Generalized Riemann Hypothesis.

Following the breadcrumbs. . .

This is encouraging, but we need a particular quadratic field variant of Artin's conjecture, not Artin's conjecture itself. Luckily, variants of Artin's conjecture for quadratic fields have been investigated by several authors (Chen, Roskam, Yitaoka, and others). Chen's work in particular is easily adapted to yield what we want.

Following the breadcrumbs. . . ctd.

Call the real quadratic field K **viable** if K has class number 1 or 2 and fundamental unit of norm -1.

Theorem (P., 2023)

Assume GRH. Let K be a viable real quadratic field. Then there are infinitely many primes p for which $\mathcal{O}_p$ is an HFD.

The 'scope' of the theorem is best possible: If K is non-viable, then at most finitely many orders in K are half-factorial. This follows from results of Halter-Koch, Coykendall, and Alan.

In principle, the density of p satisfying the conclusion of the theorem can also be computed. When $K = \mathbb{Q}(\sqrt{2})$, one gets $\frac{1}{2}A$, where $A = \prod_{q \text{ prime}}(1 - \frac{1}{q(q-1)})$.

And if you don't believe GRH?

I mentioned an unconditional result on quadratic HFDs. Where does this come from?

Again, the inspiration is from Artin's primitive root conjecture.

What do we know about Artin's primitive root conjecture unconditionally?

Bad news first: We cannot point to a single specific g which we know generates $(\mathbb{Z}/p\mathbb{Z})^\times$ for infinitely many primes p. The good news is that Artin's conjecture is true for many choices of g that we **can't** point to!

And if you don't believe GRH? ctd.

The following is due to Murty–Srinivasan and Heath-Brown (independently): There is an absolute constant M such that among any M primes, at least one generates $(\mathbb{Z}/p\mathbb{Z})^\times$ for infinitely many primes p.

Similar methods can be ported to the quadratic field setting. This was done by Joseph Cohen in the early 2000s. Using similar methods, one can show the following.

Theorem (P., 2023)

In any list of 46 *viable linearly disjoint real quadratic fields, at least one possesses infinitely many HFD orders.*

(linearly disjoint: composite field has degree 2^{46}.)

Corollary

There is a real quadratic field of the form $\mathbb{Q}(\sqrt{d})$, *with* $1 < d < 1000$, *which possesses infinitely many HFD orders.*

1 is the loneliest number

What about elasticities larger than 1?

Proposition

Let K be a quadratic field. Then

$$2\rho(\mathcal{O}_f) = \sup_{\pi} \Omega(|N\pi|),$$

where the maximum runs over all irreducibles π of $\mathcal{O}_f$.

Here $\Omega(\cdot)$ denotes the count of prime factors taken with multiplicity. For instance, $\Omega(9) = \Omega(35) = 2$.

As a consequence, elasticities of quadratic orders are always half-integers or infinite:

$$\rho(\mathcal{O}_f) \in \{1, 3/2, 2, 5/2, 3, 7/2, \dots\} \cup \{\infty\}.$$

Everything everywhere all at once

Call K **universally elastic** if $\mathcal{O}_K$ is a UFD and every one of $1, 3/2, 2, 5/2, \ldots$ and ∞ occurs as the elasticity of infinitely many orders in K.

Theorem (P., 2023)

Assume GRH. Then $\mathbb{Q}(\sqrt{2})$ is universally elastic.

Probably every viable K of class number 1 is universally elastic. This follows from GRH and a plausible hypothesis on the scarcity of "Wieferich-type" primes.

Everything everywhere ctd.

For the proof, one studies the interplay between the conductor f and the class group in determining the elasticity. There is no simple formula known for $\rho(\mathcal{O}_f)$ in terms of these quantities. But for special f, direct analysis is possible.

For example, Picavet-L'Hermitte has a simple formula for $\rho(\mathcal{O}_f)$ (in terms of the factorization of f) whenever $\mathrm{Cl}(\mathcal{O}_f)$ is trivial. Another result of this kind (used in the proof of the theorem) is ...

Lemma

Let K be a quadratic field of class number 1. Suppose p^k is a power of the prime p inert in K. Let h be the class number of $\mathcal{O}_{p^k}$. Then

$$\rho(\mathcal{O}_{p^k}) = k + \frac{1}{2}(h-1).$$

Thank You!