ELASTICITY

of orders in quadratic fields

Paul Pollack
University of Georgia

Paradise lost and paradise regained

$\mathbb{Z}[\sqrt{-5}]$ is the standard example of a non-UFD:

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

Despite its bad reputation, factorization in $\mathbb{Z}[\sqrt{-5}]$ is actually reasonably well-behaved. 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!

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.

Example

$\mathbb{Z}[\sqrt{-5}] = \mathcal{O}_K$ for $K = \mathbb{Q}(\sqrt{-5})$. For this K, we have $\#\mathrm{Cl}(\mathcal{O}_K) = 2$.

Stretching, the truth about UFT

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

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

Recall that 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.

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 $d \to -\infty$. This implies the elasticity also tends to infinity. 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!

Example

The orders in $\mathbb{Q}(\sqrt{2})$ are the rings $\mathbb{Z}[f\sqrt{2}]$ for $f = 1, 2, 3, \ldots$.

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.*

1 is the loneliest number

What about elasticities larger than 1?

Proposition

Let K be a quadratic field. Then

$$\rho(\mathcal{O}_f) = \frac{1}{2} \sup_{\pi} \Omega(|N\pi|),$$

where the supremum 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.

One can also put forward a plausible conjecture as to which K are universally elastic, but this seems hard to prove even under GRH !

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 $\mathcal{O} = \mathbb{Z}[\sqrt{-3}]$.

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. We state only one consequence, noted by Coykendall: Suppose K is real quadratic and $\mathcal{O}_K$ is a half-factorial domain. If p is a prime inert in K, then $\mathcal{O}_p$ is an HFD if and only if $\mathrm{Cl}(\mathcal{O}_p) \cong \mathrm{Cl}(\mathcal{O}_K)$.

Example

Let $K = \mathbb{Q}(\sqrt{2})$. Then $\mathcal{O}_K$ is a UFD, so certainly an HFD. Here $\mathcal{O}_f = \mathbb{Z}[f\sqrt{2}]$.

Let p be a prime inert in K. By the relative class number formula, the class group of $\mathcal{O}_p$ coincides with the class group of $\mathcal{O}_K$ if and only if the following holds: The least positive integer j with

$$(1+\sqrt{2})^j \in \mathbb{Z}[p\sqrt{2}]$$

is $j = p+1$.

Empirically, approximately $\frac{3}{8}$ of primes p inert in $\mathbb{Q}(\sqrt{-2})$ satisfy this last condition.

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.

And if you don't believe GRH?

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.*

viable: class number 1 or 2, fun. unit norm -1

Corollary

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

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!

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.