How

Paul Pollack; joint work with Kai (Steve) Fan
University of Georgia

How nonunique . . .

is your factorization?

Paul Pollack; joint work with Kai (Steve) Fan

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 $i = 1, 2, \ldots, k$.

Expulsion from paradise

At some point, every aspiring number theorist learns the harsh lesson that not all rings of arithmetic interest are unique factorization domains.

Question: To what extent does unique factorization fail in rings of arithmetic interest?

It's not immediately clear how we might measure this failure. The ring $\mathbb{Z}[\sqrt{-5}]$ provides a hint. Here UFT fails, as shown by the famous example $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

While these two factorizations of 6 are not the same up to units, they involve the same number of terms. In fact, we will see soon that factorization in $\mathbb{Z}[\sqrt{-5}]$ is length-unique, in that any two factorizations of the same element into irreducibles always involve the same of number of terms! We call $\mathbb{Z}[\sqrt{-5}]$ a **half-factorial domain** (HFD).

Stretching, the truth about unique factorization

Let D be a domain where every nonzero nonunit factors into irreducibles. 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

Theorem (Narkiewicz, Steffan, Valenza)

Let K be a number field with ring of integers $\mathcal{O}$. If $\mathcal{O}$ has class number 1, then $\rho(\mathcal{O}) = 1$. Otherwise,

$$\rho(\mathcal{O}) = \frac{1}{2} \operatorname{Dav} \operatorname{Cl}(\mathcal{O}).$$

Here $\operatorname{Dav} G$, for a finite abelian group G, is the smallest positive integer D with the following combinatorial property:

> *Every G-sequence $g_1, g_2, \ldots, g_D$ has a nonempty subsequence whose product is the identity.*

It is easy to prove that $\operatorname{Dav} G \leq 2$ if and only if $|G| \leq 2$. Hence, $\mathcal{O}$ is an HFD if and only if $h_K \leq 2$ (Carlitz, 1960).

Fun. Theorem of Stretchiness

Theorem (Narkiewicz, Steffan, Valenza)

Let K be a number field with ring of integers $\mathcal{O}$. If $\mathcal{O}$ has class number 1, then $\rho(\mathcal{O}) = 1$. Otherwise,

$$\rho(\mathcal{O}) = \frac{1}{2} \operatorname{Dav} \operatorname{Cl}(\mathcal{O}).$$

This is a lovely result, from the point of view of an algebraist. But an analyst wants to do statistics, which requires understanding how class groups vary in families!

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 in K has finite index as a subgroup of $\mathcal{O}_K$, and for each $f \in \mathbb{Z}^+$, there is a unique order whose index is f. This is denoted $\mathcal{O}_f$, and f is called the **conductor** of the order.

It is easy to be (even more) explicit about the order of conductor f inside a given quadratic field. For example, in $\mathbb{Q}(i)$, it is just $\mathbb{Z}[fi]$, while in $\mathbb{Q}(\sqrt{5})$, it is $\mathbb{Z}[f\frac{1+\sqrt{5}}{2}]$.

Our problem: How do elasticities vary among orders in a fixed quadratic field?

There be dragons here. . .

Example

Let's think about the order of conductor 5 in $\mathbb{Z}[i]$, that is, $\mathbb{Z}[5i]$.

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

But k is arbitrary! Hence, $\rho(\mathbb{Z}[5i]) = \infty$. Infinite elasticity cannot happen for a full ring of integers!

There be dragons here. . .

Example

Let's think about the order of conductor 5 in $\mathbb{Z}[i]$, that is, $\mathbb{Z}[5i]$.

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

But k is arbitrary! Hence, $\rho(\mathbb{Z}[5i]) = \infty$. Infinite elasticity cannot happen for a full ring of integers!

Halter-Koch: order of conductor f has finite elasticity $\iff$ f is not divisible by any prime split in K. (In $\mathbb{Q}(i)$: not divisible by any prime 1 mod 4.)

Half-truths

Really, for real-question: Fix a quadratic field K. How does $\rho(\mathcal{O}_f)$ vary as f varies among split-free numbers?

Theorem (P., 2023)

1. *Some real quadratic field contains infinitely many half-factorial orders, i.e., orders with* $\rho = 1$.
2. *If GRH holds, one can replace "some real quadratic field" with the field* $K = \mathbb{Q}(\sqrt{2})$.

The conclusions here were conjectured by Jim Coykendall. Coykendall himself proved the striking theorem that in the imaginary case, there is precisely one nonmaximal HFD order, namely $\mathbb{Z}[\sqrt{-3}]$.

So typical!

Steve Fan and I have been continuing these investigations. We began by looking at the "typical" size of $\rho(\mathcal{O}_f)$.

Theorem (Fan and P., 2024)

Fix K. If K is real quadratic, then under GRH,

$$\rho(\mathcal{O}_f) \approx (\log f)^{1/2}$$

for almost all split-free f. If K is imaginary quadratic, then

$$\rho(\mathcal{O}_f) \approx f/(\log f)^{\frac{1}{2}\log\log\log f + C_K}$$

for almost all split-free f (unconditionally).

Here C_K is a certain explicit (but complicated) constant, while $\approx$ means valid up to a factor of $(\log f)^{o(1)}$.

We go to extremes

Quite recently, Steve and I have been thinking about extremal orders of $\rho(\mathcal{O}_f)$, as f varies among split-free numbers.

Theorem (minimal size, imaginary case)

Let K be a fixed imaginary quadratic field. There are absolute constants $c_1, c_2 > 0$ for which the following holds. For all sufficiently large split-free f,

$$\rho(\mathcal{O}_f) > (\log f)^{c_1 \log\log\log f}.$$

On the other hand, there is a sequence of split-free f tending to infinity along which

$$\rho(\mathcal{O}_f) < (\log f)^{c_2 \log\log\log f}.$$

Giving away our secrets

Where does all of this come from?

What we are really doing is some kind of statistical analysis of the Davenport constant of the relevant order class groups (i.e., ring class groups).

For nonmaximal orders, the elasticity is not generally equal to half the Davenport constant of the class group, but the latter is still a good approximation. A good an approximation is all we need to do our statistics!

The constant $\mathrm{Dav}\, G$ is bounded below by the size of the largest cyclic subgroup of G (the exponent of G). Less obviously, $\mathrm{Dav}\, G$ bounded above by a quantity that is usually not much larger (Van Emde Boas–Kruyswijk–Meshulam). So we reduce to controlling the exponent.

Giving away our secrets, ctd.

How do we access the class group of $\mathcal{O}_f$? Put

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

Then the class group of $\mathcal{O}_f$ has a subgroup of index h_K isomorphic to

$$\mathrm{PreCl}(\mathcal{O}_f)/\langle\text{image of } \epsilon\rangle,$$

where ϵ is the fundamental unit of $\mathcal{O}_K$ if K is real, and a generator of $\mathcal{O}_K^\times$ when K is imaginary. Since K is fixed, this subgroup is always a "bounded factor away" from the full ring class group!

Getting statistics for $\mathrm{PreCl}(\mathcal{O}_f)/\langle\text{image of } \epsilon\rangle$ turns out to be analogous to studying $(\mathbb{Z}/m\mathbb{Z})^\times/\langle\text{image of } 2\rangle$, as m varies across odd positive integers. By now there are many statistical results for the latter groups (Erdős, Hooley, Kurlberg, Pomerance, etc.).

Everything old is new again, ctd.

Examples.

- Our results (conditonal and unconditional) on half-factorial real quadratic orders are based on adapting work towards Artin's primitive root conjecture; we show that ϵ generates $\mathrm{PreCl}(\mathcal{O}_p)$ for infinitely many p (satisfying certain other important conditions).

Everything old is new again, ctd.

Examples.

- Our results (conditonal and unconditional) on half-factorial real quadratic orders are based on adapting work towards Artin's primitive root conjecture; we show that ϵ generates $\mathrm{PreCl}(\mathcal{O}_p)$ for infinitely many p (satisfying certain other important conditions).
- Our $(\log f)^{c \log\log\log f}$ results on minimal elasticites of imaginary quadratic orders ... come from adapting a result of Erdős–Pomerance–Schmutz on the minimal size of $\lambda(m) := \mathrm{Exp}\ (\mathbb{Z}/m\mathbb{Z})^\times$.

Everything old is new again, ctd.

Examples.

- Our results (conditonal and unconditional) on half-factorial real quadratic orders are based on adapting work towards Artin's primitive root conjecture; we show that ϵ generates $\mathrm{PreCl}(\mathcal{O}_p)$ for infinitely many p (satisfying certain other important conditions).
- Our $(\log f)^{c \log\log\log f}$ results on minimal elasticites of imaginary quadratic orders ... come from adapting a result of Erdős–Pomerance–Schmutz on the minimal size of $\lambda(m) := \mathrm{Exp}\ (\mathbb{Z}/m\mathbb{Z})^\times$.
- Our result that $\rho(\mathcal{O}_f)$ is typically of size $\approx \sqrt{\log f}$ in the real case is based on a method used by [P., 2021] to show that $\phi(m)/\lambda(m)$ typically has $\sim \log\log m/\log\log\log m$ prime factors.

Thank You!